
netskope
Cloud und Threat Report:
Globale Trends bei Cloud- und Web-Malware
PRÄSENTIERT VON
netskope
THREAT LABS

KURZFASSUNG

In dieser Ausgabe des Cloud Threat Reports untersuchen wir Malware-Downloads aus der Cloud und dem Internet in den letzten 12 Monaten. Die überwältigende Mehrheit der Malware-Downloads entfiel auf Trojaner. Dabei nutzten Angreifer eine Vielzahl verschiedener Trojaner-Varianten und Social-Engineering-Techniken, um ihre Opfer hinters Licht zu führen. Bei der Mehrheit der Malware-Downloads handelte es sich entweder um Windows EXE/DLL-Dateien oder Microsoft Office-Dokumente, da Angreifer sich weiterhin auf das gängigste Desktop-Betriebssystem im Unternehmensumfeld konzentrieren – nämlich Microsoft Windows.

Wir untersuchen auch die Quellen der Malware-Downloads, wobei 53 % ihren Ursprung auf herkömmlichen Websites und 47 % in Cloud-Apps haben. Web-Malware-Downloads stammen aus vielen verschiedenen Website-Kategorien, allen voran von Technologie-Websites und Content-Servern. Cloud-Malware wird von Hunderten verschiedener Apps heruntergeladen, vor allem von beliebten Cloud-Storage-Apps. Sowohl Web- als auch Cloud-Malware-Downloads stammen in der Regel von Servern, die sich in derselben Region wie die Opfer befinden.

Abschließend verschaffen wir uns Einblicke in einige der Techniken, die Angreifer zur Verbreitung von Malware einsetzen, indem wir die beliebtesten Referrer von Malware-Downloads untersuchen. Zu den wichtigsten Referrern gehören Suchmaschinen, da Angreifer beliebte SEO-Techniken einsetzen, um hohe Platzierungen in Suchergebnissen zu erreichen. Kompromittierte und schädliche Websites, die das Design von gutartigen Websites imitieren, sind ebenfalls beliebte Referrer für Malware-Downloads.

ÜBERBLICK

- **Trojaner machen 77 % aller Downloads von Cloud- und Web-Malware aus.** Sie werden eingesetzt, um einen sprichwörtlichen Fuß in die Tür zu bekommen und eine Vielzahl fortschrittlicher Payloads zu verbreiten, darunter Backdoors, Infostealer und Ransomware.
- **47 % der Malware-Downloads stammen von Cloud-Apps,** 53 % von herkömmlichen Websites. Angreifer nutzen also weiterhin eine Kombination aus Cloud und Web.
- **Phishing-Downloads sind auf dem Vormarsch, angeheizt durch Angreifer, die SEO-Techniken einsetzen,** um schädliche PDF-Dateien ganz oben in den Rankings beliebter Suchmaschinen wie Google und Bing zu platzieren.
- **Bei fast der Hälfte der Malware-Downloads handelte es sich um EXE und DLL-Dateien,** da Angreifer sich weiterhin auf Microsoft Windows konzentrieren. Die Zahl der schädlichen Microsoft Office-Dateien geht hingegen zurück und hat inzwischen wieder ein ähnliches Niveau wie vor Emotet erreicht.
- **Die meisten Malware-Downloads stammen von Servern, die sich in derselben Region wie die Opfer befinden,** da Angreifer ihre Malware auf der ganzen Welt verteilen, um Geofences zu umgehen.

ÜBER DIESEN BERICHT

Netskope schützt Millionen von Nutzern weltweit vor Bedrohungen. Die in diesem Bericht dargestellten Informationen basieren auf anonymisierten Nutzungsdaten, die über die Netskope Security Cloud-Plattform mit vorheriger Genehmigung von einer Untergruppe von Netskope-Kunden erhoben wurden. Dieser Bericht enthält Informationen über Detections, die vom Netskope Next Generation Secure Web Gateway (Next Gen SWG) ausgelöst wurden, ohne die Bedeutung der Auswirkungen jeder einzelnen Bedrohung zu berücksichtigen. Die Statistiken in diesem Bericht beziehen sich auf den Zeitraum vom 1. April 2021 bis zum 31. März 2022.

Netskope Threat Labs

Netskope Threat Labs beschäftigt die branchenweit führenden Experten für Cloud-Bedrohungen und Malware. Sie spüren die neuesten Cloud- und Datenbedrohungen für Unternehmen auf, analysieren sie und entwickeln Abwehrmaßnahmen. Unsere Sicherheitsexperten sind regelmäßig als Referenten und ehrenamtliche Mitarbeiter auf den wichtigsten Sicherheitskonferenzen vertreten, darunter DefCon, BlackHat und RSA.

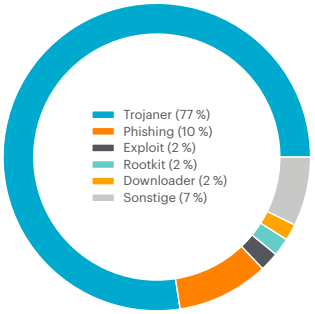
MALWARE-DOWNLOADS

Malware-Kategorien und -Varianten

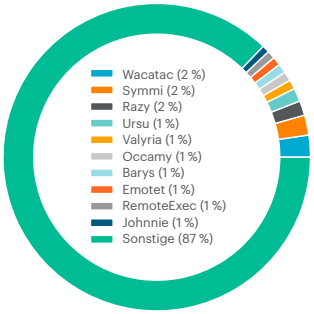
Bei der überwältigenden Mehrheit (77 %) aller Cloud- und Web-Malware-Downloads handelt es sich um Trojaner. Trojaner sind häufig die erste Stufe eines Cyberangriffs. In der Regel besteht das Ziel des Angreifers darin, das Opfer zum Download und zur Ausführung von Software zu verleiten. So bekommt der Angreifer einen ersten Fuß in die Tür. Trojaner sind oft als legitime Software getarnt und werden erst bei passender Gelegenheit aktiviert. Zum Beispiel wurde während der Pandemie eine Vielzahl von Trojanern in Umlauf gebracht, die einen Bezug zu COVID-19 herstellten. Angreifer setzen sie ein, um eine Vielzahl fortschrittlicher Payloads zu verbreiten, darunter Backdoors, Infostealer und Ransomware. Zwar handelt es sich bei der überwältigenden Mehrheit aller Cloud- und Web-Malware-Downloads um Trojaner, aber es gibt dabei keine weltweit dominante Variante. Nur 13 % aller Downloads entfallen auf die zehn wichtigsten Trojaner-Varianten. Die restlichen 87 % sind Teil eines Rattenschwanzes von weniger verbreiteten Varianten.

Trojaner machen in allen Regionen die Mehrheit der Malware-Downloads aus, mit Ausnahme des Nahen Ostens, wo die Zahl der Exploits die in den anderen Regionen übersteigt. Exploits beziehen sich in diesem Zusammenhang auf Malware-Dateien, die einen Fehler oder eine Sicherheitslücke ausnutzen, wenn sie vom Opfer geöffnet oder ausgeführt werden. Phishing-Downloads, die im Nahen Osten ebenfalls über dem Durchschnitt lagen, waren in Afrika am weitesten verbreitet. Phishing-Downloads unterscheiden sich von herkömmlichen Phishing-Websites. Es handelt sich dabei in der Regel um PDF-Dateien in Form von gefälschten CAPTCHAs, gefälschten Filesharing-Anfragen, oder gefälschten Rechnungen, die Teil einer breit angelegten Phishing-Kampagne sind. Die Zahl der Phishing-Downloads nahm im November 2021 zu, als es Angreifern mithilfe gängiger SEO-Techniken gelang, ihre Websites in gängigen Suchmaschinen zu listen.

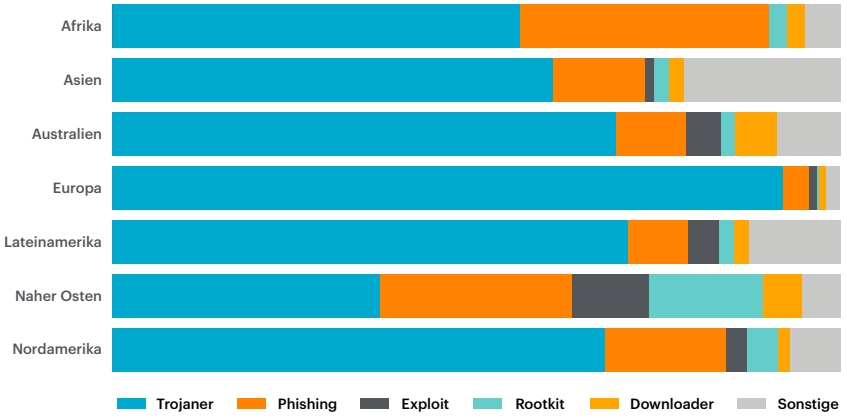
Wichtigste Malware-Kategorien der letzten 12 Monate



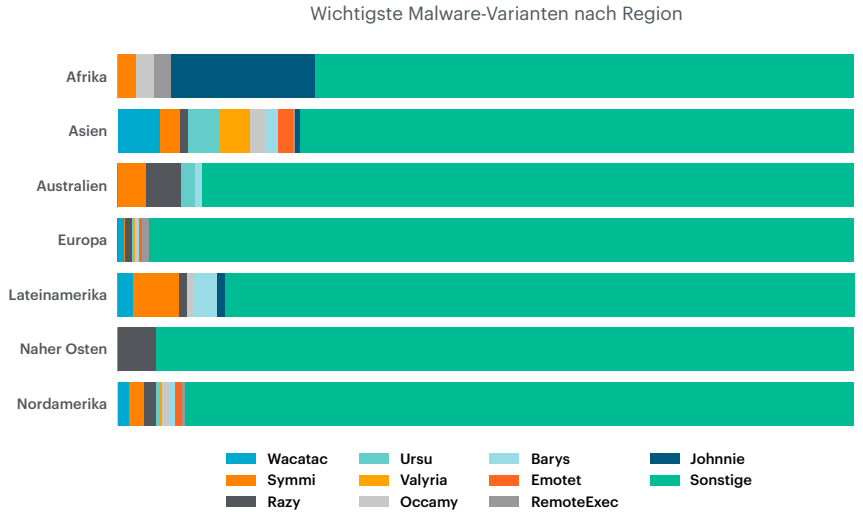
Wichtigste Trojaner-Varianten der letzten 12 Monate



Wichtigste Malware-Kategorien nach Region



Die wichtigsten Trojaner-Varianten unterscheiden sich je nach Region, da Trojaner-Angriffe in der Regel einen Bezug zu wichtigen regionalen Ereignissen haben oder auf Nutzer abzielen, die eine bestimmte Sprache sprechen oder in einem bestimmten Land leben. Einige Trojaner-Varianten waren in bestimmten Regionen besonders dominant, wie Johnnie in Afrika und Razy im Nahen Osten. In anderen Regionen wie Nordamerika und Asien waren fast alle wichtigen Varianten vertreten. In Europa machten die Top-Varianten einen geringeren Anteil aller Trojaner-Downloads aus als in jeder anderen Region.

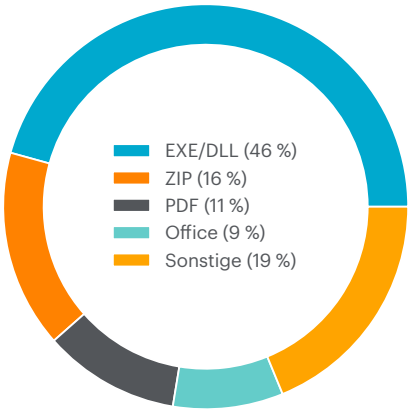


Malware-Dateitypen

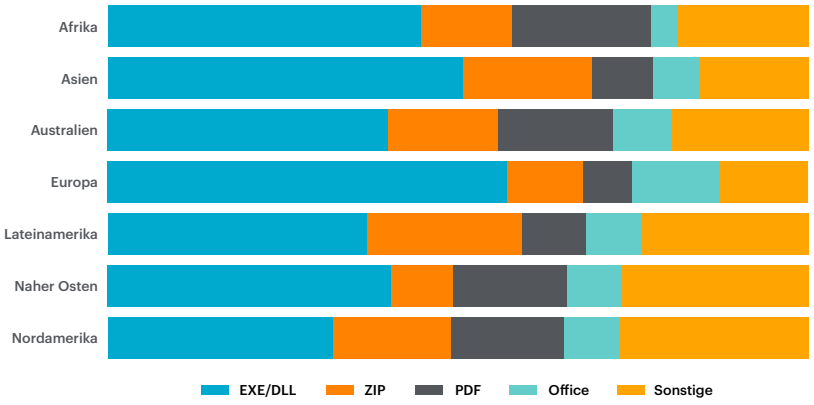
Portable ausführbare Dateien (EXE/DLL), Microsoft Office-Dateien, PDF-Dateien und ZIP-Dateien machten in den letzten zwölf Monaten 81 % aller Malware-Downloads aus. Schädliche Office-Dokumente – die 2020 und Anfang 2021 aufgrund der Emotet- und Dridex-Aktivitäten viel dominanter waren – kehrten auf ihr früheres Niveau (vor Emotet) zurück. Zwei kürzlich von Microsoft vorgenommene Änderungen – die Blockierung von Excel 4.0-Makros und die Blockierung von VBA-Makros für aus dem Internet heruntergeladene Dateien – werden diesen Prozentsatz wahrscheinlich noch weiter senken und Angreifer dazu zwingen, auf alternative Strategien auszuweichen. Neben den bereits erwähnten Phishing-PDFs nutzten Angreifer auch schädliche PDFs, um Nutzer auf Spam-, Betrugs- und Malware-Seiten umzuleiten.

Regional gibt es kaum Unterschiede in der relativen Häufigkeit der einzelnen Dateitypen. EXE/DLL-Dateien stellen in jedem Fall die meisten Malware-Downloads dar, gefolgt von PDF-, ZIP- oder Office-Dateien. Afrika, wo der Prozentsatz an Phishing-Malware-Downloads am höchsten war, verzeichnete auch den größten Anteil an PDF-Downloads, da die Mehrzahl der Phishing-Malware-Downloads in Afrika PDF-Dateien waren.

Wichtigste Malware-Dateitypen
der letzten 12 Monate



Wichtigste Malware-Dateitypen nach Region

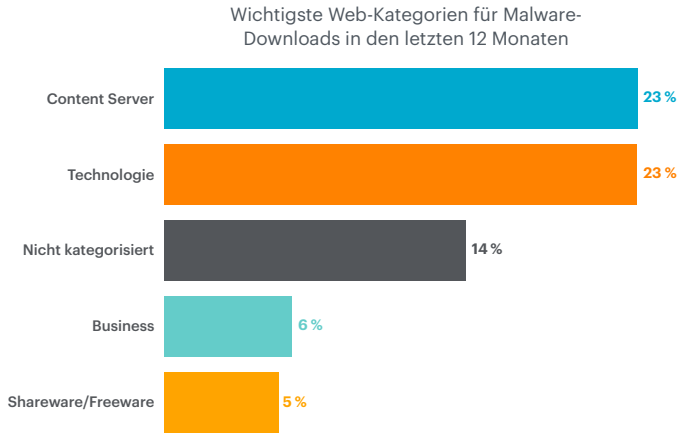


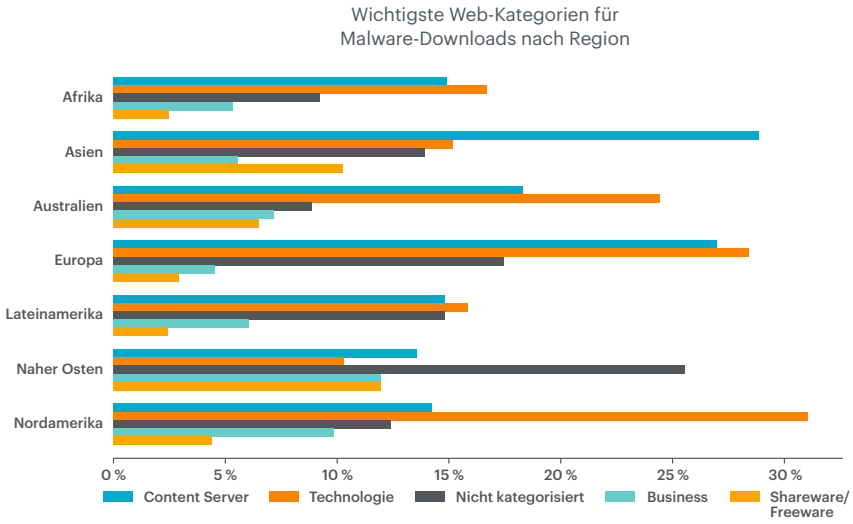
MALWARE-QUELLEN

Web-Downloads von Malware

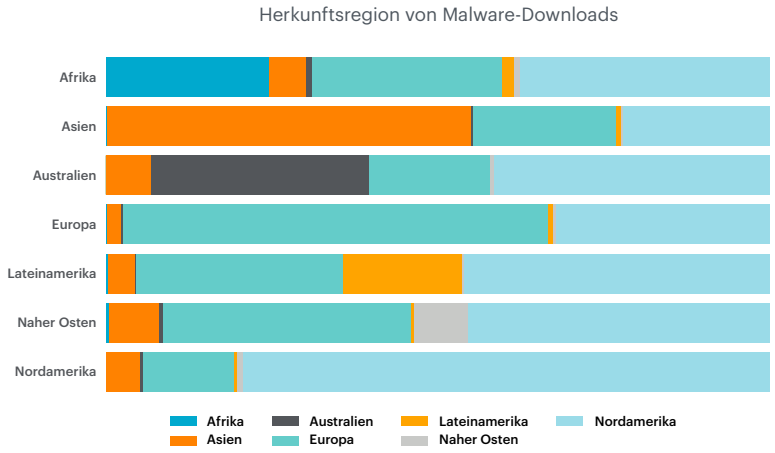
Verglichen mit Cloud-Apps stammten 53 % aller Malware-Downloads in den letzten zwölf Monaten von herkömmlichen Websites. Einige der Web-Downloads von Malware gingen von Websites aus, die traditionell mit Malware in Verbindung gebracht werden. So entfielen beispielsweise 14 % der Web-Downloads von Malware auf „nicht kategorisierte“ Websites – also Websites, die nicht populär genug sind, um einer spezifischeren Kategorie zugeordnet zu werden. Ähnlich verhält es sich mit „Shareware/Freeware“-Websites, auf denen manchmal Software gebündelt mit Spyware und anderer schädlicher Software verbreitet wird. Sie machten 5 % der Malware-Downloads im Internet aus. Die anderen Top-Kategorien „Technologie“, „Contentserver“ und „Business“ repräsentieren einen großen Teil des gutartigen Webs und können nicht so leicht gefiltert werden.

In den einzelnen Regionen gibt es einige Unterschiede bei den Website-Kategorien, in denen die meisten Malware-Downloads vorkommen. In den meisten Regionen lagen „Technologie“-Websites auf dem ersten Platz. In Asien hingegen waren Websites der Kategorie „Content Server“ und im Nahen Osten „nicht kategorisierte“ Websites an erster Stelle. In Lateinamerika gab es keine dominierende Kategorie: Die drei wichtigsten Kategorien machten jeweils etwa 15 % aller Malware-Downloads aus.





Angreifer neigen auch dazu, Opfer in einer bestimmten Region mit Malware anzugreifen, die in derselben Region gehostet wird. In den meisten Regionen stammt die Mehrzahl der Malware-Downloads aus derselben Region wie das Opfer. Dies gilt insbesondere für Nordamerika. Hier wurden 84 % aller Malware-Downloads von Opfern in Nordamerika von Websites heruntergeladen, die in dieser Region gehostet werden. Am anderen Ende des Spektrums steht der Nahe Osten, wo nur 7 % der Malware-Downloads aus der eigenen Region stammen. Viele kommen stattdessen aus den Nachbarregionen Europa und Asien. Im Durchschnitt wurden in Europa 30 % und in Nordamerika 42 % aller Malware-Downloads getätigt.

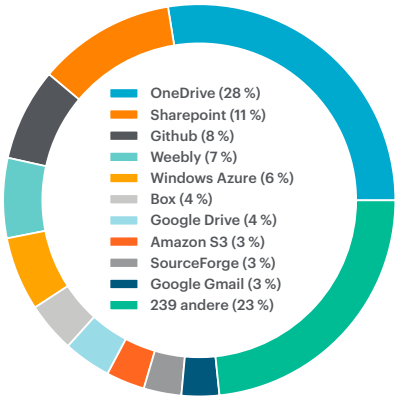


Cloud-Malware-Downloads

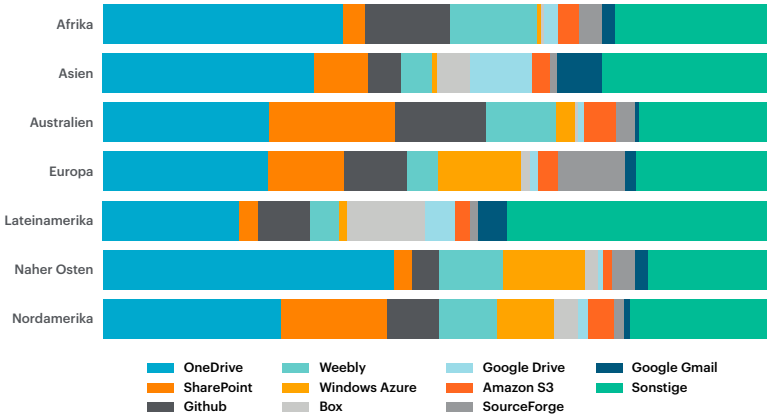
47 % aller Malware-Downloads stammen von Cloud-Apps und nicht von herkömmlichen Websites. Insgesamt gab es Malware-Downloads von 257 verschiedenen Apps. Dabei machten die zehn wichtigsten Apps 75 % aller Cloud-Malware-Downloads aus. Dies spiegelt sowohl die Aktivitäten der Angreifer als auch das Verhalten der Nutzer wider: Angreifer neigen dazu, beliebte Apps zu missbrauchen, um mehr Opfer zu erreichen. Nutzer laden wiederum Malware eher von bekannten Apps herunter, mit denen sie regelmäßig interagieren.

Innerhalb jeder Region entfiel die Mehrheit aller Cloud-Malware-Downloads auf zehn Apps. Microsoft OneDrive wurde in allen Regionen am häufigsten verwendet, wobei sich der Verwendungsgrad je nach Region unterschied. Einige Apps waren in einer bestimmten Region häufiger betroffen als in den anderen Regionen: Box in Lateinamerika, Google Drive in Asien und Windows Azure Blob Storage im Nahen Osten. Dies spiegelt sowohl die Taktiken der Angreifer als auch das Verhalten der Nutzer in der jeweiligen Region wider.

Wichtigste Apps für Malware-Downloads
in den letzten 12 Monaten



Wichtigste Apps für Malware-Downloads nach Region



Ursprung von Malware-Downloads

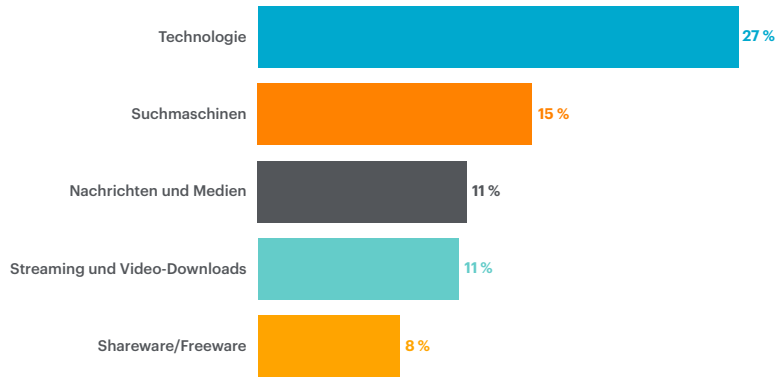
Malware-Downloads aus der Cloud oder dem Internet geschehen nicht einfach spontan. Bei Trojanern nutzen die Angreifer Social Engineering, um ihre Opfer zum Herunterladen von Malware zu verleiten. Zu den gängigsten Techniken der Angreifer gehört, dass sie sich auf bedeutende Ereignisse beziehen (wie die COVID-19-Pandemie), ein Gefühl der Dringlichkeit erzeugen(wie eine unbezahlte Rechnung) oder sich als legitime App tarnen (wie eine kostenlose Version eines Videospiels). Angreifer verwenden auch technische Mittel wie Software-Exploits, Drive-by-Downloads oder HTML Smuggling, um Malware herunterzuladen.

Der Header der HTTP-Referrer-Anfrage bietet Einblicke in die Social-Engineering-Techniken, mit denen Angreifer Nutzer zum Herunterladen von Malware verleiten. 14 % der Referrer kamen von Cloud-Apps, 86 % von traditionellen Websites. Zu den wichtigsten Referrern in Cloud-Apps gehörten beliebte Cloud-Speicher-Apps, Apps für die Zusammenarbeit und Webmail-Apps – also Apps, mit denen Angreifer ihren Opfern direkt Nachrichten in vielen verschiedenen Formen senden können, darunter E-Mails, Direktnachrichten, Kommentare und freigegebene Dokumente.

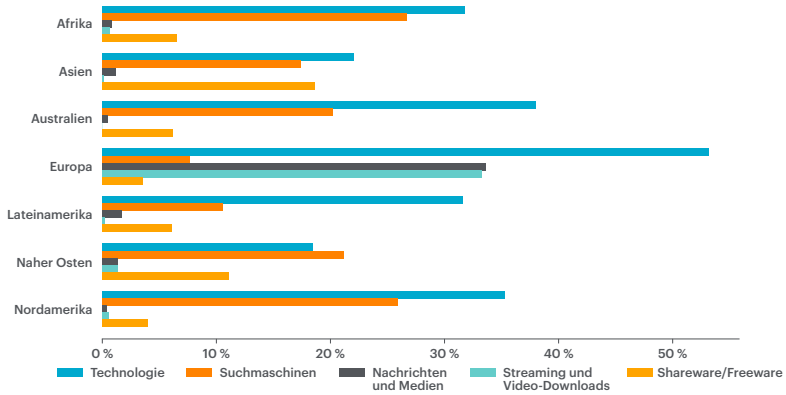
Die führenden Web-Referrer-Kategorien enthielten einige Kategorien, die traditionell mit Malware in Verbindung gebracht werden, insbesondere „Shareware/Freeware“, wurden aber von Kategorien dominiert, die traditionell nicht mit Malware in Verbindung gebracht werden. „Suchmaschinen“ ist ein besonders interessanter Eintrag in dieser Liste, denn er gibt Aufschluss darüber, wie gut einige Angreifer in Sachen Suchmaschinenoptimierung geworden sind. Bei den Malware-Downloads, die über Suchmaschinen vermittelt wurden, handelte es sich überwiegend um schädliche PDF-Dateien, darunter viele gefälschte CAPTCHAs, die Nutzer auf Phishing-, Spam-, Betrugs- und Malware-Websites umleiteten.

„Technologie“-Websites waren in allen Regionen führende Malware-Referrer, aber in bestimmten Kategorien gab es erhebliche Unterschiede. In Europa entfiel der höchste Prozentsatz auf „Nachrichten und Medien“ sowie „Streaming und Video-Downloads“, in Afrika auf „Suchmaschinen“ und in Asien auf „Shareware/Freeware“. Diese regionalen Unterschiede spiegeln sowohl die Social-Engineering-Techniken der Angreifer als auch das Verhalten der Nutzer wider.

Wichtigste Referrer-Kategorien für
Malware-Downloads in den letzten 12 Monaten



Wichtigste Referrer-Kategorien für
Malware-Downloads nach Region



EMPFEHLUNGEN

Die derzeitige Malware-Landschaft wird von Trojanern dominiert, die über beliebte Website-Kategorien und Cloud-Apps verbreitet werden und in der Regel aus derselben Region wie das Opfer stammen. Um das Risiko von Cloud- und Web-Malware zu minimieren, empfiehlt Netskope Unternehmen, folgende Maßnahmen zu ergreifen:

1. Scannen Sie alles, einschließlich Nutzer-Traffic im Web, verwaltete und nicht verwaltete SaaS, Schatten-IT, IaaS sowie geschäftliche und private Instanzen. Vermeiden Sie die Umgehung von App-Suiten mit Cloud-Speicher, wo Malware-Downloads am häufigsten vorkommen. Vermeiden Sie kategoriebasierte Umgehungen oder Sperren und konzentrieren Sie sich auf einen eher chirurgischen Ansatz.

2. Stellen Sie einen mehrschichtigen Inline-Bedrohungsschutz für den gesamten Cloud- und Web-Traffic bereit, einschließlich einer Inline-ML-Analyse von PE-Dateien (im Gegensatz zu Sandboxing im Hintergrund), um Malware aufzuspüren und zu blockieren, bevor sie die Endpunkte erreichen kann. Blockieren Sie außerdem die ausgehende Malware-Kommunikation.

3. Führen Sie die Malware-Erkennung im Hintergrund aus und nutzen Sie dabei Analysen im Vorfeld der Ausführung, Sandboxing, ML-Analysen, Patient-Zero-Alerts für neue Bedrohungen, retrospektive Analysen über IOCs und MITRE ATT&CK-Analysen für bessere Abhilfemaßnahmen.

4. Nutzen Sie Netskope Cloud Threat Exchange (CTE), um bidirektionale Threat Intelligence IOC-Updates zwischen Verteidigungssystemen zu automatisieren, den Verfall von IOCs zu verwalten und Ihren Sicherheits-Stack für SSE, Endpunkte, E-Mail-Sicherheit, SIEM, XDRs und SOAR zu integrieren.

5. Erkennen und stören Sie Bedrohungen, indem Sie riskante Websites blockieren und verwenden Sie RBI für nicht kategorisierte Websites, neu registrierte Domains und geparkte Domains. Verwenden Sie Cloud-Firewalls (FWaaS), um den ausgehenden Traffic über alle Ports und Protokolle hinweg zu filtern.

6. Verringern Sie das Risiko in Ihren Apps, indem Sie sicherere App-Alternativen empfehlen. Überwachen Sie Nutzer und erklären Sie ihnen, wie sie mangelhaften und schlecht bewerteten Apps aus dem Weg gehen können.

7. Verbinden Sie SSO/MFA über Ihre Anwendungen und Cloud-Dienste hinweg und nutzen Sie Zero Trust Network Access (ZTNA) für private Anwendungen und Ressourcen. Verwenden Sie Step-up-Authentifizierung in adaptiven Richtlinien auf der Grundlage von App-Risiko, Nutzer-Risiko, Geräte-Risiko und Datensensibilität, um Zero-Trust-Prinzipien zu ermöglichen.

8. Nutzen Sie die Verhaltensanalyse, um Insider-Bedrohungen, Datenexfiltration, kompromittierte Geräte und Anmeldeinformationen direkt im Nutzer-Traffic zu privaten Anwendungen und über API-Introspektion im Traffic zu verwalteten Anwendungen zu erkennen.

9. Automatisieren Sie Untersuchungs- und Reaktions-Workflows für festgelegte Alarme mit dem Netskope Cloud Ticket Orchestrator und verwenden Sie den Netskope Cloud Log Shipper, um Web-, Cloud- und Firewall-Protokolle an XDRs, SIEMs und Data Lakes zu senden.

10. Überwachen Sie mithilfe von Analysen kontinuierlich unbekannte Datenbewegungen, Verhaltensanomalien, App-Risiken, App-Duplizierung, Insider-Profile, riskante Nutzer und allgemeine Dashboards einschließlich Ihrer Cloud-Risikobewertung.

WEITERE INFORMATIONEN

Weitere Informationen zu cloudbasierten Bedrohungen und den neuesten Erkenntnissen der Netskope Threat Labs finden Sie unter:
NETSKOPE.COM/NETSKOPE-THREAT-LABS

Wenn Sie mehr zum Thema Risikoreduzierung erfahren möchten, kontaktieren Sie uns unter:
WWW.NETSKOPE.COM/REQUEST-DEMO

PRÄSENTIERT VON

netskope
THREAT LABS