
cp<r>
CHECK POINT RESEARCH
TRENDS BEI CYBER-ANGRIFFEN:
HALBJAHRESBERICHT
2020
Check Point
SOFTWARE TECHNOLOGIES LTD

# Inhaltsverzeichnis

Zusammenfassung ..... 3

Die Welt unter COVID-19 ..... 4

Doppelte Erpressung ..... 6

Cyber-Kriegsführung während einer Pandemie ..... 7

Mobile Trends – Neue Infektionsvektoren suchen ..... 8

Cloud-Bedrohungen ..... 9

Cyber-Angriffskategorien nach Region ..... 10

Globale Bedrohungsindexkarte ..... 10

Die bösartigsten Dateitypen (H1 2020) ..... 11

Globale Malware-Statistiken ..... 12

- Top Malware-Familien ..... 12
- Top Cryptomining-Malware ..... 14
- Top Mobile-Malware ..... 15
- Top Botnets ..... 16
- Top Infostealer ..... 17
- Top Banken-Trojaner ..... 18

Wichtige globale Schwachstellen ..... 19

Wichtige Cyber-Angriffe (H1 2020) ..... 20

Anhang – Beschreibung von Malware-Familien ..... 24

# Zusammenfassung

In den vergangenen sechs Monaten hat sich die Art und Weise, wie wir leben und arbeiten, bis zur Unkenntlichkeit verändert. Einfach gesagt: Das Leben auf der Erde ist online gegangen. Der Wandel fand nicht schrittweise, sondern scheinbar über Nacht statt. Fast alles hat sich verändert, die Art und Weise, wie wir Beziehungen pflegen, arbeiten oder sogar unsere Einkäufe erledigen. Veränderungen in derselben Größenordnung sind auch im Cyber-Bereich zu finden.

Die neue Normalität hat neben Chancen auch Herausforderungen geschaffen. Die von Unternehmen vorgenommenen Änderungen der Infrastruktur, um den Fernzugriff zu ermöglichen, erforderten auch von den Bedrohungsakteuren, sich an eine hybride Welt mit integrierten Cloud-Technologien anzupassen. Darüber hinaus haben die rasche Ausbreitung des Coronavirus und die weltweiten Forschungsaktivitäten zur Suche nach einem Impfstoff neue Phishing-Optionen geschaffen und medizinische Forschungseinrichtungen zu einem begehrten Ziel für kriminelle und staatliche Akteure gemacht.

Wir werden uns mit diesen Auswirkungen und weiteren Aspekten der Bedrohungslandschaft befassen und gleichzeitig Beispiele und Statistiken von Ereignissen aus der realen Welt bereitstellen.

Hier sind einige der Trends bei Cyber-Angriffen, die wir behandeln:

## Doppelte Erpressung

Die Ransomware-Akteure haben sich eine neue Strategie zu eigen gemacht: Sie machen nicht nur die Dateien des Opfers unzugänglich, sondern exfiltrieren jetzt auch große Datenmengen, bevor sie diese in der Endphase des Angriffs verschlüsseln. Opfer, die sich weigern, Zahlungsaufforderungen nachzukommen, finden ihre sensibelsten Daten auf speziellen Websites veröffentlicht.

## Cyber-Kriegsführung

Cyber-Aktivitäten auf nationaler Ebene verzeichnen eine zunehmende Intensität, während der Schweregrad eskaliert. In Zeiten, in denen traditionelle Taktiken zum Sammeln von Informationen und Wissen aufgrund der sozialen Distanzierung nicht mehr möglich sind, scheint der Einsatz offensiver Cyberwaffen zur Unterstützung nationaler Missionen zugenommen zu haben. Das Ziel kann ein besseres Verständnis für das Coronavirus oder die Sicherung von Geheimdienstoperationen sein, wobei Länder und Industriebranchen anvisiert werden.

## Mobil

Bedrohungsakteure haben nach neuen Infektionsvektoren in der mobilen Welt gesucht und ihre Techniken verändert und verbessert, um eine Enttarnung an Orten wie den offiziellen App-Stores zu vermeiden. Bei einem innovativen Angriff nutzten Bedrohungsakteure das Mobile Device Management (MDM)-System eines internationalen Großkonzerns, um Malware an mehr als 75 % der verwalteten Mobilgeräte zu verteilen.

## Cloud

Zur Sicherung ihrer Produktion bei der Fernarbeit waren Branchen gezwungen, ihre Infrastruktur rasch anzupassen. In vielen Fällen wäre dies ohne Cloud-Technologien nicht möglich gewesen. Allerdings wurden dadurch auch mehr falsch konfigurierte oder einfach ungeschützte Unternehmensdaten dem Internet ausgesetzt. Darüber hinaus wurden zum ersten Mal alarmierende Schwachstellen in der Microsoft Azure-Infrastruktur aufgedeckt, die es Angreifern ermöglichen könnten, der VM-Infrastruktur zu entkommen und andere Kunden zu gefährden.

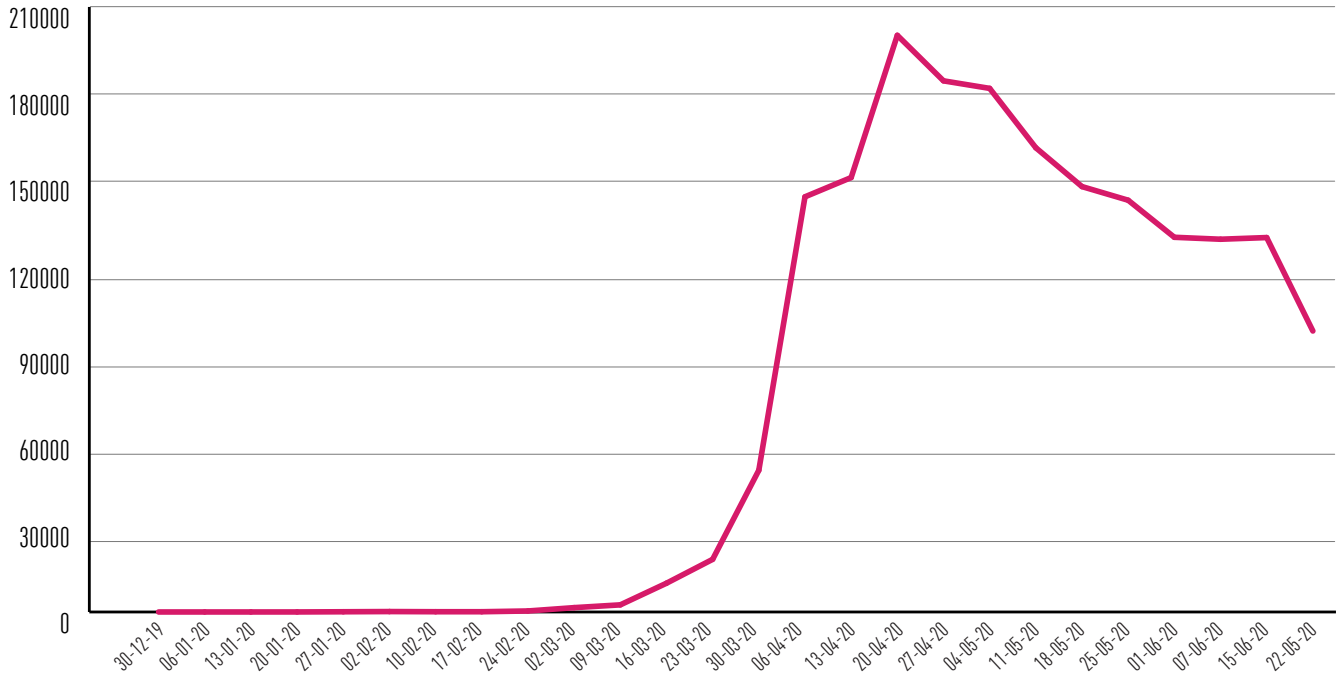
# Die Welt unter COVID-19

Die COVID-19-Pandemie hatte dramatische Auswirkungen auf praktisch jeden Aspekt des Lebens und war zweifellos das einflussreichste Ereignis im H1 2020. Auch im Cyber-Bereich führte dies zu erheblichen Auswirkungen. Eine Vielzahl von Akteuren mit unterschiedlichen Beweggründen – kriminell, politisch oder als Spionagearbeit – nutzten die Angst vor COVID-19 und verwandte Themen, um eine ganz neue Gruppe von Opfern ins Visier zu nehmen.

Die erste Folge der Pandemie war die Verbreitung von Malware-Angriffen, bei denen Social-Engineering-Techniken mit thematischen COVID-19-Ködern für die Übergabephase eingesetzt wurden. Bereits Anfang Januar berichteten wir, dass Emotet Dokumente mit Coronavirus-bezogenen Inhalten, die auf japanische Benutzer abzielen, als Waffe eingesetzt hat.

Es wurden tausende von Domainnamen im Zusammenhang mit dem Coronavirus registriert, von denen viele später für verschiedene Betrügereien verwendet werden sollten. Einige wurden verwendet, um gefälschte COVID-19-Impfungen oder Medikamente zu verkaufen, andere für verschiedene Phishing- Kampagnen und für die Verbreitung bösartiger mobiler Anwendungen. Ähnlich wie an Feiertagen und bei Verkaufsveranstaltungen boten die Betrüger Waren mit „speziellen Coronavirus-Rabatten“ an. Hacker boten sogar Malware-as-a-Service zu Sonderpreisen an.

## Wöchentliche Coronavirus-bezogene Cyber-Angriffe




Die Grafik stellt alle Coronavirus-bezogenen Angriffe dar, die von den Threat Prevention-Technologien von Check Point über Netzwerke, Endpunkte und Mobilgeräte hinweg erkannt wurden

Nicht nur finanziell motivierte Gruppen nutzten die Situation aus, in China ansässige APT-Gruppen verfassten Corona-bezogene Inhalte und verwendeten sie in böswilligen RTF-Dokumenten für eine gegen mongolische öffentliche Einrichtungen gerichtete Kampagne. Einige schätzen, dass der Rückgang der traditionellen Spionageaktivitäten, welche durch Reisebeschränkungen und soziale Distanzierung erschwert wurde, durch verstärkte Aktivitäten im Online-Bereich kompensiert wurde. Der Europäische Auswärtige Dienst (EAD) berichtete von verstärkten absichtlich koordinierten Desinformationsaktivitäten, die häufig von staatlichen oder staatlich geförderten Akteuren durchgeführt werden, die falsche Gesundheitsinformationen fördern, sowie von weiteren Bemühungen, die Schuld für den Ausbruch der Pandemie von sich zu weisen.

Mit der Entwicklung der Pandemie und der Umsetzung einer Politik der sozialen Distanzierung passte sich ein beträchtlicher Teil der Unternehmen an die Maßnahmen zur Fernarbeit an, wodurch private und öffentliche Einrichtungen zusätzlichen Angriffsflächen ausgesetzt wurden. Videokommunikations-Plattformen wurden zur Zielscheibe von Hackern, um Videositzungen zu infiltrieren, während andere Bedrohungsakteure gefälschte Domains registrierten und bösartige Apps verbreiteten, die sich als Zoom, Microsoft Teams und andere Webkonferenz-Websites darstellten. Mit der zunehmenden Nutzung von Fernzugriffstechnologien wie RDP und VPN war auch ein starker Anstieg von RDP Brute Force-Angriffen zu verzeichnen.

Der Gesundheitssektor steht unter extremem Druck, Patienten zu behandeln und einen Impfstoff sowie Medikamente zu entwickeln, die gegen das Virus wirksam sind. Trotz des Versprechens, auf Angriffe auf Organisationen im Gesundheitswesens zu verzichten, setzten Betreiber von Ransomware wie Maze ihre Angriffe mit Lösegeldforderungen fort, da sie erkannten, dass ihre Opfer in einer schlechten Verhandlungsposition sein würden. Andere Kampagnen gaben sich als pharmazeutische Organisationen aus und versuchten Ransomware, die speziell auf den Gesundheitssektor abzielte, in Italien zu verbreiten. Die WHO (Weltgesundheitsorganisation) berichtete über einen dramatischen Anstieg von Cyber-Angriffen auf ihre Mitarbeiter und Systeme.

Eine andere Art von Angriffen nutzte den weltweiten wirtschaftlichen Stress aufgrund von Lockdowns und Geschäftsschließungen aus, wobei Unternehmen und Staaten in großem Umfang betrogen wurden. Gestohlene PII (persönlich identifizierbare Informationen) wurden verwendet, um betrügerische Anträge auf Arbeitslosenunterstützung einzureichen. Unternehmen, die nach Notfall-Transaktionsgenehmigungsverfahren arbeiten, wurden Opfer von BEC-Angriffen (Business Email Compromise). Europol berichtete, dass ein französisches Pharmaunternehmen 7,25 Millionen Dollar für den Kauf von Handdesinfektionsmitteln und Schutzmasken an einen gefälschten Lieferanten überwiesen hat.

Der Coronavirus-Ausbruch hat mehrere Cyber-Sicherheitstrends verstärkt, die die Pandemie überdauern könnten. Viele Länder setzten Notstandsregelungen durch und aktivierten spezielle, zum Teil obligatorische Nachverfolgungssysteme, die zur Bekämpfung des Ausbruchs entwickelt wurden. Die indische Kontaktverfolgungs-App „Aarogya Setu"-zum Beispiel hatte mehr als 100 Millionen Downloads, und ihre Popularität wirft Fragen des Datenschutzes und der Sicherheit auf. Jedes dieser Systeme muss ein ausgewogenes Verhältnis zwischen Privatsphäre und Sicherheit wahren; eine schlechte Umsetzung der Sicherheitsstandards kann die Daten der Nutzer gefährden. Die Stadt Hangzhou in China hat bereits ihre Absicht angekündigt, ihre App dauerhaft weiter zu nutzen. Forscher warnen davor, dass Maßnahmen, die zum Schutz und zur Überwachung der Bürger unter außergewöhnlichen Umständen ergriffen werden, die gegenwärtige Krise überdauern könnten.

Es ist noch nicht abzusehen, wann die COVID-19-Pandemie vorbei sein wird. Einige sagen, dass die Auswirkungen dauerhaft sein werden und wir uns an die „neue Normalität" in einer Welt nach COVID-19 anpassen müssen. Diese neue Welt verlangt nach entsprechenden neuen Cyber-Schutzmaßnahmen.

# Doppelte Erpressung

Der jüngste Trend bei Ransomware-Angriffen kombiniert die Verschlüsselung von Dateien des Opfers mit der Drohung, gestohlene vertrauliche Informationen zu veröffentlichen, wenn die Lösegeldforderungen nicht erfüllt werden. Dieser Trend wird inzwischen von den meisten großen Ransomware-Cyber-Akteuren genutzt und macht potenziell jeden Ransomware-Angriff zu einer Verletzung des Datenschutzes. Die Zahlung des Lösegeldes garantiert nicht mehr das Ende des Angriffs, da die Opfer nie sicher sein können, dass die gestohlenen Informationen tatsächlich gelöscht wurden.

Seit ihrem Aufkommen im Jahr 1989 haben sich Ransomware-Angriffe von der massenhaften Verbreitung von Malware per E-Mail zu einem präzisen Vorgehen gegen sorgfältig ausgewählte Opfer entwickelt. Anfänglich stützten sich die Angriffe auf die Beteiligung der Benutzer (wie das Klicken auf einen Link oder das Öffnen eines Anhangs), um den Rechner eines Opfers zu infizieren. Spätere Angriffe wurden jedoch mit „Drive-by"-Methoden durchgeführt, bei denen wurmartige Verbreitungsmethoden oder vorhandene Bot-Netze genutzt wurden, um die Malware als Nutzlast auszuliefern.

Die Opfer erleiden einen doppelten Schlag: Die Angreifer verhindern den Zugriff auf ihre Dateien und Daten, indem sie diese verschlüsseln, wobei jedoch vor der Verschlüsselung ein Teil der Informationen exfiltriert wird. Wenn das Lösegeld nicht bezahlt wird, können sensible Daten öffentlich zugänglich gemacht werden, während gleichzeitig kritische Unternehmenssysteme lahmgelegt bleiben und den regulären Betrieb stören.

Der erste veröffentlichte Fall einer doppelten Erpressung ereignete sich im November 2019, als Allied Universal, ein großes amerikanisches Unternehmen für Sicherheitspersonal, von Maze-Ransomware getroffen wurde und sich weigerte, ein Lösegeld von 300 Bitcoins zu zahlen. Die Angreifer reagierten darauf mit der Veröffentlichung sensibler Informationen, die aus den Systemen von Allied Universal extrahiert wurden, darunter Verträge, medizinische Aufzeichnungen, Verschlüsselungszertifikate und mehr. TA2101, die Gruppe hinter der Maze-Ransomware, hat inzwischen eine eigene Webseite eingerichtet, die die Identitäten nicht kooperativer Opfer auflistet und regelmäßig Proben gestohlener Daten veröffentlicht. Sie haben die Details von Dutzenden von Unternehmen, Anwaltskanzleien, medizinischen Dienstleistern und Versicherungsgesellschaften veröffentlicht.

Andere Gruppen von Cyberkriminellen, darunter Sodinokibi (alias REvil), Clop, Nemty und DopplelPaymer, folgten diesem Beispiel. Die auf ihren Seiten veröffentlichten Informationen wurden bald von Ransomware-Gruppen oder anderen Kriminellen, die die Daten von den Abladeplätzen sammelten, zum Verkauf angeboten.

Traditionelle Ransomware-Angriffe, so bösartig sie auch sind, geben den Opfern die Möglichkeit, alles aus Backups zurückzuholen oder sich kriminellen Forderungen zu ergeben und Lösegeld zu zahlen, in der Hoffnung, Entschlüsselungsschlüssel zu erhalten.

Datendiebstahl hingegen gefährdet ihre Opfer durch den Verlust proprietärer Informationen und behindert ihre Fähigkeit, die personenbezogenen Daten von Kunden und Mitarbeitern zu schützen. Rechtsvorschriften wie die DSGVO der Europäischen Union und die Gesetze zur Meldung von Sicherheitsverstößen in den USA schreiben vor, dass die Opfer solcher Angriffe die Details des Angriffs sowohl den benannten Behörden als auch den Unternehmen und Einzelpersonen offenlegen müssen, zu denen die Informationen gehören. Dies erhöht den Schaden durch zusätzliche Kosten, die für den Schutz von Mitarbeitern und Kunden vor Betrug und Identitätsdiebstahl sowie für die mögliche Anfälligkeit für Klagen erforderlich sind.

# Cyber-Kriegsführung während einer Pandemie

Die COVID-19-Pandemie hat den zwischenstaatlichen Cyber-Bereich dramatisch umgestaltet. Sie forderte geheimdienstliche Einrichtungen heraus, definierte Ziele neu und schuf neue Möglichkeiten für Bedrohungsakteure. In Zeiten, in denen die traditionelle geheimdienstliche Tätigkeit aufgrund anhaltender Lockdowns, sozialer Distanzierung und internationaler Reisebeschränkungen eingeschränkt ist, scheint der Einsatz offensiver Cyber-Werkzeuge zur Durchführung von nationalen Geheimdienst- und Spionageoperationen zugenommen zu haben. Tatsächlich ist der neue Cyber-Intelligence-Bereich in vielen Ländern zur bevorzugten Waffe geworden.

Die Weltgesundheitsorganisation (WHO) berichtete über einen starken Anstieg der Cyber-Angriffe, einschließlich eines der APT-Gruppe DarkHotel zugeschriebenen Angriffs in einer Operation, in die auch andere Gesundheitsorganisationen und humanitäre Organisationen verwickelt wurden. In einer gemeinsamen Erklärung warnten die Cyber-Agenturen der USA und Großbritanniens vor verstärkten APT-Aktivitäten, die auf die Gesundheitsversorgung abzielen, und beschuldigten insbesondere China einer organisierten groß angelegten Kampagne. Es wird berichtet, dass die APT-41-Gruppe in den Monaten seit dem Virusausbruch eine der weitreichendsten Kampagnen eines chinesischen Akteurs durchgeführt hat, bei der hauptsächlich Citrix- und Cisco-Schwachstellen ausgenutzt wurden. Es wird vermutet, dass mit dem Iran in Verbindung stehende Hacker hinter einem Angriff auf den US-Medikamentenhersteller Gilead stehen, der sich in einem fortgeschrittenen Stadium der Entwicklung einer COVID-19-Behandlung befindet.

Andere regionale APT-Gruppen nutzten die COVID-19-Konversation, um ihre Routineabläufe zu verschleiern. APT-36, eine in Pakistan ansässige Bedrohungsgruppe, hat ihren CrimsonRat unter Verwendung gefälschter COVID-19-Mitteilungen gegen indische Regierungsinstanzen eingesetzt. Das auf Indien bezogene Patchwork APT richtete sich gegen chinesische Einrichtungen, indem es bösartige Excel-Dokumente verwendete, die sich als die nationale chinesische Gesundheitskommission ausgaben, während chinesische APT-Gruppen die Mongolei und die APAC-Länder mit infizierten RTF-Dokumenten im Zusammenhang mit COVID-19 angriffen und gefälschte diplomatische E-Mails versendet haben. Die nordkoreanische Gruppe Kimsuky führte unter dem Deckmantel von COVID-19-bezogenem Material einen Angriff gegen südkoreanische Organisationen durch.

Die russischstämmige Gamaredon-Gruppe richtete sich gegen ukrainische Einrichtungen und gab sich als ukrainisches Gesundheitsministerium aus. Hades, eine weitere mutmaßliche russische Gruppe, hatte es auf ukrainische Einrichtungen abgesehen, während sie sich auf der Suche nach COVID-19-bezogenen Informationen als RIA-Journalist tarnte. Es bestand der Verdacht, dass dieser Angriff im Zusammenhang mit einer späteren Falschinformationskampagne stand, als eine Flut von Nachrichten in sozialen Medien behauptete, COVID-19 sei in der Ukraine angekommen, was zu eskalierenden Ängsten und Unruhen führte.

**MEILENSTEIN**

Länder nutzen häufig Cyber-Angriffe, um ihre militärischen und politischen Ziele heimlich zu erreichen, ohne die regelmäßigen Vergeltungsmaßnahmen und Folgen kinetischer militärischer Aktionen und Provokationen. Ein kürzlich aufgetretener Cyber-Konflikt sticht besonders hervor. Bei einem Angriff auf die israelische Wasserversorgung im April versuchten mutmaßliche iranische Bedrohungsakteure, den Chlorgehalt im Trinkwasser des Bezirks zu erhöhen. Es wird vermutet, dass Israel für den Cyber-Angriff auf den iranischen Hafen Shahid Rajaee an der Straße von Hormuz verantwortlich ist und die Hafenarbeiten zum Stillstand gebracht hat, was als Vergeltungsakt angesehen wird. Keines der beiden Länder übernahm offiziell die Verantwortung für die Angriffe, doch dieser Austausch von Angriffen kennzeichnet eine neue Ebene der Integration von Cyber-Kriegsführung in die Domäne der traditionellen Kriegsführung.

# Mobile Trends – Neue Infektionsvektoren suchen

Aus Sicht der Bedrohungsakteure ist es vielleicht die größte Herausforderung, auf den Plattformen der Opfer Fuß zu fassen. Dies gilt umso mehr bei mobilen Plattformen, die einen kontrollierten Zugang zu den offiziellen App-Stores haben. Traditionell verließen sich Angreifer in der ersten Infektionsphase auf App-Stores von Drittanbietern und Benutzerfehler. Das wachsende Bewusstsein der Anwender hat die Bedrohungsakteure jedoch dazu veranlasst, sich verstärkt um zusätzliche Infektionsvektoren zu bemühen.

In den vergangenen Monaten konnten wir einen erheblichen Anstieg gefährlicher Apps im offiziellen Google Play Store beobachten. Wir haben über Anwendungen berichtet, die mit Tekya-Clicker, BearCloud,Haken und noch viel mehr Malware infiziert waren, die alle im offiziellen Google Play Store gefunden wurden.

Eine der Methoden, mit denen die bösartige Natur einer Anwendung verschleiert werden kann, ist die Verwendung der für ihre Entwicklung verwendeten muttersprachlichen Programmiersprachen. Viele Bedrohungsakteure sprechen quasi die Sprache ihrer Opfer, anstelle Java für die Entwicklung bösartiger Anwendungen zu verwenden, nutzen sie nativen Android-Code, typischerweise C und C++. Das macht es viel schwieriger, den Code zu dekompilieren und als bösartig zu identifizieren. Zudem wird die Wirksamkeit der Verfahren zur Erkennung von Malware im Google Store verringert. Tekya, Haken, Joker und Circle sind nur einige Beispiele für Malware, die eine native Implementierung verwendet, um der Erkennung zu entgehen. Und tatsächlich fanden Forscher bei einer Untersuchung von 150.000 Android-Apps heraus, dass fast 7 % der Apps in Google Play versteckte Hintertüren enthielten.

Im Falle von Mandrake etwa arbeiteten die Bedrohungsakteure in mehreren Phasen, wobei in der ersten Phase eine gutartige App geliefert wurde. Erst in späteren Phasen, nachdem die Betreiber sorgfältig überprüft hatten, dass sie nicht in einer kontrollierten (Sandbox)-Umgebung laufen, gehen sie zur nächsten Phase über und aktivieren den bösartigen Teil der Anwendung.

Andere Akteure versuchen, allgemeine Desktop-Malware-TTPs (Techniken, Taktiken und Verfahren) zu übernehmen und sie auf mobilen Plattformen zu replizieren. Trickbot wurde dabei entdeckt, wie es eine Android-App mit der Bezeichnung Trickmo zur Ergänzung seiner Fähigkeiten und zur Umgehung des 2FA-Mechanismus (Two-Factor Authentication) betreibt. Trickbot ist nicht die einzige App, die SMS-Nachrichten liest. EventBot, ein Android-Infostealer, wurde ebenfalls entwickelt, um SMS-Authentifizierungsnachrichten abzufangen, die für mehr als 200 Finanzanwendungen in den USA und Europa verwendet werden.

**MEILENSTEIN**

Von allen mobilen Angriffen, die in den letzten sechs Monaten gemeldet wurden, fanden wir einen einzigen, der auf eine neue Methode der Malware-Verbreitung hindeuten könnte. Bei diesem Angriff infizierten Bedrohungsakteure mehr als 75 % der mobilen Plattformen eines multinationalen Konzerns mit dem Cerberus-Banker. Um dies zu erreichen, nutzten sie das Mobile Device Management (MDM) des Unternehmens, das häufig als Sicherheitsmaßnahme missverstanden wird, um Cerberus zentral auf mehreren Mobilgeräten zu installieren. Dies war der erste beobachtete Angriff, der mobile Unternehmensnetzwerke der Gefahr eines koordinierten Angriffs aussetzt, den Betrieb beeinträchtigt und digitale Unternehmenswerte gefährdet.

# Cloud-Bedrohungen

Cloud-Technologien und -Dienstleistungen mit den Vorteilen der Skalierbarkeit, Agilität und Kosteneffizienz sind weithin als treibende Kraft für Unternehmen weltweit anerkannt, die einen schnellen und plötzlichen Übergang zum Arbeiten von zu Hause aus ermöglichten. Dennoch müssen wir uns Monate, nachdem COVID-19 in unser Leben getreten ist und unsere Arbeits- und Geschäftstätigkeit verändert hat, auch der Risiken bewusst werden, denen wir ausgesetzt sind, und uns vor diesen neuen Bedrohungen schützen. Die letzten Monate haben gezeigt, dass sich immer noch neue Risiken und eine gefährliche Nutzung der Cloud-Umgebung entfalten.

**MEILENSTEIN**

Im Januar wurde zum ersten Mal eine kritische Schwachstelle in einer großen Cloud-Infrastruktur gefunden und von Check-Point-Forschern gemeldet. Die Schwachstellen mit einem perfekten CVE-Wert von 10,0 könnten es Bedrohungsakteuren ermöglichen, die Infrastruktur der virtuellen Maschinen von Microsoft Azure zu umgehen und Daten und Anwendungen anderer Mieter, die unwissentlich die gleiche Hardware nutzen, zu beeinträchtigen. Anders als bei früheren Cloud-Verstößen lag die Ursache des Problems in der Infrastruktur selbst, weshalb die einzelnen Nutzer nichts tun konnten, um sich zu schützen, womit bewiesen wurde, dass die Cloud-Infrastruktur nicht ohne Fallstricke ist.

Cloud-Service-Anbieter sind ebenso anfällig für Schwachstellen in ihren ungepatchten Geräten, wie bewiesen wurde, als ein französischer Cloud-Service-Anbieter durch eine ungepatchte Citrix-Server-Schwachstelle gehackt wurde. In diesem Fall wurden 30 TB Kundendaten mittels der DoppelPaymer-Ransomware verschlüsselt.

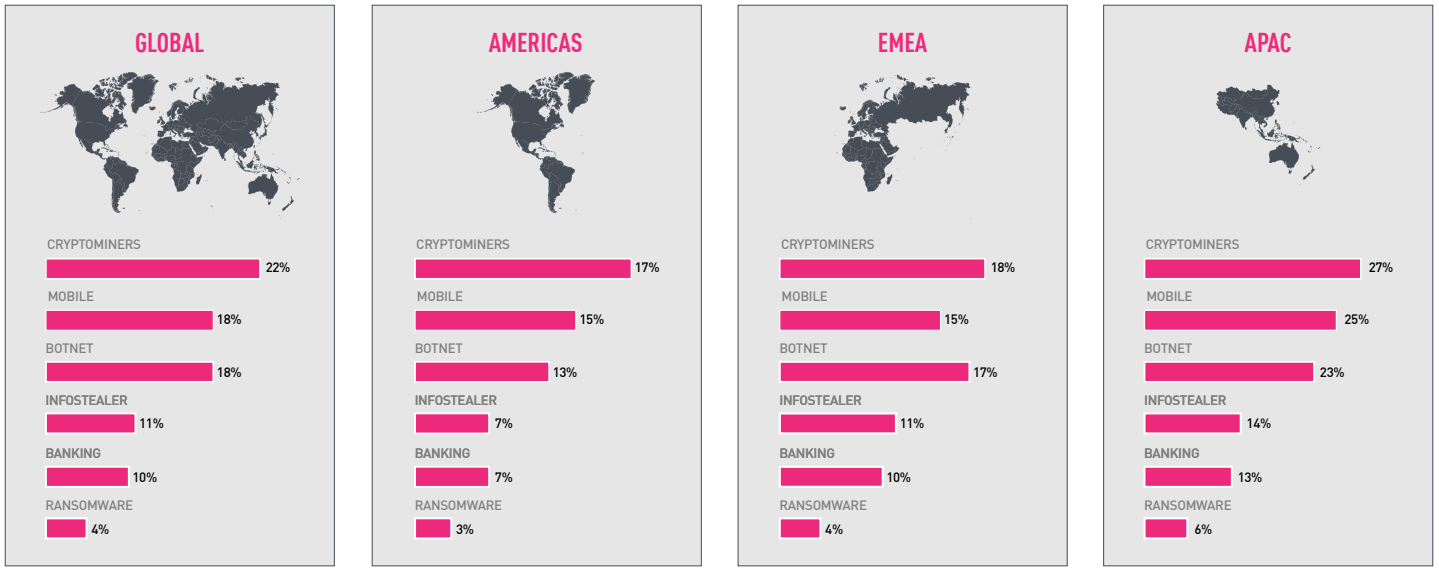
Ein weiterer wachsender Trend ist die Nutzung von Cloud-Infrastrukturen zugunsten der Bedrohungsakteure. Angreifer tarnen bösartige Nutzlasten in der Cloud-Infrastruktur und speichern sie auf GitHub, Gmail oder Alibaba um Befehle bereitzustellen oder Konfigurationsdateien zu hosten. In anderen Fällen kann das bloße Hochladen scheinbar harmloser Dokumente mit bösartigen Links auf Google Drive die zusätzliche Legitimität verleihen, die erforderlich ist, um ahnungslose Opfer zu täuschen. Cloud-Dienste sind sich der Art und Weise bewusst, wie diese TTPs Emulations- und Scan-Verfahren implementieren, doch die Bedrohungsakteure schlagen mit Verschlüsselungen und Tarntechniken zurück und bieten Dropper mit der Absicht an, Malware in der Cloud zu platzieren.

Cloud-basierte Anwendungen machen Phishing-Angriffe effektiver und erleichtern BEC-Angriffe, die der Hauptgrund für finanzielle Verluste bei Cyber-Angriffen sind. Die weitreichende Kontrolle, die den Benutzern durch Office365 und ähnliche Dienste gewährt wird, kann Angreifern, die im Besitz gestohlener, aus Phishing-Operationen erlangter Zugangsdaten sind, eine kritische Stellung innerhalb der betreffenden Organisation verschaffen. Es wurde beobachtet, wie Angreifer über lange Zeiträume die Kontrolle über gestohlene Konten behielten und schließlich unter Verwendung der erhaltenen Informationen ausgeklügelte BEC-Operationen durchführten.

Fehlkonfigurierte Cloud-Ressourcen sind nach wie vor einer der Hauptgründe für Datenpannen in der Cloud. Hunderte von Gigabyte eines Finanzunternehmens wurden durch einen AWS S3-Bucket beeinträchtigt, der keinerlei Form der Verschlüsselung, Authentifizierung oder Zugangsberechtigung verwendet hatte. Ein weiterer ungeschützter AWS-Speicher einer Gesellschaft für Studentendarlehen verlor Tausende von aufgezeichneten Anrufen und Scans von personenbezogenen Dokumenten. Hunderte von Millionen von US-Immobiliendatensätzen wurden auf einem ungeschützten und nicht identifizierten Google Cloud-Service offengelegt.

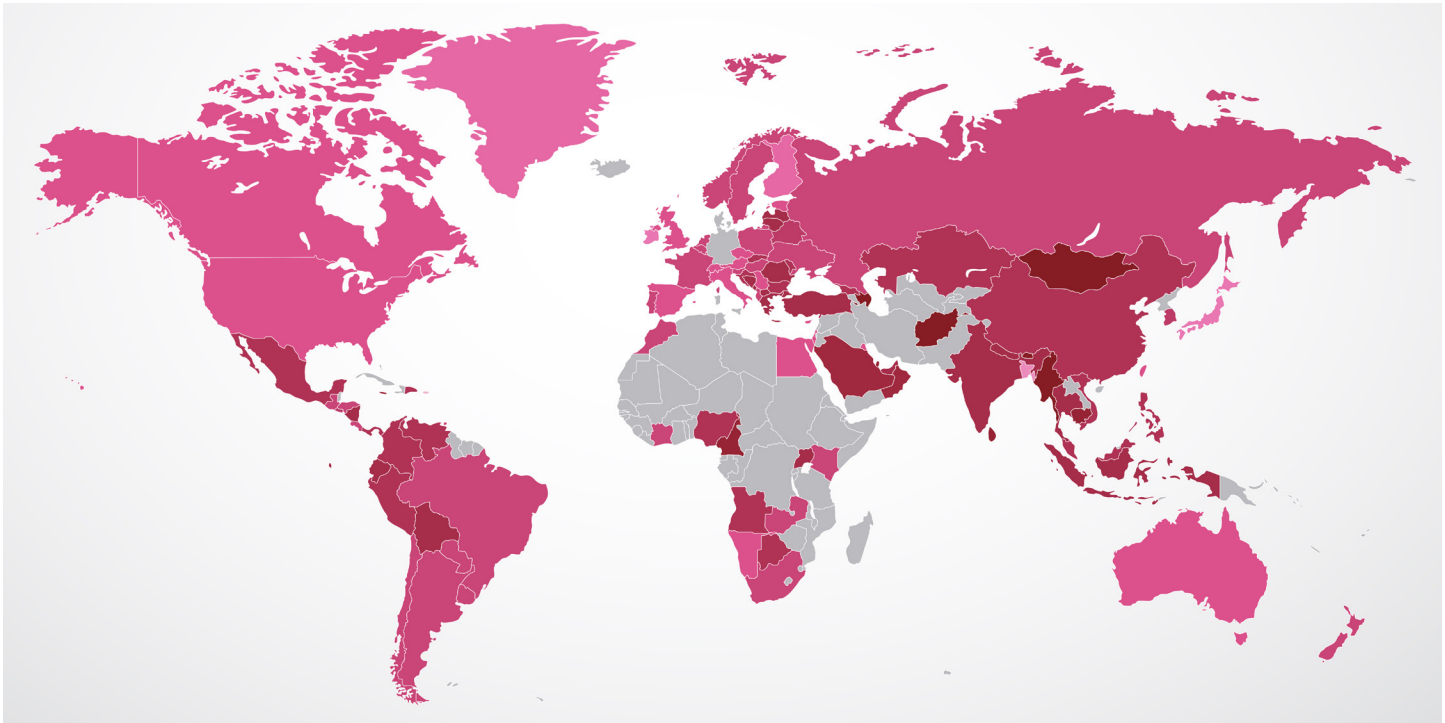
Sei es durch Schwachstellen in der Cloud-Infrastruktur, durch direkte Angriffe auf Anbieter von Cloud-Diensten oder durch Ausnutzung von Fehlkonfigurationen und Benutzerfehlern, die Cloud bleibt weiterhin ein lukratives Ziel für Bedrohungsakteure, insbesondere in der Welt nach Corona, die Tag für Tag zur neuen Normalität wird.

# Cyber-Angriffskategorien nach Region




# Globale Bedrohungsindexkarte

Der Bedrohungsindex von Check Point basiert auf der Wahrscheinlichkeit, dass eine Maschine in einem bestimmten Land von Malware angegriffen wird. Dies lässt sich an der ThreatCloud Cyberbedrohungsweltkarte ablesen, die in Echtzeit verfolgt, wie und wo Cyber-Angriffe weltweit stattfinden.



# Die heimtückischsten Dateitypen – Web vs. E-Mail

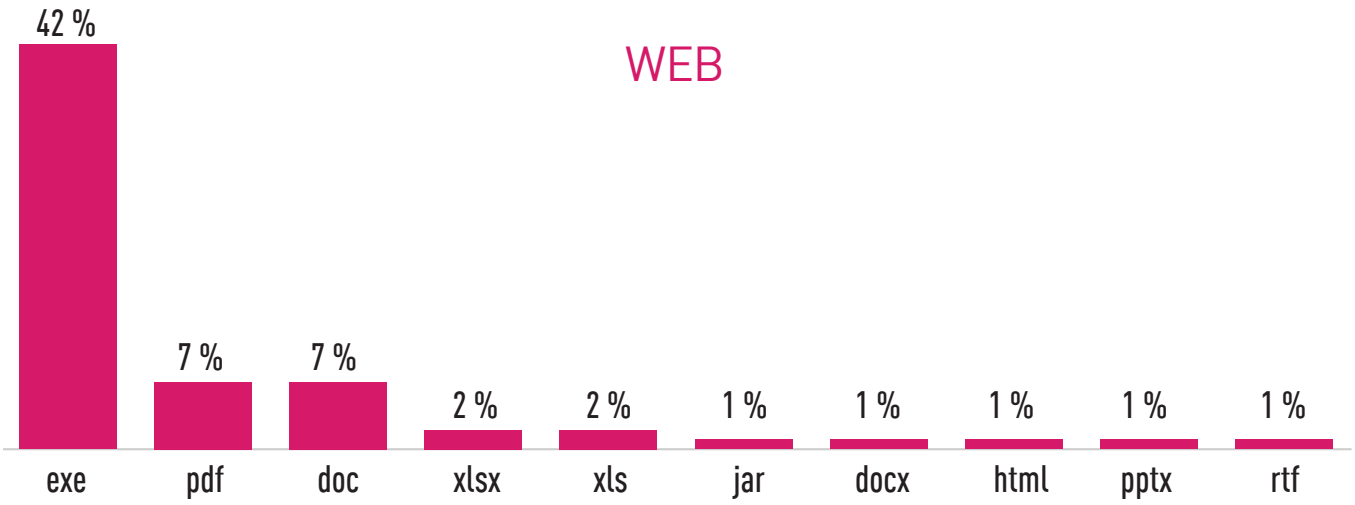



**Abbildung 1**: Web – Die bösartigsten Dateitypen

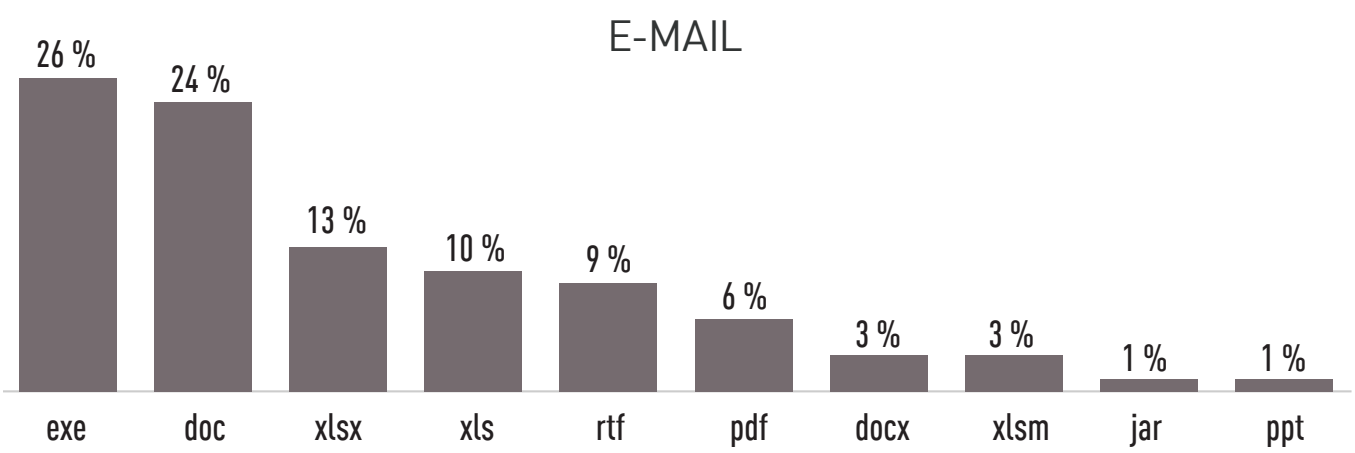



**Abbildung 2:** Email – Die bösartigsten Dateitypen

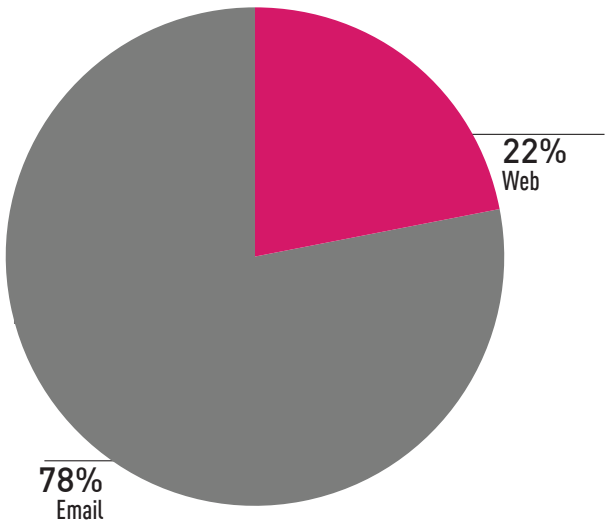



**Abbildung 3:** Vertriebswege – E-Mail vs. Web als Angriffsvektoren

# Globale Malware-Statistiken

Die in den folgenden Abschnitten dieses Berichts vorgestellten Datenvergleiche basieren auf Informationen, die aus der Check Point ThreatCloud Cyberbedrohungsweltkarte zwischen Januar und Juni 2020 entnommen wurden. Für jede der unten aufgeführten Regionen stellen wir die am weitesten verbreitete Malware vor.

## Top Malware-Familien

### Global

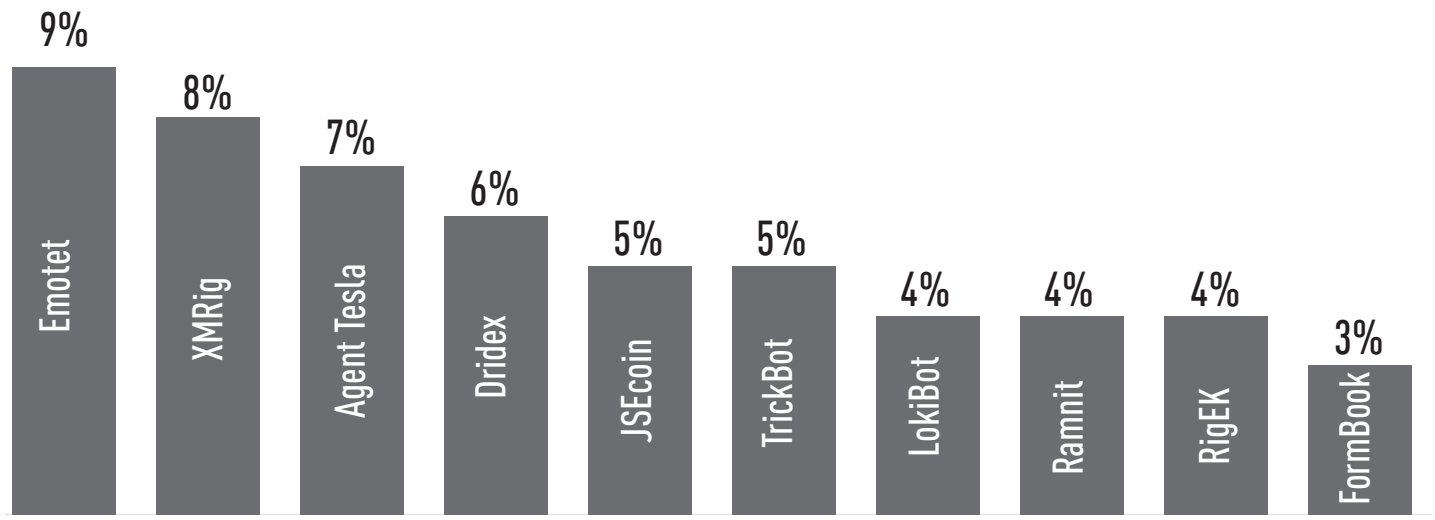



**Abbildung 4**: Meist verbreitete Malware weltweit: Anteil der Unternehmensnetzwerke, die von jeder Malware-Familie betroffen sind

### Amerika

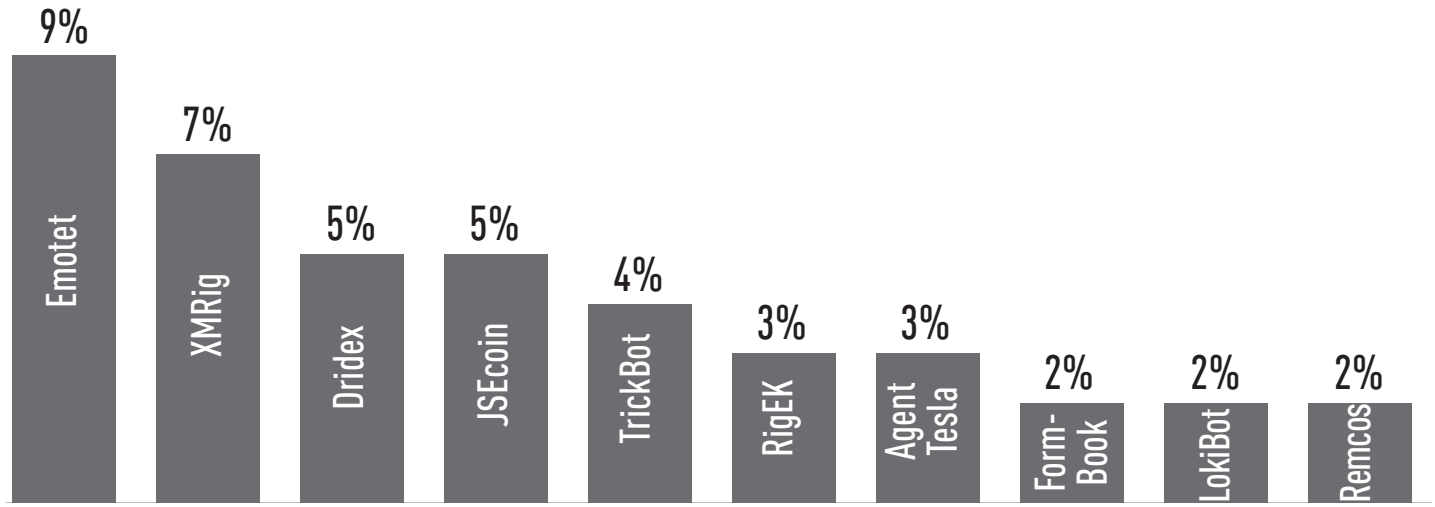



**Abbildung 5**: Die am meisten verbreitete Malware in Amerika

## Europa, Naher Osten und Afrika (EMEA)

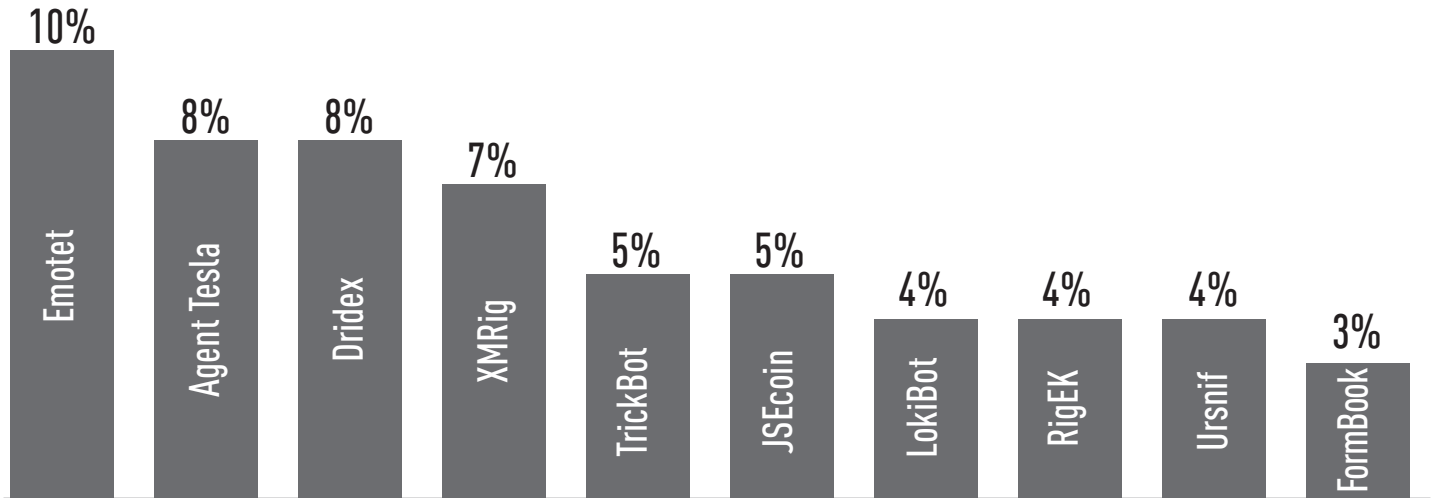



**Abbildung 6:** Die häufigste Malware in der EMEA-Region

## Asien-Pazifik (APAC)

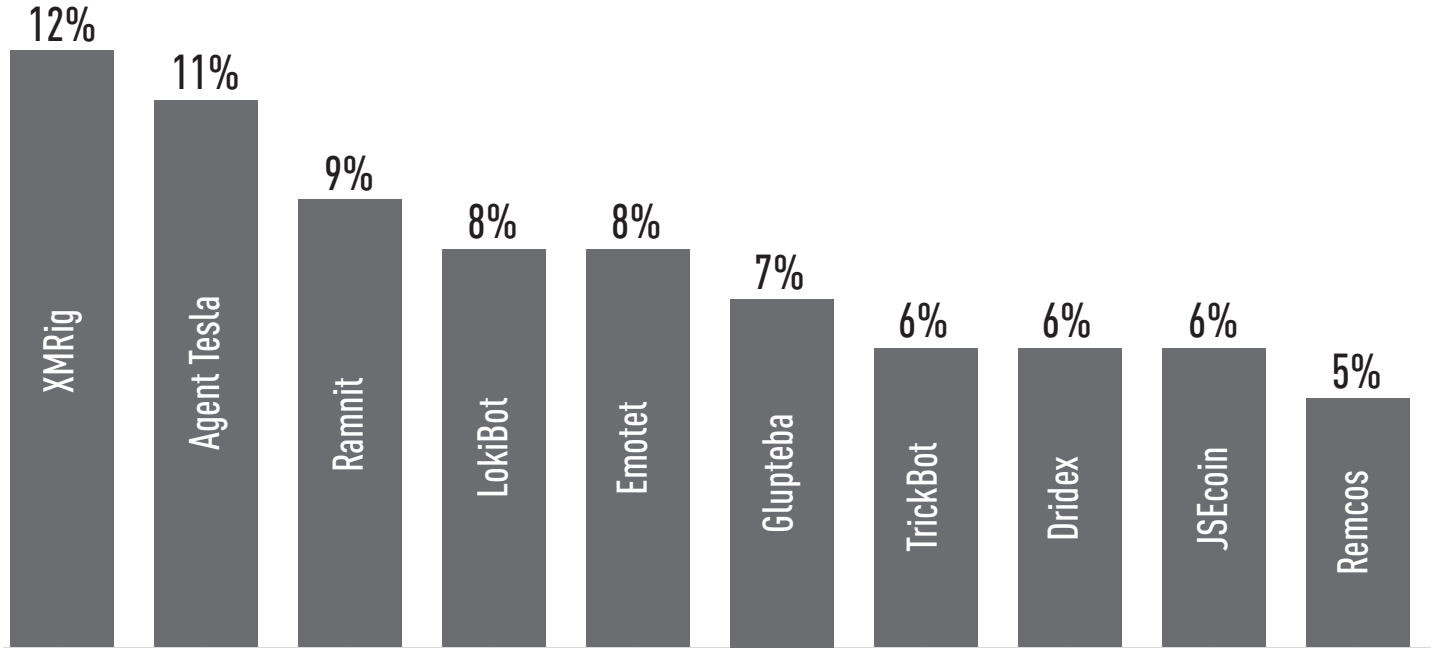



**Abbildung 7** Die häufigste Malware in der APAC-Region

## Globale Analyse der Top Malware

Trotz der Gewohnheit der Emotet-Akteure, lange Aktivitätspausen einzulegen, wobei die aktuelle Pause im Februar 2020 begann, ist Emotet im aktivierten Zustand so produktiv, dass es immer noch den unehrenhaften ersten Platz an der Spitze der weltweiten Malware-Charts erreicht hat. Emotet, ursprünglich ein Banking-Trojaner, hat sich zu einer Botnet-Operation entwickelt, die sich hauptsächlich über bösartige Dokumente verbreitet, die per E-Mail verschickt werden und deren Infektionsbasis an Ransomware-Bedrohungsakteure vermietet wird.

Die Abschaltung berüchtigter Drive-by-Crypto-Mining-Dienste wie Coinhive und JSEcoin hat XMRig als führenden Cryptominer hinterlassen. Agent Tesla, Lokibot und Remcos sind beliebte Malware-Optionen für weniger erfahrene Bedrohungsakteure. Sie ermöglichen es Angreifern, auf einfache Weise einen Trojaner per Fernzugriff zu erstellen und einzusetzen, ohne dass Kenntnisse in der Entwicklung von Malware erforderlich sind, wodurch sie sich auf vorhandene, leicht verfügbare Tools und Tutorials stützen können.

# Top-Cryptomining-Malware

## Global

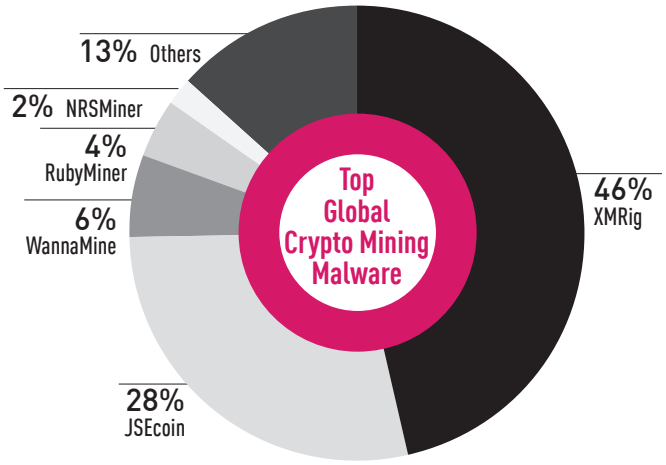



**Abbildung 8**: Top Cryptomining-Malware Global

## Amerika

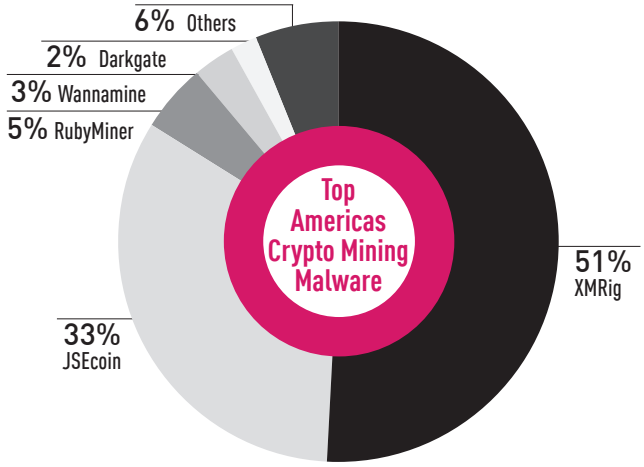



**Abbildung 9:** Top Cryptomining-Malware in Amerika

## EMEA

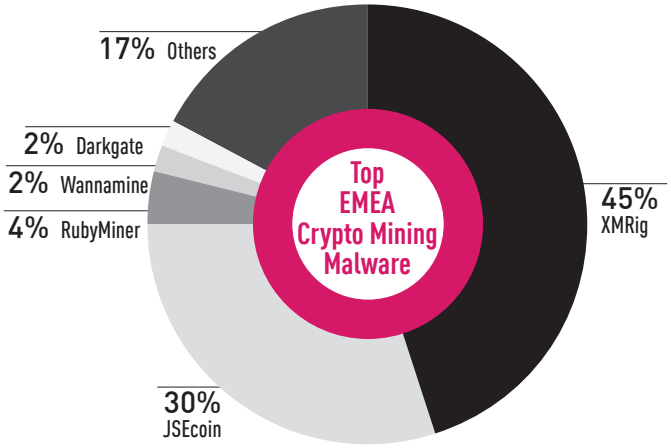



**Abbildung 10**: Top Cryptomining-Malware in EMEA

## APAC

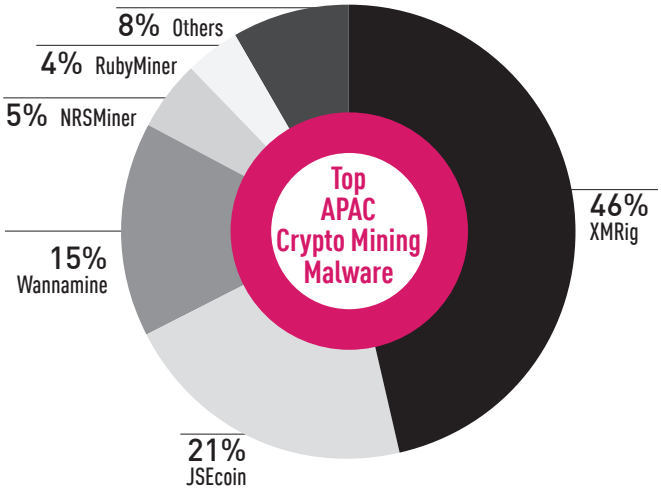



**Abbildung 11**: Top Cryptomining-Malware in APAC

## Globale Analyse der Cryptominer

Die abnehmende Rentabilität des Drive-by-Mining hat im vergangenen Jahr zur Stilllegung von Coinhive und nun auch von JSEcoin geführt. XMRig, eine beliebte Open-Source-Mining-Malware, hat ihren Platz auf der Liste der wichtigsten Crypto-Mining-Bedrohungen eingenommen.

XMRig ist ein Open-Source-Tool, das für legitime Zwecke geschaffen wurde und von Bedrohungsakteuren häufig oder in modifizierter Form als Mining-Tool für Kryptowährung eingesetzt wird. Heute wird XMRig immer noch aktiv bei verschiedenen bösartigen Aktivitäten eingesetzt, unter anderem in kompromittierten Kubernetes-Clustern. In Verbindung mit Mining-Malware wie Wannamine und RubyMiner ist XMRig vermutlich führend in der Welt des illegalen Krypto-Währungs-Minings. Angesichts der zunehmenden Rechenleistung, die derzeit für die Beschaffung erheblicher Geldmittel erforderlich ist, suchen die Bedrohungsakteure nach neuen Schauplätzen, wobei in einigen Fällen sogar zu beobachten ist, dass Supercomputer für Mining-Zwecke genutzt werden. Ein weiterer auffälliger Trend besteht darin, dass andere Malware-Genres Cryptomining als zusätzliche Einnahmequelle hinzufügen, wie wir gemeldet über das Phorpiex-Botnet berichtet haben.

# Mobile Top-Malware

## Global

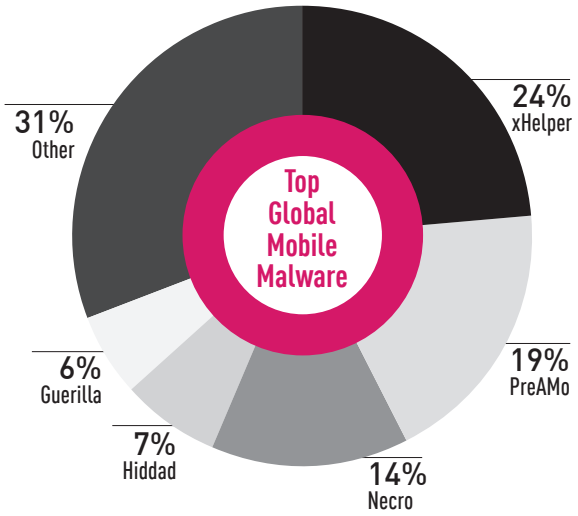



**Abbildung 12**: Mobile Top Malware weltweit

## Amerika

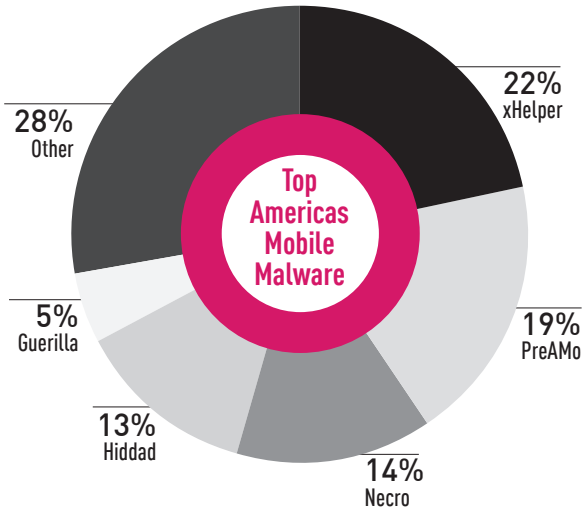



**Abbildung 13**: Mobile To Malware in Amerika

## EMEA

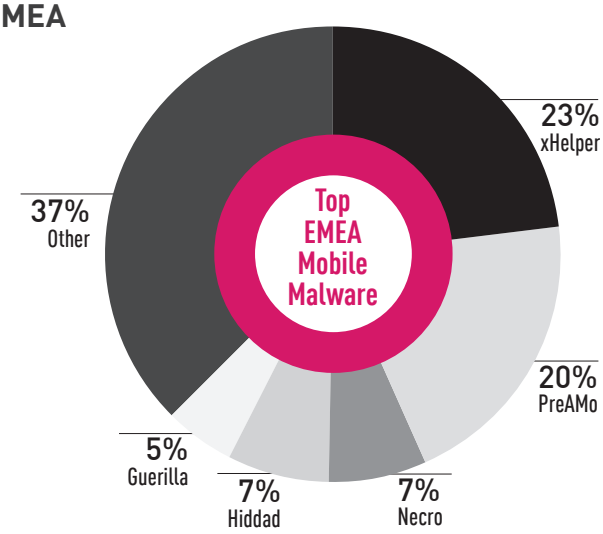



**Abbildung 14**: Mobile Top Malware in der EMEA-Region

## APAC

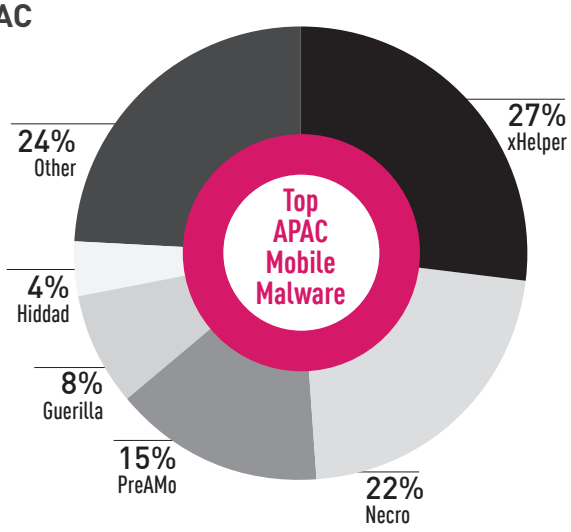



**Abbildung 15**: Mobile Top Malware in der APAC-Region

## Globale Analyse von mobiler Malware

xHelper für Android, das Mitte 2019 zum ersten Mal aufgetaucht ist, steht ganz oben auf der Liste der mobilen Malware. xHelper hat die Benutzer mit seiner außergewöhnlichen Beharrlichkeit verwirrt, durch die es einen Factory-Reset überleben kann. Anschließend folgten PreAMo, Necro, Guerrilla und Hiddad, allesamt multifunktionale Trojaner, die als Dropper fungieren, sich aber hauptsächlich durch Anzeigen und Klickbetrug finanzieren.

# Top Botnets

## Global

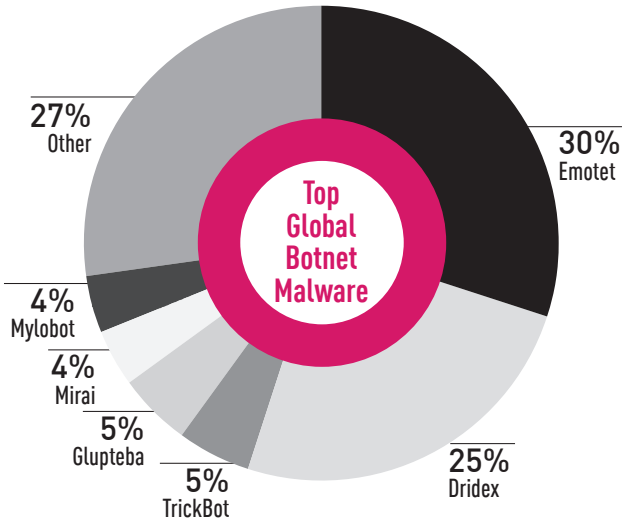



**Abbildung 16**: Die häufigsten Botnets weltweit

## Amerika

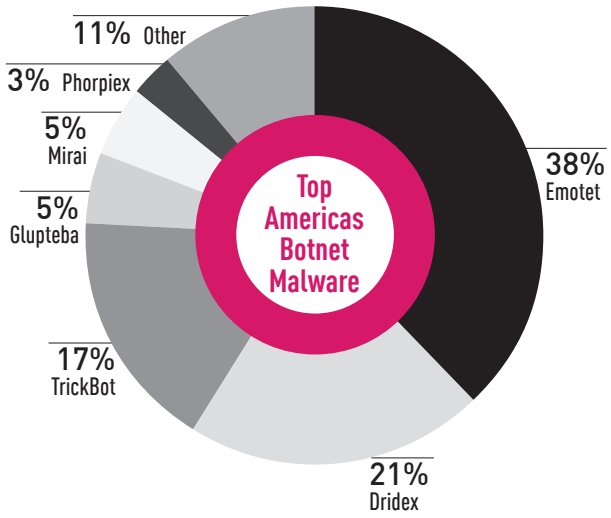



**Abbildung 17**: Die häufigsten Botnets in Amerika

## EMEA

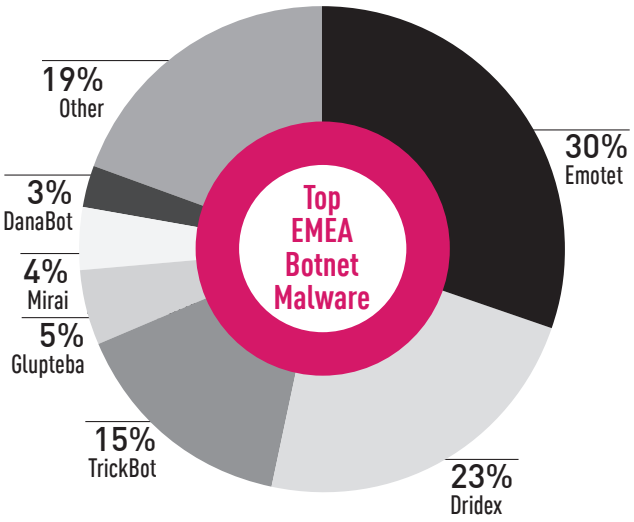



**Abbildung 18**: Die häufigsten Botnets in der EMEA-Region

## APAC

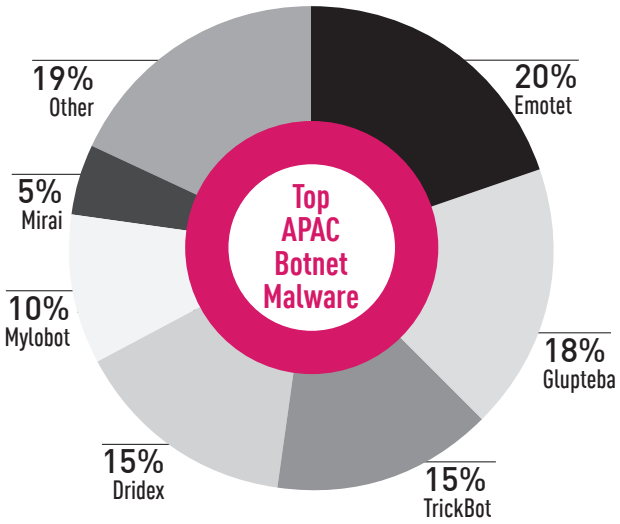



**Abbildung 19**: Die häufigsten Botnets in der APAC-Region

## Globale Analyse der Botnets

Viele Malware-Familien starteten als spezifische Malware-Arten und entwickelten sich dann zu vollwertigen Botnets. Emotet folgte einem ähnlichen Muster. Emotet verbreitet sich über thematische Malspam-Kampagnen und verfügt über eine umfangreiche Infektionsbasis. Durch eine Reihe von Kooperationen ist Emotet ein wichtiges Bindeglied in einer gefährlichen Lieferkette, die mit einer Emotet-Infektion beginnen und mit einer Ransomware enden kann. Am bemerkenswertesten ist die Zusammenarbeit zwischen den Emotet-Autoren und der TrickBot-Gang, die TrickBot als Malware einer zweiten Phase verbreitete, die sich mithilfe der Ryuk-Ransomware häufig in einen ausgewachsenen Ransomware-Angriff ausweitete. Obwohl Emotet das weltweit am weitesten verbreitete Botnet ist, setzt es seine Tätigkeit gelegentlich zeitweise aus. Im Februar dieses Jahres verschwand Emotet das letzte Mal. Nach intensiven Aktivitäten im Januar, die mit einer COVID-19-bezogenen Kampagne gegen Japan endeten, stellte Emotet seine Aktivitäten ein und dürfte noch im Laufe dieses Jahres zurückkehren.

# Top-Info-Diebstahl-Malware

## Global

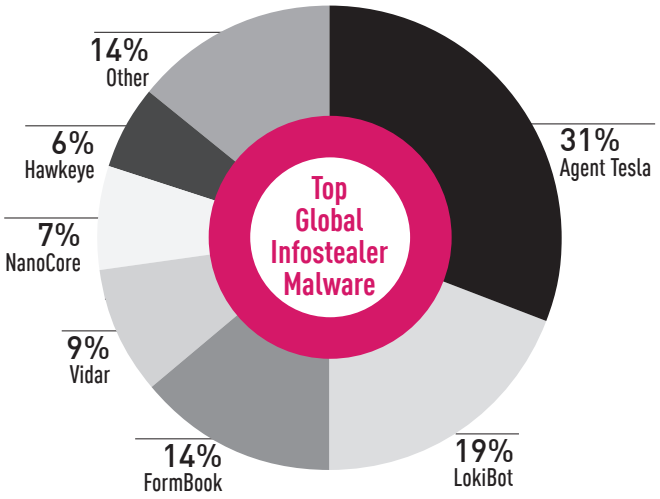



**Abbildung 20**: Top-Info-Diebstahl-Malware weltweit

## Amerika

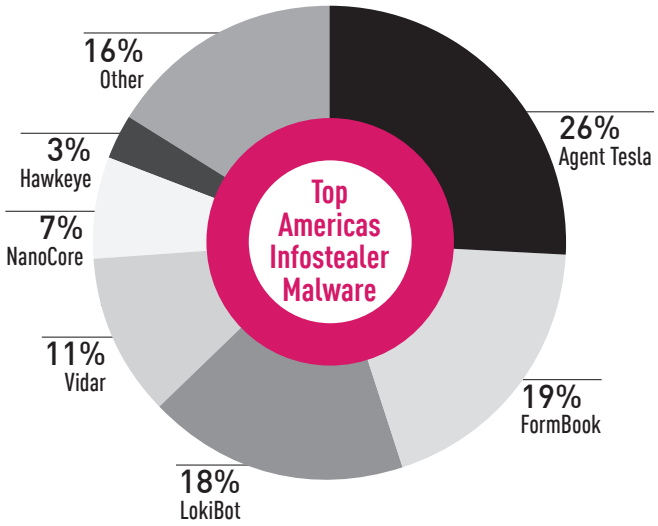



**Abbildung 21**: Top-Info-Diebstahl-Malware in Amerika

## EMEA

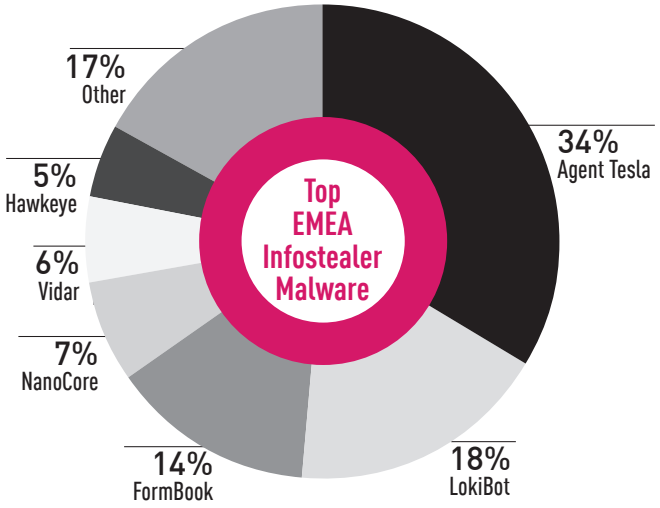



**Abbildung 22**: Top-Info-Diebstahl-Malware in der EMEA-Region

## APAC

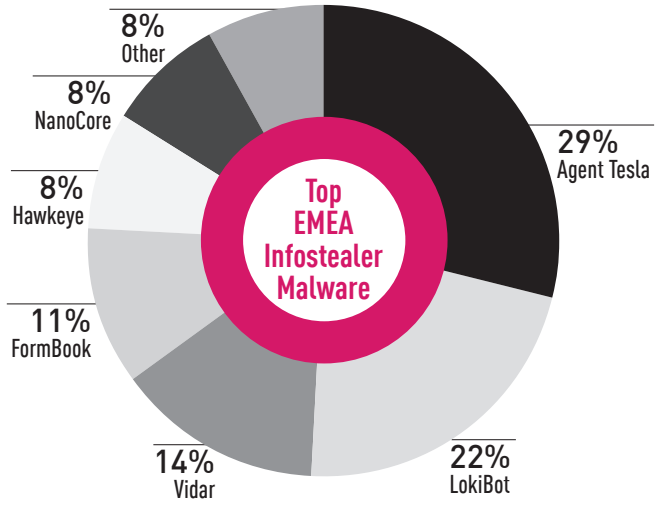



**Abbildung 23**: Top-Info-Diebstahl-Malware in der APAC-Region

## Globale Analyse der Infostealer-Malware

Agent Tesla ist eine RAT, die bereits seit 2014 existiert und in diesem Jahr zum weltweit beliebtesten Infostealer wurde. Ihre Funktionalität umfasst die Überwachung von Tastenanschlägen und der Systemzwischenablage. Sie kann auch Screenshots erstellen und Zugangsdaten für eine Vielzahl von Software wie Google Chrome, Mozilla Firefox und den E-Mail-Client Microsoft Outlook exfiltrieren. Agent Tesla wurde im Rahmen eines Malware-as-a-Service (MaaS)-Modells betrieben, wobei Kunden für Benutzerlizenzen zwischen 15 und 69 USD bezahlen. Durch die kontinuierliche Integration neuer Funktionalitäten können seit diesem Jahr Wi-Fi-Profile gestohlen werden.

# Top-Banken-Trojaner

## Global

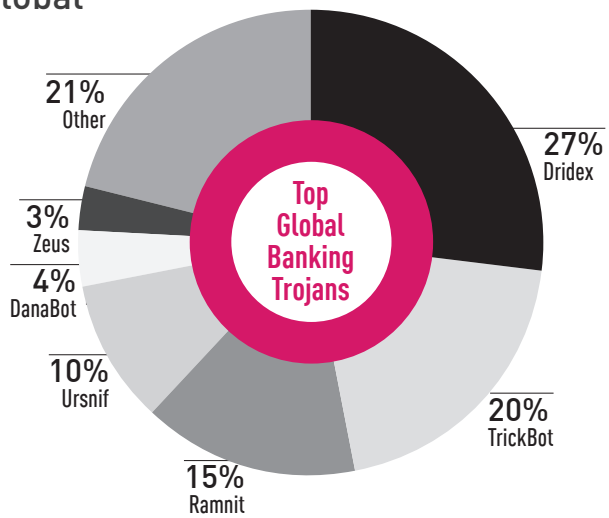



**Abbildung 24**: Die häufigsten Banken-Trojaner weltweit

## Amerika

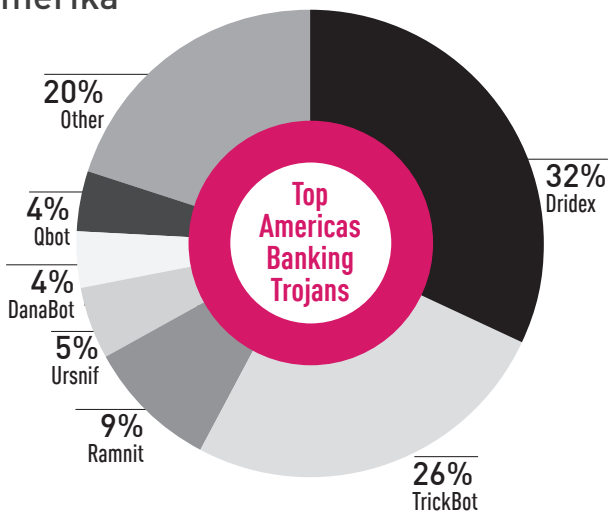



**Abbildung 25**: Die häufigsten Banken-Trojaner in Amerika

## EMEA

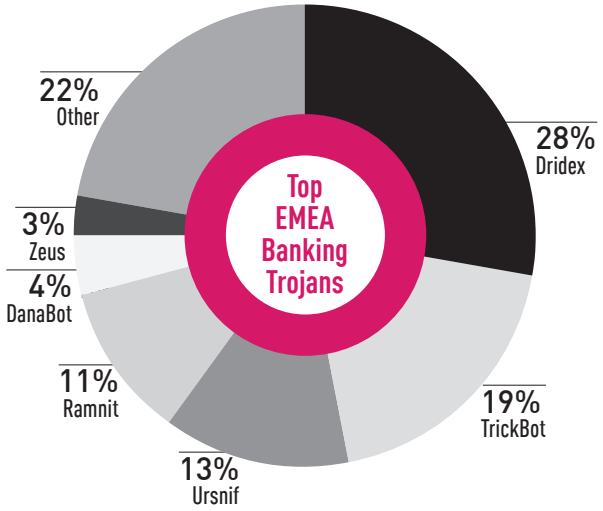



**Abbildung 26**: Die häufigsten Banken-Trojaner in der EMEA-Region

## APAC

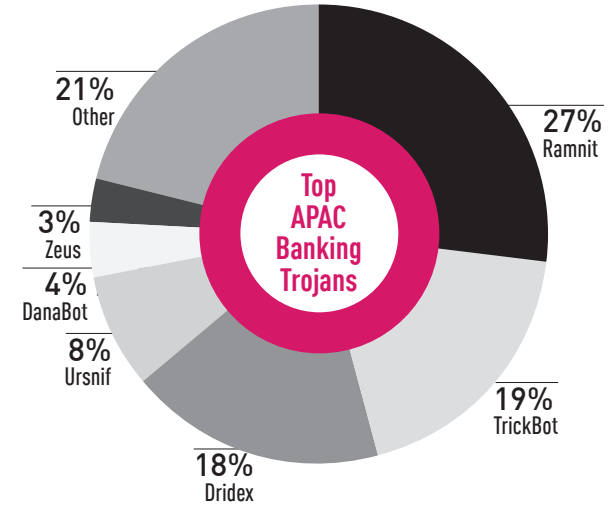



**Abbildung 27**: Die häufigsten Banken-Trojaner in der APAC-Region

## Banktrojaner-Analyse

Der Schauplatz der Bankiers wird nach wie vor von drei prominenten Trojanern dominiert – Dridex, TrickBot und Ramnit. Die verbleibenden Akteure beteiligen sich an einer Vielzahl von kriminellen Aktivitäten, in denen sie wie Botnets agieren und andere Malware-Stränge als zusätzliche Einnahmequellen liefern. Ein Beispiel dafür ist der Angriff auf die Universität Maastricht den die Bedrohungsgruppe TA505 durchgeführt hat, bei dem Dridex als Infektionsvektor eingesetzt wurde. Wie andere Malware-Arten nutzten auch die Banking-Trojaner die COVID-19-Pandemie, um neue Opfer zu erreichen.

**Trickbot:** Trickbot ist eine Dyre-Variante, die im Oktober 2016 zum ersten Mal auftauchte. Seit seinem ersten Erscheinen hat es sich nach und nach weiterentwickelt und seine Funktionalität von einem Banking-Trojaner zu einer Malware ausgebaut, die die Zugangsdaten von E-Mail-Konten, Browsern und mehr sammelt und ständig auf der Suche nach neuen Einnahmequellen ist. TrickBot spielte eine führende Rolle bei den Angriffen mit der Ryuk-Ransomware. In diesem Jahr wurde die Weiterentwicklung durch die Ergänzung einer neuen PowerShell-Hintertür mit der Bezeichnung PowerTrick und einer neuen Variante mit der Bezeichnung Anchor fortgesetzt. Anchor wurde in Verbindung mit einer PowerShell-Malware eingesetzt, die der nordkoreanischen Lazarus-Gruppe zugeschrieben wird. Die Forschung verweist auf eine mögliche Zusammenarbeit zwischen Lazarus und TrickBot-Betreibern. Während der COVID-19-Pandemie richteten sich die Trickbot-Betreiber mit gefälschten Gesundheitswarndokumenten gegen italienische Benutzer.

# Wichtige globale Schwachstellen

Die folgende Liste der häufigsten Schwachstellen basiert auf Daten, die vom IPS-Sensornetz (IPS, Intrusion Prevention Systems) von Check Point erfasst wurden, und enthält einige der beliebtesten und interessantesten Angriffstechniken und Exploits, die von Check Point-Forschern im ersten Halbjahr 2020 beobachtet wurden.

- **Schwachstelle in der Software des Exim Mail Transfer Agent (MTA) (CVE-2019-10149** – Exim wird zur Übertragung von E-Mail-Nachrichten verwendet und ist häufig in Linux-Versionen vorinstalliert. Die Schwachstelle bei der E-Mail-Übertragung in Exim wurde im März 2019 gefunden und gemeldet. Eine unsachgemäße Handhabung der Überprüfung von Empfängeradressen auf Servern mit Exim 4.87 bis 4.91 könnte zur Remote-Code-Ausführung führen und wurde daher als kritisch eingestuft. Obwohl bis Juni 2019 ein Sicherheits-Update veröffentlicht wurde, gibt es immer noch fast eine Million ungepatchte Server, die täglich online sind, hauptsächlich in den USA, Deutschland und Russland. Diese Lücke wird aktiv ausgenutzt, weshalb ein Berater der NSA davor warnte, dass der russische Sandwurm APT seit fast einem Jahr missbraucht wird.
- **Schwachstelle bei Draytek Vigor Command Injection (CVE-2020-8515)** – Eine interessante Schwachstelle, die in diesem Jahr aufgedeckt wurde, betrifft Router und VPN-Gateways des taiwanesischen Herstellers DrayTek. Die kritische RCE-Schwachstelle, die als CVE-2020-8515 verfolgt wird, wurde erstmals im Januar 2020 gemeldet, worauf bald ein PoC folgte. Es hat nun den Anschein, als sei die Schwachstelle mindestens seit Dezember 2019 ausgenutzt worden. Obwohl ein Patch veröffentlicht wurde, berichteten Forscher bis März 2020 über Hinweise auf aktive Kampagnen, die diesen Patch ausnutzen und versuchen, ein neues DDoS-Botnet einzurichten. Am Ende des ersten Halbjahres waren 24 % der Organisationen von Ausbeutungsversuchen des Draytek-Vigor-Bugs betroffen.
- **Microsoft Windows SMBGhost RCE Exploit (CVE-2020-0796)** – Ein alarmierender wurmganfälliger Fehler im Microsoft SMB-Protokoll, der Windows 10 und Windows Server 2019 betrifft, wurde im März 2020 der Öffentlichkeit gemeldet. Die ersten PoCs zeigten nur Local Privilege Escalation (LPE)-Fähigkeiten, woraufhin Microsoft schnell einen Patch veröffentlichte. Bis Juni 2020 veröffentlichten die Forscher einen PoC für RCE, der Bedenken hinsichtlich Millionen von nicht gepatchten Computern aufwarf, die ausgebeutet werden könnten. Die US-amerikanische CISA veröffentlichte eine beratende Warnung dass „Cyberakteure mit dem neuen PoC ungepatchte Systeme ins Visier nehmen."

In der ersten Hälfte des Jahres 2020 nutzten 80 % der beobachteten Angriffe Schwachstellen aus, die 2017 und früher gemeldet und registriert wurden. Mehr als 20 % der Angriffe wurden Schwachstellen verwendet, die mindestens sieben Jahre alt waren.

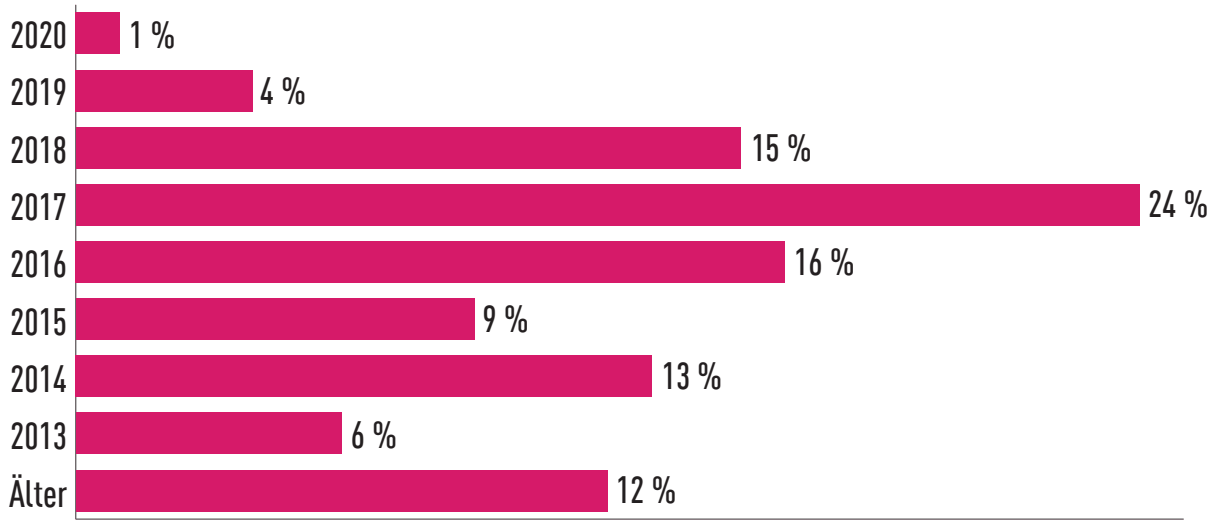



**Abbildung 28**: Prozentualer Anteil der Angriffe, die Schwachstellen ausnutzen, nach Offenlegungsjahr

# Wichtige Cyber-Verstöße (H1 2020)

In der ersten Jahreshälfte 2020 zählten Cyber-Angriffe weiterhin zu einer der größten Bedrohungen für Unternehmen in allen Branchen und Regionen und gefährdeten sensible Informationen von Milliarden Menschen. Nachfolgend finden Sie eine Zusammenfassung der wichtigsten Angriffe in jeder Region.

## Amerika

- **Januar:** Nach der Ermordung des iranischen Generalmajors Qasem Soleimani warnte die US-CISA (Cybersecurity and Infrastructure Agency) offiziell vor einer Zunahme iranischer Cyber-Angriffe, die sich gegen US-Unternehmen und Regierungsbehörden richten. Bei einem solchen Vorfall beschädigten Hacker, die als „Hacker der Iran Cyber Security Group" identifiziert wurden, vorübergehend die Homepage des U.S. Federal Depository Library Program.
- **Januar:** Nach der Weigerung von Travelex, eine Lösegeldforderung von 6 Millionen USD im Austausch gegen Entschlüsselungsschlüssel zu zahlen, drohte die Gruppe hinter der Sodinokibi-Ransomware (alias REvil) damit, 5 GB an persönlichen Kundendaten zu verkaufen, die vor der Verschlüsselung gestohlen und exfiltriert worden waren, und setzte das Unternehmen damit einem GDSVO-Verfahren aus.
- **Januar:** Die Flughafenbehörde von Albany County (NY) gab bekannt, dass sie Opfer eines Sodinokibi-Ransomware-Angriffs wurde, wobei ihre Server und Backup-Systeme verschlüsselt wurden.
- **Februar:** Die US Federal Trade Commission warnte vor Phishing-Angriffen im Zusammenhang mit den Ängsten um das Coronavirus, bei denen E-Mails und SMS mit der Bitte um Spenden oder Beratungen für Angriffe verwendet werden.
- **Februar:** MGM Resorts erlitten eine Datenpanne, durch den die Namen, Adressen und Passnummern von über 10,6 Millionen Gästen offengelegt wurden. Die Datenpanne geht auf einen Sicherheitsvorfall zurück, der sich im vergangenen Jahr ereignete. Zu den Betroffenen gehörten Geschäftsreisende, Journalisten, die an Tech-Konferenzen teilnahmen, CEOs, Regierungsbeamte und Prominente wie Justin Bieber und Twitter-Gründer Jack Dorsey.
- **März:** Cyberkriminelle missbrauchen weiterhin die Angst bezüglich des COVID-19-Ausbruchs und verbreiten Instanzen von AZORult-Infostealer und nutzen dabei bevorzugt eine Anwendung für die Coronavirus-Heatmap. Die App zeigt eine legitime Coronavirus-Karte an, während der Infostealer im Hintergrund läuft.
- **März:** Die Betreiber hinter der Sodinokibi-Ransomware behaupten, dass sie im Besitz von 70.000 Finanz- und Arbeitsdokumenten sowie 60.000 Kundendatensätzen des US-Modehauses Kenneth Cole sind. Die Betreiber haben einen Teil der Daten veröffentlicht und drohen mit der Freigabe aller Daten, falls das Modehaus sich weigert, Lösegeld zu zahlen.
- **April:** Die Marriott-Hotels haben einen Sicherheitsverstoss aufgedeckt, von dem 5,2 Millionen Gäste betroffen sind. Das Unternehmen informierte die Gäste per E-Mail und stellte den Betroffenen Überwachungsdienste für personenbezogene Informationen zur Verfügung. Marriott wurde im vergangenen Jahr zu einer Geldstrafe von 123 Millionen Dollar verurteilt, nachdem im Jahr 2018 insgesamt 327 Millionen Datensätze geknackt worden waren.

- **April:** Hammersmith Medicines Research LTD (HMR), ein Forschungsunternehmen, das für die Durchführung von Lebendversuchen mit Coronavirus-Impfstoffen bereitsteht, erlitt durch die Maze-Ransomware eine Datenpanne. Die HMR beschloss, das Lösegeld nicht zu zahlen, woraufhin die gestohlenen Daten eine Woche später auf der „News"-Website des Angreifers veröffentlicht wurden. Der Angriff hat die Identitätsdokumente und Testergebnisse der Freiwilligen kompromittiert, darunter positive HIV- und Drogentests.

- **Mai:** Check Point Research hat einen zielgerichteten Angriff auf ein multinationales Konglomerat entdeckt. Der Mobile Device Manager (MDM)-Server des Unternehmens wurde kompromittiert und zur Installation des Banking-Trojaners Cerberus auf den Mobilgeräten der Mitarbeiter verwendet. Diese neue Variante von Cerberus verfügt über verbesserte RAT-Fähigkeiten und kann umfangreiche Daten einschließlich Zugangsdaten, SMS-Nachrichten (zusammen mit Zwei-Faktor-Authenticaiton-SMS-Codes)
und mehr exfiltrieren.

- **Juni:** Die US-amerikanische NSA warnte davor, dass die russische Sandworm-APT-Gruppe, ein Zweig des russischen Militärgeheimdienstes, seit August letzten Jahres eine Schwachstelle im Exim-Mailverkehr-Agenten ausnutzt und ihn mit Fähigkeiten zur Remote-Codeausführung ausstattet. Es wird angenommen, dass Sandworm für die Netzstörungen in der Ukraine im Jahr 2015 verantwortlich ist.

## Europa, Naher Osten und Afrika (EMEA)

- **Januar:** Bretagne Télécom, ein französisches Unternehmen für Cloud-Services, erlitt einen DoppelPaymer-Ransomware-Angriff. Die Angreifer haben die damals ungepatchte Schwachstelle in Citrix (CVE-2019-19781) erfolgreich ausgenutzt und es geschafft, 148 Rechner zu verschlüsseln. Die Angreifer haben während des Angriffs einige Daten gestohlen und Muster davon auf der kürzlich von DopplePaymer gestarteten Datenleck-Website veröffentlicht.

- **Februar:** Die kroatische Tankstellenkette INA-Gruppe wurde Opfer der „CLOP"-Ransomware. Der Angriff betraf den normalen Betrieb wie die Ausgabe von Mobiltelefongutscheinen und elektronischen Vignetten sowie die Bezahlung von Rechnungen von Versorgungsunternehmen.

- **März:** Die weltweite Angst vor der Coronavirus-Epidemie wird nach wie vor für bösartige Cyber-Operationen ausgenutzt. Punktforschung prüfen berichtete über Tausende von neu registrierten Coronavirus-bezogenen Domains, die im Vergleich zu anderen Domains mit einer 50 % höheren Wahrscheinlichkeit bösartig sind. CPR enthüllte auch eine Trickbot-Kampagne, bei der ein gefälschtes Warndokument für italienische Benutzer verwendet wurde.

- **März:** Der in Großbritannien ansässige Telekommunikationsanbieter Virgin Media berichtete von einem einjährigen Datenleck, bei dem die personenbezogenen Daten von 900.000 Kunden offengelegt wurden, was auf die Fehlkonfiguration einer Marketingdatenbank zurückzuführen war.

- **April:** Travelex entschied sich zur Zahlung von 2,3 Millionen USD für die Freigabe seiner Informationen. Travelex, ein in London ansässiges Devisenunternehmen, wurde wochenlang aufgrund eines Ransomware-Angriffs der Sodinokibi-Gang lahmgelegt. Travelex führte in den letzten Wochen Verhandlungen mit der Gruppe, bis eine einvernehmlich vereinbarte Zahlung zustande kam.

- **April:** Der portugiesische Stromversorger Energias de Portugal (EDP) wurde Opfer der Ragnar-Locker-Ransomware. Die Angreifer forderten 1.580 Bitcoin, den Gegenwert von 10,9 Millionen US-Dollar, für die Wiederbeschaffung von 10 TB gestohlener Daten. Um zu beweisen, dass sie im Besitz der Unternehmensdaten waren, ließen die Bedrohungsakteure Daten aus dem KeePass-Passwortmanager der EDP an die Öffentlichkeit gelangen, die die Login-Berechtigungsnachweise, Konten, URLs und Notizen der Mitarbeiter enthielten.

- **April:** Sonatrach, Algeriens nationale Ölgesellschaft, ist das jüngste Opfer der Maze-Ransomware-Gruppe. Als Teil ihrer Strategie der doppelten Erpressung veröffentlichten die Angreifer die Investitionspläne, Finanzen und andere Einzelheiten von Sonatrach auf einer speziellen Website und drohten damit, zusätzliche Informationen zu veröffentlichen, sofern kein Lösegeld gezahlt werde.

- **Mai:** Ein fehlkonfigurierter Elasticsearch-Server der französischen Zeitung Le Figaro legte über 8 TB an Daten offen, die 7,4 Milliarden Datensätze mit PII (persönlich identifizierbare Informationen) von Reportern, Angestellten und mindestens 42.000 Benutzern enthielten.

- **Mai:** Das britische National Cyber Security Centre (NCSC) warnte vor gezielten Cyber-Angriffen auf britische Universitäten und wissenschaftliche Einrichtungen, die an der COVID-19-Forschung beteiligt sind.

- **Juni:** Die Hacker richteten sich gegen Führungskräfte einer deutschen Task Force, die Gesichtsmasken und medizinische Ausrüstung für den Einsatz gegen COVID-19 lieferten. Die Hacker starteten eine Spear-Phishing-Kampagne, um Microsoft-Anmeldedaten zu stehlen, die sich gegen mehr als 100 Führungskräfte in 40 Organisationen richtete.

## Asien-Pazifik (APAC)

- **Januar:** Eine Cyber-Spionagekampagne, die gegen NGOs, politische Organisationen und Regierungsbehörden in Asien gerichtet war, wurde aufgedeckt. Die Aktion, die dem chinesischen APT-Gruppen-Bronzepräsidenten zugeschrieben wird, ist seit mindestens Mitte 2018 aktiv und setzt eine Vielzahl von bekannten und maßgeschneiderten Werkzeugen ein. Der erste Zugriff erfolgt wahrscheinlich über Phishing-E-Mails mit bösartigen Links.

- **Februar:** Der australische Logistik- und Transportkonzern Toll Group wurde Opfer eines gezielten Ransomware-Angriffs, der über 1000 Server betraf und die meisten Dienstleistungen des Unternehmens lahm legte. Die Toll Group gibt an, dass die bei dem Angriff verwendete Ransomware eine Variante von Mailto alias Kokoklock war.

- **März:** APT36, ein in Pakistan ansässiger Bedrohungsakteur, hat die Crimson RAT über eine Spear-Phishing-Kampagne verbreitet, wobei er ein Dokument mit einem Coronavirus-Thema verwendete, das als E-Mail zur Gesundheitsberatung getarnt war. Die RAT stiehlt die Berechtigungsnachweise aus dem Browser des Opfers, erstellt Screenshots, sammelt Informationen über Antiviren-Software, listet laufende Prozesse auf und vieles mehr.

- **März:** Eine Kampagne, die die COVID-19-Pandemie nutzt, um den öffentlichen Sektor in der Mongolei ins Visier zu nehmen, wurde von Check Point Research erkannt. Die Kampagne, die einer mit China verbundenen APT-Gruppe zugeschrieben wird, verwendete Spear-Phishing- und Coronavirus-Dokumente, um einen benutzerdefinierten Trojaner mit Fernzugriff zu installieren.

- **April:** Eine Datenbank mit 400.000 Zahlungskartendatensätzen von südkoreanischen und US-amerikanischen Banken und Finanzunternehmen wurde in ein Hacking-Forum hochgeladen. Die Quelle der Daten bleibt unbekannt.

- **April:** Hacker haben das Login-System von Nintendo missbraucht, was dazu führte, dass die Daten von 160.000 Benutzerkonten offengelegt wurden. Der Verstoß wurde entdeckt, nachdem sich eine Reihe von Benutzern über den Zugriff auf ihre Konten beklagt hatten, viele der gehackten Konten wurden zum Kauf von Spielfunktionen und virtuellen Münzen missbraucht.

- **April:** Bedrohungsakteure haben den bisher unbekannten Trojaner PoetRAT in einer Coronavirus-Kampagne eingesetzt, die sich gegen die aserbaidschanische Regierung und Versorgungsunternehmen richtete. Die über Phishing verbreitete Malware infizierte ICS- und SCADA-Systeme, die zur Steuerung der Windkraftanlagen im Bereich der erneuerbaren Energien eingesetzt werden.

- **Mai:** Check Point Research deckte eine laufende Cyber-Spionage Operation gegen Regierungsstellen in der Region Asien-Pazifik (APAC) auf. Die Operation wird der Naikon APT-Gruppe zugeschrieben und bedient sich einer Hintertür mit der Bezeichnung Aria-body, um die Kontrolle über die Netzwerke der Opfer zu übernehmen. Einer der Angriffsvektoren infizierte eine ausländische Botschaft als Startrampe, um den Angriff über bösartige E-Mails an Regierungsstellen zu verbreiten.

- **Mai:** Unacademy, eine in Indien ansässige Online-Lernplattform, erlitt eine schwerwiegende Datenpanne, bei der die Daten von 22 Millionen Nutzern offengelegt wurden. Die kompromittierten Informationen umfassten Benutzernamen, gehashte Passwörter, Vor- und Nachnamen und andere Kontoprofildaten und wurden in Dark-Net-Foren für 2.000 USD zum Verkauf angeboten.

- **Mai:** Thailands Android-Benutzer wurden von einer neuen Variante von DenDroid mit der Bezeichnung „WolFraT“ ins Visier genommen und von „Wolf Research“ über Messaging-Apps wie WhatsApp, Facebook Messenger und Line betrieben. Die neue Variante führt Spionagefunktionen aus, stiehlt Fotos, Audio, Textnachrichten und mehr.

- **Juni:** Hacker haben eine Domain des japanischen Kryptogeldwechslers CoinCheck gekapert, nachdem es ihnen gelungen war, auf deren Konto bei der Oname.com Domain-Registrierungsstelle zuzugreifen. Die gekaperte Domain wurde dazu verwendet, Spear-Phishing-Angriffe auf Kunden durchzuführen und den Haupt-DNS-Eintrag der Firmendomain zu verändern.

- **Juni:** Die in Delhi ansässige Hack-for-hire-Gruppe BellTroX hat angeblich Tausende von hochkarätigen Einzelpersonen und Hunderte von Organisationen weltweit in einer sieben Jahre andauernden Kampagne im Visier gehabt. Die Gruppe benutzte Phishing-Kits, um sensible Daten von den Opfern zu stehlen und Wirtschaftsspionage im Namen ihrer Kunden zu betreiben.

- **Juni:** Der Betrieb des australischen Getränkeherstellers Lion wurde lahmgelegt da ein Ransomware-Angriff erfolgte. Der Angriff ist der jüngste in einer Reihe von Lösegeldforderungen an australische Unternehmen wie Toll logistics und BlueScope Steel Limited.

# Anhang – Beschreibung von Malware-Familien

- **Agent Tesla –** AgentTesla ist ein fortgeschrittener RAT, der als Keylogger und Passwort-Stealer fungiert und seit 2014 aktiv ist. AgentTesla kann die Tastatureingabe des Opfers überwachen und erfassen, die Systemzwischenablage auslesen, Screenshots erstellen und Anmeldeinformationen stehlen, die zu einer Vielzahl von Software gehören, die auf dem Computer des Opfers installiert ist (einschließlich Google Chrome, Mozilla Firefox und den E-Mail-Client Microsoft Outlook). Agent Tesla wird auf verschiedenen Online-Märkten und in Hacking-Foren verkauft.
- **AZORult –** AZORult ist ein Trojaner, der Daten aus dem infizierten System sammelt und ausfiltriert. Sobald die Malware auf einem System installiert ist (normalerweise von einem Exploit-Kit wie RIG bereitgestellt), kann sie gespeicherte Passwörter, lokale Dateien, Krypto-Wallets und Computer-Profilinformationen an einen Remote-C&C-Server senden. Der im Dark Web verfügbare Gazorp-Builder ermöglicht es jedem, einen AZORult-C&C-Server mit vergleichsweise geringem Aufwand zu hosten.
- **Cerberus –** Cerberus, der im Juni 2019 erstmals öffentlich zu sehen war, ist ein Remote Access Trojaner mit spezifischen Banking-Overlay-Funktionen für Android-Geräte. Cerberus arbeitet in einem Malware-as-a-Service (MaaS)-Modell und tritt damit an die Stelle von auslaufenden Bankern wie Anubis und Exobot. Er verfügt über Funktionen wie SMS-Kontrolle, Keylogging, Audioaufzeichnung, Standorterfassung und mehr.
- **Clop –** Clop ist eine Ransomware, die erstmals Anfang 2019 entdeckt wurde und sich vor allem gegen große Firmen und Konzerne richtet. Sie wurde bei einem Angriff auf die niederländische Universität von Maastricht eingesetzt, den einige Forscher mit der russischen Cyberkriminalitätsgruppe TA505 in Verbindung brachten. Im Laufe des Jahres 2020 begann Clop die Strategie einer doppelten Erpressung, bei der die Angreifer nicht nur die Daten des Opfers verschlüsseln, sondern auch damit drohen, gestohlene Informationen zu veröffentlichen, wenn keine Lösegeldforderungen erfüllt werden.
- **Coinhive –** Coinhive ist ein heute nicht mehr existierender, einst populärer Cryptomining-Dienst, der entwickelt wurde, um unautorisiertes Online-Mining der Monero-Cryptowährung durchzuführen, wenn ein Benutzer eine bestimmte Webseite besucht. Das eingepflanzte JavaScript verwendet einen großen Teil der Rechenressourcen der Endbenutzer-Maschinen, was sich nachteilig auf die Leistung auswirkt.
- **DanaBot –** Danabot ist ein in Delphi geschriebener modularer Banken-Trojaner, der auf die Windows-Plattform abzielt. Die Malware, die erstmals 2018 aufgetreten ist, wird über bösartige Spam-E-Mails verbreitet. Sobald ein Gerät infiziert ist, lädt die Malware aktualisierten Konfigurationscode und andere Module vom C&C-Server herunter. Zu den verfügbaren Modulen gehören ein „Sniffer" zum Abfangen von Zugangsdaten, ein „Stealer" zum Stehlen von Passwörtern aus gängigen Anwendungen, ein „VNC"-Modul zur Fernsteuerung und vieles mehr.
- **DarkGate –** DarkGate ist eine multifunktionale Malware, die seit Dezember 2017 aktiv ist und Ransomware, Diebstahl von Zugangsdaten, RAT und Kryptomining kombiniert. DarkGate ist hauptsächlich auf Windows-Betriebssysteme ausgerichtet und setzt eine Vielzahl von Ausweichtechniken ein.
- **DopplePaymer –** DopplePaymer ist eine Variante der 2019 entdeckten BitPaymer-Ransomware. Sie war an mehreren hochkarätigen gezielten Angriffen beteiligt, darunter Angriffe auf die Stadt Florenz, Alabama und Bretagne Télécom. Sie wird in der Regel als letzte Phase nach einem erfolgreichen Eindringen in das Netzwerk der Opfer eingesetzt. DoppelPaymer richtet sich vor allem an mittlere bis große Unternehmen und fordert hohe Lösegelder. Im Jahr 2020 begannen die Betreiber von DoppelPaymer mit der Strategie einer doppelten Erpressung, bei der sie nicht nur die Daten des Opfers verschlüsseln, sondern auch damit drohen, gestohlene Informationen zu veröffentlichen, wenn keine Lösegeldforderungen erfüllt werden.
- **Dridex –** Dridex ist ein Banken-Trojaner, der auf die Windows-Plattform abzielt. Er wird durch Spam-Kampagnen und Exploit Kits verbreitet und ist auf WebInjects angewiesen, um Bankdaten abzufangen und an einen vom Angreifer kontrollierten Server umzuleiten. Dridex kontaktiert einen Remote-Server, sendet Informationen über das infizierte System und kann auch zusätzliche Module zur Fernsteuerung herunterladen und ausführen.
- **Emotet –** Emotet ist ein fortgeschrittener, sich selbst verbreitender und modularer Trojaner. Emotet wurde früher als Banken-Trojaner und jetzt als Verteiler für andere Malware oder bösartige Kampagnen eingesetzt. Er verwendet mehrere Methoden zur Aufrechterhaltung von Persistenz- und Ausweichtechniken, um eine Erkennung zu vermeiden. Darüber hinaus kann Emotet auch durch Phishing-Spam-E-Mails mit bösartigen Anhängen oder Links verbreitet werden.
- **FormBook –** FormBook ist ein Infostealer für Windows-Betriebssysteme, der erstmals 2016 entdeckt wurde. Es wird als Malware-as-a-Service (MaaS) in Untergrund-Hacking-Foren aufgrund seiner starken Ausweichtechniken und seines relativ niedrigen Preises vermarktet. FormBook sammelt Anmeldeinformationen von verschiedenen Webbrowsern, erstellt Screenshots, überwacht und protokolliert Tastatureingaben und kann gemäß den Anweisungen seines C&C-Servers Dateien downloaden und ausführen.
- **Glupteba –** Glupteba ist eine seit 2011 bekannte Hintertür, die nach und nach zu einem Botnet gereift ist. 2019 umfasste es einen Mechanismus zur Aktualisierung der C&C-Adressen über öffentliche BitCoin-Listen, eine integrierte Browser-Stealer-Funktion und einen Router-Exploiter.
- **Guerilla –** Guerilla ist ein Android-Trojaner, der in mehrere legitime Anwendungen eingebettet ist und zusätzliche bösartige Nutzlast herunterladen kann. Guerrilla generiert betrügerische Werbeeinnahmen für die App-Entwickler.

- **Hawkeye –** Hawkeye ist eine seit 2013 aktive Infostealer-Malware für Windows, die in erster Linie dafür gedacht ist, Benutzerdaten von infizierten Geräten zu stehlen und an einen C&C-Server zu senden. In den letzten Jahren hat sich Hawkeye die Möglichkeit verschafft, zusätzlich zu den ursprünglichen Funktionen wie Passwortdiebstahl von E-Mail- und Webbrowsern sowie Keylogging Screenshots zu erstellen, sich über USB und andere Wege zu verbreiten. Hawkeye wird oft als MaaS (Malware-as-a-Service) vertrieben.
- **Hiddad –** Eine Android-Malware, die legitime Apps neu verpackt und sie an einen Drittanbieter weitergibt. Ihre Hauptfunktion ist die Anzeige von Werbung, wobei sie aber auch Zugriff auf wichtige, im Betriebssystem integrierte Sicherheitsdetails erhalten kann.
- **JSEcoin –** Web-basierter Cryptominer, der entwickelt wurde, um unautorisiertes Online-Mining der Monero-Kryptowährung durchzuführen, wenn ein Benutzer eine bestimmte Website besucht. Das implantierte JavaScript verwendet einen großen Teil der Rechenressourcen der Endbenutzergeräte, um Währungen abzubauen,, was sich nachteilig auf die Systemleistung auswirkt. JSEcoin stellte seine Tätigkeit im April 2020 ein.
- **LokiBot –** LokiBot ist ein Waren-Infostealer für Windows. Es sammelt Anmeldeinformationen aus einer Vielzahl von Anwendungen, Webbrowsern, E-Mail-Clients, IT-Administrationswerkzeugen wie PuTTY und anderen. LokiBot wurde in Hacker-Foren verkauft und es wird angenommen, dass sein Quellcode durchgesickert ist, so dass eine Reihe von Varianten erscheinen konnten. Er wurde erstmals im Februar 2016 identifiziert.
- **Maze –** Maze ist eine Ransomware, die erstmals Mitte 2019 aufgetaucht ist und als erste Ransomware die Strategie der doppelten Erpressung praktizierte. Maze-Betreiber haben eine spezielle Webseite eingerichtet, auf der sie nicht nur die Daten der Opfer verschlüsseln, sondern auch gestohlene sensible Informationen von Opfern veröffentlichen, die sich weigerten, das Lösegeld zu zahlen. Viele andere Bedrohungsgruppen folgten dieser Strategie.
- **Mirai –** Mirai ist eine berühmte Internet-of-Things (IoT)-Malware, mit der anfällige IoT-Geräte wie Webkameras, Modems und Router erfasst und in Bots verwandelt werden. Das Botnet wird von seinen Betreibern genutzt, um massive DDOS (Distributed Denial of Service)-Angriffe durchzuführen. Das Mirai Botnet tauchte erstmals im September 2016 auf und machte schnell Schlagzeilen aufgrund einiger groß angelegter Angriffe, darunter ein massiver DDoS-Angriff, mit dem das gesamte Land Liberia außer Gefecht gesetzt wurde, und ein DDoS-Angriff auf das Internet-Infrastrukturunternehmen Dyn, das einen erheblichen Teil der Infrastruktur des Internets der Vereinigten Staaten darstellt.
- **Mylobot –** Mylobot ist ein hochentwickeltes Botnet, das im Juni 2018 erstmals auftauchte und mit komplexen Ausweichtechniken ausgestattet ist, darunter Anti-VM-, Anti-Sandbox- und Anti-Debugging-Techniken. Das Botnet ermöglicht es einem Angreifer, die vollständige Kontrolle über das System des Benutzers zu übernehmen und zusätzliche Nutzlast von seinem C&C herunterzuladen.
- **Necro –** Necro ist ein Android Trojan-Dropper. Er kann andere Malware herunterladen, aufdringliche Werbung anzeigen und in betrügerischer Weise für bezahlte Abonnements Gebühren erheben.
- **NRSMiner –** NSRMiner ist ein Kryptominer, der um November 2018 auftauchte und sich vor allem in Asien, insbesondere in Vietnam, China, Japan sowie Ecuador verbreitete. Nach der Erstinfektion nutzt er den berühmten EternalBlue SMB-Exploit, um sich auf andere anfällige Computer in internen Netzwerken zu verbreiten, und beginnt schließlich mit dem Abbau der Monero (XMR)-Kryptowährung.
- **Phorpiex –** Phorpiexecro ist ein Botnet (alias Trik), das seit 2010 aktiv ist und in der Spitze mehr als eine Million infizierte Wirte gesteuert hat. Es ist dafür bekannt, andere Malware-Familien über Spam-Kampagnen zu verbreiten sowie groß angelegte Spam- und Sextorsionskampagnen zu unterstützen.
- **PreAmo –** PreAMo ist eine Clicker-Malware für Android-Geräte, die erstmals im April 2019 gemeldet wurde. PreAMo generiert Einnahmen, indem es den Benutzer imitiert und ohne dessen Wissen auf Werbeanzeigen klickt. Die auf Google Play gefundene Malware wurde über 90 Millionen Mal über sechs verschiedene mobile Anwendungen heruntergeladen.
- **Qbot –** Qbot AKA Qakbot ist ein Banken-Trojaner, der 2008 erstmals auftauchte. Er wurde entwickelt, um die Bankdaten und Tastatureingaben eines Benutzers zu stehlen. Qbot setzt verschiedene Anti-VM-, Anti-Debugging- und Anti-Sandbox-Techniken ein, um die Analyse zu erschweren und einer Entdeckung zu entgehen.
- **Ragnar Locker –** Ragnar Locker ist eine erstmals im Dezember 2019 entdeckte Ransomware. Sie setzt ausgeklügelte Umgehungstechniken ein, einschließlich der Bereitstellung als virtuelle Maschine auf Zielsystemen, um ihre Aktivität zu verbergen. Ragnar wurde bei einem Angriff gegen Portugals nationalen Stromversorger in einem Akt doppelter Erpressung eingesetzt, wobei die Angreifer sensible Daten veröffentlichten, die dem Opfer gestohlen worden waren.
- **Ramnit –** Ramnit ist ein modularer Banken-Trojaner, der erstmals 2010 entdeckt wurde. Ramnit stiehlt Informationen zu Websitzungen und ermöglicht es den Betreibern, Kontodaten für alle vom Opfer genutzten Dienste zu stehlen, einschließlich Bankkonten, Unternehmenskonten und Konten in sozialen Netzwerken. Der Trojaner verwendet sowohl hartkodierte Domains als auch von einem DGA (Domain Generation Algorithmus) generierte Domains, um den C&C-Server zu kontaktieren und zusätzliche Module herunterzuladen.

- **Remcos –** Remcos ist eine RAT, die 2016 erstmals in freier Wildbahn aufgetreten ist. Remcos verbreitet sich über bösartige Microsoft Office-Dokumente, die an SPAM-E-Mails angehängt sind und ist so konzipiert, dass es die Microsoft Windows-UAC-Sicherheit umgeht und Malware mit hohen Berechtigungen ausführt.
- **RiGeK –** RigEK, das älteste und bekannteste der derzeit in Betrieb befindlichen Exploit Kits, existiert seit Mitte 2014. Es wird in Hacker-Foren und über das TOR-Netzwerk angeboten. Einige „Unternehmer" bieten inzwischen sogar Infektionen für Malware-Entwickler in kleinen Mengen an, die sich bislang keine vollumfänglichen Dienste leisten können. RigEK hat sich im Laufe der Jahre weiterentwickelt, um alles von AZORult und Dridex bis hin zu wenig bekannter Ransomware und Cryptominern zu liefern.
- **RubyMiner –** RubyMiner wurde erstmals im Januar 2018 im Einsatz entdeckt und zielt sowohl auf Windows- als auch auf Linux-Server ab. RubyMiner sucht nach anfälligen Webservern (wie PHP, Microsoft IIS und Ruby on Rails), die für das Cryptomining mit dem Open-Source Monero Miner XMRig verwendet werden können.
- **Ryuk –** Ryuk ist eine Ransomware, die von TrickBot-Gangs bei gezielten und geplanten Angriffen gegen mehrere Organisationen weltweit eingesetzt wird. Die Ransomware wurde ursprünglich von der Hermes-Ransomware abgeleitet, deren technische Fähigkeiten relativ gering sind und die einen einfachen Dropper und ein unkompliziertes Verschlüsselungsschema umfasst. Dennoch war Ryuk in der Lage, den Zielorganisationen schweren Schaden zuzufügen und sie zu extrem hohen Lösegeldzahlungen in Bitcoin zu zwingen. Im Gegensatz zur meisten Ransomware, die systematisch über massive Spam-Kampagnen und Exploit-Kits verbreitet wird, wird Ryuk ausschließlich für gezielte Angriffe verwendet.
- **Sodinokibi –** Sodinokibi ist eine Ransomware-as-a-Service, die ein „Partnerprogramm" betreibt und 2019 erstmals „in freier Wildbahn" entdeckt wurde. Sodinokibi verschlüsselt Daten im Verzeichnis des Benutzers und löscht Schattenkopien, um die Datenwiederherstellung zu erschweren. Darüber hinaus verwenden die Partner von Sodinokibi verschiedene Taktiken, um sie durch Spam und Server-Exploits sowie durch Hacking in Backends von Managed Service Providern (MSPs) und durch Malvertising-Kampagnen zu verbreiten, die an das RIG-Exploit-Kit weitergeleitet werden.
- **TrickBot –** TrickBot ist ein modularer Banken-Trojaner, der auf die Windows-Plattform abzielt und meist über Spam-Kampagnen oder andere Malware-Familien wie Emotet verbreitet wird. Trickbot sendet Informationen über das infizierte System und kann darüber hinaus beliebige Module aus einer Vielzahl von verfügbaren Modulen herunterladen und ausführen, darunter ein VNC-Modul zur Fernsteuerung und ein SMB-Modul zur Verbreitung innerhalb eines kompromittierten Netzwerks. Sobald ein Rechner infiziert ist, nutzt die Trickbot-Gang, die Bedrohungsakteure hinter dieser Malware, dieses breite Spektrum an Modulen nicht nur, um Bankdaten vom Ziel-PC zu stehlen, sondern auch zur Querverschiebung und Aufklärung über die Zielorganisation selbst, bevor sie einen unternehmensweiten gezielten Ransomware-Angriff durchführen.
- **Ursnif –** Ursnif ist eine Variante des Gozi-Banken-Trojaners für Windows, dessen Quellcode online weitergegeben wurde. Er verfügt über Man-in-the-Browser-Fähigkeiten, um Bankinformationen und Zugangsdaten für beliebte Online-Dienste zu stehlen. Darüber hinaus kann er Informationen aus lokalen E-Mail-Clients, Browsern und Kryptowährungs-Brieftaschen stehlen. Schließlich kann er zusätzliche Dateien auf das infizierte System herunterladen und ausführen.
- **WannaMine –** WannaMine ist ein hoch entwickelter Monero-Cryptomining-Wurm, der sich mithilfe des EternalBlue-Exploits verbreitet. WannaMine implementiert einen Verbreitungsmechanismus und Persistenztechniken, indem es die Abonnements für permanente Ereignisse der Windows Management Instrumentation (WMI) nutzt.
- **xHelper –** xHelper ist eine Android-Malware, die hauptsächlich aufdringliche Popup-Werbung und Benachrichtigungs-Spam zeigt. Nach der Installation ist sie aufgrund seiner Fähigkeit zur Neuinstallation sehr schwer zu entfernen. Seit diese erstmals im März 2019 entdeckt wurde, hat sie inzwischen über 45.000 Geräte infiziert.
- **XMRig –** XMRig ist eine Open-Source-CPU-Mining-Software, die für das Mining von Monero-Kryptowährung verwendet wird. Bedrohungsakteure missbrauchen diese Open-Source-Software häufig durch die Integration in ihre Malware, um illegales Mining auf den Geräten der Opfer durchzuführen.
- **Zeus –** Zeus ist ein weit verbreiteter Windows-Trojaner, der hauptsächlich zum Stehlen von Bankdaten verwendet wird. Wenn ein Computer angegriffen wird, sendet die Malware Informationen, wie z. B. die Konto-Berechtigungsnachweise, mithilfe einer Kette von C&C-Servern an die Angreifer.


# KONTAKTIEREN SIE UNS

**Worldwide Headquarters**
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 |
E-Mail: info@checkpoint.com

**U.S. Headquarters**
959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-439 | 650-628-2000 | Fax: 650-654-4233

**checkpoint.com**