Google Cloud

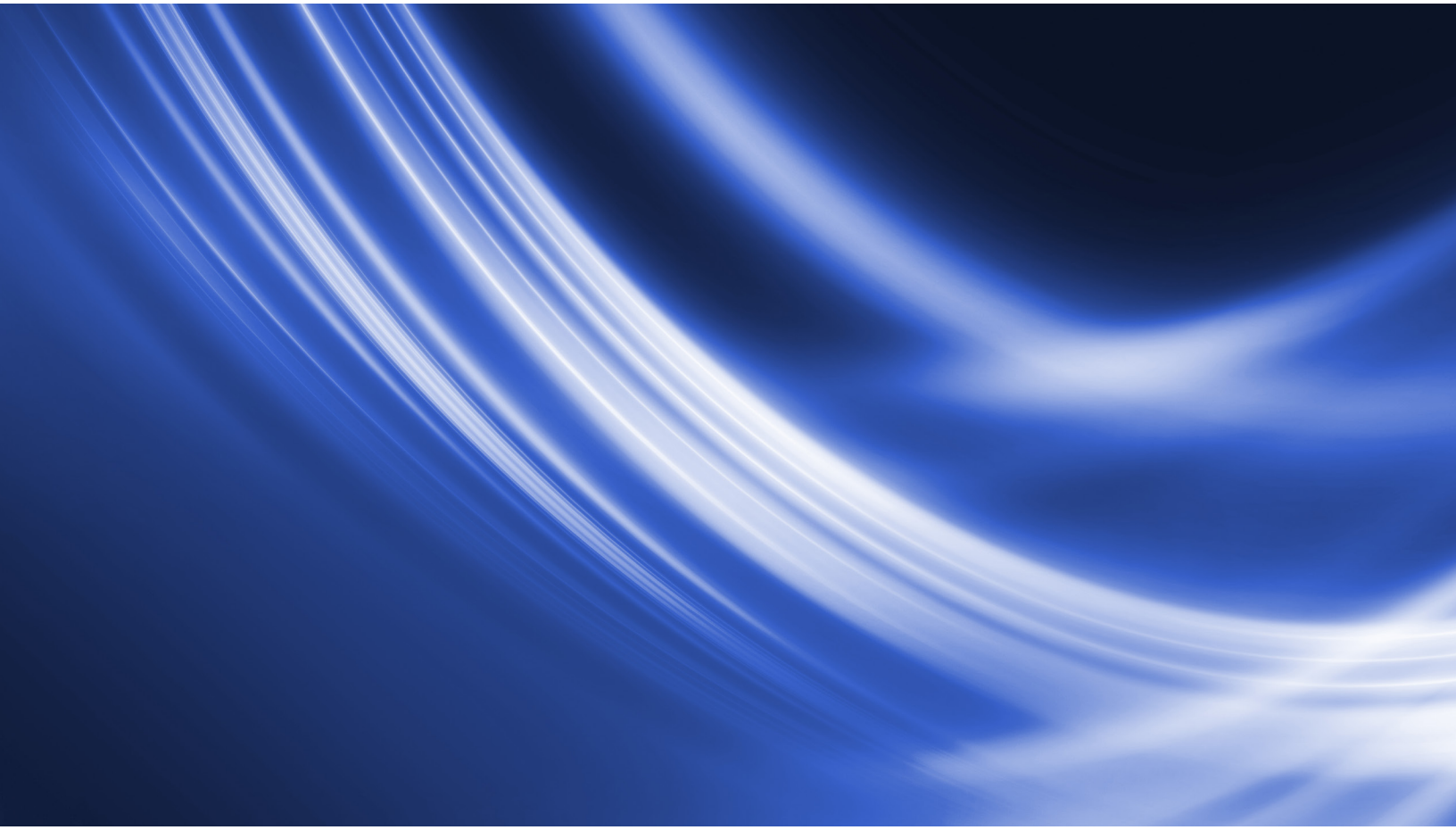
Threat Horizons

August 2023 Threat Horizons Report

Office of the CISO

August 2023

Table of contents



Mission statement

The Google Cloud Threat Horizons Report provides decision-makers with strategic intelligence about threats to cloud enterprise users, along with cloud-specific research. Most importantly, the report delivers recommendations from Google's intelligence and security teams.

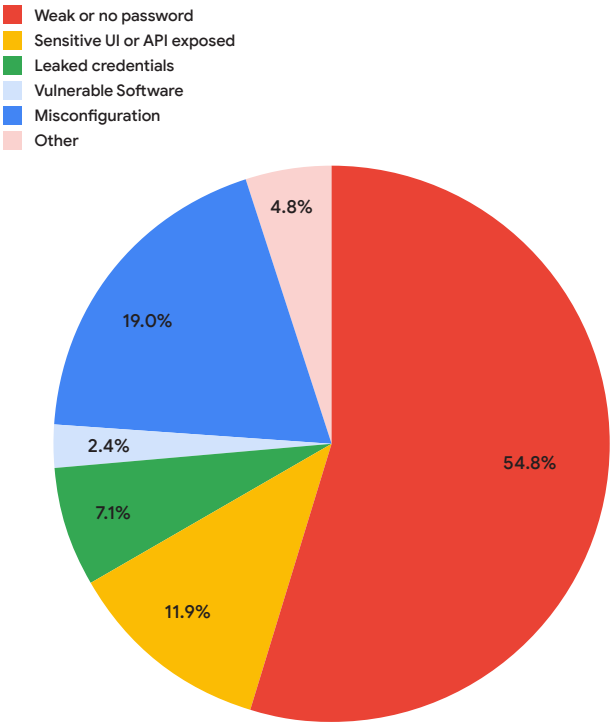
Credentials factor into over half of incidents in Q1 2023

The following statistics are based on observations by our Google Cloud incident response teams, which will be skewed to the platforms in the sample and may not be representative of all customer environments and verticals on Google Cloud, but should be representative of general trends.

In Q1 2023, Google Cloud's incident response teams observed that credential issues continue to be a consistent challenge, accounting for over 60% of compromise factors— which could be addressed by stronger identity management guardrails in place at the organization level.

Misconfiguration accounted for 19% of compromise factors, which were also associated with other compromise factors such as sensitive UI or APIs exposed. An example of how these two factors are associated could include a misconfigured firewall that unintentionally provided public access to a UI.

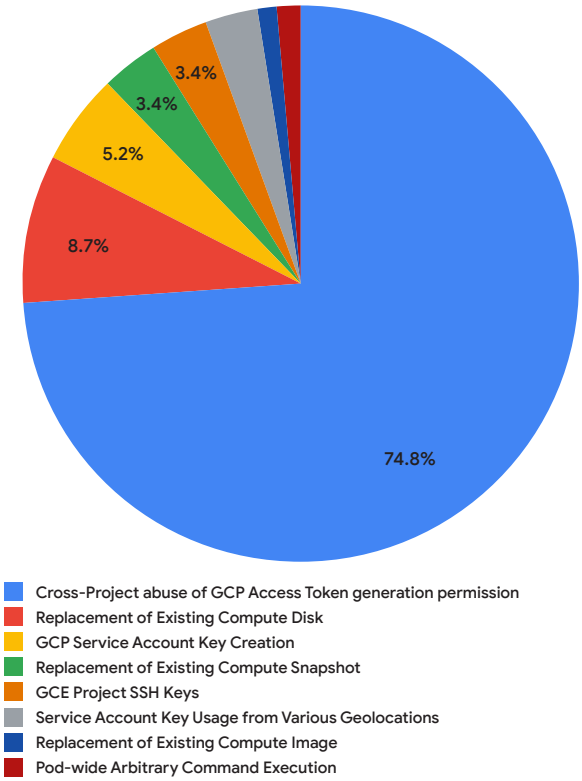
Cloud compromise factors Q1 2023



(Credentials, cont'd.)

We also analyzed anonymized alert statistics from Chronicle Security Operations in Q1 2023 to determine the top risky actions that can lead to compromises, which were identified as: cross-project abuse of access token generation permission, replacement of existing compute disks/snapshots, service account key creation, and GCE project SSH keys.

Chronicle signals overly permissive key creation consistent risk



Google Cloud's Chronicle Security Operations can help provide instant analysis and context on such risky activities, indicating an anomaly in the normal workflow of traffic in the environment.

The predominant alerts for Q1 2023 at nearly 75% were for cross-project abuse of access token generation permission associated with MITRE ATT&CK® tactic of Privilege Escalation (TA0004) and technique of Valid Accounts: Cloud Accounts (T1078.004). This aggregate data could help organizations looking to harden their security posture prioritize efforts based on these risks signals.

Alerts for the replacement of existing compute disks or snapshots are triggered when Chronicle Security Operations detects that a compute disk or snapshot is deleted and replaced by one with the same name which is commonly associated with cryptocurrency mining. These together accounted for 12% of anomalous behavior, the second highest risk for Q1 2023 and associated with ATT&CK's Defense Evasion (TA0005) > Modify Cloud Compute Infrastructure (T1578).

The Service Account Key Creation detection identifies these long-lived credentials which are associated with ATT&CK Persistence (TA0003) tactic and Account Manipulation: Additional Cloud Credentials (T1098.001) technique. The April 2023 Threat Horizons Report highlighted the risks for Service Account keys with mitigations such as minimizing or avoiding the use of service account keys and considering alternatives to service account keys.

Google Compute Engine (GCE) project SSH keys trigger when a new key is created where none previously existed and grants persistent access to all virtual machines (VMs) within the project. This alert is associated with the Persistence (TA0003) tactic and Account Manipulation: SSH Authorized Keys (T1098.004) technique. Wherever possible, we recommend using OS Login instead of self-managed SSH keys to control remote access.

Mobile Apps Evading Cloud Enterprise Detection through Versioning

Researchers have identified instances of Android applications downloading malicious updates after installation, attempting to evade Google Play Store's malware detections. In this article, we'll explore the use of deploying one version of an app to gain the Play Store's "trust" before issuing a malicious update of that same application. Campaigns using versioning commonly target users' credentials, data, and finances. In an enterprise environment, versioning demonstrates a need for defense-in-depth principles, including but not limited to limiting application installation sources to trusted sources such as Google Play or managing corporate devices via a mobile device management (MDM) platform.

Evading Detection through Versioning

We thoroughly evaluate apps on the Google Play Store and estimate that less than 1% of all downloads from Google Play are Potentially Harmful Applications (PHAs). When Google Play identifies indications of malicious functionality in applications, we take appropriate enforcement actions that may include removal of apps and termination of developer accounts.

One way malicious actors attempt to circumvent Google Play's security controls is through versioning. Versioning occurs when a developer releases an initial version of an app on the Google Play Store that appears legitimate and passes our checks, but later receives an update from a third-party server changing the code on the end user device that enables malicious activity.

One common form of versioning is using dynamic code loading (DCL). DCL is defined as an app which downloads and loads code files from untrusted sources.

(Mobile Apps Evading Cloud Enterprise Detection, cont'd.)

An app distributed via Google Play may not modify, replace, or update itself using any method other than Google Play's update mechanism. Likewise, an app may not download executable code (for example, dex, JAR, .so files) from a source other than Google Play.
Play Policy Center

Apps engaging in DCL violate Google Play Deceptive Behavior policy and may be categorized as a backdoor.

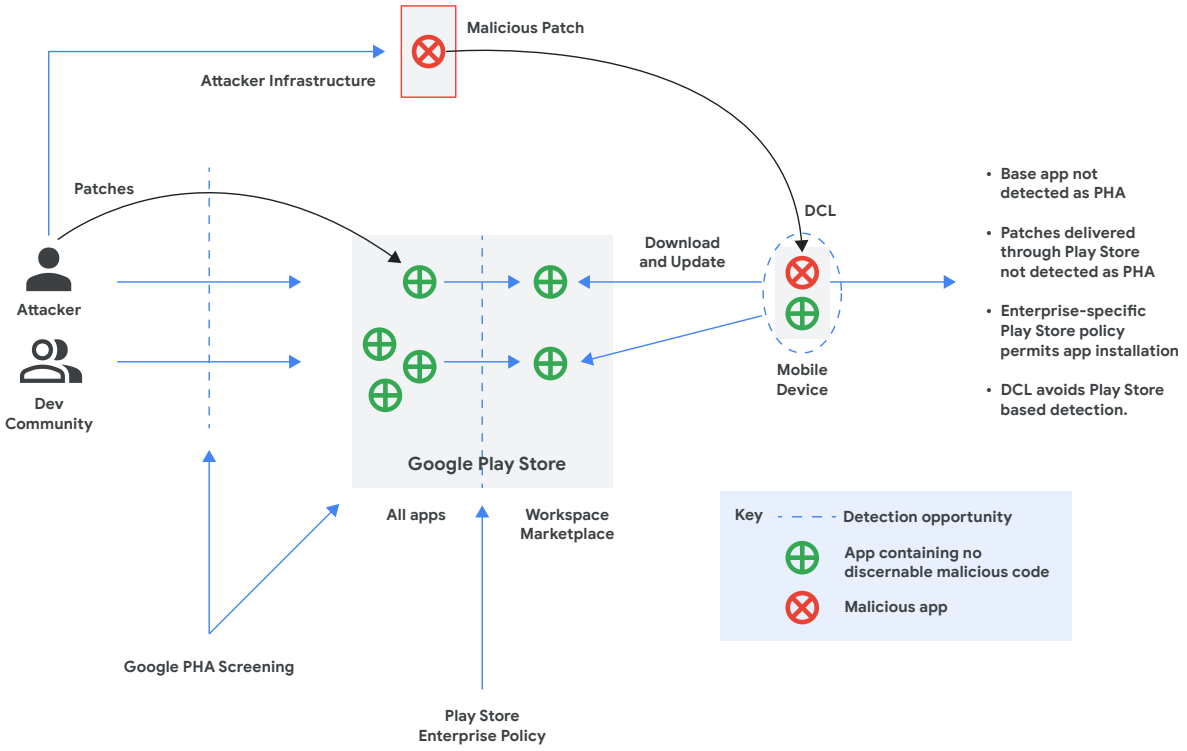


Fig 1. DCL circumvention of Play Store based security controls to patch malicious behaviors into already-installed applications.

(Mobile Apps Evading Cloud Enterprise Detection, cont'd.)

Google conducts rigorous PHA screening on applications and their patches through the Play Store; however, DCL circumvents some of those controls. For enterprise environments, the most reliable detection of this type of attack rests in the enterprise policy and configurations (through tooling such as Android Enterprise, as detailed in the mitigations section) where the DCL delivery can be detected or the resultant malicious behavior post-update.

Malware: Sharkbot

DCL (aka MITRE T1407) enables attackers to download and execute code not included in the original application after installation. The technique enables an attacker to evade static analysis and pre-publication checks by the Google Play Store.

One well-known malware variant using this technique is SharkBot. SharkBot is a banking malware that initiates money transfers from compromised devices using the Automated Transfer Service (ATS) protocol. The variants of SharkBot that appeared on Google Play had reduced functionality, a common tactic threat actors use to help their apps look less suspicious to Play Store detection systems. Once a user downloaded the app, the app would download a full version of the malware.

Mitigations

It takes a defense-in-depth approach to tackle these issues:

- The best way to avoid downloading malware to your Android device is to make sure that you only install applications from trusted sources such as the Google Play Store. We continuously monitor apps in the Play Store and seek to ensure that the apps are not malicious or abusing the trust of our users. You can learn more about the security of the Google Play Store through our Transparency Report. We also recommend keeping your device's software up-to-date.
- For a holistic mobile device management solution, Android Enterprise provides a suite of tools to manage the distribution of devices and their applications across your enterprise. This can provide increased visibility of device status and valuable security monitoring capabilities. Whether you choose a third party Enterprise Mobility Management (EMM) solution or work with Google's Endpoint Management, ensure that the relevant logging can be monitored from centralized security tooling to layer both endpoint state and runtime security monitoring. Whichever MDM you choose to implement, ensure that it is kept up to date with the latest detection rulesets in order to identify known-malicious applications and behaviors.
- Application allowlists, as part of a custom Workspace Marketplace for your enterprise, can ensure that only pre-approved applications can be installed on enterprise devices. Whilst the applications on the allowlists may still be involved in DCL attacks, limiting the available applications to only trusted developers may significantly reduce the likelihood.
- Especially in support of application allowlists, ensure that the applications allowed are only from known and reputable developers. If applications are required from less trusted sources, consider enforcing more strict supply chain monitoring and controls of those applications..

Identifying Compromised Customer Domains and IPs on Google Cloud

We encourage all Google Cloud customers to periodically examine their domains and IPs for malicious activity. Protecting online reputations – avoiding "spam" and associated denylist-type of labels – will ensure uninterrupted online interactions with such assets.

Using 2022-23 VirusTotal and Mandiant data, we discovered 13 customer domains and one IP hosted on Google Cloud that were compromised in Q1 2023[1]. Each of the uncovered 13 websites had at least one malicious file downloaded from it, while the one IP had bi-directional communications with external malware, using ports above the well-known port range (i.e. numbering 1024-65535).

Customers can mitigate such risks by using a variety of governance controls, including:

- Installing endpoint protection tools, to prevent the storage of malicious files;
- Performing vulnerability scans on external and internal cloud infrastructure to identify suspicious assets and rectify uncovered vulnerabilities;
- Examining cloud logs and improving credential management to identify and fix existing and original risks that may have precipitated such compromises.

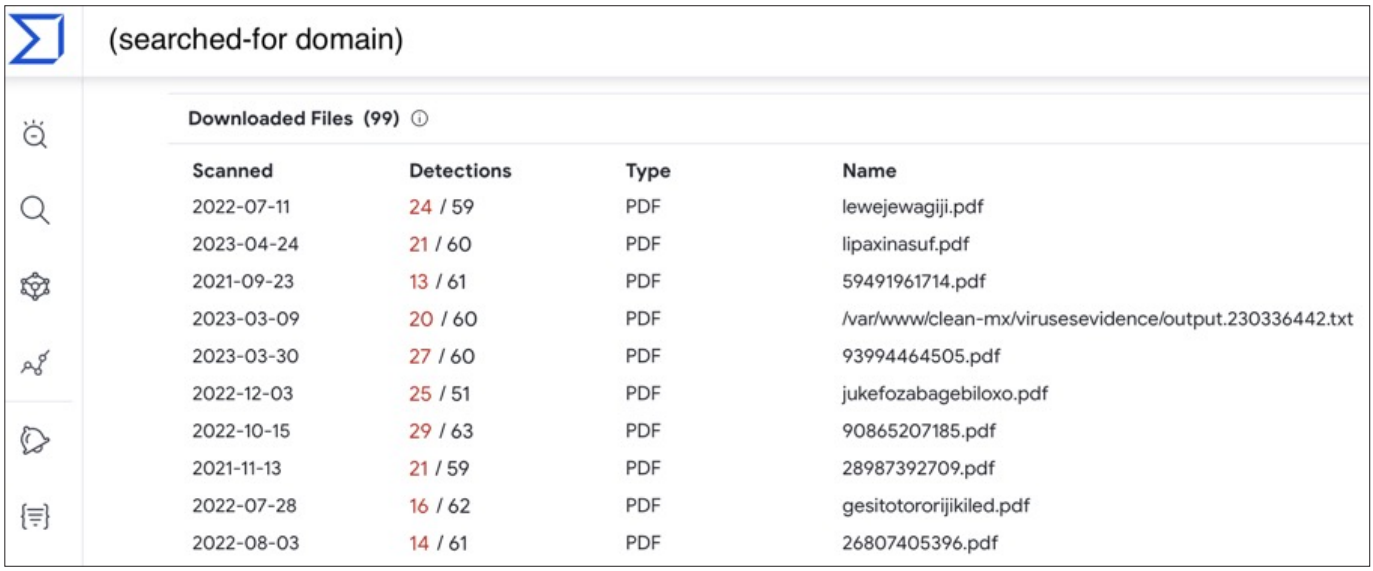
Customers can also use the new methodology we discuss in this article to identify the unique characteristics of their compromised domains and IPs for a more robust and focused mitigation.

(Compromised Customer Websites, cont'd.)

Identifying Compromised Customer Assets

Compromised Domains

To identify compromised domains, we searched VirusTotal for domains that had malware downloaded from them in Q1 2023[2]. We reduced this set to domains hosted on Google Cloud IPs, and reduced further to domains that Mandiant classified as suspicious or malicious. We finally reduced this result set to domains likely belonging to Google Cloud customers. The below is an illustration from the VirusTotal UI of a general domain with malicious file downloads associated with it. Of note, customers can also analyze their own domains this way using the VirusTotal UI and VirusTotal API. General VirusTotal API documentation and specific VirusTotal UI and API usage documentation can be used to examine such domains.



[1] *The VirusTotal and Mandiant data and analysis used in this article, is accessible to any regular user through standard customer-facing VirusTotal and Mandiant APIs.*

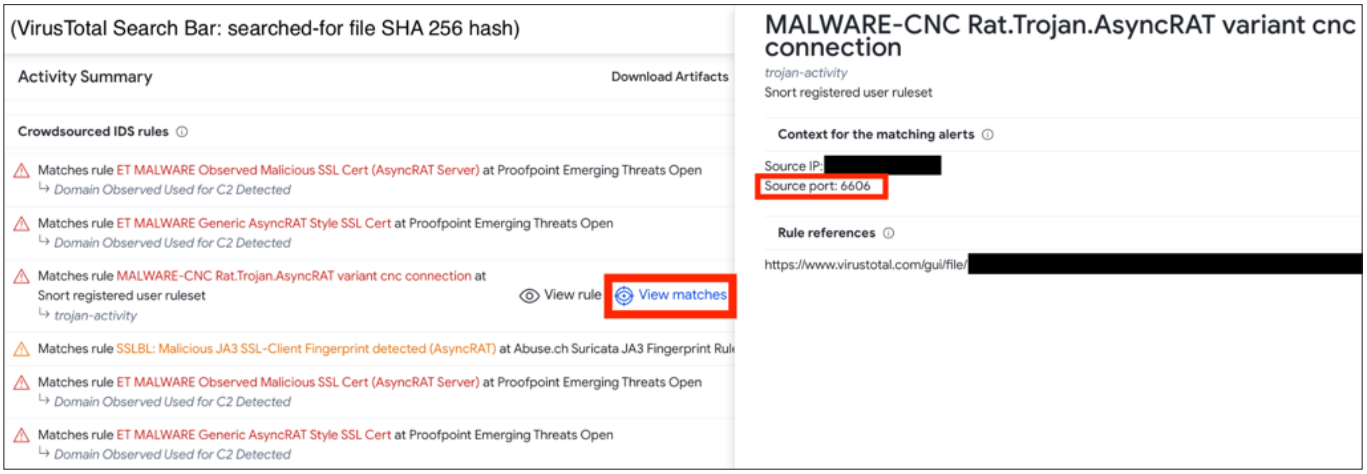
[2] *In this article, "malware" identified by using VirusTotal is software having malicious "verdicts" issued by at least 5 VirusTotal anti-virus engines.*

(Compromised Customer Websites, cont'd.)

Compromised IPs

We also searched VirusTotal for malware communicating with IP addresses, which responded to such requests over ports greater than 1023. We were looking for 'dialogue' between cloud instances and malware as opposed to for example port scans, or other potentially coincidental reasons why malware might communicate with a particular IP. Communicating above the well-known port range makes for a possibly easier investigation, rather than examining communications over well-known ports used by many services/users.

VirusTotal detonates malware submitted by users in sandboxes hosting Intrusion Detection Systems (IDSs) which monitor the sandboxes' inbound and outbound traffic. We searched VirusTotal for triggered IDS rules containing remote Google Cloud IP 'source ports' > 1023, indicating that Google Cloud IPs were responding to the sandboxed malware over registered/ephemeral ports. The example below illustrates a VirusTotal search result in which a malicious file communicates with a general IP – which responds to the malware on port 6606. (Customers can also use the VirusTotal API to search across many malware files potentially communicating with their IPs, and responding over ports > 1023).



We reduced our initial set of general IPs responding to malware to just responding Google Cloud IPs, and reduced the list further to just IPs Mandiant classified as suspicious/malicious, as well as to IPs belonging only to Google Cloud clients.

(Compromised Customer Websites, cont'd.)

Results

Ultimately, we found 13 compromised domains likely belonging to Google Cloud customers and malware having bi-directional communications with one compromised customer-owned IP. After further analyzing these entities using VirusTotal and Mandiant data, they could be characterized as follows:

13 domains

22 malicious files were downloaded from the 13 malicious domains. The files were characterized as:

- Mandiant confirms that one of the downloaded files is the malware STORMKITTY
- Almost half the files are for the Windows OS
- The diverse files types include Rich Text Format, EXE, Javascript, HTML, Powershell, Text file, and Microsoft Word files

13 domains

Mandiant classified the 13 domains as:

- 1 suspect domain
- 12 malicious domains

Mandiant categorized the domains as (note: not all domains have a categorization; and one domain can also have more than one categorization):

- "malware": 4
- "phishing": 6
- "malware/download location": 3

The 13 domains were spread over 8 Google Cloud customer IPs

1 IP Address

Mandiant classified the IP as malicious

2 malicious files were communicating with the IP, and getting responses over ports > 1023

- VT characterized both files as MetasploitShellCode, and further characterized one file as CobaltStrike software

(Compromised Customer Websites, cont'd.)

Suggested Mitigations for Google Cloud Customers

We recommend customers take the following actions to monitor and prevent such malicious activities in their environments.

1. Configure endpoint protection tools to examine and remove malicious files and processes in their instances.
2. Investigate any malicious communications occurring over all ports (registered/ephemeral in particular, but well-known as well). Malicious activity occurring in an instance can be identified by signing up and using anomaly-detection tools like Event Threat Detection in Security Command Center Premium. Overall, any open ports participating in suspect communications that don't need to stay open should be closed; and any involved software behind the ports should be removed or re-configured, as required.
3. Perform vulnerability scans; patching instance vulnerabilities in a timely fashion.
4. Examine domains, IPs, and ports in VirusTotal and Mandiant. From a defense in depth perspective, not all endpoint protection, intrusion detection, and/or other tools will detect all malware (e.g. malware signatures may have not yet been updated in a given AV platform; file downloads may appear inconspicuous until broader context is associated with them; etc). VirusTotal and Mandiant tooling provide additional malicious activity identification, which other tools might occasionally miss.
5. Malicious files can often be downloaded into or communicate with cloud infrastructure because of poor credential management (e.g. attackers compromising weak instance passwords, and installing malicious software in the instance; service account credentials accidentally being uploaded to Github–permitting attackers scraping them to perform certain instance management with the corresponding service account; etc. See article #1 in this journal on general credential abuse statistics that underpin Google Cloud instance compromises). To this end–customers should strengthen their Identity and Access Management practices–such as enforcing complex passwords, and scanning their source code for hardcoded credentials before checking it into repos. More generally, customers can try to examine the root cause of malware downloaded into their Google Cloud-hosted domains or having bidirectional communications with their Google Cloud IPs by using Chronicle. Feeding their instance's DNS resolution, firewall, system activity and other Google Cloud logs into Chronicle, customers can explore Chronicle's merged data 'views' to look for infection vectors which possibly originally led to their compromised assets. If found, associated infrastructure gaps can be examined, and relevant controls installed as required.
6. Use the Mandiant Digital Threat Monitoring (DTM) tool, to identify any compromised domains and IPs. DTM tracks compromised online assets, as mentioned or resold in dark web channels. If customers identify their own assets with DTM, an incident response process should be launched to investigate and mitigate the associated threats.

Telecommunications Industry Profile: How Zero Trust with Cloud Adoption Can Help Mitigate Threats

This is the first article in a new series from our research and analysis team exploring the implications of cloud services adoption and security across various industries. This article provides telecommunications organizations with data driven insights on the cyber threat landscape and actionable cloud security risk management recommendations to enhance their defensive posture against threats.

As the telecommunications industry adopts cloud services, threats from nation states and cybercriminals will likely persist—along with pre-existing systemic cyber risk—that can be addressed by modern cybersecurity approaches such as Zero Trust.

The telecom industry is responsible for critical infrastructure and is trusted with highly sensitive customer and communications data. As a result, the industry is consistently targeted by state actors and cybercriminals with malware campaigns seeking to steal sensitive personal and financial data or to disrupt services.

- The most frequently targeted telecom subsectors observed by Mandiant over the last two years include wireless telecommunications, IT and telecom services, and data services (Figure 1).

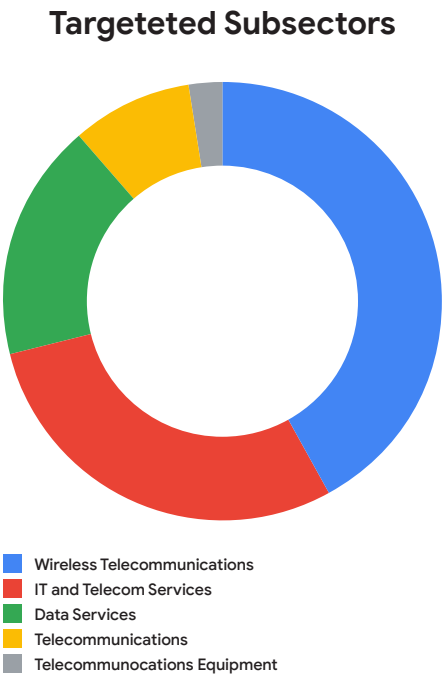


Figure 1: Most Frequently Targeted Telecommunications Industry Subsectors

(Q2 2021-Q1 2023)

- There have been multiple high-profile data breaches reported at communications services providers in recent years. Within the U.S. alone, T-Mobile, AT&T and Dish were breached during the first half of 2023, impacting the personal data of millions of customers.

(Telecommunications Industry Profile, cont'd.)

- Multiple cyber attacks affected national critical infrastructures in 2022, including Vodafone Portugal's loss of an entire network for several hours, Optus' leak of more than 2 million customers' personal information, Slovak Telekom's limited operations of its website, telephone, and store-front operations, and compromises to subsea cables off the coast of the UK and Denmark.
- Eighty-five percent of the largest 1,000 distributed denial-of-service attacks that Lumen mitigated in Q1 2023 targeted the telecom industry.
- Significant telecom ransomware attack cases since 2020 include the REvil attack on Telecom Argentina, the Nefilim attack on Orange, and the Lapsus$ attack on Portuguese Media Group Impresa.

Geopolitical activity is likely driving state actors to focus on targeting the telecom industry while financially motivated cybercriminals are evolving their tools and methods for doing so.

As of March 2023, Google's Threat Analysis Group (TAG) observed China-backed APT groups heavily focusing on telecom firms and Information and Technology (IT) services and solutions providers. TAG identified victims in West, Central and Southeast Asia, the Middle East, Oceania, and Africa. Additionally, TAG observed multiple China-backed groups engaged in sustained targeting of telecom firms in Southeast Asia, with a strong focus on Taiwan, the Philippines, and Malaysia. This activity is likely driven by China's economic and security interests, territorial disputes in the South China Seas, and growing tensions over Taiwan's sovereignty.

- Chinese government hackers siphoned data from critical infrastructure organizations in Guam in May 2023 in a campaign nicknamed Volt Typhoon. The largest telecom in Guam, Docomo Pacific, suffered a cyber attack in March 2023 that took multiple services offline. Other state-owned telecom companies in the Pacific Islands that have recently dealt with cyber attacks include Tonga, Guadeloupe, and Vanuatu.
- Mandiant has reported on significant malware campaigns impacting networking devices since 2021, including the exploitation of Pulse Secure VPN appliances and SonicWall's Email Security (ES) product. These cases likely indicate continuing interest by China to embed cyber campaigns in the overarching telecom and networking architecture used by organizations worldwide.
- Mandiant has observed a financially motivated threat group, UNC3944, targeting telecom organizations to obtain credentials to enable SIM swapping operations and utilizing malware that has been signed through the attestation-signing process. The group has also been observed deploying a malicious driver and its loader, POORTRY and STONESTOP, in an attempt to terminate the endpoint detection and response (EDR) agent on a Windows system.
- UNC3944 employed SIM swapping to gain privileged access to the Serial Console on Microsoft Azure Virtual Machines (VM) to install third-party remote management software within client environments in 2022. This attack method is unique because it avoided many of the traditional detection methods employed within Azure and provided the attacker with full administrative access to the VM.

(Telecommunications Industry Profile, cont'd.)

- The threat actors that Mandiant most frequently observed in tracked and targeted activity over the past two years in the telecom industry include UNC3840, UNC1543, and UNC3512 (Figure 2).

Top Threat Actors

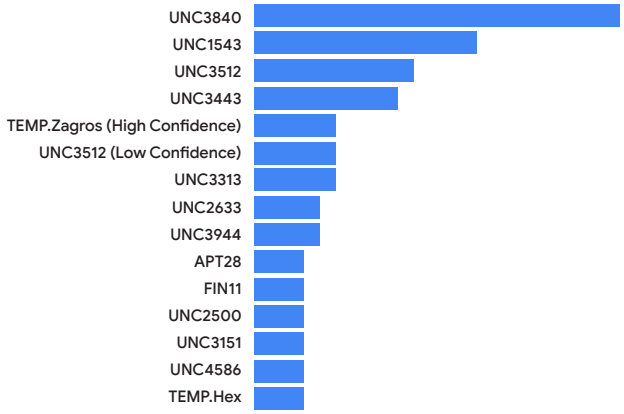


Figure 2: Top Threat Actors Targeting the Telecommunications Industry

(Q1 2021-Q1 2023)

Digital security threats to telecom industry business continuity and use of legacy systems will likely persist, along with increased focus on cloud service providers, as the industry continues migrating critical IT operations and business support systems to the cloud.

Physical and virtual ecosystems of partners, suppliers, employees, and customers across telecommunications, water, energy, and utility sectors create systemic cyber risks that will linger post cloud services adoption by the industry.

- Critical telecom infrastructure such as wireless and satellite communications may face state-sponsored cyber threats. Officials worldwide have expressed concern that Chinese state control over 5G telecom vendors could allow for Chinese state influence over data flows, which has resulted in equipment bans in North America, Europe, and Asia.
- Telecom is highly dependent on subsea data network cables, which are the subject of increasing concern due their vulnerability to physical attacks by state or non-state actors. Since the start of the Ukrainian conflict in 2022, Russian military activity has increased in the vicinity of key subsea installations and the 2022 NordStream pipeline attack highlighted the possibility that subsea cables could be targeted.
- Telecom networks are highly complex, typically comprising several generations of technology that include fixed, mobile, and satellite infrastructure. Due to the risk of negatively impacting availability, some operators are reluctant to update legacy equipment, which increases the risk of unpatched security vulnerabilities.
- The heavily connected nature of the industry and its role in critical infrastructures are driving increased focus by governments worldwide on how cloud service providers supporting the industry will maintain resilience—either from a cybersecurity incident or underlying technologies and systems failures—that could create cascading consequences. The U.S. Cybersecurity Strategy calls for cloud service provider requirements, while the European Commision is leading cross-sector initiatives to introduce cybersecurity certification for cloud providers.

(Telecommunications Industry Profile, cont'd.)

Modern cybersecurity approaches such as Zero Trust can help the telecom industry create and secure new services and reduce risk of data breaches.

There is emerging consensus that Zero Trust can help improve cybersecurity within critical infrastructure sectors such as telecom. For example, U.S. mandates and national standards are driving adoption of Zero Trust, including the Executive Order on Improving the Nation's Cybersecurity and NIST SP 800-27: Zero Trust Architecture (Figure 3). In the UK, the National Cyber Security Centre has provided Zero Trust principles.

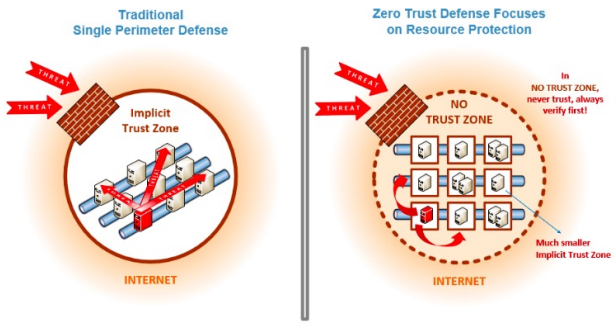


Figure 3: Traditional, Firewalled Network vs. Zero Trust Network

- **Create new services for customers**: Within telecom, 5G is experiencing rapid growth. Beyond mobile broadband, 5G is expected to be used for private networks for industrial Internet of Things (IoT), enterprise networking, and critical infrastructure communications (such as power grids). These types of new service offerings increase the criticality of security and availability, while the distributed nature of 5G also increases the potential attack surface. In response, Zero Trust tenets are already included in 5G network standards and can help secure 5G.
- **Reduce risk of data breaches**: The SolarWinds, Log4j, and Kaseya supply chain attacks exploited perimeter-based security approaches. Perimeter-less security such as Zero Trust can help mitigate the risk of attacks that exploit security perimeters. Additionally, Zero Trust approaches help implement the NIST principles of least privilege and continuous verification.

Adoption of cloud services and cloud-native security paradigms, including Zero Trust, can help the telecom industry improve cybersecurity, maintain resiliency of operations, and enhance security operations.

- **Zero Trust**: Google was one of the pioneers of Zero Trust security, which means that users, devices and applications are not trusted simply because they are inside a traditional security perimeter, but are continuously authenticated and monitored as potential security risks. These principles are applied within Google's Cloud network, where the hardware and software of every machine, as well as every API call, and every network access, is cryptographically authenticated to continuously verify trust. Google Cloud's BeyondCorp Enterprise empowers customers to implement a Zero Trust approach within their own hybrid cloud deployments.
- **Secure Authentication**: Loss or abuse of credentials is now one of the largest security risks faced by organizations, with SIM swap being a particular risk for telecom. Google Cloud and BeyondCorp enforce multi-factor authentication. Google recommends the use of physical security keys to counter SIM swap risks.
- **Supply Chain Security**: Google provides the Software Delivery Shield solution to enhance software supply chain security across the entire

(Telecommunications Industry Profile, cont'd.)

software development life cycle and Assured Open Source Software (AOSS) to help organizations obtain Open Source packages that are trusted and verified by Google.

- **Secure, Planet-Scale Network Resources**: Google operates a global network with private WAN connectivity and multiple layers of physical security protection. Google has sufficient network scale to absorb the largest DDoS attacks without impacting availability.
- **Maintain Resiliency of Operations**: The cloud offers faster recovery time, more flexibility to support high availability, and more tools that provide sophisticated infrastructure resilience capabilities. To capture these benefits, companies need to design, architect, and implement the right availability strategy to meet their business and customer needs.
- **Security Operations**: Customers can leverage Cloud's scale, automation and machine learning capabilities to improve threat detection, threat hunting and security incident response and act as a force multiplier for security operations teams.
- **Threat Intelligence**: Customers can gain increased understanding and protection against threat actors targeting them and their peers by accessing high-quality, actionable threat intelligence
- **Regulatory Compliance**: Cloud supports compliance with many global and regional security standards (and can also provide tooling to help monitor compliance).

Threat Insights: Implications of Source Code Leaks

This article increases awareness of how compromises or leaks of source code can help cyber threat actors facilitate a variety of exploitation activities, including exposure and abuse of legitimate credentials and certificates, unauthorized reproduction and use of leaked software, the development or insertion of vulnerabilities, and supply chain compromise.

Common Causes of Source Code Leaks: While credential or authentication token compromise are often cited as causes for source code incidents, there have been cases in which a compromise of a third-party service involved in hosting the code or the continuous integration/continuous development (CI/CD) process led to compromises of users of these services, as well as malicious insider incidents and misconfigurations (Figure 1).

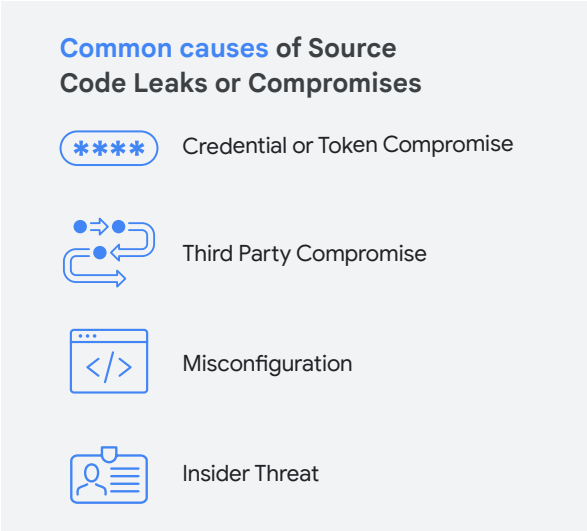


Figure 1: Common causes of source code leaks or compromise

Source Code Leaks Caused by Credential or Token Compromise: Recent examples of publicly reported source code compromises linked to credential or authentication token compromise include sophisticated phishing attacks and source code repository exploitation.

- Reddit disclosed that it experienced a "sophisticated and highly targeted phishing attack" in 2023, during which attackers managed to successfully access the company's internal documents, code, and some unspecified business systems. The hackers sent targeted victims "plausible-sounding prompts" that redirected them to a website purporting to be the Reddit intranet portal to ultimately steal victims' credentials and two-factor authentication tokens.
- Slack reported in 2022 that attackers used stolen employee tokens to access and download private code repositories hosted on GitHub.
- After an alert from Github, Okta confirmed that an attacker accessed and stole source code related to the Okta Workforce Identity Cloud (WIC) in 2022.
- Dropbox revealed a phishing attack in 2022 that led to malicious actors gaining unauthorized access to 130 of the company's source code repositories stored on GitHub and credentials and API keys used by developers. The attackers employed legitimate-looking emails directing Dropbox employees to visit a fake CircleCI login page, enter their GitHub username and password, and then use their hardware authentication key to pass a

(Implications of Source Code Leaks, cont'd.)

One Time Password (OTP) to the malicious site. Prior to this activity, CircleCI had issued a warning describing similar phishing activity impersonating the organization (Figure 2).

Figure 2: CircleCI warning about phishing campaign impersonating the company

Source Code Leaks Caused by Third-party Compromise: Some cases in which a compromise of a third-party service involved in hosting code or the continuous integration/continuous development (CI/CD) process have led to compromises of users of these services.

- In 2022, GitHub reported that dozens of companies were compromised after a hacker used stolen OAuth tokens maintained by Heroku and Travis CI to gain access to their private code repositories.
- Codecov, which offers software auditing tools and a platform to host code testing reports and statistics, disclosed in 2021 that an unknown threat actor managed to modify its Bash Uploader script and potentially export information stored in their users' continuous integration (CI) environments to a third-party server outside of Codecov's infrastructure.

Source Code Leaks Caused by Misconfiguration: Mandiant routinely observes reports of inadvertent data exposures due to misconfiguration or other errors. Open source reporting does not typically explain the source of the misconfiguration in detail; however, it reinforces the importance of using and verifying the use of best practices, including applying authorization and access controls to data and systems exposed to the internet or hosted in the cloud and encrypting data.

- A Swiss hacker claimed to have discovered an unsecured Amazon Web Services (AWS) cloud server hosted by the Ohio-based "CommuteAir" regional airline server containing the identities of "hundreds of thousands" of individuals whose names were included in an old version of the U.S. Government's No Fly and Terrorist Screening database.
- Researchers reported that the prestigious Paris, France-based Stade Français rugby club's website was leaking its own source code from its publicly accessible .git directory for more than 420 days.
- New York-based educational publishing company McGraw Hill suffered a data breach after leaving misconfigured AWS S3 buckets exposed on the internet containing more than 100,000 students' personally identifiable information (PII), company source code, and digital keys.

Source Code Leaks Caused by Insiders: Malicious insiders have targeted IP and source code, though these incidents are less frequently reported. In some instances, employees have leveraged legitimate authorized access to commit malicious activity to source code.

(Implications of Source Code Leaks, cont'd.)

- The increase in popularity of Large Language Model (LLM) generative artificial intelligence (AI) tools has led to users submitting proprietary data inputs into these tools. Samsung employees reportedly unwittingly leaked secret Samsung data after using the "ChatGPT" chat service to share internal documents that included meeting notes and source code.
- The chief technology officer (CTO) of the SushiSwap decentralized finance company reported an apparent insider threat in 2021 in which a contractor with access to the organization's MISO platform GitHub repository published a malicious commit replacing the wallet address for an auction on the platform with his personal address.
- In 2020, a former Cisco employee was sentenced to 24 months in prison for accessing the company's AWS cloud infrastructure and deploying code from his personal Google Cloud Project account that resulted in the deletion of approximately 450 virtual machines related to the Cisco Webex Team application.

Implications of Source Code Compromises: Compromises and leaks of source code could allow cyber threat actors to facilitate a variety of exploitation activities, including the exposure and abuse of legitimate credentials and certificates, the development or insertion of vulnerabilities, or supply chain compromise (Figure 3). Well-resourced nation-states or financially motivated groups may leverage leaked or compromised source code to identify exploitable vulnerabilities in the code that often enable deeper or more persistent access to victim networks.

Figure 3: Implications of source code leaks or compromise

- Mandiant cited a 2023 intrusion in which the threat actor accessed a victim organization's cloud-based code repository and identified plain text, hard-coded credentials in the source code for an application.
- Financially motivated actors regularly attempt to monetize source code through extortion or by offering it for sale in underground forums. Recent underground forum advertisements Mandiant has observed include "full" source code and secrets of a French payment services company, an offer for admin RDP access to a Canadian point-of-sale (POS) software provider with support access into client environments, and source code and backups and PII allegedly stolen from a Chinese technology company.

(Implications of Source Code Leaks, cont'd.)

- Cyber espionage and financially motivated actors have exploited access to source code to steal and re-use code signing certificates in their operations and execute software supply chain compromises. Following the Lapsus$ Group (also known as UNC2661) leak of NVIDIA data in 2022, threat actors quickly incorporated stolen NVIDIA code signing certificates to sign malware, other tools, and malicious drivers. Additionally, the Chinese state-sponsored espionage group APT41 has targeted the video game industry for financially motivated intrusions and to steal source code and digital certificates.
- Cyber actors have exploited access to source code to execute software supply chain compromises. PHP maintainer Nikita Popov confirmed that threat actors pushed two malicious commits to the PHP source code repository in 2021, suggesting that the attackers may have compromised the server to upload a backdoor. Additionally, Russian military sponsored Sandworm Team deployed EternalPetya (aka NotPetya, NonPetya, ExPetr) ransomware to various European targets in 2017 by compromising a software update mechanism (backdoored DLL inserted into update package) in the Ukrainian tax preparation service M.E.Doc.

Mitigation recommendations for code repositories and third-party resources reflect commonly cited IT security best practices, including adhering to the principle of least privilege, network segmentation, and log monitoring. Additionally, performing regular hygiene operations, such as user account lifecycle management, patching vulnerabilities, and performing regular audits to identify and remove internet access to ports and resources that should not be internet accessible. Organizations may also consider the following:

- As part of the software development lifecycle, ensure there are policies around the usage of third-party software along with credential usage. Implement technical controls and tools that check code prior to commits.
- Adopt tooling and processes to monitor your software dependencies. Google provides the Software Delivery Shield solution to enhance software supply chain security across the entire software development life cycle.
- Use Data loss prevention (DLP) tools.
- Refrain from using plaintext credentials, secrets, or access keys in remote code repositories.
- Limit the number of principals with privileged access and the use of administrative credentials where not required.
- Host relational database service (RDS) engines and other resources in non-internet accessible virtual private clouds.

Organizations should be especially sensitive to the possibility that malicious actors may impersonate trusted partners and conduct spear-phishing operations using legitimate email accounts. Mitigations for this include training/exercising caution and calling the sender to confirm they sent the email.

Organizations entrusting their sensitive data to third parties should take steps to ensure their data is properly being handled in transit and at rest, both through contractual obligations and auditing of the third party's security posture when and where possible. For example, user accounts assigned to service and logistics providers, contactors, etc., should be created sparingly and closely monitored and managed through the host organization's identity and access management system.

Threat Insights: Leveraging third-party services while reducing risk

The Cloud Security Alliance identified Unsecure Third-Party Resources as one of the Top Threats to Cloud Computing with a reference to research from Colorado State University indicating "that two-thirds of breaches are a result of a supplier or third-party vulnerabilities." Bad actors looking to evade detection can exploit these trusted relationships to gain access to organizations through supply chain attacks. These threats can be categorized as reputable third parties being compromised or bad actors intentionally creating malicious third-party services and luring users to use them.

Mandiant recently published details on the 3CX security incident, which resulted from a previous supply chain compromise where a financial trading software was compromised and resulted in the compromise of 3CX's desktop application. Notably, Mandiant highlighted that this was the first time it had seen a software supply chain attack lead to another software supply chain attack.

There are various third-party services and distribution channels for customers to use such as cloud marketplaces, browser extensions, OAuth applications, and IDE extensions. Though each offers different levels of security to help secure their users and reduce risk, they are essentially black boxes for organizations integrating with them given the lack of visibility into the underlying software supply chain and dependencies that are included.

In this article, we highlight where malicious behavior with third-party services has been observed, where we assess threat actors may target, and measures organizations can take to mitigate these risks.

(Leveraging third-party services while reducing risk, cont'd.)

Supply chain threats

Supply chain threats can be introduced in several locations of the software development lifecycle, many of which are not transparent to end users managing applications. Figure 1 below highlights eight different ways the supply chain can be compromised between the developer producing software and the end user consuming it. Though a developer may be creating software with good intent, this doesn't stop malicious actors from compromising the supply chain before it reaches customers.

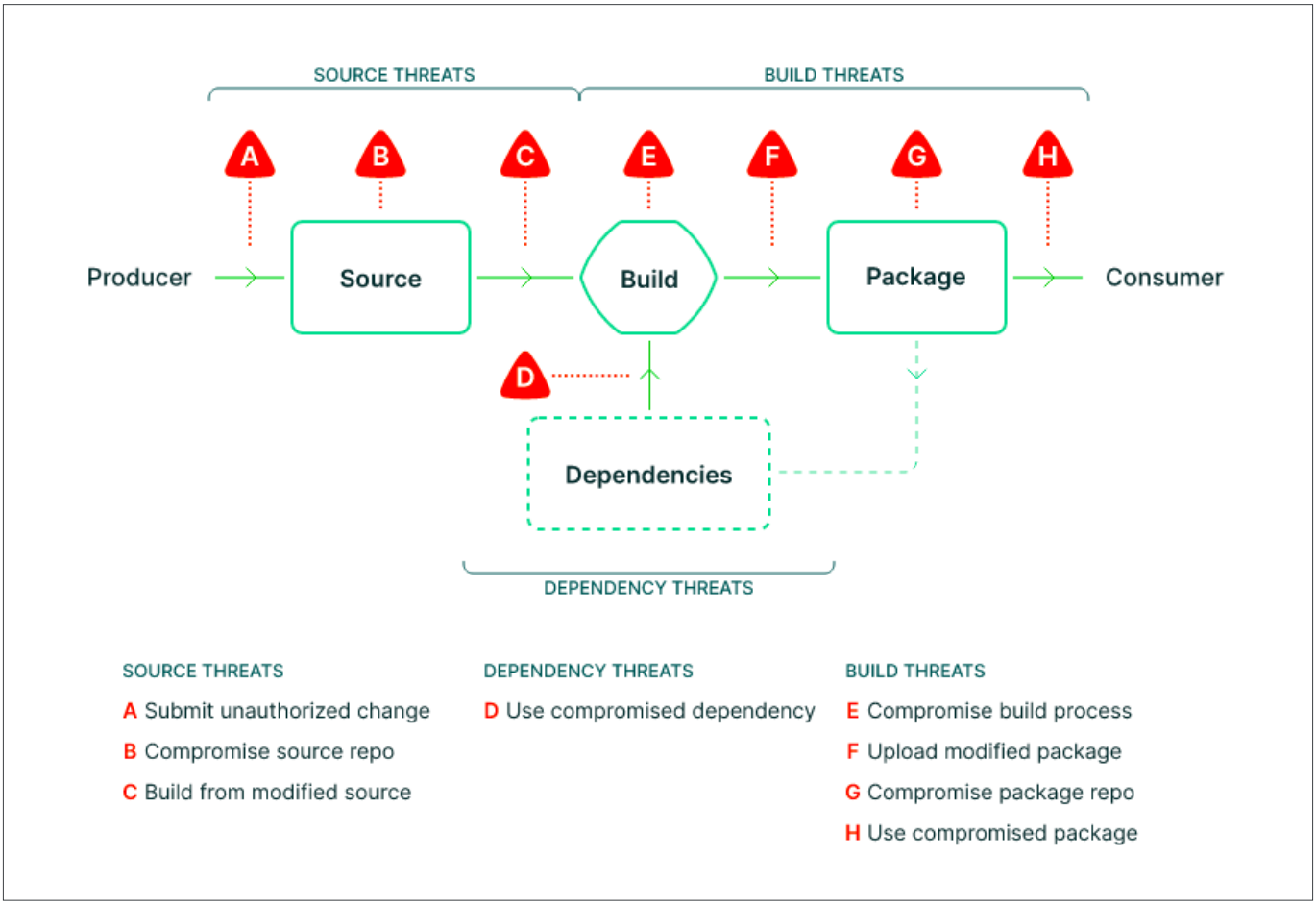


Figure 1. Graphic outlighting supply chain threats. Source: Supply-chain Levels for Software Artifacts

(Leveraging third-party services while reducing risk, cont'd.)

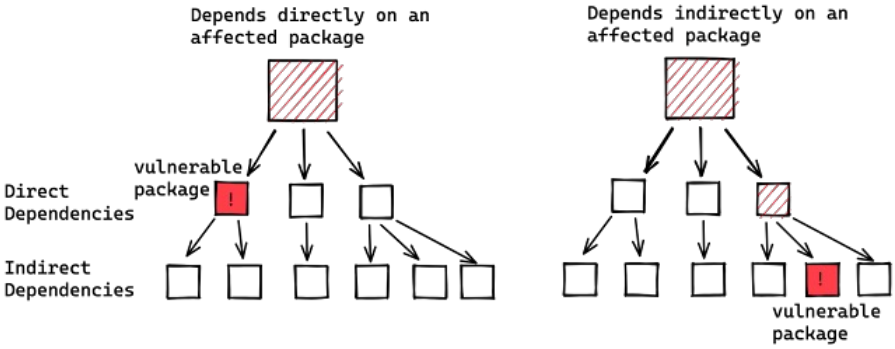


Figure 2. Graphic of software dependencies. Source: Google Security Blog.

Among the threats highlighted are dependencies and during the Apache Log4j vulnerabilities (1, 2), 17,000 packages were impacted (as of December 2021) either as a direct or indirect dependency as depicted in Figure 2. These vulnerabilities and an Executive Order led to the emergence of a Software Bill of Materials (SBOM) – an inventory of software in the codebase which helps organizations reduce their risk and secure their software. While thinking of dependencies like a tree structure is easier to understand, in reality, the relationship is more complicated, as illustrated in Figure 3 with an example from the javascript framework Express 4.18.2 dependencies (gray colored nodes) interrelated and represented on a graph. When available, organizations should review and regularly audit the SBOM of third-party software or services to assure they are not at risk for any critical vulnerabilities.

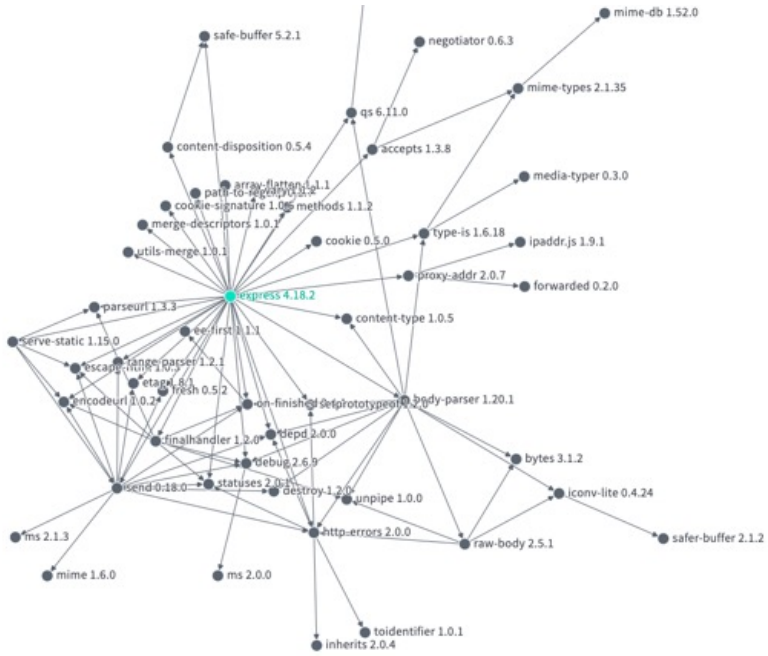


Figure 3. Example dependency graph of Express framework with 30M weekly downloads highlighting the importance of vulnerability management and SBOMs. Source: Open Source Insights

(Leveraging third-party services while reducing risk, cont'd.)

Artifact registries

Artifact registries offer centralized management of container images and language packages allowing organizations to store, push, pull, and deploy these assets. Organizations can create their own artifacts or use those provided by other organizations and the community. There are various public artifact registries available as well as each of the major Cloud Service Providers (CSPs) offering a managed artifact repository.

Research from SysDig uncovered 1,652 malicious images on Docker Hub, the world's largest artifact repository, where the most common types were cryptomining images followed by embedded secrets such as SSH or API keys allowing attackers to gain access to containers once deployed. There were also instances of typosquatting masquerading as legitimate software such as ubuntu, golang, and drupal. These malicious images can impact customers in various ways such as increased cloud costs due to utilization from cryptomining to data loss from exfil and leaked credentials.

Cloud Marketplaces

CSPs also offer marketplaces that host containers, VM images, Software as a service (SaaS) applications, and more. In the case of Google Cloud, customers are billed from one central location and containers and VMs are distributed from Google-managed infrastructure. Google scans VMs and containers for vulnerabilities however once deployed in a customer's environment, it is the responsibility of the customer to continue scanning for vulnerabilities which highlights the importance of vulnerability management.

In the case of managed SaaS services, under the shared responsibility model customers are responsible for access controls and the data shared with third-party applications. Some of these SaaS offerings are multi-cloud management tools that can help monitor, manage, and optimize cloud resources and operate by customers granting the tool access to their cloud environment with the use of IAM permissions and service accounts. Though many follow the principle of least privilege and some only require read-only access, there is still an inherent risk that bad actors may target these third-party services which have been granted persistent access to an organization's cloud environment.

Managed Service Providers (MSPs)

MSPs allow organizations to outsource their information technology (IT) to third parties to actively manage the day to day services such as infrastructure or security. These relationships often require privileged access and network connectivity to their customers.

There are several instances where attackers have gained access to organizations through MSPs exploiting the trusted relationship that is often scrutinized less than other methods defenders are monitoring. The U.S. and other nations released a joint advisory specifically about these threats to MSPs and impact to their customers. Two well known examples of this include the SolarWinds and Kaseya breaches. Mandiant attributed the SolarWinds compromise from December 2020 to APT29, a Russia-based espionage group, and noted "Since 2020, APT29 increasingly sought to exploit trust relationships between customers and third parties". Over 18,000

(Leveraging third-party services while reducing risk, cont'd.)

organizations were impacted with the trojan in SolarWinds Orion software. Kaseya was attacked by the REvil ransomware operators and in a press release noted that only 50 customers were impacted by the cyberattack, however given that most of their customers are MSPs, this resulted in 800 to 1,500 organizations being impacted.

OAuth Apps

Other prevalent distribution channels for extending functionality are browser extensions and OAuth apps – both of which require end user consent and present granularly scoped permissions. One of the methods OAuth apps are distributed are through marketplaces such as Google Workspace Marketplace and Microsoft's AppSource however the apps can also be distributed and installed outside of marketplaces. The apps on the Workspace Marketplace use OAuth scopes to grant granular access to an end-user's account once they've consented by the user or a Workspace administrator deploying an app for its domain users. Figure 4 is an example of a Google Workspace app with ~1M installs and the associated permissions it requires. This particular app requests restricted scopes which would require additional verification by Google and an independent security assessment of the application before publication.

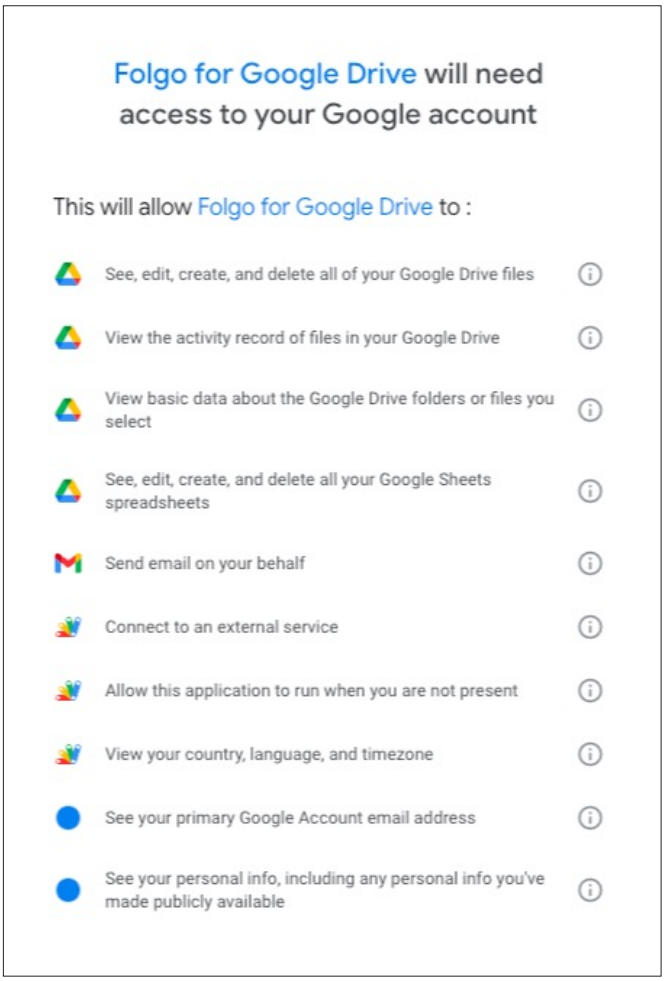


Figure 4. Example of permissions from the OAuth application Folgo for Google Drive with ~1M installs. Source: Google Workspace Marketplace.

(Leveraging third-party services while reducing risk, cont'd.)

One of the most prominent examples of OAuth abuse was described in Mandiant's M-Trends 2017 report regarding the 2016 presidential election, where attackers created a malicious OAuth app called "Google Scanner." Attackers sent phishing emails with a link to register the app, and once the user consented, the attackers had access to the user's emails in Gmail and files in Google Drive. This risk has since been mitigated with the additional verification process linked above that triggers when restricted scopes are requested.

A more recent example of how OAuth apps could be leveraged to attack organizations includes a recently fixed bug dubbed GhostToken where researchers demonstrated how an attacker could make an invisible and unremovable OAuth app by repeating a process of deleting and restoring a Google Cloud project hosting the OAuth app. However, depending on the scopes requested, apps that have not been verified and reviewed by Google would present end-users with an unverified app warning prior to consent.

OAuth applications can request single access tokens or persistent refresh tokens, which can allow an app to bypass multi-factor authentication. The default Google Workspace setting for enterprise accounts is to allow users to install any app available in the Marketplace – however, depending on the scope requested (non-sensitive, sensitive, and restricted), Google enforces different requirements to protect users and reduce the risk of malicious apps in the Marketplace. For instance, the ability to read all Google Drive files or emails in Gmail (restricted scope) triggers a more rigorous review and approval process for developers, including a software security assessment with over 70 controls. Additionally, app developers can opt into the highest tier of independent security reviews to earn a user-facing badge.

Browser Extensions

Public browser extensions are another example of third-party resources that can get integrated into organizations' environments. Extensions are usually distributed from online marketplaces however many browsers, including Chromium based ones, also allow users to manually download and side-load extensions (CRX files). Extensions can be granted various permissions such as the following with an example screenshot in Figure 5:

- Read and change all your data on all websites
- Read and modify data you copy and paste
- Capture content of your screen
- Read your browsing history

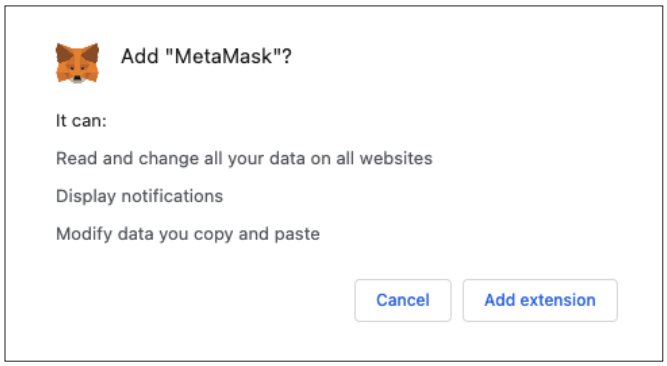


Figure 5. Example of a Chrome extension, MetaMask, and associated permissions. Source: Chrome Web Store

(Leveraging third-party services while reducing risk, cont'd.)

Mandiant has observed actors distributing browser extensions with malware that "monitors the URLs visited by victims, screenshots their browser tab views, and injects remote Javascript into select websites." McAfee researchers identified a malicious phishing chrome extension with over 100k downloads that lured users into downloading the extension with fake twitter accounts and reviews. When installed, the extension would look for information from gift balance-related websites that users visited, such as Target and Nordstrom, and capture the gift card numbers.

Integrated Development Environment (IDE) Extensions

Recently, bad actors were also observed injecting malicious code into IDE extensions. Checkpoint recently identified VS Code extensions that were stealing PII and enabling backdoors, and Aqua even deployed a proof of concept extension into the VS Code marketplace which was downloaded over 1,000 times within 48 hours masquerading as another popular extension.

When evaluating third-party resources, organizations are encouraged to perform vendor security audits – including partnering with privacy and legal teams to review privacy policies and terms of service. When controls are available, organizations should exercise enforcing policies – such as the case in Chrome Enterprise and Google Workspace – and continually monitor and audit the usage of third-party apps and services to ensure the supply chain has not been compromised prior to reaching its intended consumer or after trust has been established.

Mitigations

Supply Chain Threats

Google, Mandiant, and the security community have released various resources organizations can leverage to help secure their software supply chains which include:

- Open Source Insights provides an accurate view of the complete dependency graph with information about security vulnerabilities, licenses, recent releases, and more.
- Google Cloud published a software supply chain security guide with links to additional resources and Cloud services to aid in security of the supply chain.
- The US government released guidance through the Enduring Security Framework, CISA's Security-by-Design and -Default, and NIST's Secure Software Development Framework (SSDF).
- Google's Open source vulnerability database along with Mandiant's Vulnerability Intelligence provide a catalog of advisories to help organizations manage and prioritize vulnerabilities in their environments.
- Google Cloud offers OS Vulnerability scanning with VM Manager and Security Command Center Premium. For organizations using Kubernetes, in the April 2023 Threat Horizons Report we introduced solutions for balancing availability and security patching within GKE.
- Organizations developing apps and services can strengthen their supply chains to protect their customers by leveraging projects such as the Supply-chain Levels for Software Artifacts (SLSA) and Graph for Understanding Artifact Composition (GUAC) that help prevent tampering of software and aid organizations in their audit, policy, and risk management efforts.

(Leveraging third-party services while reducing risk, cont'd.)

Artifact Repositories and Third-party Software

- Google Cloud Assured Open Source Software (OSS) allows organizations to obtain OSS from a trusted and known supplier - the same OSS packages that Google uses.
- When using public artifact repositories like Docker Hub, assure developers are pulling from trusted sources and also checking containers for vulnerabilities.

Managed Service Providers (MSPs)

- Regularly audit this trusted relationship and review the guidance from CISA and other government agencies on how both MSPs and their customers can protect themselves against cyber threats.

OAuth Apps

- Workspace administrators have several tools and controls available to audit apps and their associated scopes, enforce policies on the types of permissions that are allowed in your organization, create allowlists, and even set session lengths for Google and Google Cloud services.
- Control which third-party & internal apps access Google Workspace data in your organization.

Browser Extensions

- Chrome Enterprise customers can set organization-wide browser policies and scale the management of extensions using these best practices.
- Leverage central management tools such as Chrome Browser Cloud Management or Microsoft Group Policy Objects (GPO) to enforce browser policies.
- Explore the Chrome Extension workflows to safeguard your data and allow users to request and install extensions in your organization

Google Cloud