
netskope
Cloud and Threat Report:
Global Cloud and Web
Malware Trends
netskope
+
Threat Labs

ABOUT THIS REPORT

Netskope Threat Labs publishes a quarterly Cloud and Threat Report to highlight a specific set of cybersecurity challenges. The purpose of this report is to provide strategic, actionable intelligence on active malware threats against enterprise users worldwide.

Netskope provides threat and data protection to millions of users worldwide. Information presented in this report is based on anonymized usage data collected by the Netskope Security Cloud platform relating to a subset of Netskope customers with prior authorization. This report contains information about detections raised by Netskope's Next Generation Secure Web Gateway (SWG), not considering the significance of the impact of each individual threat. Stats in this report are based on the period starting January 1, 2023 through March 22, 2023. Stats are reflection of attacker tactics, user behavior, and organization policy.

Netskope Threat Labs

Staffed by the industry's foremost cloud threat and malware researchers, Netskope Threat Labs discovers, analyzes, and designs defenses against the latest web, cloud, and data threats affecting enterprises. Our researchers are regular presenters and volunteers at top security conferences, including DEF CON, Black Hat, and RSA.

EXECUTIVE SUMMARY

The purpose of this Cloud and Threat Report is to provide strategic, actionable intelligence on active malware threats against enterprise users. Malware is a significant and ongoing enterprise cybersecurity challenge, as attackers continue to develop new and sophisticated techniques to evade detection and compromise systems. On average, 5 out of every 1000 enterprise users attempted to download malware in Q1 2023.

The two primary malware themes in Q1 were social engineering and detection evasion. Attackers used social engineering in at least 73% of malware infiltration attempts in Q1. Social engineering techniques included using SEO to weaponize search engine data voids and trick victims into downloading Trojans based on their search queries. Themes used by attackers to lure victims into downloading malware included the earthquake in Turkey and Syria and the collapse of Silicon Valley Bank.

At the same time, attackers continued to find new ways to evade detection. In Q1, 72% of all malware downloads detected by Netskope were new, as attackers added new malicious functionality and made changes to evade detection. Attackers also gravitated toward network services that are already widely used in the enterprise, abusing cloud services to deliver malware and using HTTP and HTTPS to communicate with infected systems.

Protecting enterprises against the onslaught of malware will require cross-functional collaboration across multiple teams, including network, security operations, incident response, leadership, and even individual contributors.

REPORT HIGHLIGHTS

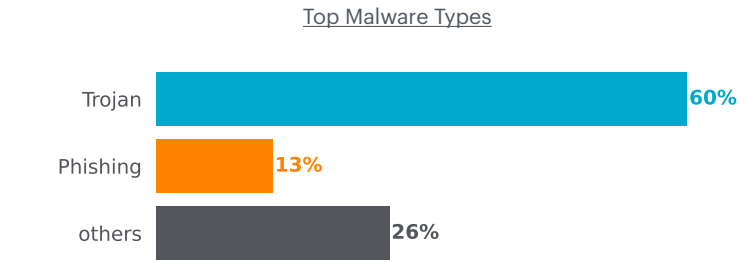
- Social engineering continues to be a dominant malware infiltration technique, with attackers abusing search engines, email, collaboration apps, and chat apps to trick their victims into downloading Trojans.
- To evade detection, attackers are increasingly abusing popular apps to deliver malware, with 55% of HTTP/HTTPS malware downloads in Q1 2023 coming from popular cloud apps.
- To blend in with normal traffic and avoid enterprise firewall rules, most malware use HTTP and HTTPS for all types of communication, including command and control and next stage payload delivery.
- New malware families and variants represented 72% of all malware downloads in Q1, as attackers made changes to provide additional malicious functionality and evade detection.

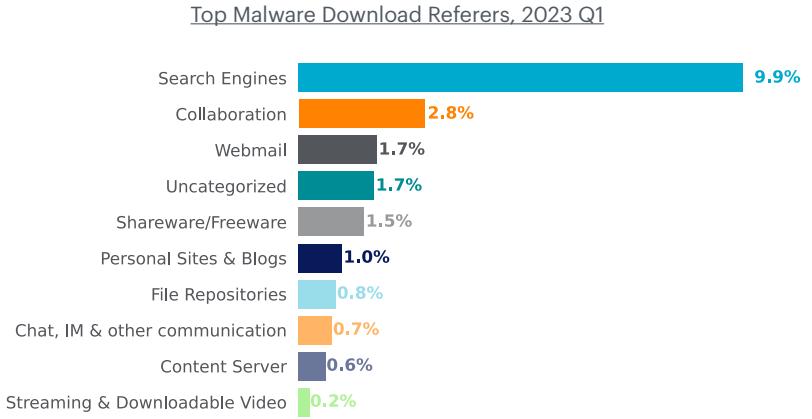
Social Engineering: Trojans and Data Voids

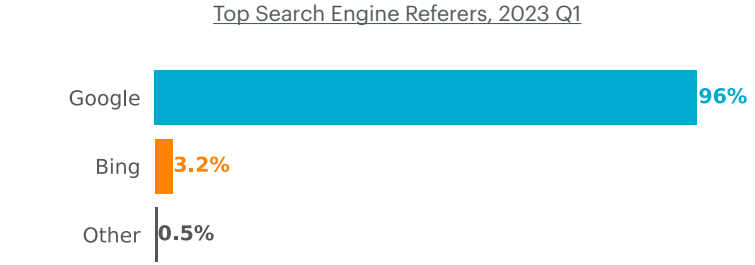
Social engineering remains a top tactic that attackers use to gain an initial foothold into victim organizations. In the first quarter of 2023, attackers tried to capitalize on major events, including the ongoing Russo-Ukrainian war, the earthquake in Turkey and Syria, and the collapse of Silicon Valley Bank. Attackers also continued to use the tried-and-true technique of using fake invoices to create a false sense of urgency.

Trojans are a social engineering technique wherein an attacker disguises malware samples as legitimate files to trick victims into downloading them. Trojans are commonly used by attackers to gain an initial foothold and deliver other types of malware, such as infostealers, backdoors, and ransomware. Trojans accounted for 60% of all malware downloads in Q1, indicating not only that Trojans are a popular technique used by attackers but also that attackers have a high rate of success in tricking victims into downloading them. Phishing downloads accounted for 13% of malware downloads and represent another type of social engineering, wherein an attacker uses an Office or PDF document to either direct the victim toward a phishing website or to instruct the victim to reach out to the attacker via phone, email, or chat app.

Another social engineering technique that is on the rise is the weaponization of search engine data voids. Data voids are combinations of search terms that have very few results, which means that any content matching those terms is likely to appear very high in the result set. Attackers have cleverly crafted malware payloads and malware delivery sites to exploit data voids, using those uncommon combinations of search terms to trick victims into downloading malware. Nearly 10% of all malware downloads in Q1 were referred from search engines, the result of both weaponized data voids and, to a lesser extent, malicious ads appearing alongside search engine results. Webmail, collaboration, and chat apps are also common places where attackers use social engineering to trick their victims into downloading malware.







Detection Evasion: Transferring Malware Over Crowded Channels

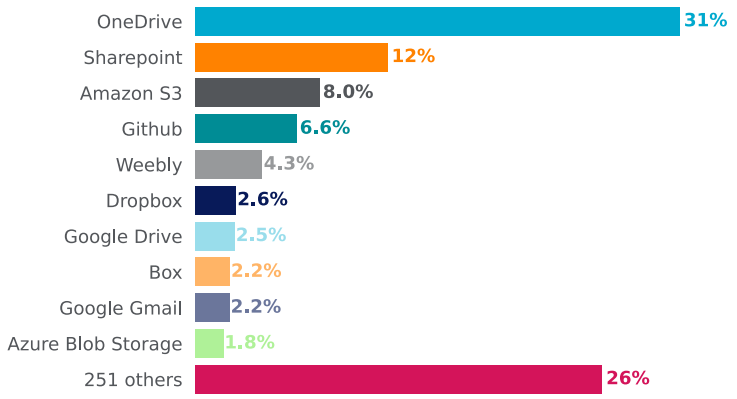
One of the ways attackers try to fly under the radar is to distribute malware over channels that are widely used in the enterprise, in hopes that the malware transfer bypasses security controls and blends in with normal traffic. Cloud apps, especially those apps that are popular in the enterprise, are becoming an increasingly popular channel for malware delivery.

In Q1 2023, 55% of HTTP/HTTPS malware downloads came from cloud apps, up from 35% for the same period one year earlier. Cloud malware downloads have seen quarter-over-quarter increases since Q1 2022, with the trend poised to continue through 2023. At the same time, the number of apps with malware downloads also continued to increase, with malware downloads from 261 distinct apps in Q1 2023. However, the primary driver of the increase in cloud malware downloads is an increase in malware downloads from the most popular enterprise cloud apps.

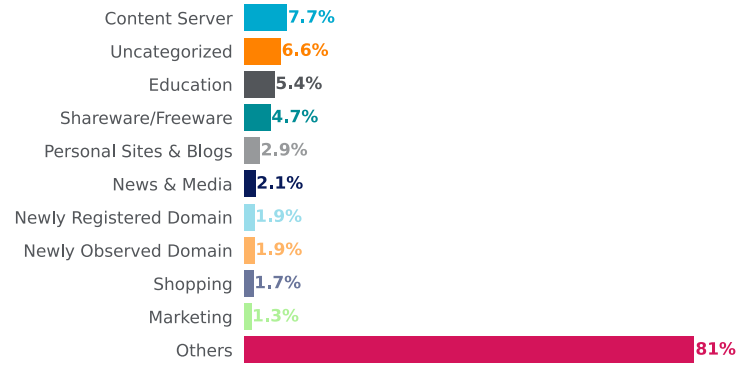
The top apps for malware downloads are some of the most popular enterprise cloud apps, mostly cloud storage apps (OneDrive, Amazon S3, DropBox, Google Drive, Box, and Azure Blob Storage), but also collaboration apps (SharePoint), free software hosting services (GitHub), free web hosting services (Weebly), and, of course, webmail apps (Gmail). Microsoft OneDrive, the most popular enterprise app by a wide margin, continues its multi-year stand at the top of the malware download list, a position it is poised to retain throughout 2023. Cloud apps are also commonly abused as a form of social engineering, where attackers use app features familiar to the victims to entice them into downloading malware.

Even when attackers deliver malware over traditional websites, they make similar efforts to blend-in with benign traffic. Only a small fraction of total web malware downloads were delivered over web categories traditionally considered risky, such as uncategorized sites, newly registered domains, and newly observed domains. Instead, downloads are spread out among a wide variety of sites, with content servers (CDNs) responsible for the largest slice, at 7.7%.

Top Apps for Malware Downloads, 2023 Q1



Top Web Categories for Malware Downloads, 2023 Q1

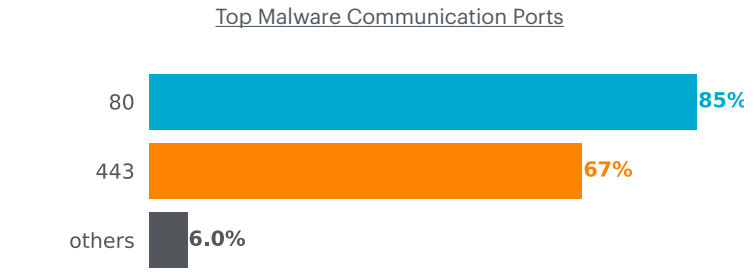


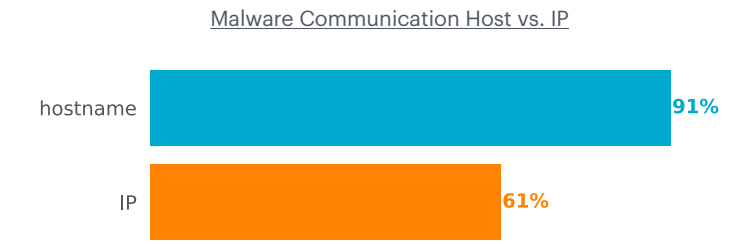
Detection Evasion: Communicating Over Crowded Channels

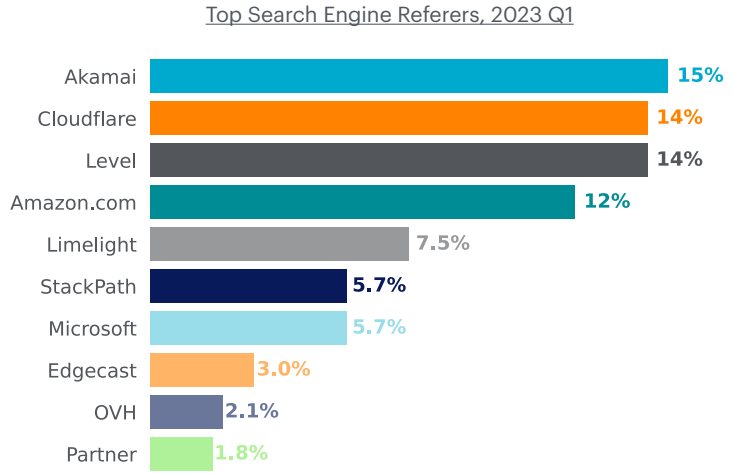
After attackers gain an initial foothold in their victims' environments, they often need to establish a communications channel to download additional malware payloads, to receive commands, or to exfiltrate data. To evade detection, attackers are increasingly using HTTP and HTTPS over ports 80 and 443 as their primary communication channels. This approach has the advantage that the traffic is likely to be allowed from an infected system and will blend in with the abundance of HTTP and HTTPS traffic already on the network. Contrast this approach with malware that communicate over rarely used ports or protocols, where such communications are easily blocked by egress firewall controls in enterprise environments. Of the new malware executables analyzed by Netskope that communicated with external hosts, 85% did so over port 80 (HTTP) and 67% did so over port 443 (HTTPS), with many using both. Using TLS to encrypt malware communications is becoming commonplace as attackers either abuse services that are already using TLS or obtain their own certificates from one of the many free certificate services. Only 6% of the executables initiated outbound connections over a different port, with port 21 (FTP) being most common. Port 8080 was also commonly used as an alternative port for HTTP communication.

To evade DNS-based security controls, some malware samples sidestep DNS lookups, instead reaching out directly to remote hosts using their IP addresses. In Q1 2023, most malware samples that initiated external communications did so using a combination of IP addresses and hostnames, with 61% communicating directly with at least one IP address and 91% communicating with at least one host via a DNS lookup.

Attackers also attempt to blend in by routing their malware communications through popular content delivery networks (CDNs) and cloud service providers. The new malware executables communicated with destination IP addresses in a variety of ASNs, with the most popular being owned by Akamai. IP addresses associated with Amazon Web Services and Microsoft Azure were also among the top destinations.







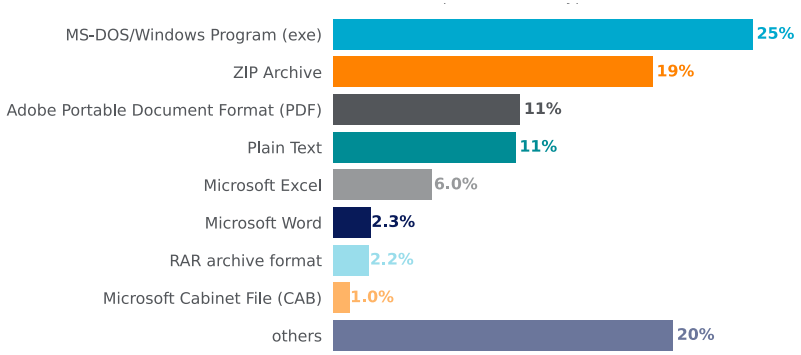
Detection Evasion: Innovation and Evolution

Malware detection is a challenging problem partially because there are so many different malware families, each with their own characteristics and attack methods. Furthermore, the number of families and variants is constantly growing. In Q1 2023, Netskope detected downloads of more than 60,000 distinct malware samples, 72% of which were either new malware families or new variants of existing families. By file type, Microsoft Windows executables accounted for the plurality of malware downloads, at 25%, while ZIP archives and other types of archive files followed closely behind as they continue to rise in popularity.

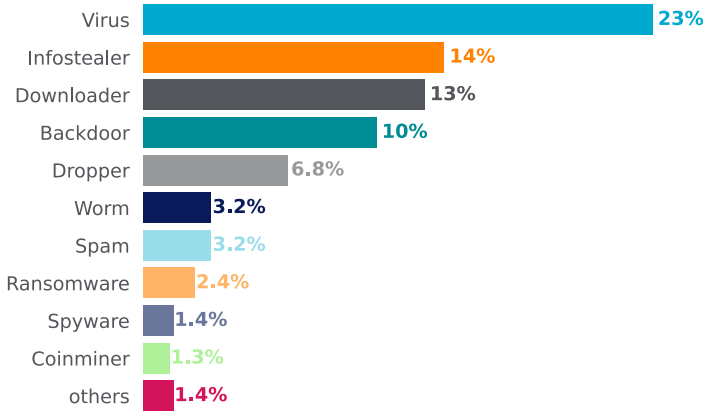
The reason for the rise of ZIP files is primarily detection evasion, with attackers designing files to evade certain types of defenses. For example, a new Emotet variant that emerged in March 2023 uses binary padding to create files in excess of 500 MB and then distributes them in ZIP files. Because the files are padded with low-entropy data, they compress very efficiently to make for easy transport. The intention is to bypass security controls that ignore large files. Attackers also use archive files to bypass the Mark-of-the-Web on Windows to make it easier to trick their victims into executing Trojans.

At the same time, attackers continue to deliver a wide variety of different types and families of malware. Excluding Trojans and phishing malware discussed earlier in this report, the most common malware types included viruses, infostealers, and backdoors. Downloaders and droppers are similar to Trojans in that they are used to deliver additional malware payloads. Ransomware, while it only accounts for 2.5% of downloads, has an outsized impact on the organizations it infects and continues to be a major enterprise security concern. While old ransomware families like Ryuk and Ragnar continue to circulate, new groups like BlackSnake continue to emerge. BlackSnake also provides new functionality to directly steal cryptocurrency from its victims on top of traditional ransomware functionality, an example of how attackers continue to evolve their malware.

Top Malware File Types, 2023 Q1



Top Malware Types



RECOMMENDATIONS

Protecting enterprises against the onslaught of malware will require cross-functional collaboration across multiple teams, including network, security operations, incident response, leadership, and even individual contributors. Some of the steps that organizations can take to reduce their risk include:

1. Inspect all HTTP and HTTPS downloads, including all web and cloud traffic, to prevent malware from infiltrating your network. Netskope customers can configure their Netskope NG-SWG with a Threat Protection policy that applies to downloads of all file types from all sources.

2. Ensure that your security controls recursively inspect the content of popular archive files such as ZIP files for malicious content. Netskope Advanced Threat Protection recursively inspects the content of archives, including ISO, TAR, RAR, 7Z, and ZIP.

3. Ensure that high-risk file types, like executables and archives, are thoroughly inspected using a combination of static and dynamic analysis before being downloaded. Netskope Advanced Threat Protection customers can use a Patient Zero Prevention Policy to hold downloads until they have been fully inspected.

4. Configure policies to block downloads from apps that are not used in your organization to reduce your risk surface to only those apps and instances (company vs. personal) that are necessary.

5. Block downloads of all risky file types from newly registered domains, newly observed domains, and other risky categories to reduce your risk surface.

6. Use an egress firewall to restrict outbound network traffic to only those ports, protocols, and applications that are required for normal operations. Use DNS security to block lookups of potentially malicious domains.

7. Educate users about social engineering techniques being used against the organization and set up a channel for users to easily report and receive feedback on anything they find suspicious.

8. Use Remote Browser Isolation (RBI) technology to provide additional protection when there is a need to visit websites that fall in categories that can present higher risk, like newly observed and newly registered domains.

9. Ensure that all of your security defenses share intelligence and work together to streamline security operations. Netskope customers can use Cloud Exchange to share IOCs, import threat intel, export event logs, automate workflows, and exchange risk scores.

LEARN MORE

For more information on cloud-enabled threats and our latest findings from Netskope Threat Labs, go to:
NETSKOPE.COM/NETSKOPE-THREAT-LABS

For more information on how to mitigate risk, contact us today:
WWW.NETSKOPE.COM/REQUEST-DEMO

netskope
+ Threat Labs