netskope

Cloud and Threat Report:

Global Cloud and Web Malware Trends

BROUGHT TO YOU BY

netskope

THREAT LABS

EXECUTIVE SUMMARY

In this edition of the Cloud Threat Report, we examine the past twelve months of malware downloads from the cloud and web. Trojans accounted for the overwhelming majority of malware downloads, with attackers using a variety of different Trojan families and social engineering techniques to target their victims. The majority of malware downloads were either Windows EXE/DLL files or Microsoft Office documents, as attackers continue to target Microsoft Windows, still the most popular desktop operating system in the enterprise.

We also examine the sources of malware downloads, where 53% come from traditional websites and 47% come from cloud apps. Web malware downloads originate from many different website categories, led by technology sites and content servers. Cloud malware downloads originate from hundreds of different apps, led by popular cloud storage apps. Both web and cloud malware downloads tend to originate from servers located within the same regions as their victims.

Finally, we gain insight into some of the techniques attackers use to deliver malware by examining the most popular referrers of malware downloads. The top referrers include search engines, as attackers use popular SEO techniques to achieve high search engine rankings. Compromised websites and malicious websites designed to mimic benign websites are also popular referrers of malware downloads.

REPORT HIGHLIGHTS

- **Trojans account for 77% of all cloud and web malware downloads**, used to gain an initial foothold and to deliver a variety of next-stage payloads, including backdoors, infostealers, and ransomware.
- **47% of malware downloads originate from cloud apps** compared to 53% from traditional websites, as attackers continue to use a combination of both cloud and web to target their victims.
- **Phishing downloads are on the rise, fueled by attackers using SEO techniques** to get malicious PDF files ranked highly on popular search engines, including Google and Bing.
- **EXE and DLL files account for nearly half of all malware downloads** as attackers continue to target Microsoft Windows, while malicious Microsoft Office files are on the decline and have returned to pre-Emotet levels.
- **Most malware downloads originate from servers located within the same regions as their victims,** as attackers stage their malware throughout the world to evade geofences.

ABOUT THIS REPORT

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 (Next Gen SWG), not considering the significance of the impact of each individual threat. Stats in this report are based on the twelve month period from April 1, 2021 through March 31, 2022.

Netskope Threat Labs

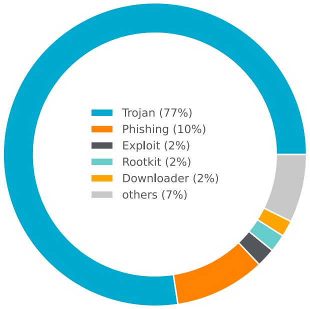
Staffed by the industry's foremost cloud threat and malware researchers, Netskope Threat Labs discovers, analyzes, and designs defenses against the latest cloud and data threats affecting enterprises. Our researchers are regular presenters and volunteers at top security conferences, including DefCon,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

Malware Categories and Families

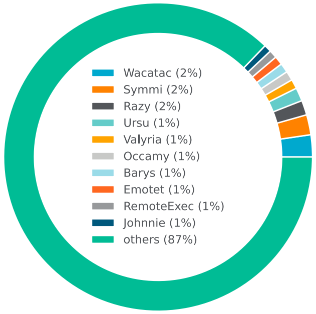
The overwhelming majority (77%) of all cloud and web malware downloads are Trojans. Trojans are a common first stage of a cyberattack, where the goal of the attacker is to fool the victim into downloading and executing software that will give the attacker an initial foothold. Trojans are often disguised as legitimate software and used to capitalize on significant events. For example, there have been a wide variety of COVID-19 Trojans circulated during the pandemic. Attackers use Trojans to deliver a variety of next-stage payloads, including backdoors, infostealers, and ransomware. While the overwhelming majority of malware downloads are Trojans, there is no single family of Trojans that is globally dominant. The top ten Trojan families account for only 13% of all downloads, with the remaining 87% coming from a long tail of less common families.

Trojans accounted for the plurality of malware downloads in every region, and the majority in every region except the Middle East, which saw a higher incidence of exploits than other regions. Exploits here refer to malware files that take advantage of a bug or vulnerability when they are opened or executed by the victim. Phishing downloads, also above average in the Middle East, were highest in Africa. Phishing downloads differ from traditional phishing websites. They are typically PDF files that take the form of fake CAPTCHAs, fake file sharing requests, or fake invoices, and are part of a broader phishing campaign. Phishing downloads increased in November 2021 when attackers enjoyed increased success getting them listed on popular search engines using common SEO (search engine optimization) techniques.

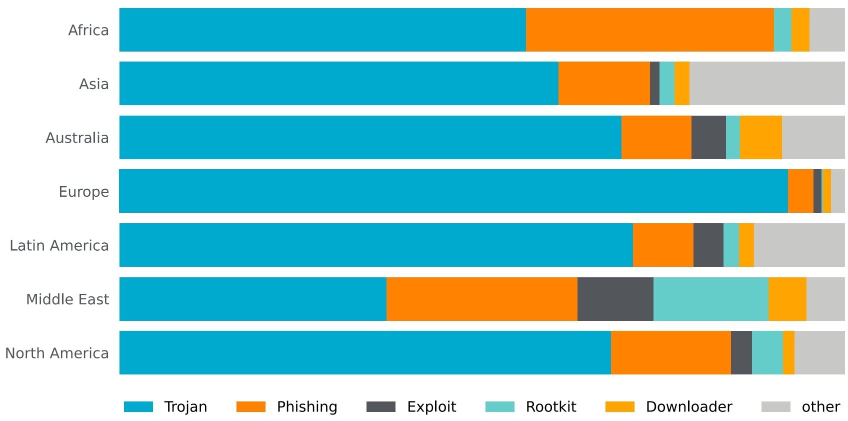
Top malware categories over the past 12 months



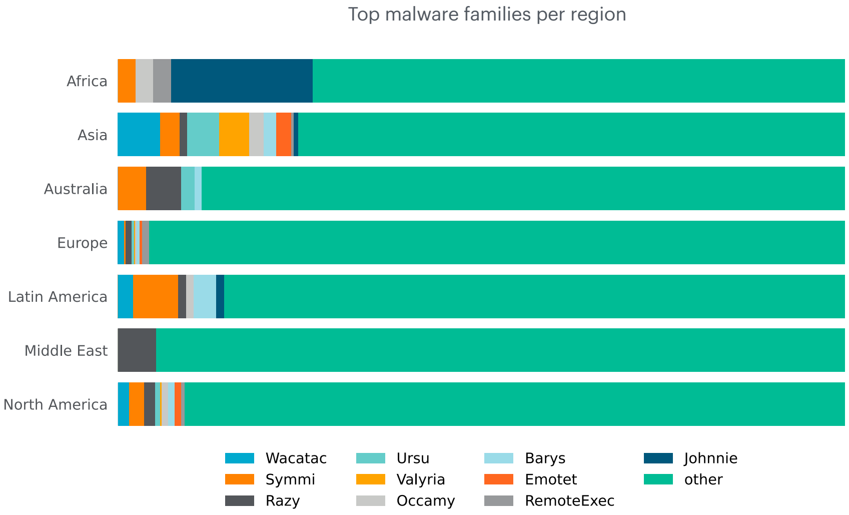
Top Trojan families over the past 12 months



Top malware categories per region



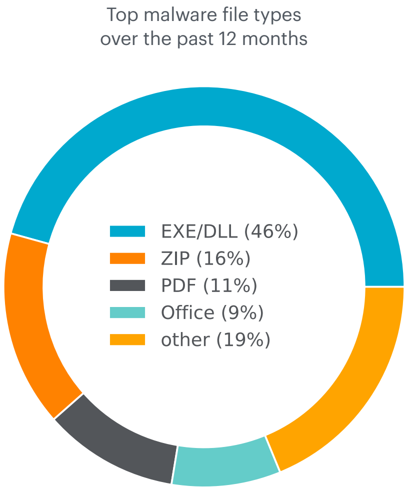
The top Trojan families vary regionally, as Trojan campaigns are typically targeted toward users speaking a specific language or living in a specific country, or are themed around significant regional events. Some Trojan families stood out as more dominant in specific regions, like Johnnie in Africa and Razy in the Middle East. Other regions like North America and Asia saw nearly all of the top families. In Europe, the top families represented a smaller percentage of all Trojan downloads than any other region.

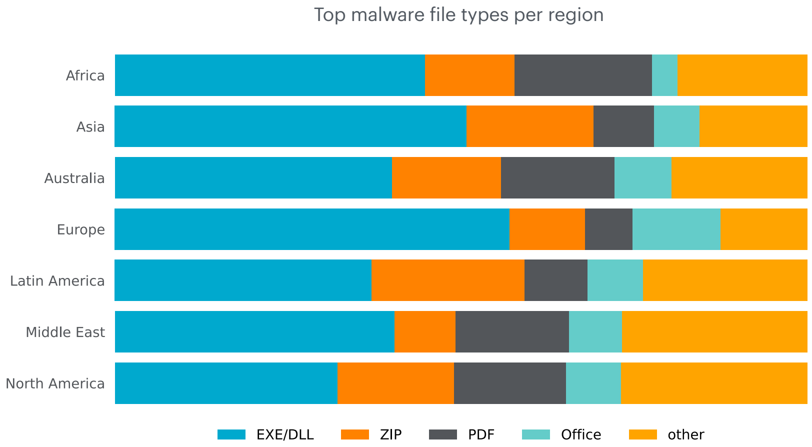


Malware File Types

Portable Executable (EXE/DLL) files, Microsoft Office files, PDF files, and ZIP files accounted for 81% of all malware downloads over the past twelve months. Malicious Office documents – which were much more dominant in 2020 and early 2021 due to Emotet and Dridex activity – returned to their previous, pre-Emotet levels. Two recent changes from Microsoft, blocking Excel 4.0 macros and blocking VBA macros for files downloaded from the internet, will likely drive that percentage down even lower, forcing attackers to pivot to alternative strategies. In addition to the phishing PDFs mentioned earlier in this report, attackers also used malicious PDFs to redirect users to spam, scam, and malware distribution sites.

Regionally, there is little variation in the relative frequencies of each file type. EXE/DLL files always represent the plurality of malware downloads, followed by either PDF, ZIP, or Office files. Africa, which had the highest percentage of phishing malware downloads, also had the highest percentage of PDF downloads, as the majority of the phishing malware downloads in Africa were PDF files.



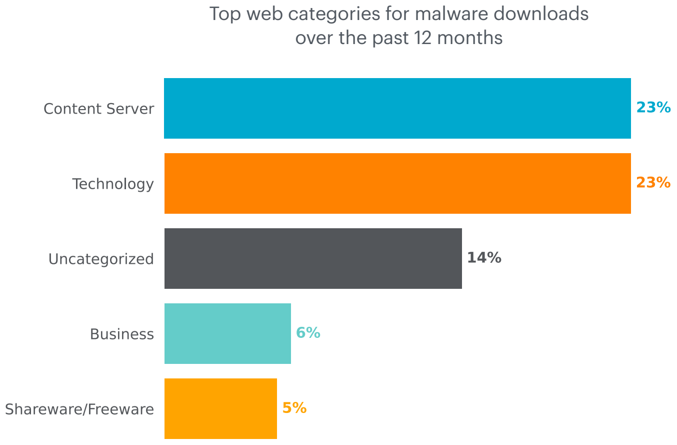


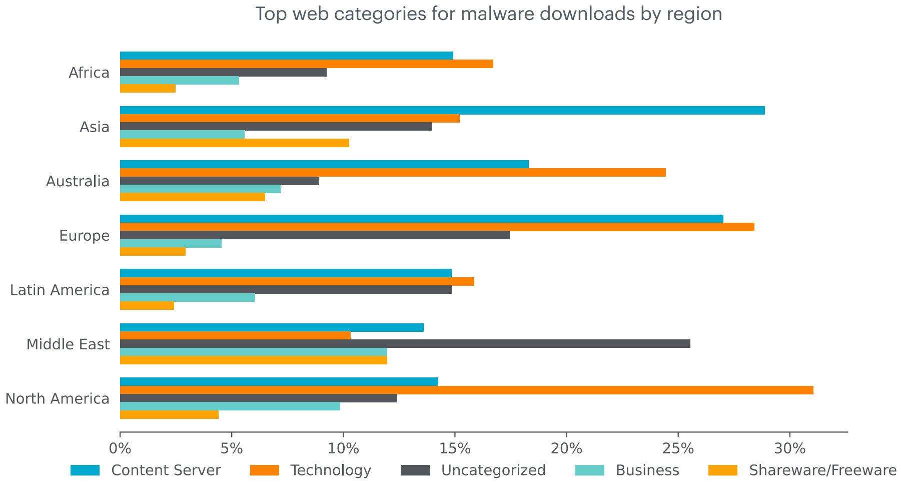
MALWARE SOURCES

Web Malware Downloads

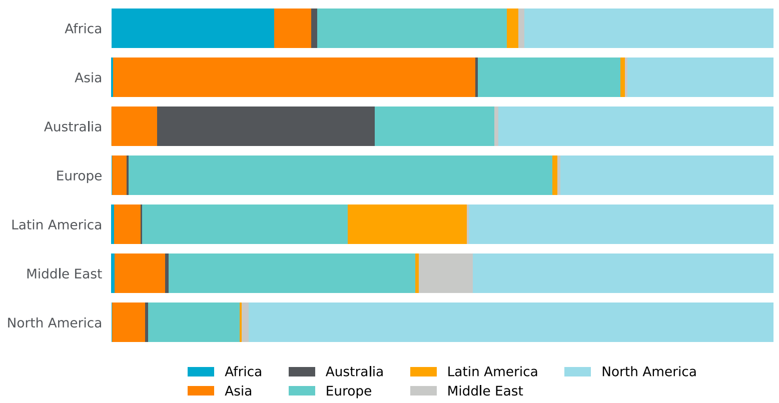
53% of all malware downloads over the past twelve months came from traditional websites compared to cloud apps. Of the web malware downloads, some originated from sites traditionally associated with malware. For example, "Uncategorized" sites–those not popular enough to have been assigned a more specific category–accounted for 14% of web malware downloads. Similarly, "Shareware/Freeware" sites sometimes distribute software bundled with spyware and other malicious software and accounted for 5% of web malware downloads. The other top categories, "Technology," "Content Server," and "Business" represent a large portion of the benign web and cannot be as easily filtered.

Regionally, we see some variation in which website categories are most popular for malware downloads. While "Technology" websites took the top spot in most regions, "Content Server" took the top spot in Asia and "Uncategorized" websites took the top spot in the Middle East. In Latin America, there was no one dominant category: the top three categories each accounted for approximately 15% of all malware downloads.





Attackers also tend to target victims located in a specific region with malware hosted within the same region. In most regions, the plurality of malware downloads originated from the same region as the victim. This is especially true for North America, where 84% of all malware downloads by victims in North America were downloaded from websites hosted in North America. At the other end of the spectrum is the Middle East, where only 7% of malware downloads originate from within the region, with many coming instead from neighboring regions Europe and Asia. On average, Europe was the source of 30% and North America was the source of 42% of all malware downloads across all regions.



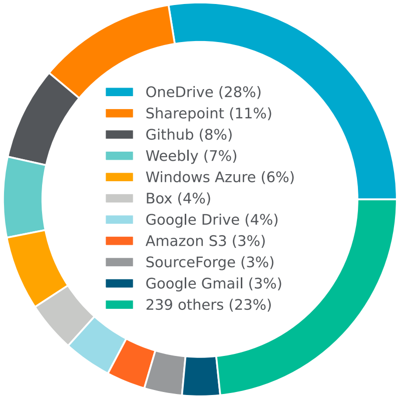
Region of origin of malware downloads

Cloud Malware Downloads

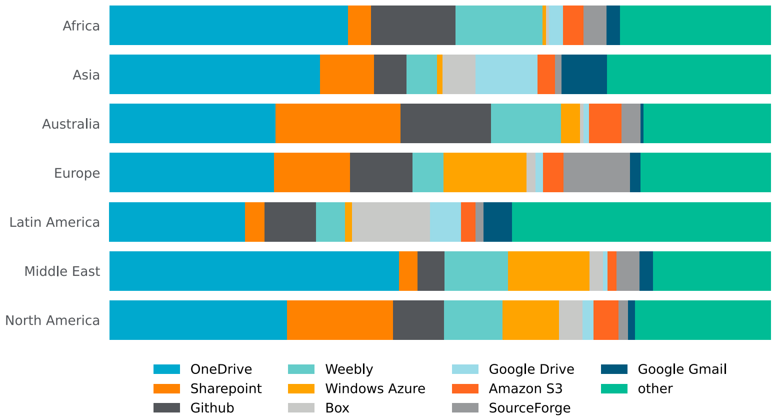
47% of all malware downloads came from cloud apps rather than traditional websites. In total, there were malware downloads from 257 different apps, with the top ten apps accounting for 75% of all cloud malware downloads. This is a reflection of both attacker activity and user behavior: attackers tend to abuse popular apps to reach more victims, and users are more likely to download malware from popular apps with which they interact regularly.

Within each region, the top ten apps accounted for the majority of all cloud malware downloads. Microsoft OneDrive was most popular in every region to varying degrees. Certain apps stood out as more common in a specific region compared to the other regions: Box in Latin America, Google Drive in Asia, and Windows Azure Blob Storage in the Middle East. This is a reflection of both attacker tactics and user behavior within each region.

Top apps for malware downloads over the past 12 months



Top apps for malware downloads by region



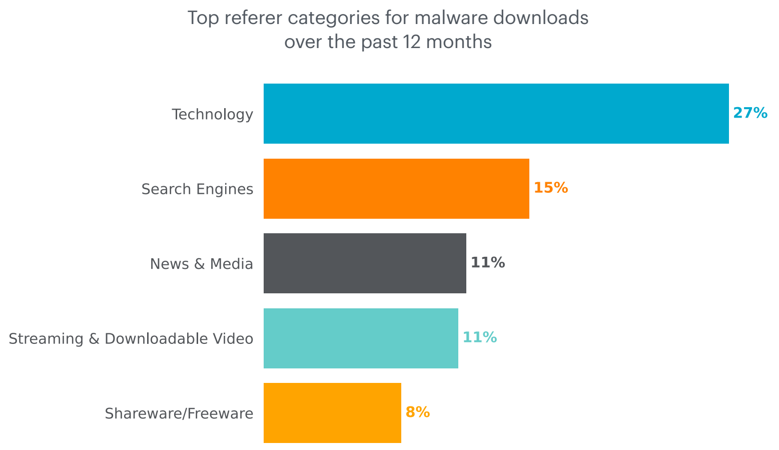
Origins of malware downloads

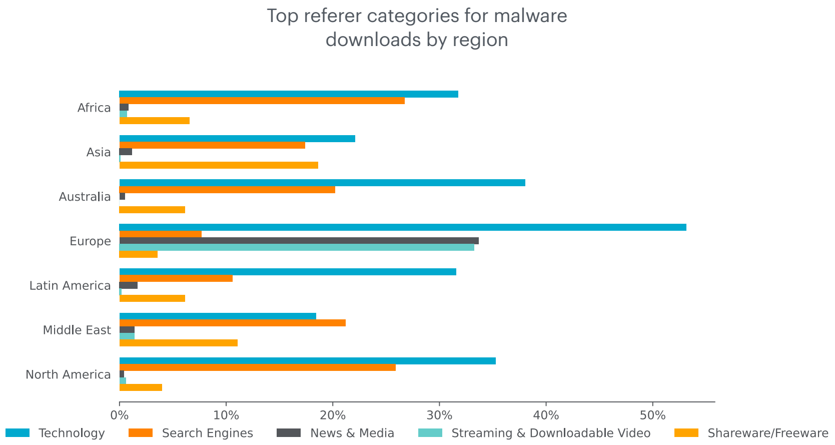
Malware downloads from the cloud or web do not just occur spontaneously. With Trojans, attackers use social engineering to trick their victims into downloading malware. Common techniques include designing lures to capitalize on major events (like the COVID-19 pandemic), creating a sense of urgency (like a shipping invoice that needs to be paid), or masquerading as a legitimate app (like a free version of a popular video game). Attackers also use technical approaches like software exploits, drive-by downloads, or HTML smuggling to download malware.

The HTTP "referer" request header provides some insight into the social engineering techniques attackers use to trick users into downloading malware. 14% of referrers were from cloud apps compared to 86% from traditional websites. The top cloud app referrers included popular cloud storage, collaboration, and webmail apps–apps where attackers can send messages directly to their victims in many different forms, including emails, direct messages, comments, and document shares.

The top web referrer categories contained some categories traditionally associated with malware, particularly "Shareware/Freeware," but were dominated by categories not traditionally associated with malware. "Search Engines" is a particularly interesting entry in this list because it provides insights into just how good some attackers have become at SEO (search engine optimization). Malware downloads referred by search engines were predominantly malicious PDF files, including many malicious fake CAPTCHAs that redirected users to phishing, spam, scam, and malware websites.

"Technology" sites led the malware referrers in all regions, but there were significant differences in other categories. Europe had the highest percentage of "News & Media" and "Streaming & Downloading Video" referrers, Africa had the highest percentage of "Search Engine" referers, and Asia has the highest percentage of "Shareware/Freeware" referers. These regional differences are a reflection of both attacker social engineering techniques attackers and user behavior.


Top referer categories for malware downloads over the past 12 months


Top referer categories for malware downloads by region

RECOMMENDATIONS

The current malware landscape is dominated by Trojans, being delivered using popular website categories and popular cloud apps, and typically delivered from within the same region as the victim. To mitigate the risk posed by cloud and web-delivered malware, Netskope recommends organizations implement the following controls:

1. Scan everything, including user traffic lanes for web, managed and unmanaged SaaS, shadow IT, IaaS, and company and personal instances. Avoid bypassing app suites with cloud storage where malware downloads are most common. Avoid category-based bypass or block, favoring a more surgical approach.

2. Deploy multi-layered, inline threat protection for all cloud and web traffic, including inline ML analysis of PE files (vs background sandboxing), to detect and block malware from making it to endpoints, plus blocking outbound malware communications.

3. Perform background malware detection using pre-execution analysis, sandboxing, ML analysis, issuing patient zero alerts for new threats, providing retrospective analysis using IOCs, and MITRE ATT&CK analysis for enhanced response mitigation.

4. Leverage Netskope Cloud Threat Exchange (CTE) to automate bi-directional threat intelligence IOC updates between defenses, manage decay of IOCs, and integrate your security stack for SSE, endpoints, email security, SIEM, XDRs, and SOAR.

5. Detect and disrupt threats by blocking risky websites, use RBI for uncategorized sites, newly registered domains, and parked domains. Use cloud firewalls (FWaaS) to filter egress traffic across all ports and protocols.

6. Reduce risk in your apps by recommending safer app alternatives, plus monitor and coach users to avoid poor and low-rated apps.

7. Federate SSO/MFA across your apps and cloud services, plus leverage zero trust network access (ZTNA) for private apps and resources. Use step-up auth in adaptive policies based on app risk, user risk, device risk, and data sensitivity to enable zero trust principles.

8. Use behavioral analysis to detect insider threats, data exfiltration, compromised devices, and compromised credentials across all lanes of user traffic inline, to private apps, and to managed apps via API introspection.

9. Automate response workflows for curated alerts using Netskope Cloud Ticket Orchestrator for investigations and response, plus use Netskope Cloud Log Shipper to send web, cloud, and firewall logs to XDRs, SIEMs, and data lakes.

10. Continuously monitor via analytics for unknown data movements, behavior anomalies, apps risks, app duplication, insider profiles, risky users, and common dashboards including your cloud risk assessment.

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

BROUGHT TO YOU BY

netskope
THREAT LABS