CROWDSTRIKE

USE OF FANCY BEAR ANDROID MALWARE IN TRACKING OF UKRAINIAN FIELD ARTILLERY UNITS

PUBLISHED DECEMBER 22, 2016
UPDATED MARCH 23, 2017

CROWDSTRIKE GLOBAL INTELLIGENCE TEAM
web: WWW.CROWDSTRIKE.COM | twitter: @CROWDSTRIKE

> EXCLUDING THE NAVAL INFANTRY BATTALION IN THE CRIMEA WHICH WAS EFFECTIVELY CAPTURED WHOLESALE, THE UKRAINIAN ARMED FORCES LOST BETWEEN 15% AND 20% OF THEIR PRE-WAR D-30 INVENTORY IN COMBAT OPERATIONS.
>
> —HENRY BOYD, International Institute for Strategic Studies (IISS) Research Associate for Defence and Military Analysis

MARCH 2017 UPDATE: The information about the combat losses of the D-30 artillery units suffered by Ukrainian forces has been updated with the latest analysis from Henry Boyd, International Institute for Strategic Studies (IISS) Research Associate for Defence and Military Analysis

KEY POINTS

- From late 2014 and through 2016, FANCY BEAR X-Agent implant was covertly distributed on Ukrainian military forums within a legitimate Android application developed by Ukrainian artillery officer Yaroslav Sherstuk.

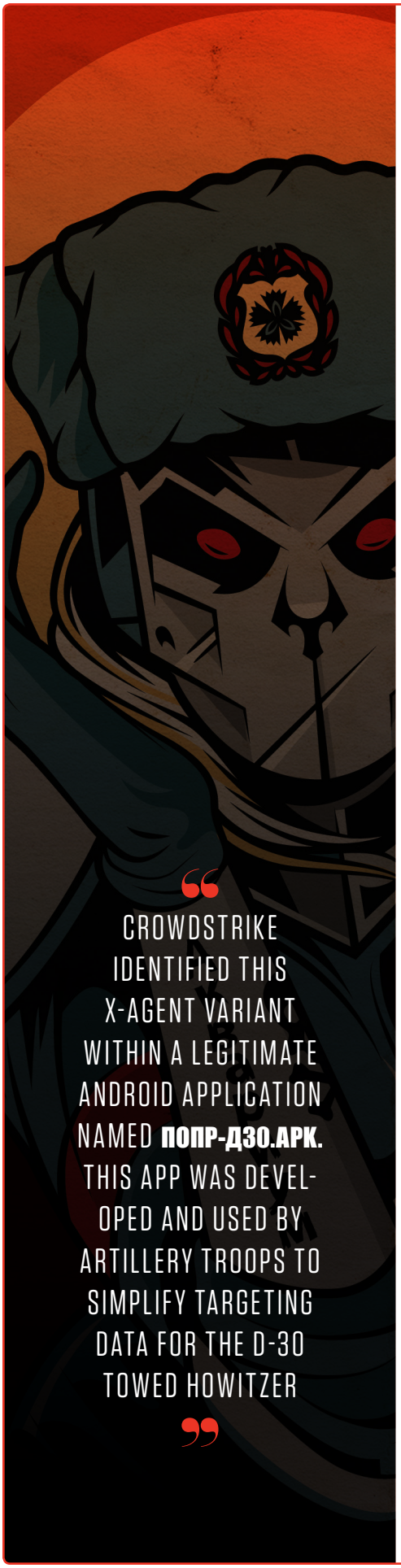
- The original application enabled artillery forces to more rapidly process targeting data for the Soviet-era D-30 Howitzer employed by Ukrainian artillery forces reducing targeting time from minutes to under 15 seconds. According to Sherstuk's interviews with the press, over 9000 artillery personnel have been using the application in Ukrainian military.

- Successful deployment of the FANCY BEAR malware within this application may have facilitated reconnaissance against Ukrainian troops. The ability of this malware to retrieve communications and gross locational data from an infected device makes it an attractive way to identify the general location of Ukrainian artillery forces and engage them.

- According to an update provided in March 2017 by the International Institute for Strategic Studies (IISS) Research Associate for Defence and Military Analysis, Henry Boyd, "excluding the Naval Infantry battalion in the Crimea which was effectively captured wholesale, the Ukrainian Armed Forces lost between 15% and 20% of their pre-war D–30 inventory in combat operations.

- This previously unseen variant of X-Agent represents FANCY BEAR's expansion in mobile malware development from iOS-capable implants to Android devices, and reveals one more component of the broad spectrum approach to cyber operations taken by Russia-based actors in the war in Ukraine.

- The collection of such tactical artillery force positioning intelligence by FANCY BEAR further supports CrowdStrike's previous assessments that FANCY BEAR is likely affiliated with the Russian military intelligence (GRU), and works closely with Russian military forces operating in Eastern Ukraine and its border regions in Russia.

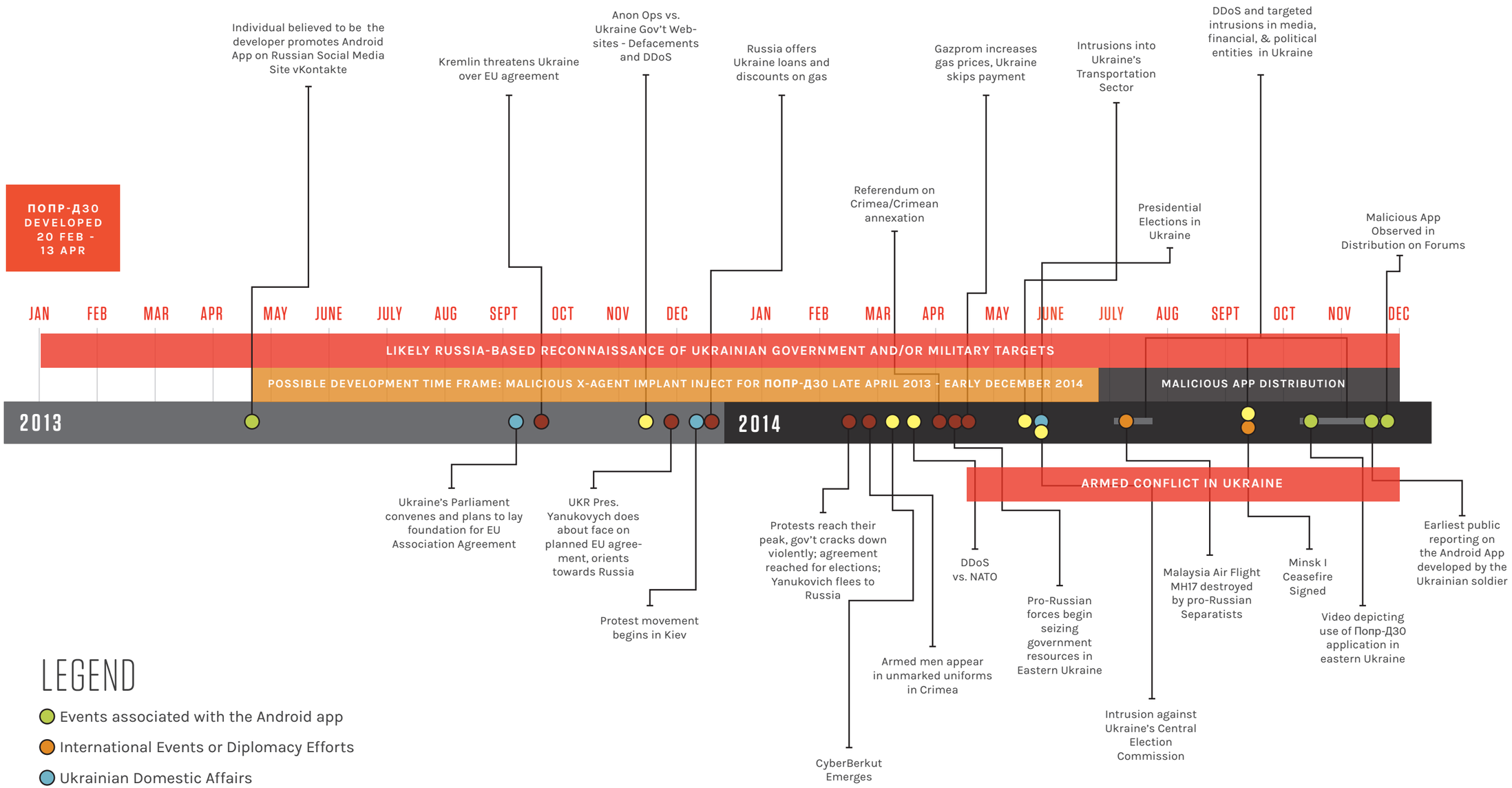


> “CROWDSTRIKE IDENTIFIED THIS X-AGENT VARIANT WITHIN A LEGITIMATE ANDROID APPLICATION NAMED **ПОПР-Д30.АРК.** THIS APP WAS DEVELOPED AND USED BY ARTILLERY TROOPS TO SIMPLIFY TARGETING DATA FOR THE D-30 TOWED HOWITZER”

BACKGROUND

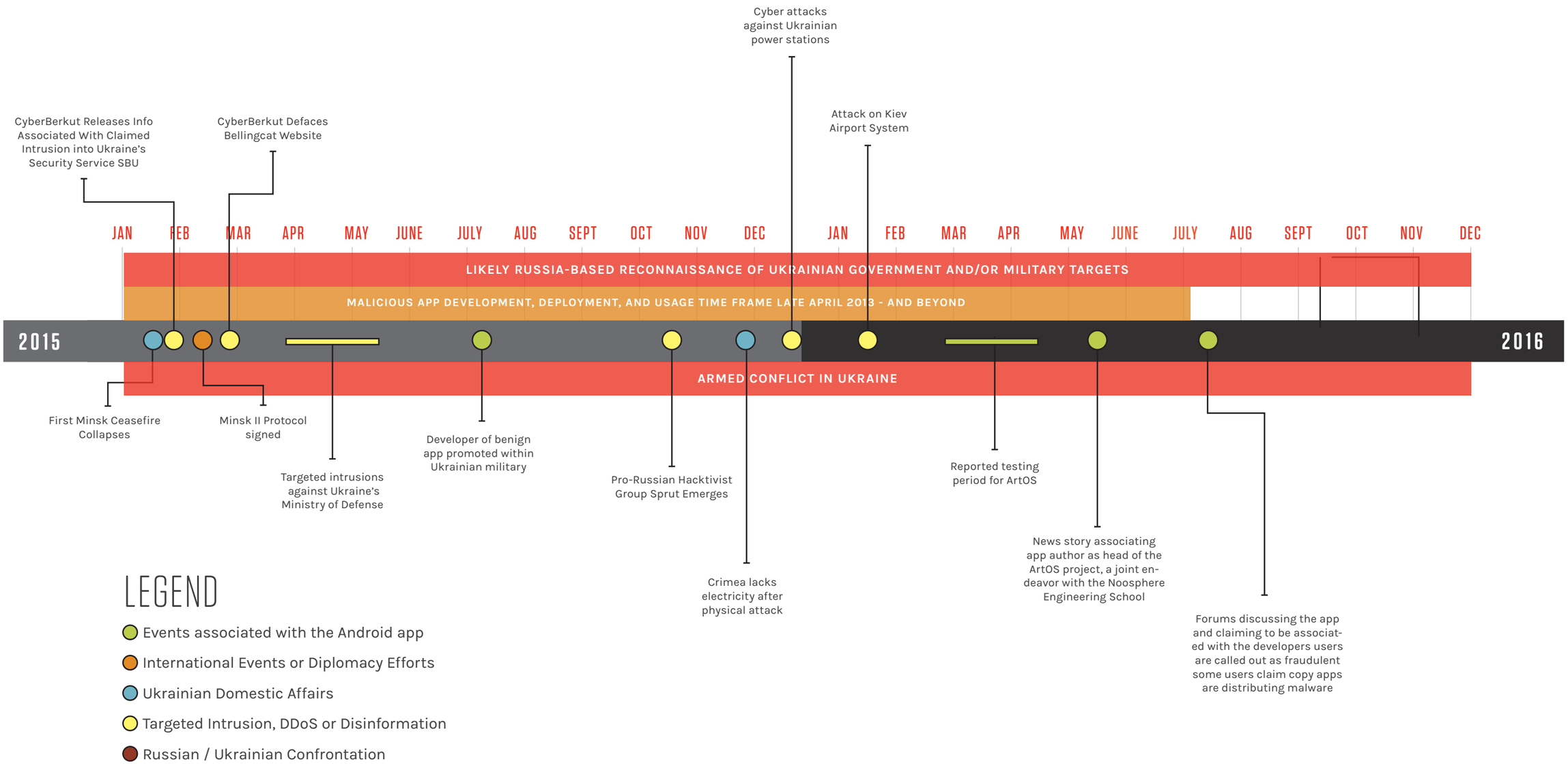
In late June and August 2016, CrowdStrike Intelligence provided initial reporting and technical analysis of a variant of the FANCY BEAR implant X-Agent that targeted the Android mobile platform[2]. CrowdStrike identified this X-Agent variant within a legitimate Android application named Попр-Д30.apk. This app was developed and used by artillery troops to simplify targeting data for the D-30 towed howitzer. CrowdStrike investigation reveals that this app has been utilized in a possible training or operational role in at least one unit of the Ukrainian military. Therefore, the implant likely targeted military artillery units operating against pro-Russian separatists in Eastern Ukraine.

This implant represents further advancements in FANCY BEAR’s development of mobile malware for targeted intrusions and extends Russian cyber capabilities to the front lines of the battlefield. This Tipper builds on CrowdStrike’s previous reporting by providing a timeline of events, contextual discussion regarding the potential drivers for development and deployment of the malware, and a description of the analytical process resulting in targeting assessments. Finally, this Tipper leverages these assessments, in conjunction with more recently observed activity by Russia-based adversaries, to determine the potential for any future activity in the mobile malware threat space.



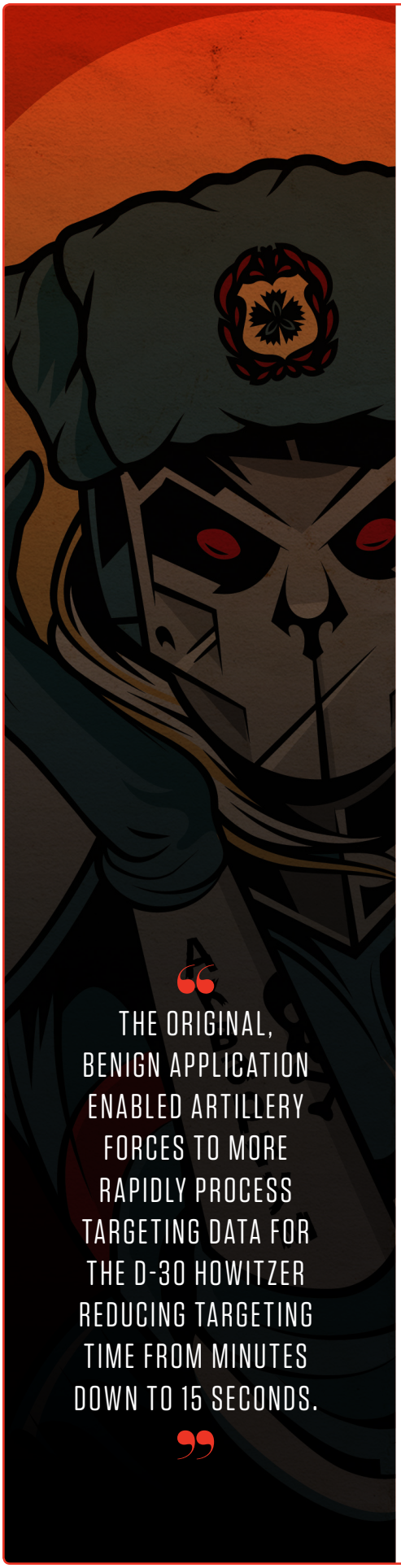
LEGEND

- Events associated with the Android app
- International Events or Diplomacy Efforts
- Ukrainian Domestic Affairs
- Targeted Intrusion, DDoS or Disinformation
- Russian / Ukrainian Confrontation



LEGEND

- Events associated with the Android app
- International Events or Diplomacy Efforts
- Ukrainian Domestic Affairs
- Targeted Intrusion, DDoS or Disinformation
- Russian / Ukrainian Confrontation



> THE ORIGINAL, BENIGN APPLICATION ENABLED ARTILLERY FORCES TO MORE RAPIDLY PROCESS TARGETING DATA FOR THE D-30 HOWITZER REDUCING TARGETING TIME FROM MINUTES DOWN TO 15 SECONDS.

TIMELINE OF EVENTS

DEVELOPMENT AND DISTRIBUTION PROCESS OF THE BENIGN APPLICATION

The original application central to this discussion, Попр-Д30.apk, was initially developed domestically within Ukraine by a member of the 55th Artillery Brigade. Based on the file creation timestamps as well as the app signing process, which occurred on 28 March 2013, CrowdStrike has determined that the app was developed sometime between 20 February and 13 April 2013.

Shortly after that time frame, on 28 April 2013, an individual bearing the same name as the application's developer promoted the application on Russian vKontakte[3] pages associated with the artillery forces. The promotion of the program was likely limited to social media, and the distribution was controlled from the author's main page, «Програмное обеспечение современного боя» (translation: "Modern combat software").[4] As an additional control measure, the program was only activated for use after the developer was contacted and issued a code to the individual downloading the application.

No evidence of the application has been observed on the Android app store, making it unlikely that the app was distributed via that platform. The control measures established by the developer to limit the use and proliferation of the Попр-Д30.apk application, coupled with its unique purpose, make its broad distribution on the Android store improbable.

At the time of this writing, it is unclear to what degree and for how long this specific application was utilized by the entirety of the Ukrainian Artillery Forces. Based on open source reporting, social media posts, and video evidence, CrowdStrike assesses that Попр-Д30.apk was potentially used through 2016 by at least one artillery unit operating in eastern Ukraine.

RECONNAISSANCE, DEVELOPMENT AND DISTRIBUTION OF THE MALICIOUS APPLICATION

RECONNAISSANCE

Given the estimated development timeframe and the promotional period for the benign Попр-Д30.apk application, the program was likely available online for distribution after late April 2013. CrowdStrike Intelligence assesses that the application likely came to the attention of Russia-based adversaries around this time frame as a result of ongoing Russian

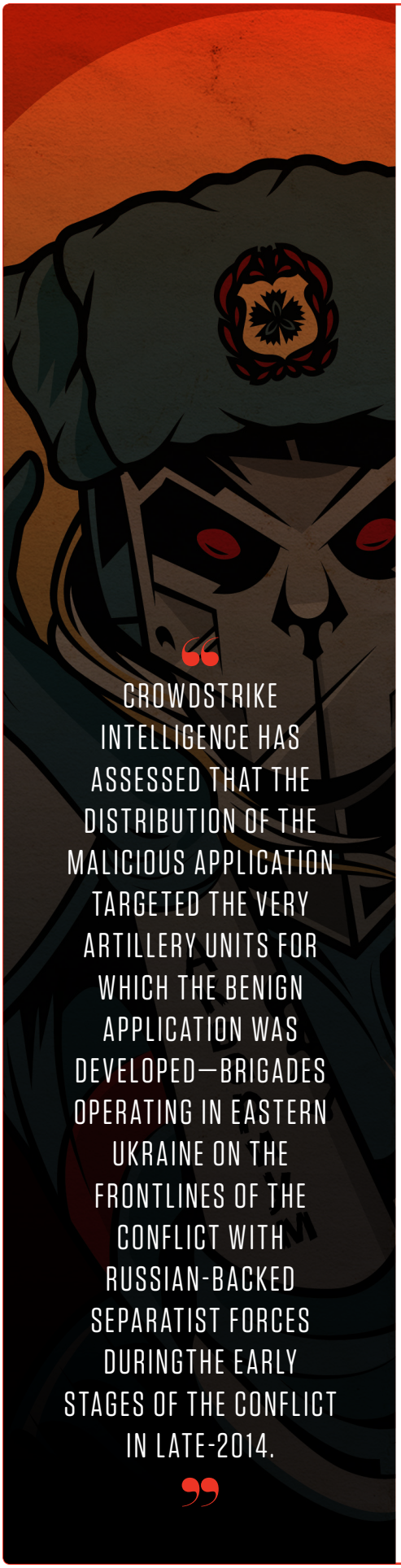
reconnaissance associated with the revolution in Ukraine. Actors with a nexus to Russia regularly monitor social media sites in order to better understand or formulate operations against their targets.

CrowdStrike Intelligence has noted instances in which some Russia-based actors and attribution front groups have leveraged information obtained from Ukrainian social media sites in order to perform operations. The most notable recent example of this was in the case of extortion-based threats directed against the Polish Government.[5] In this particular case, the perpetrators likely sought out openly available account information from a vKontakte page belonging to a Ukrainian citizen, who was soliciting donations to aid volunteer soldiers fighting in eastern Ukraine. The adversary then used this profile information, in conjunction with the name "Pravyy Sector," to make it appear as though the extortion threats against the Polish government were originating from an ultranationalist Ukrainian group.

CrowdStrike has assessed that by performing this type of deceptive operation the perpetrator likely sought to make it appear as though Ukrainian interests were threatening the Polish government. In addition, because the individual account hijacked for this operation had been used to try to raise funds for Ukrainian forces, the adversary may have been trying to aggravate Western governments enough to freeze the individual's accounts. The attack did not appear to achieve its intended result. Poland rebuffed the threats, and the owner of the vKontakte page denounced any involvement in the threat. Subsequently the Pravyy Sector group scrubbed their social media page of much of the information associated with this failed operation.

This particular incident is an example of how a disinformation operation is staged. While this incident is not likely to be related to the development of the X-Agent Android variant, it demonstrates the reconnaissance and pre-planning tactics that precede the rest of a campaign. Development and Distribution

CrowdStrike has discovered indications that as early as 2015 FANCY BEAR likely developed X-Agent applications for the iOS environment, targeting "jailbroken" Apple mobile devices. The use of the X-Agent implant in the original Попр-Д30.apk application appears to be the first observed case of FANCY BEAR malware developed for the Android mobile platform. On 21 December 2014 the malicious variant of the Android application was first observed in limited public distribution on a Russian language, Ukrainian military forum. A late 2014 public release would place the development timeframe for this implant sometime between late-April 2013 and early December 2014.



> “CROWDSTRIKE INTELLIGENCE HAS ASSESSED THAT THE DISTRIBUTION OF THE MALICIOUS APPLICATION TARGETED THE VERY ARTILLERY UNITS FOR WHICH THE BENIGN APPLICATION WAS DEVELOPED—BRIGADES OPERATING IN EASTERN UKRAINE ON THE FRONTLINES OF THE CONFLICT WITH RUSSIAN-BACKED SEPARATIST FORCES DURINGTHE EARLY STAGES OF THE CONFLICT IN LATE-2014.”

During that proposed development timeframe, a number of significant events unfolded between Ukraine, Russia, and the international community. Most notably, Russian attempts to influence Ukrainian-EU relations resulted in the large-scale, Maidan protest movement, eventually resulting in the ouster of then-president Victor YANUKOVYCH, the invasion and annexation of the Crimean Peninsula by Russia, and the protracted armed conflict in eastern Ukraine. Therefore, the creation of an application that targets some of the front line forces pivotal in Ukrainian defense on the eastern front would likely be a high priority for Russian adversary malware developers seeking to turn the tide of the conflict in their favor.

CrowdStrike Intelligence has assessed that the distribution of the malicious application targeted the very artillery units for which the benign application was developed—brigades operating in eastern Ukraine on the frontlines of the conflict with Russian-backed separatist forces during the early stages of the conflict in late-2014. This assessment is based on a number of factors, but chief among them is the likelihood that a military member would only trust and use an application designed to calculate something as critical as targeting data if it was developed and promoted by a member of their own forces. The type of operational activity described here suggests an extremely sophisticated understanding of the target that only a skilled adversary would likely possess.

By late December 2014, the total number of Russian forces in the region was approximately 10,000 troops.[6] Because the Android malware could facilitate gross position information, its successful deployment could have facilitated anticipatory awareness of Ukrainian artillery force troop movement, thus providing Russian forces with useful strategic planning information. Indeed, the 55th Artillery Brigade and similar artillery units operated frequently against pro-Russian separatists in eastern Ukraine. A video posted on 18 October 2015[7] specifically shows them employing the Попр-Д30.apk application and operating in the vicinity of eastern Ukraine.

The choice of the Russian language character set in the application further underscores the targeting of forces within eastern Ukraine, as Russian is the predominant language utilized in that region. An assessment of languages spoken by region based on the most recent census information illustrates the permeation of the Russian language in that region and highlights the value of providing Russian in the malicious Попр-Д30.apk application.

One alternative theory regarding the use of the Russian language in the application could be that targeting may have been directed at pro-Russian

LANGUAGES SPOKEN BY REGION

	WEST	CENTER	SOUTH	EAST	DONBASS
UKRANIAN	92.6%	78.2%	35.3%	37.4%	19.9%
UKRANIAN & RUSSIAN EQUALLY	2.9%	16.6%	38.4%	34.4%	34%
RUSSIAN	2%	4.2%	20%	25.9%	40.4%
OTHER	1.6%	.4%	5.4%	1.3%	5.2%
UNCLEAR	.9%	.6%	.9%	1%	.5%

Distribution of Russian/Ukrainian Language Use in Ukraine[8]

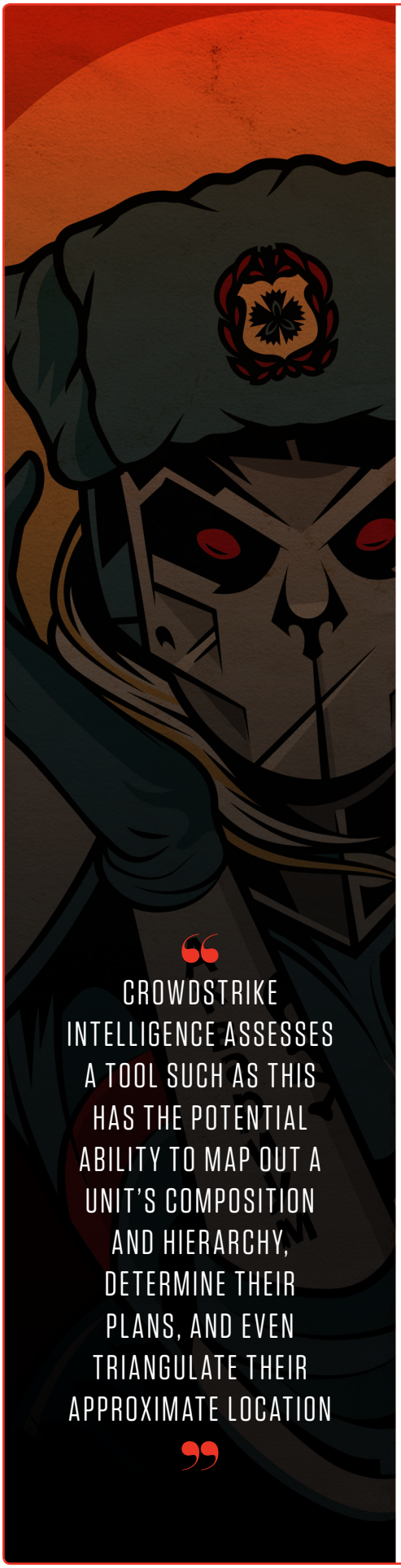
forces operating in eastern Ukraine. A relevant and likely counterargument for this theory, however, is that Russian forces likely have employed fire support systems and other technologies that can already calculate targeting data, negating the need for an application to perform this task. Additionally, the application was initially developed by a member of the Ukrainian army. An opposing force would probably not adopt technology developed by the enemy for use on the battlefield.

OUTCOMES AND CONCLUSION

The eastern Ukrainian front has been markedly impacted by heavy fighting involving Russian troops and pro-Russian rebel fighters deployed to this region. Artillery forces on both sides of the conflict have served an important role. For Ukrainian troops, artillery forces have also shouldered a heavy cost. According to an update provided in March 2017 by the International Institute for Strategic Studies (IISS) Research Associate for Defence and Military Analysis, Henry Boyd, "excluding the Naval Infantry battalion in the Crimea which was effectively captured wholesale, the Ukrainian Armed Forces lost between 15% and 20% of their pre-war D-30 inventory in combat operations.

Between July and August 2014, Russian backed forces launched some of the most decisive attacks against Ukrainian forces, resulting in significant loss of life, weaponry, and territory. According to open sources, Ukrainian service personnel from the 24th and 72nd Mechanized Brigade, as well as the 79th Airborne Brigade, were among the units to have suffered casualties. International monitoring groups later assessed some of the attacks were likely to have come from inside Russian territory.[9]

A malware-infected Попр-Д30.apk application probably could not have provided all the necessary data required to directly facilitate the types of tactical strikes that occurred between July and August 2014. Eyewitness accounts from individuals within the impacted units reported seeing an unmanned aerial vehicle (UAV) used in the area prior to one attack, underscoring the need for precise locational data for these particular strikes and introducing the possibility



> CROWDSTRIKE INTELLIGENCE ASSESSES A TOOL SUCH AS THIS HAS THE POTENTIAL ABILITY TO MAP OUT A UNIT'S COMPOSITION AND HIERARCHY, DETERMINE THEIR PLANS, AND EVEN TRIANGULATE THEIR APPROXIMATE LOCATION

that the Android malware served to support the reconnaissance role of traditional battlefield assets. Although traditional overhead intelligence surveillance and reconnaissance (ISR) assets were likely still needed to finalize tactical movements, the ability of this application to retrieve communications and gross locational data from infected devices, could provide insight for further planning, coordination, and tasking of ISR, artillery assets, and fighting forces.

The X-Agent Android variant does not exhibit a destructive function and does not interfere with the function of the original Попр-Д30.apk application. Therefore, CrowdStrike Intelligence has assessed that the likely role of this malware is strategic in nature. The capability of the malware includes gaining access to contacts, Short Message Service (SMS) text messages, call logs, and internet data, and FANCY BEAR would likely leverage this information for its intelligence and planning value.

CrowdStrike Intelligence assesses a tool such as this has the potential ability to map out a unit's composition and hierarchy, determine their plans, and even triangulate their approximate location. This type of strategic analysis can enable the identification of zones in which troops are operating and help prioritize assets within those zones for future targeting.

The development of the X-Agent Android malware represents an expansion of FANCY BEAR capabilities in terms of mobile malware, and illustrates the practical application of full-spectrum combat as envisioned in the eponymous doctrinal writings of General Valery GERASIMOV. As a part of full-spectrum operations in Ukraine, Russia-based adversaries have leveraged malware on the battlefield, in the civil sector, and against critical infrastructure. They have also engaged in aggressive information operations in the media. In relation to this broader picture of Russian computer operations, the approach to targeting mobile smartphone and tablet devices in order to gain strategic insight into communications is a tactic that cannot be disregarded.

CrowdStrike assesses that the observed and described X-Agent implant targeting Ukrainian military Android devices running the Попр-Д30.apk application is likely only the initial iteration of this type of malware. While this malware was initially discovered in a battlefield environment, an adversary could also leverage it in attacks against non-military targets. Mobile devices and internet-connected technology have increasingly proliferated civilian and military organizations. This technique may very likely be deployed in the political, government, or non-governmental sectors in the near future.

“THE COLLECTION OF SUCH TACTICAL ARTILLERY FORCE POSITIONING INTELLIGENCE BY FANCY BEAR FURTHER SUPPORTS CROWDSTRIKE’S PREVIOUS ASSESSMENTS THAT FANCY BEAR IS LIKELY AFFILIATED WITH THE RUSSIAN MILITARY INTELLIGENCE (GRU)”

1-The name Попр-Д30.apk is an abbreviated variant of Поправки-Д30 which translates to Correction-D30.

2-For more information, contact CrowdStrike

3-vKontakte is a Russian social media networking site alike in layout and functionality to Facebook.

4-http://programs-art.at.ua

5-For more information, contact CrowdStrike

6-Igor Sutyagin, Russian Forces in Ukraine, Royal United Services Institute, March 2015, https://rusi.org/sites/default/files/201503_bp_russian_forces_in_ukraine.pdf

7-https://www.youtube.com/watch?v=qp-7e_ZGH8I

8-Data for image circa 2015. Note: These maps do not provide data for Crimea. According to various sources, there are estimates suggesting that, in greater Crimea 80% speak Russian, 10% speak Ukrainian, and 10% speak Tatar. The percentage of Russian speakers is estimated to be higher in Sevastopol, most likely dues to the Russian Naval Base in the region. Source: The Razumkov Center report on "The Ukranian Citizen's Identity in the New Environment: Status, Trends, Regional Differences," 7 June 2016, razumkov.org.ua/upload/identi-2016.pdf.

9-For more information, see Origin of Artillery Attacks on Ukrainian Military Positions in Eastern Ukraine between 14 July 2014 and 8 August 2014, "https://www.bellingcat.com/news/uk-and-europe/2015/02/17/origin-of-artillery-attacks/."