Providing threat intelligence to those in the Cloud

Google Cloud is pleased to publish this "Snapshot" of its most recent *Threat Horizons* report. The information provided is based on threat intelligence observations from the Threat Analysis Group, Google Cloud Threat Intelligence for Chronicle, Trust and Safety, and other internal teams. It summarizes actionable intelligence that enables organizations to protect against ever-evolving threats. In these and future threat intelligence reports, Google will provide threat horizon scanning, trend tracking, and *Early Warning* announcements about emerging threats requiring immediate action.

Snapshot Summary

While cloud customers continue to face a variety of threats across applications and infrastructure, many successful attacks are due to poor hygiene and a lack of basic control implementation. Most recently, our team has responded to cryptocurrency mining abuse, phishing campaigns, and ransomware. Given these specific observations and general threats, organizations that put emphasis on secure implementation, monitoring and ongoing assurance will be more successful in mitigating these threats or at the very least reduce their overall impact.

Current observations include:

- **Compromised GCP instances used for cryptocurrency mining**
  Malicious actors were observed performing cryptocurrency mining within compromised Cloud instances. Of 50 recently compromised GCP instances, 86% of the compromised Cloud instances were used to perform cryptocurrency mining, a Cloud resource-intensive, for-profit activity. Additionally, 10% of compromised Cloud instances were used to conduct scans of other publicly available resources on the Internet to identify vulnerable systems, and 8% of instances were used to attack other targets. While data theft did not appear to be the objective of these compromises, it remains a risk associated with the cloud asset compromises as bad actors start performing multiple forms of abuse.

- **Russia launches Gmail phishing campaign**
  Based on research from Google's Threat Analysis Group (TAG), the Russian government-backed attackers APT28 / Fancy Bear, which typically targeted Yahoo! and Microsoft users, was observed at the end of September sending a large-scale attack to approximately 12K+ Gmail accounts in a credential phishing campaign. The attackers were using patterns similar to TAG's government-backed attack alerts to lure users to change their credentials on the attacker's phishing page. Google blocked these messages and no users were compromised.

- **Fraudsters employ new Threat, Tactics, and Procedures (TTPs) to abuse Google Cloud resources**
  TAG observed a group of attackers abusing Google Cloud resources to generate traffic to YouTube for view count manipulation. Attackers have also used various approaches to gain free Cloud credits, including the use of free trial projects, abusing start up credits with fake companies, and joining Google Developer Communities for free projects. Upon detection and enforcement by Google's Cloud abuse team, the attackers quickly switched to Qwiklab projects and the Cloud abuse team pivoted to counter this offensive.

- **North Korea actors impersonate employment recruiters**
  TAG observed a North Korean government-backed attacker group that has previously targeted security researchers posing as Samsung recruiters and sending fake job opportunities to employees at multiple South Korean information security companies that sell anti-malware solutions. The emails included a PDF allegedly claiming to be of a job description for a role at Samsung; however, the PDFs were malformed and did not open in a standard PDF reader. When targets replied that they could not open the job description, attackers responded with a malicious link to malware purporting to be a "Secure PDF Reader" stored in Google Drive which has now been blocked.

- **Black Matter ransomware rises out of DarkSide**
  Based on research from Google Cloud Threat Intelligence for Chronicle, Black Matter is one of many ransomware families currently being used to extort money from victims by locking their files using encryption; however, the ransomware does not transfer files off-network as its ransom note claims. While the Black Matter group is a relatively new player in this space, evidence suggests it is the immediate offspring of DarkSide. Black Matter is capable of encrypting files on a victim's hard drive and network shares in a relatively short period of time by distributing the

workload across multiple threads.

Recommendations

As Google Cloud works with its customers in a "shared fate" partnership, valuable trends and lessons-learned emerge from other incidents that Google helped address:

- Audit published projects to ensure certificates and credentials are not accidentally exposed. Certificates and credentials are mistakenly included in projects published on GitHub and other repositories on a regular basis. Exposed certificates and credentials could allow an attacker to unauthorized access to your projects in Google Cloud. A regular audit of published projects can help ensure this mistake can be detected and fixed quickly.
- Code downloaded by clients should undergo hashing authentication. It is a common practice for clients to download updates and code from cloud resources, raising concern that unauthorized code may be downloaded in the process. Meddler in the Middle (MITM) attacks may cause unauthorized source code to be pulled into production. By hashing and verifying all downloads, the integrity of the software supply chain can be preserved and an effective chain of custody can be established.
- Use multiple layers of defense to combat credential and cookie theft. Cloud-hosted resources have the benefit of high availability and "anywhere, anytime" access. While cloud-hosted resources streamline workforce operations, bad actors can try to take advantage of the ubiquitous nature of the cloud to compromise cloud resources. Despite growing public attention to cybersecurity, spear-phishing and social engineering tactics are frequently successful. As for other forms of IT security, defensive measures need to be robust and layered to protect cloud resources due to ubiquitous access. In addition to enabling 2-Step Verification on accounts used to access Cloud resources, administrators should strengthen their environment through Context-Aware Access and solutions such as BeyondCorp Enterprise and Work Safer, which enables better cybersecurity.

Based on these observations there are a number of mitigating measures to counter these threats.

Risk	Countermeasures
Exploiting vulnerable GCP instances	Follow password best practices and best practices for configuring Cloud environments. Update third-party software prior to a Cloud instance being exposed to the web. Avoid publishing credentials in GitHub projects. Use Container Analysis to perform vulnerability scanning and metadata storage. Leverage Web Security Scanner in the Security Command Center to identify security vulnerabilities in App Engine, Google Kubernetes Engine, and Compute Engine. Use service accounts with Compute Engine to authenticate apps instead of using user credentials. Implement Policy Intelligence tools to help understand and manage policies. Use predefined configurations through Assured Workloads to reduce misconfigurations. Set up conditional alerts in the Cloud Console to send alerts upon high resource consumption. Enforce and monitor password requirements for users through the Google Admin console.
Spear-phishing	Engage in email best practices. Employ 2-Step Verification. Enroll in the Advanced Protection Program.. Use Google's Work Safer and BeyondCorp Enterprise. Deploy Context-Aware Access.
Downloading software updates	Establish a strong chain of custody by hashing and verifying downloads.
Using public code repositories	Audit projects published on GitHub and other sites to ensure credentials and certificates were not included.