Microsoft Security Intelligence Report

AUSGABE 23

Microsoft

Inhaltsverzeichnis

Vorwort

Willkommen bei der 23. Ausgabe des *Microsoft Security Intelligence Report*, einer zweijährigen Publikation, die Microsoft für Kunden, Partner und die Branche erstellt. Der Zweck dieses Berichts besteht darin, Organisationen über den aktuellen Status von Bedrohungen, empfohlene bewährte Methoden und Lösungen zu informieren.

Was den *Microsoft Security Intelligence Report* von anderen unterscheidet, ist das Volumen und die Vielfalt der Microsoft-Analyse. Diese Analyse umfasst Cloud-Services für Unternehmen und einzelne Verbraucher, von Websites bis zu Identitäten und von E-Mails bis zu Endpunkten. Dazu gehören z. B. 400 Milliarden gescannte E-Mail-Nachrichten, 450 Milliarden Authentifizierungen und mehr als 18 Milliarden Webseiten-Scans pro Monat.

Diese Ausgabe konzentriert sich auf drei Themen, die sich aus den seit Februar 2017 gesammelten Daten ergeben: Botnets, Hacker-Methoden und Ransomware.

Microsoft entwickelt auf seinen Plattformen weiterhin neue Funktionen, die Machine Learning, Automatisierung und fortschrittliche Echtzeit-Erkennungstechniken nutzen. Unser Ziel ist es, die Fähigkeit unserer Kunden zu stärken, sich nicht nur vor sich ausweitenden, ausgefeilten Bedrohungen zu schützen, sondern einen Angriff auch schnell zu erkennen und zu reagieren.

Wir hoffen, dass die Leser die in diesem Bericht bereitgestellten Daten, Erkenntnisse und Anleitungen nützlich finden, um ihre Organisationen, ihre Software und ihre Benutzer zu schützen.

Microsoft Security

Executive Summary

Auffallende Trends in diesem Jahr:

Über die Vorfälle hinaus, die im Jahr 2017 die Schlagzeilen beherrschten, hat Microsoft die Threat Intelligence analysiert, die von der weltweiten Kundenbasis in mehr als 100 Ländern und auf Millionen von Computern erfasst wurde. Diese Analyse hat drei interessante Themen hervorgehoben:

1. **Botnets** beeinflussen weiterhin Millionen von Computern weltweit und infizieren sie mit alter und neuer Schadsoftware. Dieser Bericht enthält Informationen über das bekannte Botnet Gamarue, an dessen Zerschlagung Microsoft im Jahr 2017 beteiligt war.

2. **Hacker hatten es auf die einfachen Ziele abgesehen.** Wenn Cyberkriminalität ein Geschäft ist, haben Hacker sich im Jahr 2017 auf kostengünstige Angriffsmethoden mit potenziell hohen Erträgen konzentriert.

3. **Ransomware** ist immer noch eine Kraft, mit der gerechnet werden muss und die in absehbarer Zeit nicht nachlassen wird.

Der Bereich der Sicherheit hat natürlich ein arbeitsreiches Jahr hinter sich, und dieser Bericht soll nicht alle Neuigkeiten des Jahres zusammenzufassen. Stattdessen behandelt er diese drei Trends und stellt Kontext auf Basis der Threat Intelligence bereit, die von Microsoft-Forschungsteams aus mehreren Quellen, einschließlich On-Premises- und Cloud-Lösungen und -Services, zusammengetragen wird. Wir sprechen auch Empfehlungen zur Abwehr und Reaktion auf Bedrohungen aus und beleuchten für zusätzliche Informationen weitere Ressourcen.

ABSCHNITT 1

Zerschlagen von Botnets

Cyberkriminelle infizieren weiterhin unerbittlich Computer und beteiligen sich an Botnet-Aktivitäten, um sich eine große Infrastruktur zu verschaffen, die sie nach sensiblen Daten durchforsten und zu Geld machen können, wie es bei Bedrohungen mit Ransomware der Fall ist. Die Verteidigung gegen Botnet-Aktivitäten ist keine einfache Aufgabe und erfordert wie in den vergangenen Jahren massive Anstrengungen und die Zusammenarbeit von privaten und öffentlichen Organisationen.

Ein Bot ist ein Programm, mit dem ein Angreifer die Kontrolle über einen infizierten Computer übernehmen kann. Ein Botnet ist ein Netzwerk von infizierten Computern, die mit Command-and-Control-Servern kommunizieren. Cyberkriminelle nutzen Botnets für eine Vielzahl von Online-Angriffen, z. B. für die Verwendung von Spam, die Durchführung von Denial-of-Service-Angriffen auf Websites, die Verbreitung von Schadsoftware, die Unterstützung von Klickbetrug bei Online-Werbung und vieles mehr.

Bis zurück zum Conficker-Botnet im November 2008 konnte die Microsoft Digital Crimes Unit (DCU) die Bekämpfung mehrerer Botnets koordinieren. Am 29. November 2017 leitete die Microsoft Digital Crimes Unit (DCU) die Zerschlagung des Gamarue-Botnets (auch Andromeda genannt).

Analyse und Erläuterung

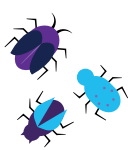
Die Zerschlagung des Gamarue-Botnets war der Höhepunkt einer Reise, die im Dezember 2015 begann, als das Microsoft Windows Defender-Forschungsteam und die Microsoft Digital Crimes Unit für Gamarue eine Coordinated Malware Eradication (CME)-Kampagne zur koordinierten Bekämpfung von Schadsoftware startete. In Kooperation mit der Internetsicherheitsfirma ESET unterzogen die Sicherheitsforscher der Microsoft Digital Crimes Unit und Teams der Windows Defender Security Intelligence die Schadsoftware Gamarue und ihre Infrastruktur einer gründlichen Erforschung. Microsoft analysierte mehr als 44.000 Malware-Muster und deckte so die ausgedehnte Infrastruktur des Botnets auf. Strafverfolgungsbehörden auf der ganzen Welt wurden detaillierte Informationen über diese Infrastruktur zur Verfügung gestellt, darunter:

1.214

Domänen und IP-Adressen der Command-and-Control-Server des Botnets

464

verschiedene Botnets



80+

zugehörige Malware-Familien

Die koordinierte weltweite Operation führte am 29. November 2017 zur Trennung der Botnet-Server und damit zur Zerschlagung einer der größten Malware-Operationen der Welt.

Die Zerschlagung des Gamarue-Botnets kam durch die Kooperation von Microsoft mit Strafverfolgungsbehörden rund um den Globus zustande, einschließlich des US-amerikanischen Federal Bureau of Investigation, der Zentralen Kriminalinspektion Lüneburg aus Deutschland und des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität von Europol.

Seit 2011 hat Gamarue sich über fünf Versionen von Schadsoftware weiterentwickelt und eine Vielzahl anderer Bedrohungen verbreitet, darunter:

- Petya- und Cerber-Ransomware
- Kasidet- Schadsoftware (auch als Neutrino-Bot bekannt), die für DDoS-Angriffe eingesetzt wird
- Lethic, ein Spam-Bot
- Schadsoftware für Informationsdiebstahl, unter anderem Ursnif, Carberp und Fareit

Bis zur Zerschlagung war Gamarue eine sehr aktive Familie von Schadsoftware und nichts deutete auf ein Nachlassen hin. Seit der Zerschlagung haben mit Gamarue infizierte Geräte mit 23 Millionen verschiedenen IP-Adressen eine Verbindung mit dem DCU-Sinkhole hergestellt, was die weltweite Verbreitung des Gamarue-Botnets herausstreicht (Abbildung 1).

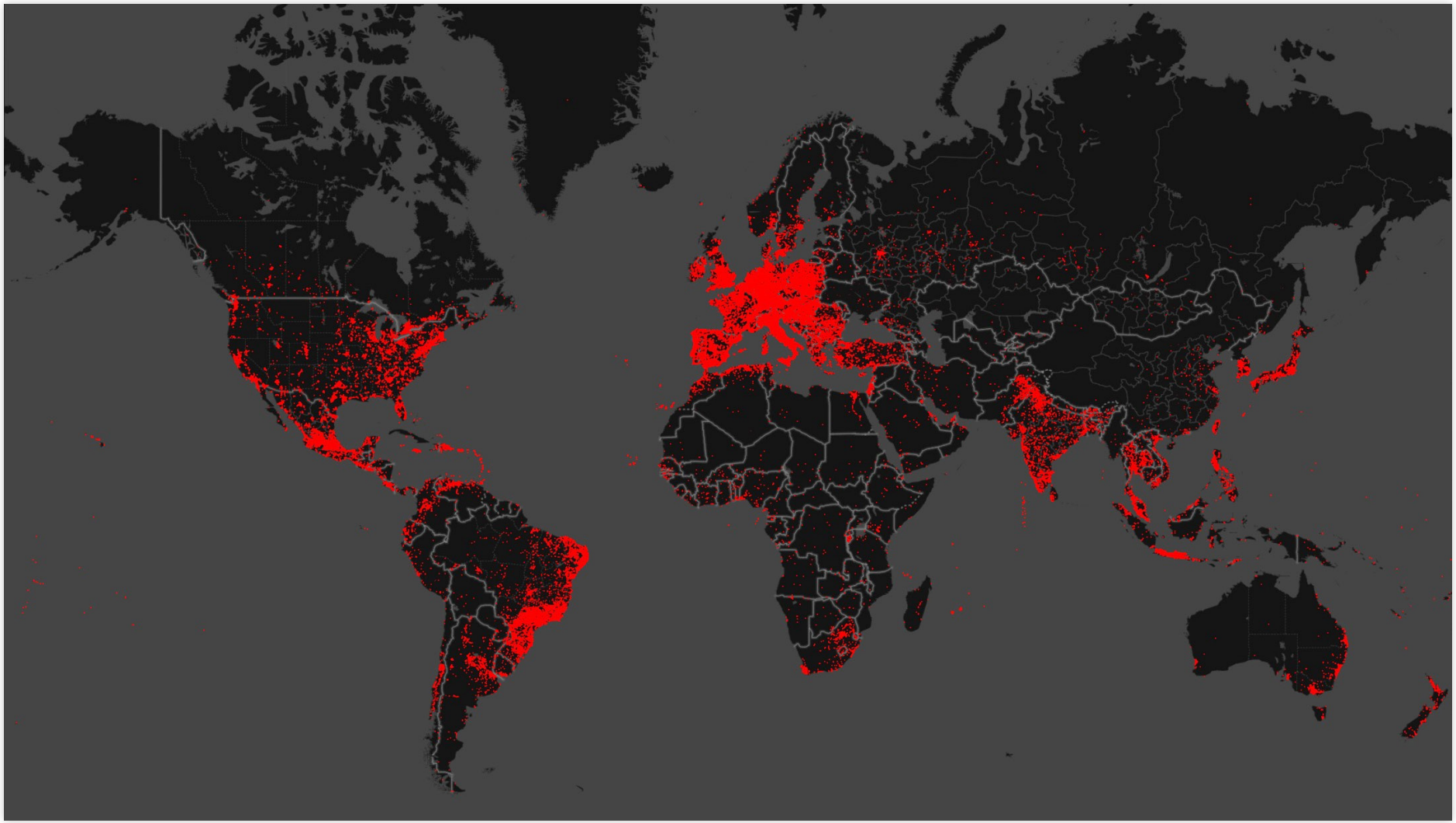


***Abbildung 1**. Telemetrische DCU-Daten zeigen die weltweite Verbreitung von infizierten Geräten von Dezember 2017 bis Januar 2018*

Das Gamarue-Botnet

Gamarue ist auf dem Untergrundmarkt der Cyberkriminalität als Andromeda-Bot bekannt. Wie viele andere Bots auch wurde Gamarue als Unterwelt-Set beworben, das Hacker käuflich erwerben können.

Das Gamarue-Set enthält folgende Komponenten:

- Einen Bot-Builder, der die Binärdatei der Schadsoftware erstellt, mit der Computer infiziert werden
- Eine Command-and-Control-Anwendung, bei der es sich um eine PHP-basierte Dashboard-Anwendung handelt, mit der Hacker die Bots verwalten und steuern können
- Dokumentation zum Aufbau eines Gamarue-Botnets

Die Entwicklung des Gamarue-Bots war Gegenstand zahlreicher gründlicher Analysen von Sicherheitsforschern. Zum Zeitpunkt der Zerschlagung waren fünf aktive Gamarue-Versionen bekannt: 2.06, 2.07, 2.08, 2.09 und 2.10. Die neueste und aktivste Version ist die Version 2.10.

***Abbildung 2**. Oberfläche des Gamarue-Bot-Builders*

Modulare Schadsoftware

Gamarue ist modular aufgebaut, seine Funktionalität kann also durch Plug-Ins erweitert werden, die entweder im Set enthalten sind oder separat erworben werden können. Zu den Gamarue-Plug-Ins gehören:

- **Keylogger ($150)**
  Verwendet für die Protokollierung von Tastatureingaben und Mausaktivitäten, um Benutzernamen und Kennwörter, Finanzdaten usw. zu stehlen.
- **Rootkit (im Crime Kit enthalten)**
  Fügt Rootkit-Codes in alle Prozesse ein, die auf dem Computer eines Opfers ausgeführt werden, um für die Persistenz von Gamarue zu sorgen.
- **Socks4/5 (im Set enthalten)**
  Verwandelt den Computer des Opfers in einen Proxyserver, um Schadsoftware oder schädliche Anweisungen für andere Computer im Internet bereitzuhalten.
- **Formgrabber ($250)**
  Erfasst alle Daten, die über Webbrowser (z. B. Chrome, Firefox und Internet Explorer) übermittelt werden.
- **TeamViewer ($250)**
  Ermöglicht es Angreifern unter anderem, den Computer des Opfers remote zu steuern, den Desktop auszuspähen und Dateiübertragungen durchzuführen.
- **Spreader**
  Ermöglicht zusätzlich die Verbreitung der Gamarue-Schadsoftware selbst über Wechseldatenträger (z. B. tragbare Festplatten oder Flash-Laufwerke, die über einen USB-Anschluss verbunden sind). Für die Server, auf die Updates heruntergeladen werden, werden auch Domain Generation Algorithms (DGA) verwendet.

Monetarisierung: Bezahlte Installationen von Schadsoftware

Das wichtigste Ziel von Gamarue besteht darin, andere gängige Familien von Schadsoftware zu verbreiten. Die Installation anderer Schadsoftware erweitert das Spektrum der möglichen Aktionen von Hackern mit dem Netzwerk infizierter Computer. Hacker können auf verschiedene Weise Geld mit Gamarue verdienen. Da es der Zweck von Gamarue ist, andere Schadsoftware zu verbreiten, können Hacker Geld verdienen, indem sie ein Zahlungsmodell verwenden, das auf der Anzahl von Installationen basiert. Mithilfe der Plug-Ins kann Gamarue auch Benutzerinformationen stehlen, und gestohlene Informationen können auf den Untergrundmärkten der Cyberkriminalität an andere Hacker verkauft werden. Der Zugang zu Gamarue-infizierten Computern kann auch verkauft, vermietet, geleast oder zwischen kriminellen Gruppen getauscht werden. Microsoft DCU stellte fest, dass mindestens 80 verschiedene Familien von Schadsoftware durch Gamarue verbreitet wurden. Die drei wichtigsten Klassen von Schadsoftware, die vom Gamarue-Botnet verbreitet wurden, waren Ransomware, Trojaner und Backdoor-Programme.

***Abbildung 3**. Klassen von durch Gamarue verbreiteter Schadsoftware*

Anti-Sandbox-Techniken

Gamarue setzt Anti-AV-Techniken ein, um die Analyse und Erkennung zu erschweren. Vor der Infektion eines Computers überprüft Gamarue eine Liste von Hashes derjenigen Prozesse, die auf dem Computer eines potenziellen Opfers ausgeführt werden. Wenn ein Prozess gefunden wird, der möglicherweise mit Tools zur Schadsoftwareanalyse, wie etwa virtuellen Computern oder Sandbox-Tools, verknüpft ist, infiziert Gamarue den Computer nicht. In älteren Versionen tritt beim Ausführen in einem virtuellen Computer eine gefälschte Nutzlast in Erscheinung.

```
analysis_prog_hash_list dd 99DD4432h    ; DATA XREF: chk_dbg+C8↓r
                                        ; chk_dbg+DD↓r
                                        ; vmwareuser.exe
                dd 2D859DB4h            ; vmwareservice.exe
                dd 64340DCEh            ; vboxservice.exe
                dd 63C54474h            ; vboxtray.exe
                dd 349C9C8Bh            ; sandboxiedcomlaunch.exe
                dd 3446EBCEh            ; sandboxierpcss.exe
                dd 5BA9B1FEh            ; procmon.exe
                dd 3CE2BEF3h            ; regmon.exe
                dd 3D46F02Bh            ; filemon.exe
                dd 77AE10F7h            ; wireshark.exe
                dd 0F344E95Dh           ; netmon.exe
```

***Abbildung 4**. Anti-Sandbox-Assembly-Code von Gamarue*

Manipulation des Betriebssystems

Gamarue versucht, die Betriebssysteme infizierter Computern zu manipulieren, indem die Funktionen Windows-Firewall, Windows Update und Benutzerkontensteuerung deaktiviert werden. Diese Funktionen können erst wieder aktiviert werden, wenn die Gamarue-Infektion vom infizierten Computer entfernt wurde. Die von Gamarue genutzte Manipulation des Betriebssystems funktioniert jedoch nicht unter Windows 10.

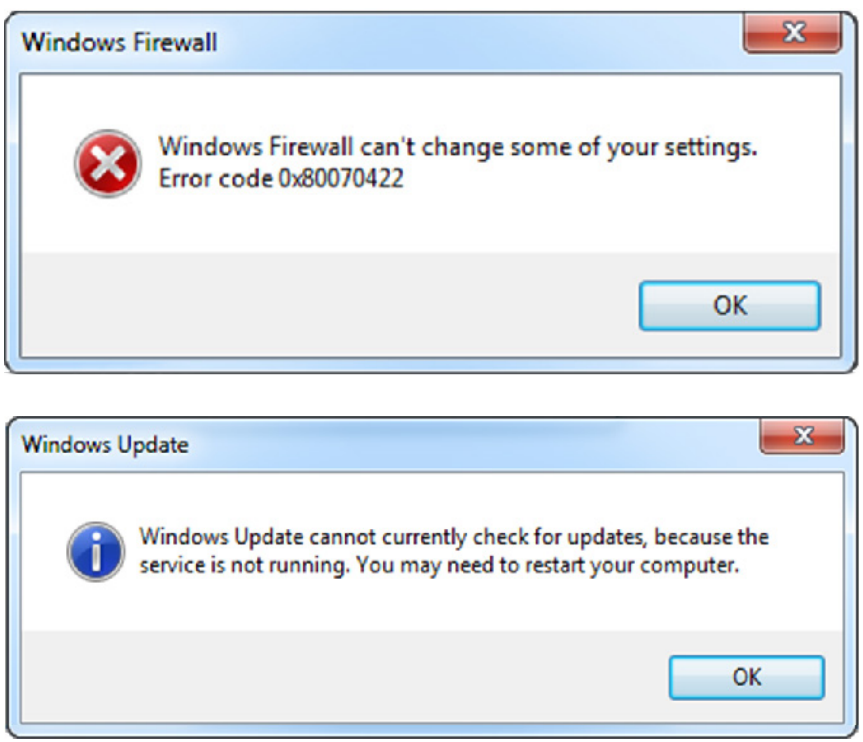


***Abbildung 5**. Deaktivierte Windows-Firewall und Windows Update*

Das Avalanche-Botnet

Das Gamarue Botnet und das Avalanche-Botnet nutzen in gewissem Umfang eine gemeinsame Infrastruktur, um die beiden Familien von Schadsoftware zu steuern und zu kontrollieren. Microsoft DCU unterstützte die weltweiten Strafverfolgungsbehörden bei der Zerschlagung von Avalanche durch technische Forschung und Analyse. DCU arbeitete mit dem Microsoft Windows Defender Security Intelligence-Team zusammen, um die Tools zum Erkennen und Entfernen von Avalanche und anderer Schadsoftware zu entwickeln, die durch das Avalanche-Botnet verbreitet wurde.

Auswirkungen der Zerschlagung

Die weltweite Koordinierung von Forschungs-und Ermittlungsbemühungen ist der Schlüssel zur Zerschlagung einer Malware-Operation von der Größenordnung von Gamarue. Aufgrund dieser Komplexität sind öffentlich-private Partnerschaften zwischen weltweiten Strafverfolgungsbehörden und Partnern aus der Privatwirtschaft für ein erfolgreiches Ergebnis unerlässlich.

Ein wesentlicher Aspekt der Zerschlagung von Gamarue war der Kill-Chain-Effekt, den die Operation auf die Verbreitung von 80 weiteren Familien von Schadsoftware hatte. Durch Zerschlagung einer bedeutenden Familie von Schadsoftware wie Gamarue können wir potenzielle Schäden für Millionen von Nutzern weltweit verhindern und beginnen, die Geräte der Opfer wiederherzustellen.

Seit der Botnet-Zerschlagung im November 2017 verzeichnete das von Microsoft geschaffene Sinkhole einen Rückgang der Gamarue-Opfer weltweit um 30 %, wie in Abbildung 6 dargestellt ist.

Microsoft arbeitet weiterhin mit Partnern aus der öffentlichen und privaten Industrie zusammen, um die betroffenen Geräte über das Cyber Threat Intelligence-Programm der Microsoft Digital Crimes Unit zu identifizieren, damit die Beseitigung der Auswirkungen beschleunigt werden kann.

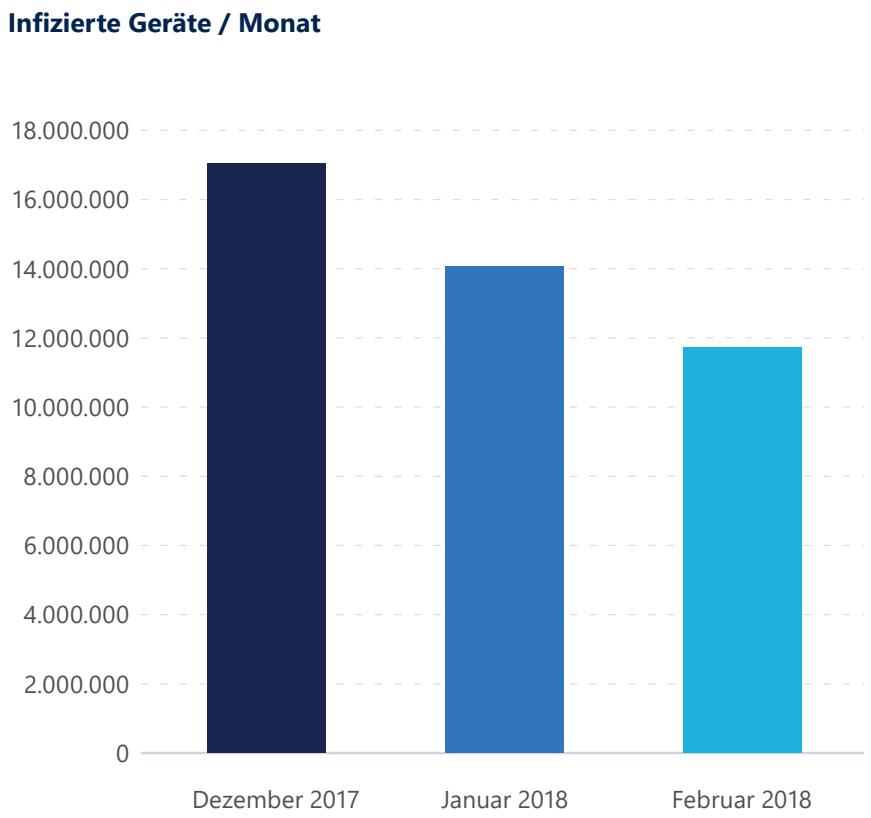


***Abbildung 6**. Rückgang der mit Gamarue-Schadsoftware infizierten Geräte nach der Botnet-Zerschlagung*

Lösungen und Empfehlungen

Um Gamarue und andere Schadsoftware zu erkennen und Computer davor zu schützen, verwenden Sie Sicherheitslösungen, die fortschrittliche Machine-Learning-Modelle sowie generische und heuristische Techniken einsetzen. Microsoft setzt die gemeinsamen Anstrengungen fort, mit Gamarue infizierte Computer zu säubern, und stellt ein einmaliges Paket mit Mustern bereit (über die Virus Information Alliance), um Organisationen beim Schutz ihrer Mitarbeiter und Kunden zu unterstützen.

ABSCHNITT 2

Hacker wenden sich den einfachen Aufgaben zu

Da die Kosten für die Umgehung von Sicherheitsmaßnahmen steigen, nutzen Hacker die Vorteile von „niedrig hängenden Früchten" (z. B. Infrastrukturen und Anwendungen, die von Organisationen und Verbrauchern verwendet werden), um Computer zu infizieren und Zugang zu sensiblen Daten wie etwa Anmeldeinformationen zu erhalten. In diesem Abschnitt zeigen wir drei der Routen, die niedrig hängenden Früchten entsprechen und von Cyberangreifern genutzt werden: Social Engineering, schlecht gesicherte Cloud-Anwendungen und zulässige Funktionen von Softwareplattformen.

Social Engineering

Da Softwarehersteller stärkere Sicherheitsmaßnahmen in ihre Produkte integrieren, wird es für Hacker immer aufwendiger, erfolgreich in Software einzudringen. Im Gegensatz dazu ist es einfacher und kostengünstiger, einen Benutzer mit einem Trick zu veranlassen, auf einen schädlichen Link zu klicken oder einer Phishing-E-Mail zu öffnen.

Microsoft Office 365 Advanced Threat Protection (ATP) hat Ende des Jahres 2017 ein erhebliches Volumen von Phishing-basierten E-Mail-Nachrichten festgestellt. In der zweiten Hälfte des Kalenderjahres 2017 war Phishing der wichtigste Bedrohungsvektor (> 50 %) für Office 365-basierte Bedrohungen.

Häufigste Bedrohungen (Juni bis Dezember 2017)

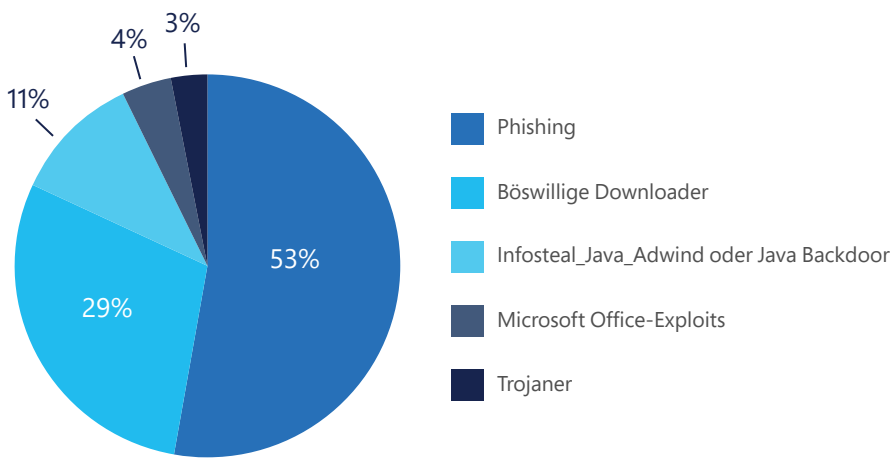


***Abbildung 7**: Die häufigsten Bedrohungen, die von Microsoft Office 365 ATP erkannt wurden*

Analyse und Erläuterung

Ein Angreifer, der z. B. eine Phishing-E-Mail in großer Menge an 1.000 Personen versendet, muss nur eine einzige Person erfolgreich täuschen, um Zugriff auf die Anmeldeinformationen dieser Person zu erhalten. Betrachten Sie eine Phishing-Kampagne, die auf Online-Banking-Kunden ausgerichtet ist, wie in Abbildung 8 dargestellt ist. Wenn Benutzer abgelenkt sind und die scheinbar legitime, aber gefälschte Phishing-E-Mail überfliegen, klicken sie vielleicht versehentlich auf einen Link und geben Details weiter, indem sie z. B. ihre Anmeldeinformationen eingeben, die dann von dem Hacker zur missbräuchlichen Verwendung protokolliert/gespeichert werden. Der Punkt ist, dass Phishing und andere Social-Engineering-Taktiken einfacher und effektiver als andere Methoden sein können und meistens für mehr Menschen funktionieren. Verglichen mit dem Ausnutzen einer Schwachstelle, das immer kostspieliger und schwieriger wird, ist Phishing im Erfolgsfall die einfachere Methode, um an Anmeldeinformationen zu gelangen.

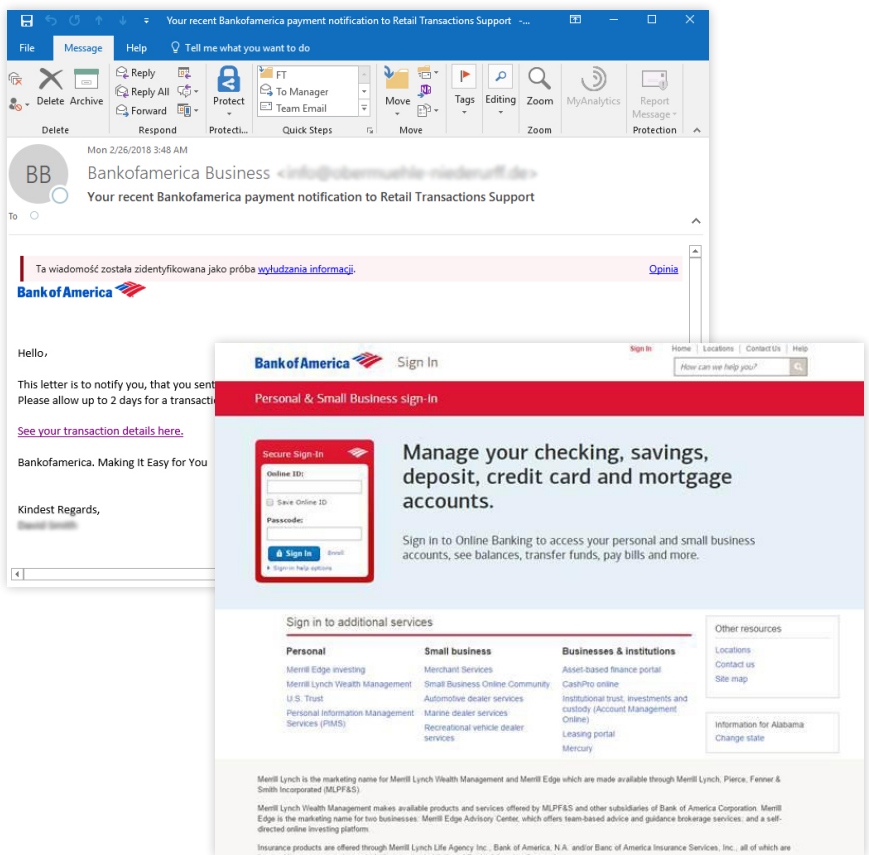


***Abbildung 8**: Beispiel einer Phishing-E-Mail*

Phishing kann viele Formen annehmen

Phishing als Angriffsvektor umfasst ein ganzes Spektrum von Angriffen, von breit angelegten bis hin zu zielorientierten Angriffen, wie in Abbildung 9 dargestellt ist. Die breit angelegten Phishing-Scams zielen darauf ab, mithilfe von Techniken wie Textködern und Domain-Spoofing in den Besitz von persönlichen Informationen (z. B. Identitäts-und Finanzinformationen) zu gelangen. Während Hacker mit dem Aufbau besser ausgerichteter Kampagnen beginnen, die Spear-Phishing verwenden, das auf hochwertige Konten abzielt (z. B. auf Konten der obersten Unternehmensebene), stellen wir fest, dass sie als Lockmittel für Benutzer häufig den Benutzer- oder Domänenidentitätswechsel einsetzen.

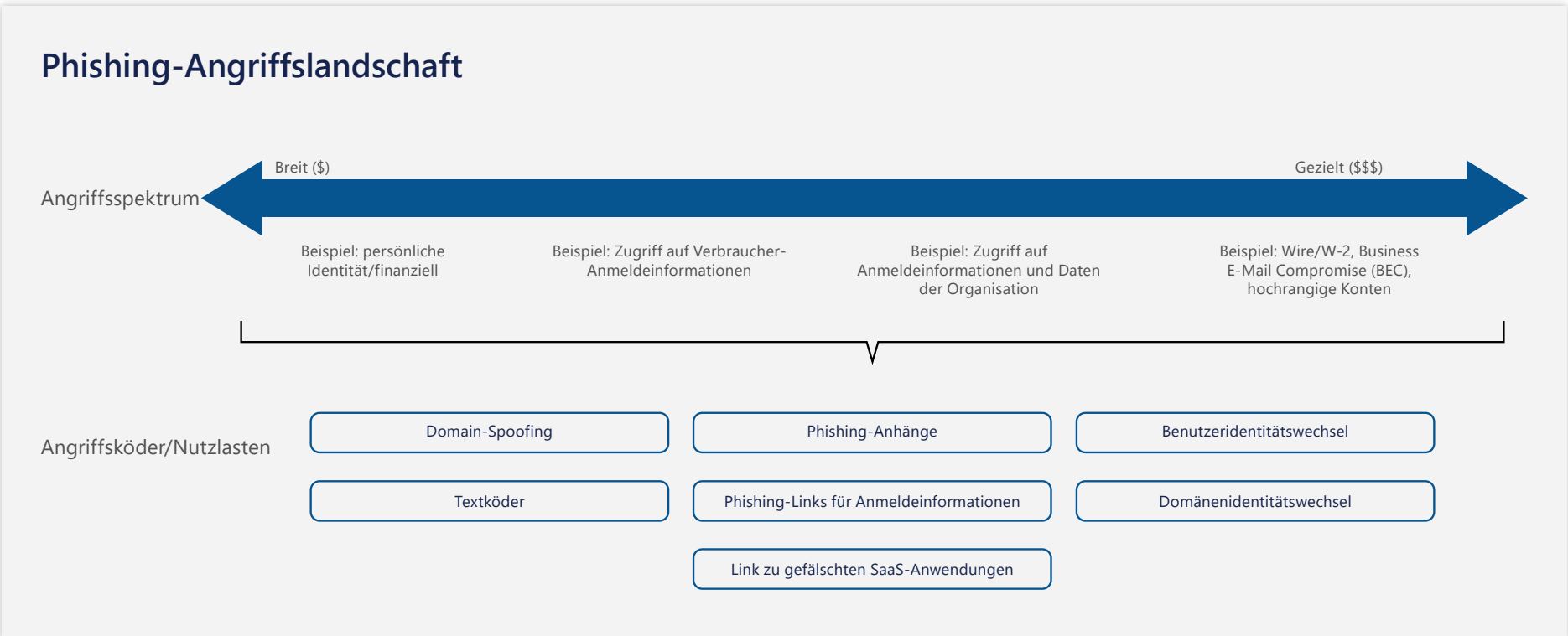


***Abbildung 9**: Die Phishing-Angriffslandschaft variiert von breit angelegten bis hin zu gezielten Angriffen*

Wichtige Ergebnisse im Zusammenhang mit Phishing

Basierend auf Threat Intelligence von Office 365 Advanced Threat Protection und Exchange Online Protection über drei Monate (November 2017 – Januar 2018) hat das Microsoft Office 365 Security Research-Team jeden Monat etwa 180-200 Millionen Phishing-E-Mails entdeckt.

- Das Forschungsteam hat etwa 30 % Domain-Spoofing-Angriffe festgestellt (basierend auf Office 365-Bereitstellungen).
- Mehr als 75 % der Phishing-E-Mails enthalten böswillige URLs zu Phishing-Sites. Andere Varianten enthalten böswillige Phishing-Anhänge und Links in Anhängen.
- Phishing-E-Mails nehmen die Identität beliebter Marken an
  - Mit Microsoft verbundene Marken (z. B. Office 365)
  - Andere häufig missbrauchte Marken sind insbesondere DocuSign, Dropbox, Apple und Amazon.
  - Jüngste Untersuchungen zeigen Angriffe, bei denen die Identität von beliebten Kurierdiensten wie FedEx, DHL und UPS angenommen wird.
  - Das Forschungsteam stellte auch Identitätswechsel im Zusammenhang mit Banken und staatlichen Dienstleistungen fest.
- Obwohl der Umfang der Techniken (Anzahl von Instanzen, in denen Techniken verwendet wurden) zum Benutzer- und Domänenidentitätswechsel gering war, handelte es sich um Angriffe mit hohem Schweregrad.

Die am niedrigsten hängende Frucht wechselt ständig

Ein Beispiel für den Abwärtstrend bei Exploits: Bis 2016 waren Makro-Exploits sehr verbreitet. Im Laufe der Zeit stiegen die Kosten solcher Exploits jedoch erheblich. Angreifer müssen nicht nur über sehr fein abgestimmte Fähigkeiten verfügen, um Sicherheitsmaßnahmen zu umgehen. Die meisten Anbieter bieten seither eine verbesserte und effektivere E-Mail-Sandbox-Technologie zur Erkennung und Abwehr von Bedrohungen durch makrobasierte Schadsoftware. Als makrobasierten Angriffen der Erfolg daraufhin verwehrt blieb, wandte sich die Kontrahenten den PDF-Exploits zu. Dieser Trend war eine Zeit lang sehr verbreitet, aber wie schon bei der Erkennung von Makros verbesserten die Hersteller im Laufe der Zeit die Erkennung von PDF-basierten Exploits, und die Angreifer gingen zu phishing-basierten Angriffen über.

Lösungen und Empfehlungen

Menschen werden oft als das schwächste Glied in der Cybersicherheit bezeichnet, aber mit der richtigen Schulung und Ausbildung können sie auch die erste Verteidigungslinie darstellen. Ein Mitarbeiter, der eine verdächtige E-Mail entdeckt und meldet, könnte eine umfangreiche Phishing-Kampagne abwenden. Mitarbeiter, denen unerwartete Latenzzeiten in Systemen auffallen, können Untersuchungen auslösen, die Akteure lauernder Bedrohungen ans Licht bringen. Organisationen können Mock-Phishing-Übungen durchführen und in Erwägung ziehen, externe Experten einzustellen, um eine Schulung zum Sicherheitsbewusstsein zu erhalten, die auf eine Aufklärung über Phishing beinhaltet. Weitere Ressourcen für die Schulung der Benutzer:

Tipps zum Erkennen von Phishing-E-Mails, -Links oder -Telefonaten

Übersicht über Phishing-und Sicherheitstipps von der US-amerikanischen Federal Trade Commission

Phishing-Übersicht und -Ressourcen für Berichte und weitere Informationen von US CERT

Schlecht gesicherte Cloud-Anwendungen

Da Cloud (SaaS)-Anwendungen (auch als Cloud-Dienste bekannt) zunehmend zur Unterstützung geschäftlicher Produktivität, Effizienz und sogar Kosteneinsparungen angenommen werden, ist es unerlässlich, dass die Cloud-Anwendungen sicher erstellt werden, damit sie nicht versehentlich die Tür zur Datenkompromittierung öffnen. Das Microsoft Cloud App Security R & D-Team hat basierend auf unserer Sicht und Bewertung von mehr als 30 Cloud-Anwendungen einen Mangel an Web-Session-Sicherheit und zuverlässiger Datenverschlüsselung in SaaS-Speicher- und SaaS Collaboration-Anwendungen beobachtet.

Analyse und Erläuterung

Schlecht gesicherte Cloud-Anwendungen können für Angreifer niedrig hängende Früchte darstellen. Ein Grund dafür ist, dass die mangelnde Sicherheit für Websitzungen (HTTP-Header-Sitzungen) in einer bestimmten Anwendung Angreifern die Ausführung von Angriffen auf der Anwendungsschicht ermöglichen könnte (z. B. Cross-Site-Scripting und Cookie-Hijacking). Außerdem könnte eine schlechte Verschlüsselung zu einem Szenario führen, in dem ein Angreifer, nachdem er den Cloud-Dienst erfolgreich kompromittiert oder den Datenverkehr abgefangen hat, die im Dienst enthaltenen Informationen gefährdet.

Das Erstellen verschiedener Sicherheitsmechanismen in HTTP-Headern bietet Schutz vor verschiedenen Angriffsvektoren für Websitzungen, z. B. Protokoll-Downgrade, Cookie-Hijacking, Clickjacking und Cross-Site-Scripting.

Die folgende Beschreibung für HTTP-Header ist der OWASP-Website entnommen:

HTTP Strict Transport Security (HSTs) ist ein Mechanismus für Web-Sicherheitsrichtlinien, der Websites vor Protokoll-Downgrade-Angriffen und Cookie-Hijacking schützt. Es ermöglicht einem Webserver, festzulegen, dass Webbrowser (oder andere konforme Benutzer-Agents) nur über sichere HTTPS-Verbindungen und niemals über das unsichere HTTP-Protokoll mit ihm interagieren sollen.

Das Microsoft Cloud App Security R & D-Team hat die Websicherheit und die Datenverschlüsselung für mehrere SaaS-Speicher- und SaaS-Collaboration-Anwendungen bewertet. Die folgenden Diagramme zeigen, wo die häufigsten Schwachstellen der SaaS-Anwendungen beobachtet wurden.

Microsoft Cloud App Security hat den Schutz von HTTP-Header-Sitzungen in SaaS-Speicher- und SaaS-Collaboration-Anwendungen bewertet. Die Abbildungen 10 und 11 zeigen die Ergebnisse dieser Bewertung.

Unterstützung für den Schutz von HTTP-Header-Sitzungen

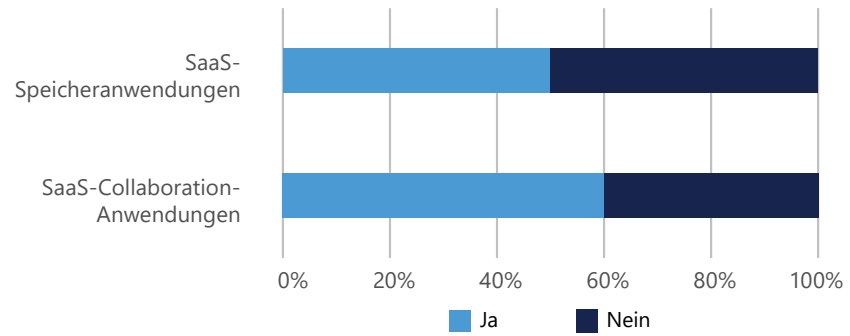


***Abbildung 10**: 50 % der SaaS-Speicheranwendungen und 40 % der SaaS-Collaboration-Anwendungen unterstützen den Schutz von HTTP-Header-Sitzungen nicht*

Unterstützung für alle Methoden zum Schutz von HTTP-Header-Sitzungen

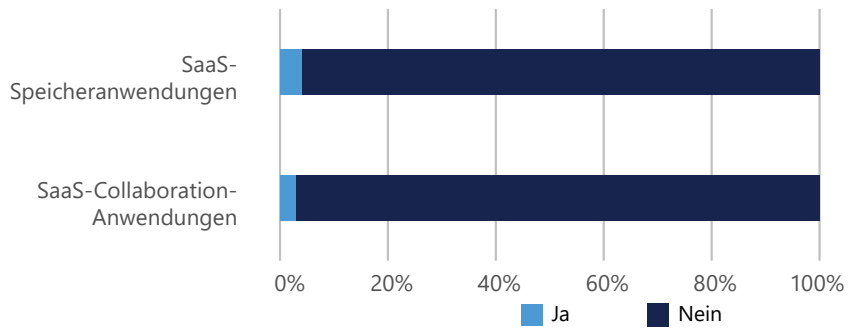


***Abbildung 11**: Nur 4 % der SaaS-Speicheranwendungen und 3 % der SaaS-Collaboration-Anwendungen unterstützen alle Methoden zum Schutz von HTTP-Header-Sitzungen*

Microsoft Cloud App Security hat auch die Datenverschlüsselung in SaaS-Speicher- und SaaS-Collaboration-Anwendungen bewertet. Die Abbildungen 12 und 13 zeigen die Ergebnisse dieser Bewertung.

Unterstützung für einige Formen der Datenverschlüsselung

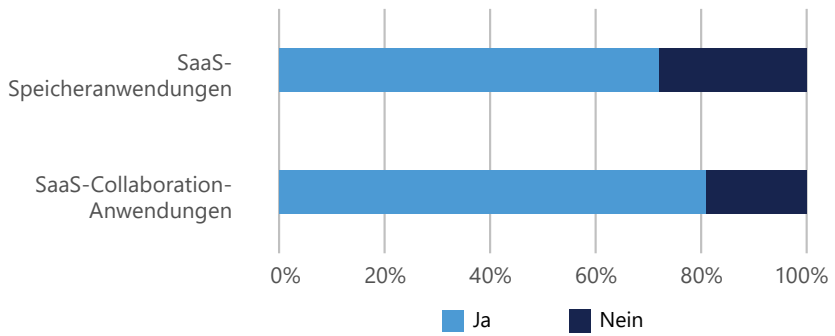


***Abbildung 12**: 28 % der SaaS-Speicheranwendungen und 19 % der SaaS-Collaboration-Anwendungen unterstützen keinerlei Datenverschlüsselungsmethode*

Schützen Sie ruhende und übertragene Daten.

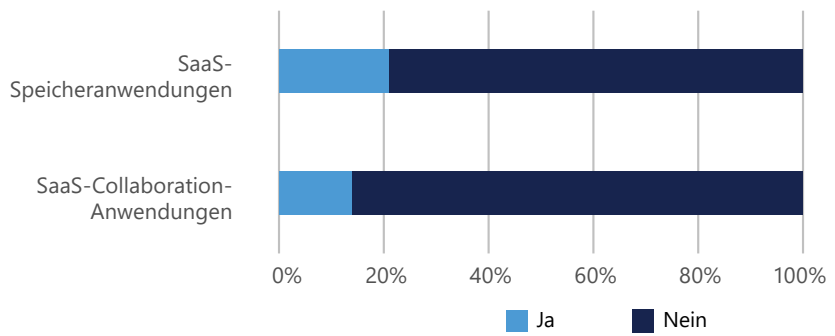
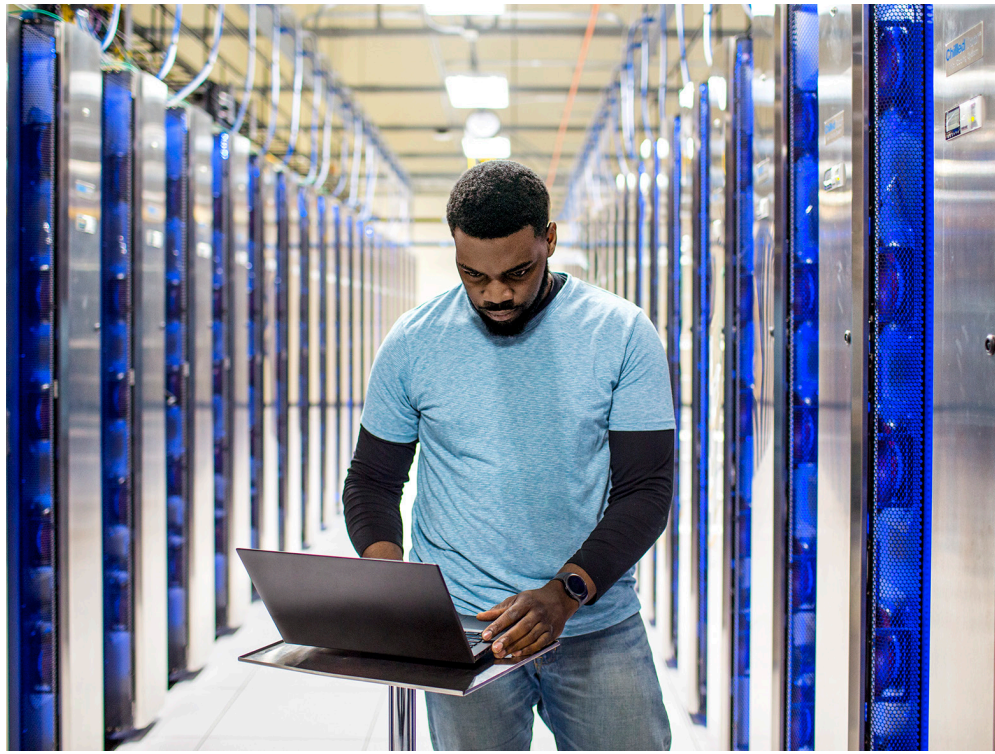


***Abbildung 13**: 79 % der SaaS-Speicheranwendungen und 86 % der SaaS-Collaboration-Anwendungen verschlüsseln Daten weder im Ruhezustand noch während der Übertragung*

Lösungen und Empfehlungen

Bei der Einführung von Cloud-Anwendungen sollten Sie sicherstellen, dass nur Anwendungen mit Websitzungsschutz und Verschlüsselung in ihrer Umgebung zulässig sind. Unternehmen sollten über eine Lösung verfügen, mit der sie die gesamte Cloud-Apps-Nutzung überblicken und kontrollieren können. Einige Mitarbeiter könnten z. B. nicht genehmigte SaaS-Anwendungen zum Speichern von Unternehmensdaten oder anderen Formen sensibler Daten verwenden. Die Verwendung einer Cloud Access Security Broker (CASB)-Sicherheitslösung der Enterprise-Klasse ist für eine Organisation die einzige Möglichkeit, sicherzustellen, dass Mitarbeiter keine derartigen Anwendungen nutzen.



Nutzen legitimer Plattformfunktionen

Die Verwendung von Geschäftssoftware ist für die Produktivität entscheidend. Cyberkriminelle wissen das und nutzen legitime Funktionen von Softwareplattformen, um Computer zu infizieren. Im letzten Quartal 2017 entdeckte das Windows Defender Security Intelligence-Team z. B. einige Vorfälle, bei denen Hacker legitime Geschäftssoftware verwendet hatten, um „unter dem Radar" zu bleiben, während sie Benutzern auf betrügerische Weise Daten entlockten und Computer infizierten. Es folgt ein Beispiel für diese Bedrohung.

Microsoft Windows Dynamic Data Exchange (DDE) ist ein Feature, das die elektronische Übertragung von Office-Dateien mithilfe von gemeinsamem Speicher und gemeinsamen Daten erleichtert. Anfang Oktober 2017 wurde öffentlich bekannt gegeben, dass eine neue Variante der Locky-Ransomware durch missbräuchliche Verwendung von DDE bereitgestellt wird (Microsoft hat im Dezember 2017 ein Sicherheitsupdate veröffentlicht, das DDE in allen unterstützten Editionen von Word und Excel standardmäßig deaktiviert.) Das Microsoft Windows Defender Security Intelligence-Team sah auch zusätzliche Beispiele für diesen Angriff, und in diesem Bericht wird ein solches Beispiel vorgestellt.

Analyse und Erläuterung

Von Anfang Oktober bis November 2017 traten vermehrt Hacker mit DDE-Exploits auf, die Techniken zur Ausführung von Schadsoftware auf dem Computer eines ahnungslosen Endbenutzers nutzten. In einem bestimmten Fall wurde ein Word-Dokument an eine böswillige Spam-E-Mail angehängt. Nachdem der Benutzer geklickt hatte, um den Anhang zu öffnen, und auf eine Reihe von Popupdialogfeldern reagiert hatte, die die Softwareanwendung zur Ausführung einer Aktion aufforderten, wurde mit einem DDE-Angriff eine schädliche Nutzlast (z. B. Locky-Ransomware) auf den Computer geladen und dort ausgeführt. Das Problem liegt darin, dass Benutzer über eine legitime Softwareplattform mit Inhalten interagieren, ohne zu erkennen, dass es sich um böswillige Absicht handelt.

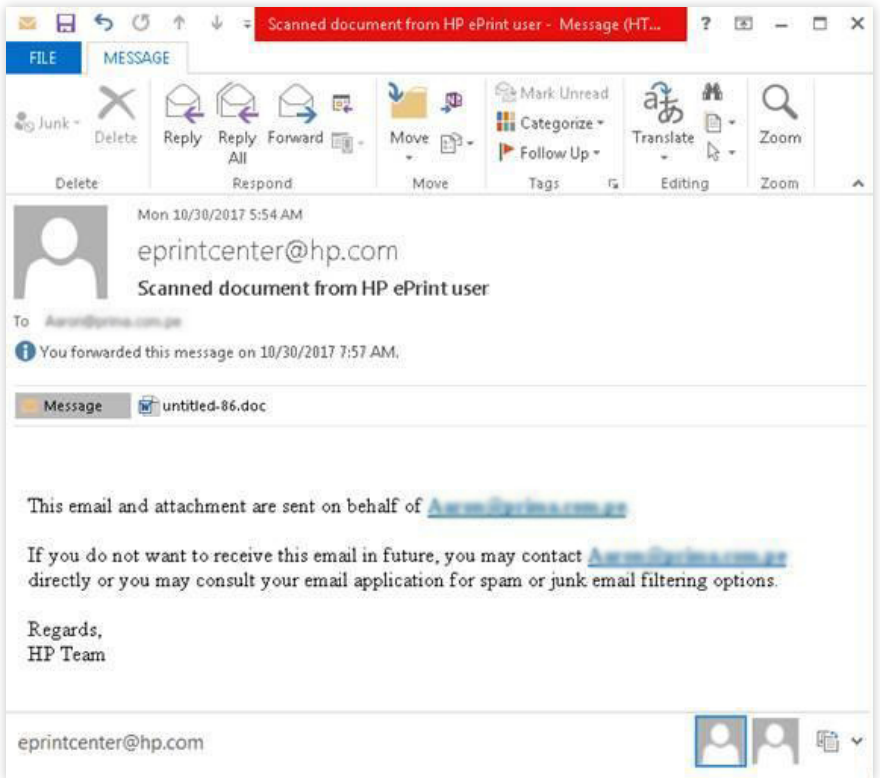


***Abbildung 14**: Beispiel für eine böswillige Spam-E-Mail mit Anhang, die Locky-Ransomware durch Nutzung der DDE-Funktionalität überträgt.*

Lösungen und Empfehlungen

In Hinblick auf die schädlichen Nutzlasten, die mit DDE-Angriffen verbunden sind, bietet Microsoft in neueren Versionen von Windows, z. B. Windows 10, standardmäßigen Schutz vor Schadsoftware. Wir empfehlen außerdem die folgenden bewährten Methoden:

Schützen Sie Ihren Computer

Wir ermutigen die Kunden auch weiterhin, die grundlegenden Anleitungen zum Schutz Ihrer Computer zu befolgen, indem sie eine Firewall aktivieren, Antivirus-Software installieren und Softwareupdates (On-Premises- und cloudbasierte Sicherheitsupdates) abrufen.

Halten Sie Ihre Betriebssystem-Software auf dem neuesten Stand

Sie sollten die neuesten Sicherheitsupdates für die Betriebssystem-Software anwenden, um sicherzustellen, dass Ihr Computer bestmöglich geschützt ist. Wenn Sie nicht sicher sind, ob die Software auf dem neuesten Stand ist, besuchen Sie die Website des Herstellers, um die neuesten Softwareupdates anzuzeigen, den Computer nach verfügbaren Updates zu durchsuchen und alle Ihnen angebotenen Updates mit hoher Priorität zu installieren. Selbst wenn Sie automatische Softwareupdates für Ihren Computer aktiviert und konfiguriert haben und die Updates zum Zeitpunkt ihrer Freigabe an Sie übermittelt werden, sollten Sie überprüfen, ob sie installiert sind.

ABSCHNITT 3

Bekämpfen von Ransomware

Cyberkriminelle führen ein Unternehmen und für jedes Unternehmen ist Geld eine wichtige Ressource. Daher ist Ransomware weiterhin eine beliebte Methode, die von Cyberkriminellen verwendet wird, um Geld (Bitcoin oder andere Form) von den Opfern zu fordern und in mehreren Fällen erfolgreich zu erhalten. Im Gegenzug für das Lösegeld übergeben Angreifer dem Opfer in der Regel den privaten Schlüssel, der erforderlich ist, um die Daten zu entschlüsseln, oder stellen den Zugang des Opfers zum Computer anderweitig wieder her – ein Versprechen, dass trotz Zahlung häufig nicht erfüllt wird. Ransomware war eine der häufigsten Formen von Schadsoftware, die durch das weiter oben im Bericht beschriebene Gamarue-Botnet verbreitet wurde. Ransomware wird auch bei einigen der Wege für niedrig hängende Früchte, die im Bericht erwähnt werden, als Infektionsvektor verwendet, z. B. bei Phishing-E-Mails und legitimen Softwareplattformen.

Analyse und Erläuterung

Für den Zeitraum von Februar bis Dezember 2017 wurden die folgenden Ransomware-Trends ermittelt:

- Die geographische Region mit der größten Anzahl von Kontakten mit Ransomware war Asien.
- Drei globale Ausbrüche (WannaCrypt, Petja/NotPetya und BadRabbit) zeigten die Durchschlagskraft von Ransomware in Hinblick auf konkrete Auswirkungen. Sie betrafen Unternehmensnetzwerke und brachten wichtige Dienstleistungen wie Krankenhäuser, Transport- und Verkehrssysteme zu Fall.
- Die drei häufigsten Ransomware-Familien waren Win32/WannaCrypt,Win32/LockScreen und Win32/Cerber.
- Zu den Standorten mit den meisten Ransomware-Fällen gehören Myanmar (0,48 Prozent), Bangladesch (0,36 Prozent) und Venezuela (0,33 Prozent).
- Zu den Standorten mit den wenigsten Ransomware-Fällen gehören Japan, Finnland und die USA. In all diesen Ländern lag das monatliche Vorkommen von Ransomware bei 0,03 Prozent.

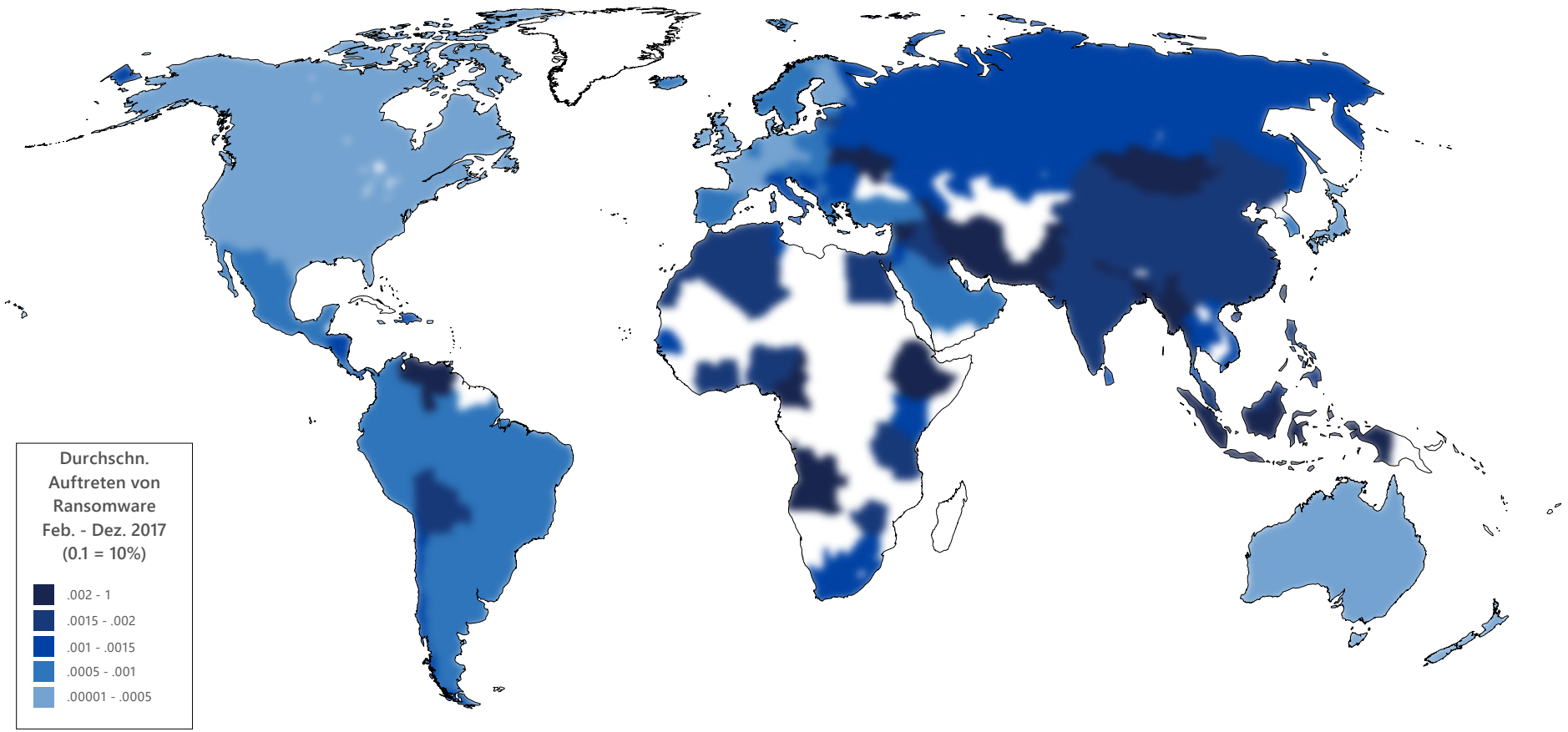


***Abbildung 17**: Auftreten von Ransomware-Familien nach Land/Region, Februar bis Dezember 2017*

- Win32/LockScreen, die häufigste Ransomware-Familie im Jahr 2017, zeigt eine Meldung im Vollbildmodus an, die den Benutzer daran hindert, auf den Desktop zuzugreifen, und fordert vom Benutzer, ein Strafgeld in Form einer SMS-Nachricht zu zahlen, die an eine Premium-Nummer gesendet werden muss, um die Kontrolle über den Computer zurückzuerlangen. LockScreen betrifft in erster Linie Android. Android-Schadsoftware findet sich auch auf Windows-Rechnern. Dazu kann es z. B. kommen, wenn Android-Benutzer unter Windows ihre Smartphones synchronisieren oder Android-Anwendungen herunterladen und sich die Anwendungen, die nicht genehmigt sind (z. B. nicht aus dem offiziellen Google Play Store stammen), per Sideloading verschaffen. Die Region Südostasien weist eine tendenziell höhere Akzeptanzrate von Android auf, was ein vermehrtes Auftreten in dieser Region erklären würde.
- Win32/WannaCrypt (auch als WannaCry bekannt) trat Anfang 2017 in Erscheinung und zielte auf eine Sicherheitslücke in Windows ab, mit der sich Microsoft zuvor im Sicherheitsbulletin MS17-010 befasst hatte.
- Win32/Cerber wird häufig über die Exploit-Kits Rig (Meadgive) und Magnitude (Pangimop) verbreitet. Cerber ist eine Ransomware-as-a-Service-Familie, die von ihren Schöpfern an potenzielle Angreifer verkauft wird und für den problemlosen Einsatz durch Neulinge konzipiert wurde.

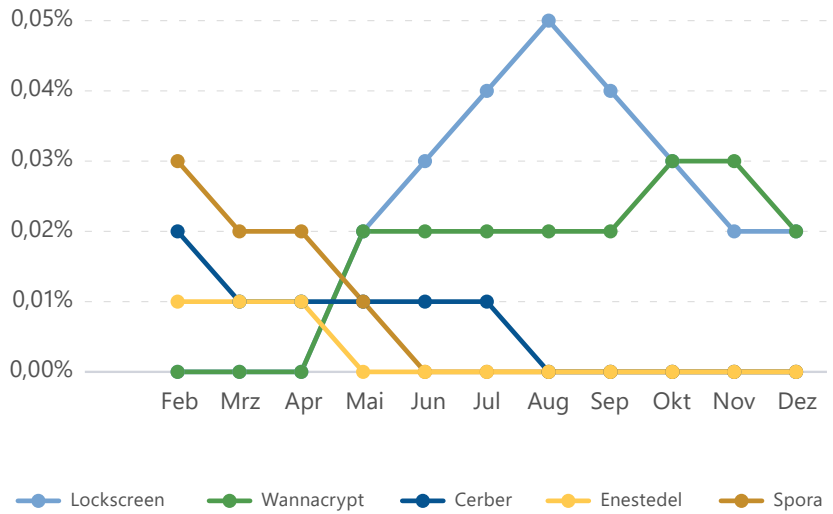


***Abbildung 18**: Trends für mehrere häufige Ransomware Familien, Februar bis Dezember 2017*

Die Auswirkungen von schnellen, destruktiven Angriffen wie WannaCrypt und Petja/NotPetya waren beispiellos. Opfer dieser Angriffe oder von Bad-Rabbit-Ransomware-Angriffen verlieren den Zugriff auf Dateien, oft auf unbestimmte Zeit.

WannaCrypt nutzt EternalBlue, einen Exploit für eine zuvor behobene SMBv1-Schwachstelle, um sich schnell in Netzwerken zu verbreiten, was in kurzer Zeit eine große Anzahl von Computern betrifft. (Microsoft hat im März 2017 das Sicherheitsbulletin MS17-010 veröffentlicht, um die Schwachstelle zu beheben.)

Petya (Ransom:Win32/Petya.B) verwendete den gleichen Exploit, der WannaCrypt seine Verbreitungsmöglichkeiten verlieh, und fügte weitere Verbreitungs- und Infektionsmethoden hinzu, um die wohl komplexeste Ransomware des Jahres 2017 zu schaffen. Der anfängliche Infektionsvektor von Petja war eine kompromittierte Software-Supply-Chain, aber die Ransomware konnte sich mithilfe der Exploits EternalBlue und EternalRomance und eines Moduls für laterale Bewegungen mit gestohlenen Anmeldeinformationen schnell ausbreiten.

Bad Rabbit-Ransomware (Ransom:Win32/Tibbar.A) infizierte Geräte, indem sie sich als Adobe Flash-Installationsprogramm ausgab, das auf kompromittierten Websites zum Download bereitstand. Wie WannaCry und Petja verfügte Bad Rabbit über Möglichkeiten zur Verbreitung, wenn auch eher traditionelle: diese Ransomware verwendete eine hartcodierte Liste von Benutzernamen und Kennwörtern. Wie Petja kann auch sie das Hochfahren infizierter Geräte unmöglich machen, da sie zusätzlich zur Verschlüsselung von Dateien ganze Festplatten verschlüsselt.

Lösungen und Empfehlungen

Sichern Sie Ihre Daten

Die Bedeutung der Sicherung von Dateien für eine Wiederherstellung im Falle eines Ransomware-Angriffs kann, Dateien zu sichern, um im Falle eines Ransomware-Angriffs wiederhergestellt werden zu können, kann gar nicht hoch genug angesetzt werden. Erstellen Sie unbedingt zerstörungsfeste Sicherungen Ihrer kritischen Systeme und Daten. Für die Sicherung von Dateien, die Wiederherstellung vorheriger Dateiversionen und die Wiederherstellung gesicherter Dateien stehen zahlreiche Tools und Dienste zur Verfügung. Sie sollten außerdem regelmäßig testen, ob die Sicherungen funktionieren.

Wenden Sie mehrschichtige Sicherheitsmaßnahmen an

Verwenden Sie eine E-Mail-Sicherheitslösung oder einen entsprechenden Dienst, die bzw. der E-Mail-Anhänge scannt und idealerweise schützt, wenn ein Benutzer auf einen Anhang klickt, z. B. durch Isolieren eines verdächtigen Anhangs zur weiteren Untersuchung. Antivirus-Software kann zumindest hilfreich sein, den Download und die Installation mancher Ransomware zu erkennen und zu blockieren. Um die Auswirkungen hochentwickelter Ransomware zu erkennen und zu entschärfen, ist zusätzlicher Schutz erforderlich. Ein fortschrittlicher Bedrohungsschutz, der Machine Learning und Technologien für künstliche Intelligenz nutzt, um Dateien auswertet, um vermutete Schadsoftware erkennen zu können, kann hilfreich sein.

Halten Sie sämtliche Software auf dem neuesten Stand

Um die Einstiegspunkte für Ransomware zu minimieren, achten Sie darauf, sämtliche Software, einschließlich Betriebssystem, Webbrowser, Webbrowser-Plug-Ins (nur diejenigen, die für geschäftliche Zwecke erforderlich sind), und Sicherheitssoftware, auf dem neuesten Stand zu halten. Patches für neue Versionen sollte zudem Priorität eingeräumt werden, um einen stärkeren Schutz vor Schwachstellen zu ermöglichen.

Isolieren Sie bestimmte Computer oder nehmen Sie sie außer Betrieb

Wenn einige Computer nicht mit der neuesten Software gepatcht oder aktualisiert werden können, isolieren Sie diese Computer oder nehmen Sie sie außer Betrieb, um das Expositionsprofil gegenüber einem Ransomware-Angriff und einer Ransomware-Infektion zu minimieren.

Verwalten und steuern Sie den privilegierten Zugriff auf Daten

Um das Risiko der Kompromittierung und des Missbrauchs von Anmeldeinformationen zu minimieren, implementieren Sie auf allen Systemen eindeutige Kennwörter für lokale Administratoren, trennen und schützen Sie privilegierte Konten, und reduzieren Sie umfangreiche Berechtigungen für Datei-Repositorys.

Zusätzliche nennenswerte Threat Intelligence

Die Daten, die den folgenden Themen zugrunde liegen, stammen zum Teil aus der fortlaufenden Verfolgung von Bedrohungen, die von Microsoft Azure Cloud Services und Windows-Endgeräten weltweit beobachtet werden. Ein umfassenderer Blick auf diese Daten aus der Bedrohungsverfolgung folgt.

Threat Intelligence für Clouds

Cloud-Dienste wie Microsoft Azure sind das ganze Jahr über das Ziel von Angreifern, die versuchen, virtuelle Computer und andere Dienste zu kompromittieren und als Waffe einzusetzen. In einem Bedrohungsszenario für die Umwandlung einer Cloud in eine Waffe fasst ein Angreifer in einer Cloud-Infrastruktur Fuß, indem er eine oder mehrere virtuelle Computer kompromittiert und die Kontrolle über sie übernimmt. Der Angreifer kann diese virtuellen Computer dann verwenden, um Angriffe zu starten, darunter Brute-Force-Attacken gegen andere virtuelle Computer, Spam-Kampagnen, die für E-Mail-Phishing-Angriffe genutzt werden können, Ausspähungen wie etwa Port-Scans zur Identifizierung neuer Angriffsziele und andere schädliche Aktivitäten. Die beiden folgenden Abbildungen zeigen den Ausgangspunkt ein- und ausgehender Angriffe.

Fast zwei Drittel der eingehenden Angriffe auf Azure-Dienste im zweiten Halbjahr 2017 stammten zu jeweils 31,7 Prozent, 18,0 Prozent und 15,9 Prozent von IP-Adressen in China, den USA bzw. Russland. Frankreich lag mit 6,7 Prozent auf dem vierten Rang, wobei auf kein anderes Land und keine andere Region mehr als 5 Prozent der Gesamtzahl entfiel.

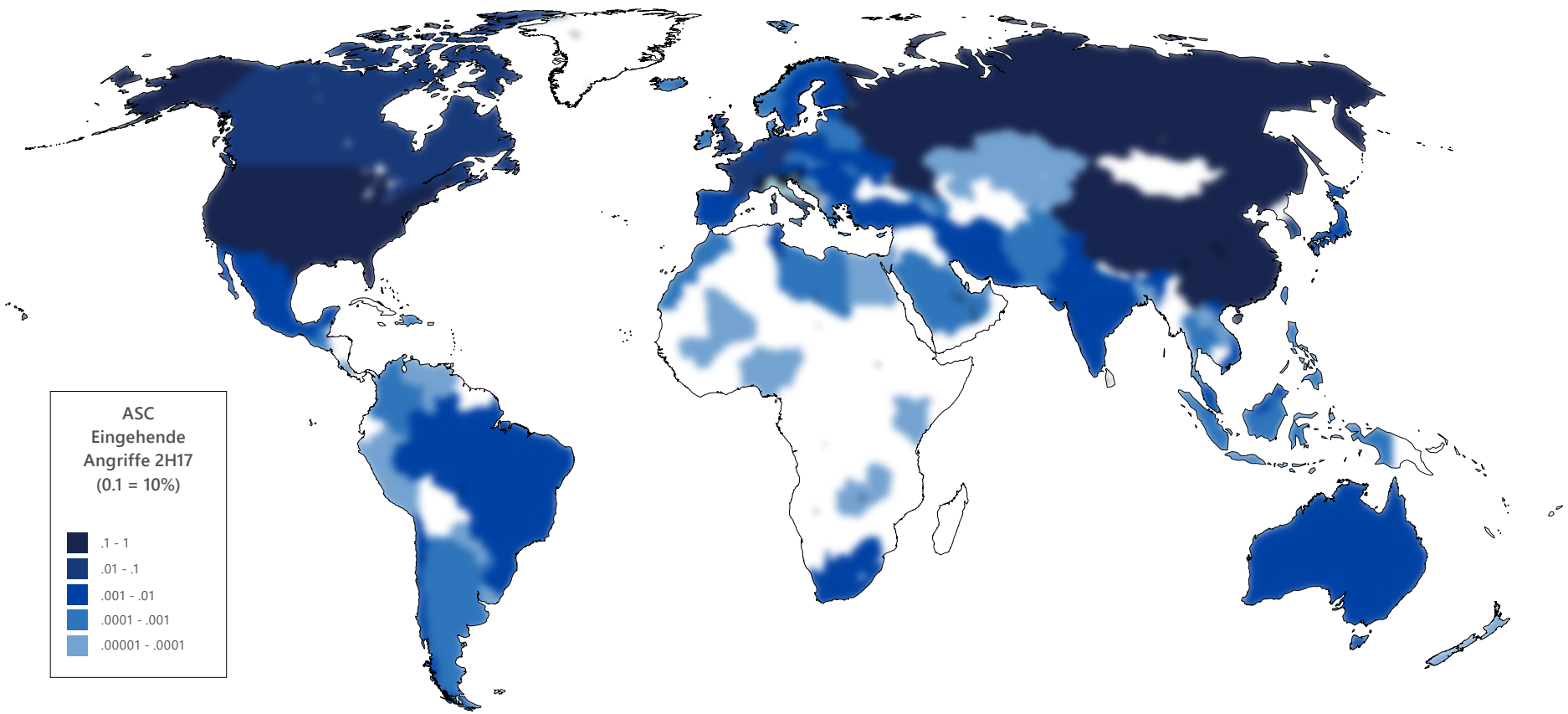


***Abbildung 19**: Eingehende Angriffe nach Herkunftsland/-region, die im zweiten Halbjahr 2017 von Azure Security Center erkannt wurden*

Kompromittierte virtuelle Computer kommunizieren häufig mit Command-and-Control (C&C)-Servern unter bekannten böswilligen IP-Adressen, um Anweisungen zu erhalten. 54 Prozent der böswilligen IP-Adressen, die im zweiten Halbjahr 2017 von kompromittierten virtuellen Azure-Computern kontaktiert wurden, befanden sich in China, gefolgt von den USA mit 22 Prozent.

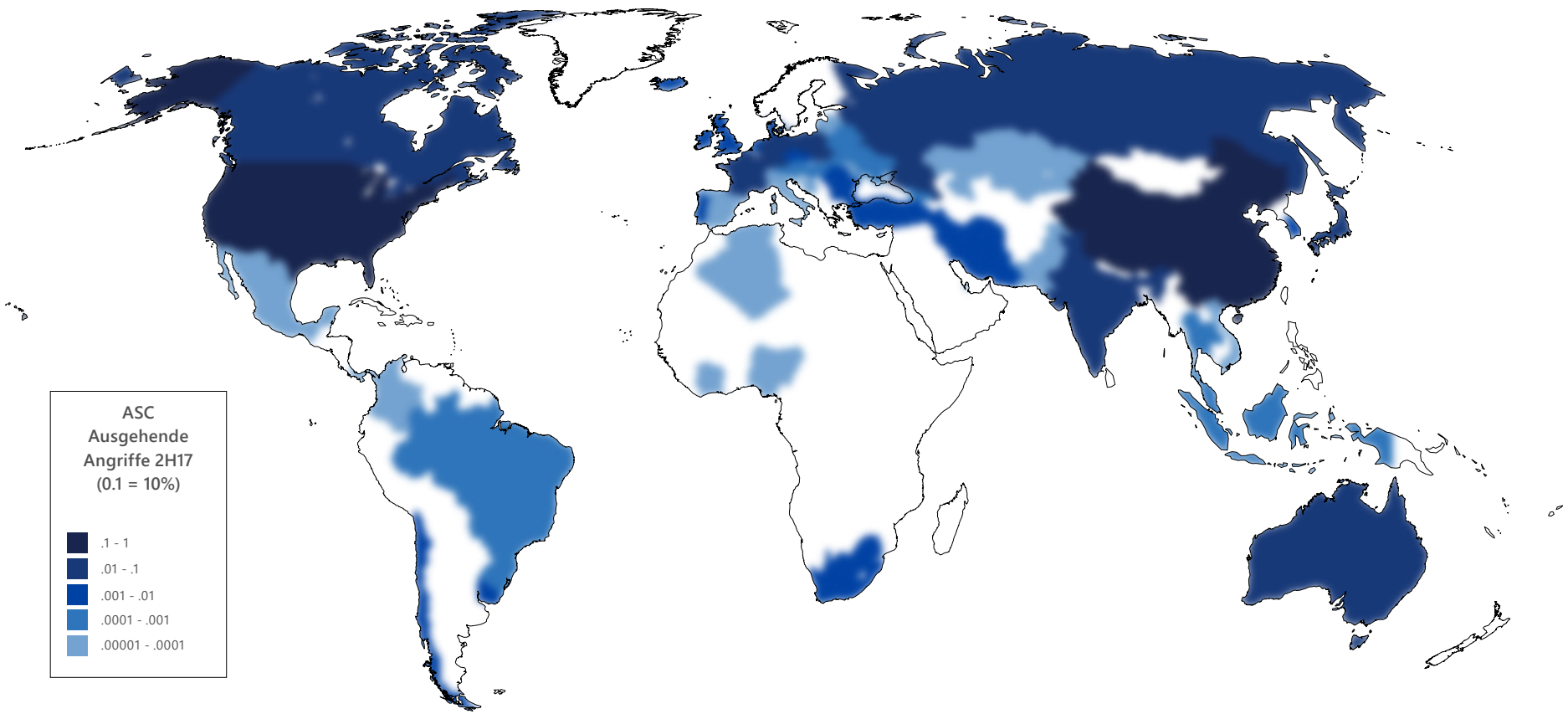


***Abbildung 20**: Ausgehende Kommunikation mit böswilligen IP-Adressen nach Adressenstandort, die im zweiten Halbjahr 2017 von Azure Security Center erkannt wurde*

Drive-by-Downloadsites

Zu den bedeutenden Standorten mit einer hohen Konzentration von Drive-by-Download-URLs gehörten Taiwan mit durchschnittlich 6,4 Drive-by-URLs für jeweils 1.000 von Bing nachverfolgte URLs sowie Iran mit 1,4 und die Vereinigten Arabischen Emirate mit 1,3 Drive-by-URLs.

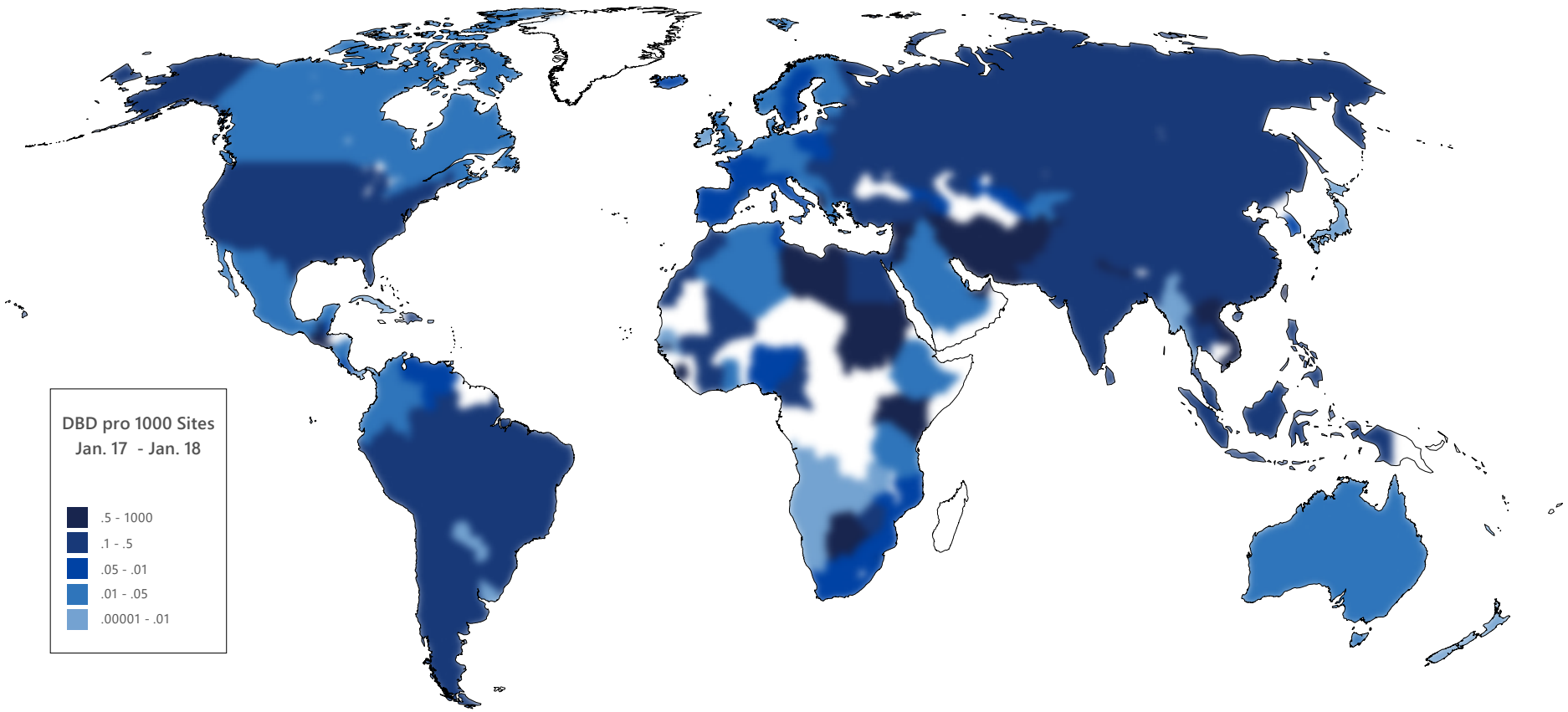


***Abbildung 21**: Monatliche Durchschnittszahl von Downloadsites, die von Bing zwischen Januar 2017 und Januar 2018 indiziert wurden, pro 1.000 URLs in den einzelnen Ländern/Regionen*

Threat Intelligence für Endgeräte

Schadsoftware und unerwünschte Software

Das *Auftreten* (Encounter Rate) in den folgenden Abbildungen entspricht dem Prozentsatz der Computer, auf denen Microsoft-Echtzeit-Sicherheitsprodukte ausgeführt werden, die das Auftreten von Schadsoftware melden.[1] Das monatliche Vorkommen in Kanada zwischen Februar 2017 und Januar 2018 lag z. B. bei 14,2 Prozent. Diese Daten bedeuten, dass 14,2 Prozent der Computer in Kanada, auf denen in diesem Zeitraum Microsoft-Echtzeit-Sicherheitssoftware ausgeführt wurde, das Auftreten von Schadsoftware meldeten, und 85,8 Prozent nicht. Das Auftreten einer Bedrohung bedeutet nicht, dass der Computer infiziert wurde. Bei der Berechnung des Auftretens werden nur Computer berücksichtigt, deren Benutzer sich für die Bereitstellung von Daten an Microsoft entschieden haben.

[1]Das Auftreten umfasst keine Bedrohungen, die von einem Webbrowser blockiert werden, bevor sie von Antimalware-Software erkannt werden. Insbesondere kann Sicherheitssoftware mithilfe von **IExtensionValidation** in Internet Explorer 11 das Laden von Seiten blockieren, die Exploits enthalten. Daher geben die Zahlen für das Auftreten vielleicht nicht alle Bedrohungen vollständig wieder, die bei Computerbenutzern auftraten.

- Zu den Standorten mit hohem Vorkommen gehörten Pakistan, Nepal, Bangladesch und die Ukraine. In all diesen Ländern lag das monatliche Vorkommen im Jahr 2017 bei 33,2 Prozent oder höher.
- Zu den Standorten mit geringem Vorkommen zählten Finnland, Dänemark, Irland und die USA. In all diesen Ländern lag das monatliche Vorkommen im Jahr 2017 bei 11,4 Prozent oder niedriger.

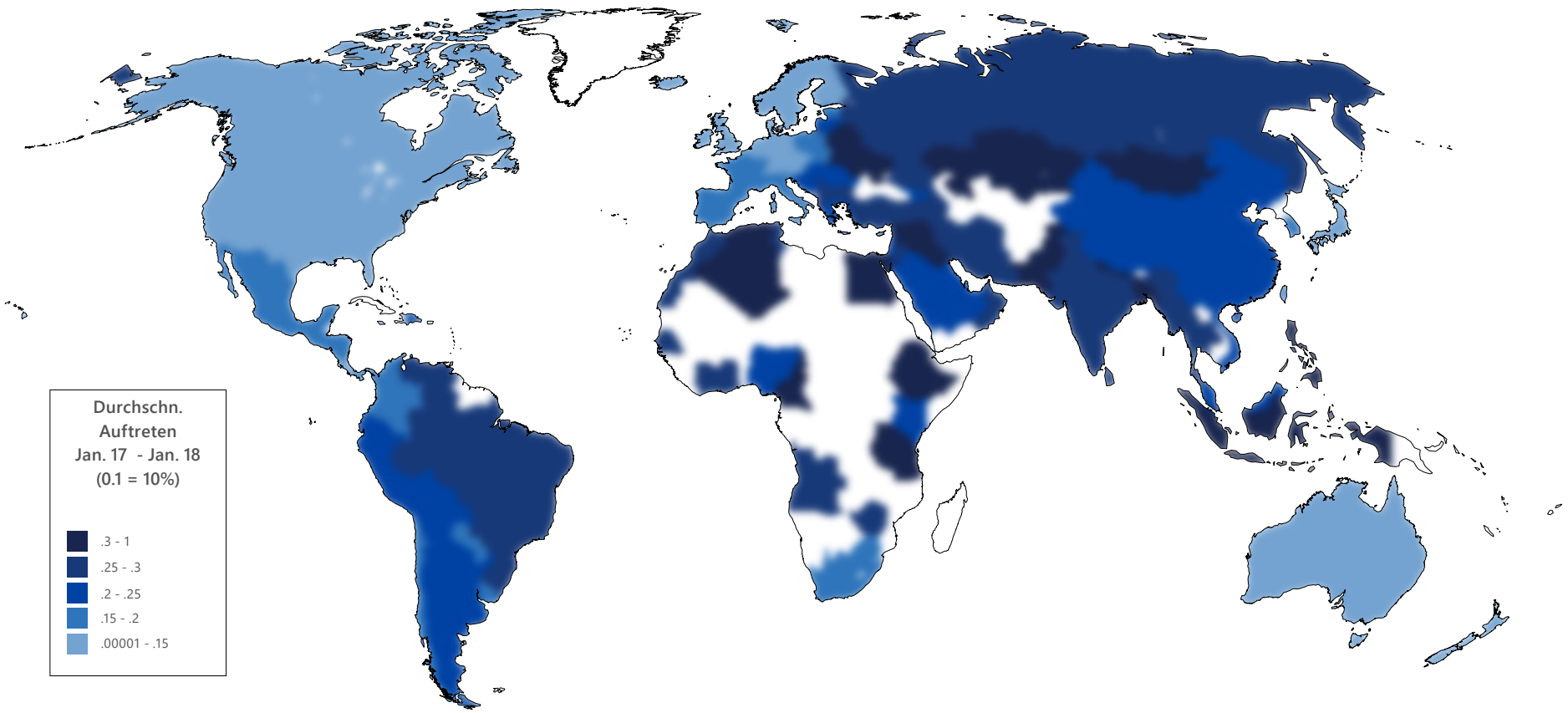


***Abbildung 21**: Auftreten nach Land/Region, Februar 2017 bis Januar 2018*

Die Einordnung einzelner Bedrohungen in Typen durch Windows Defender Security Intelligence (WDSI) erfolgt auf Basis einer Reihe von Faktoren, darunter die Verbreitungsweise der Bedrohung und ihr vorgesehener Zweck. Um die Darstellung dieser Informationen zu vereinfachen und leichter verständlich zu machen, werden diese Typen im Microsoft Security Intelligence Report in Kategorien gruppiert, die auf Ähnlichkeiten in Funktion und Zweck basieren.

- Trojaner waren 2017 in jedem Monat mit großem Abstand die häufigste Kategorie schädlicher Software, die von mehreren generischen und cloud-basierten Erkennungen für eine Vielzahl von Bedrohungen angeführt wurde.
- Das Vorkommen für andere Kategorien war viel niedriger und in aufeinander folgenden Monaten gleichbleibender.

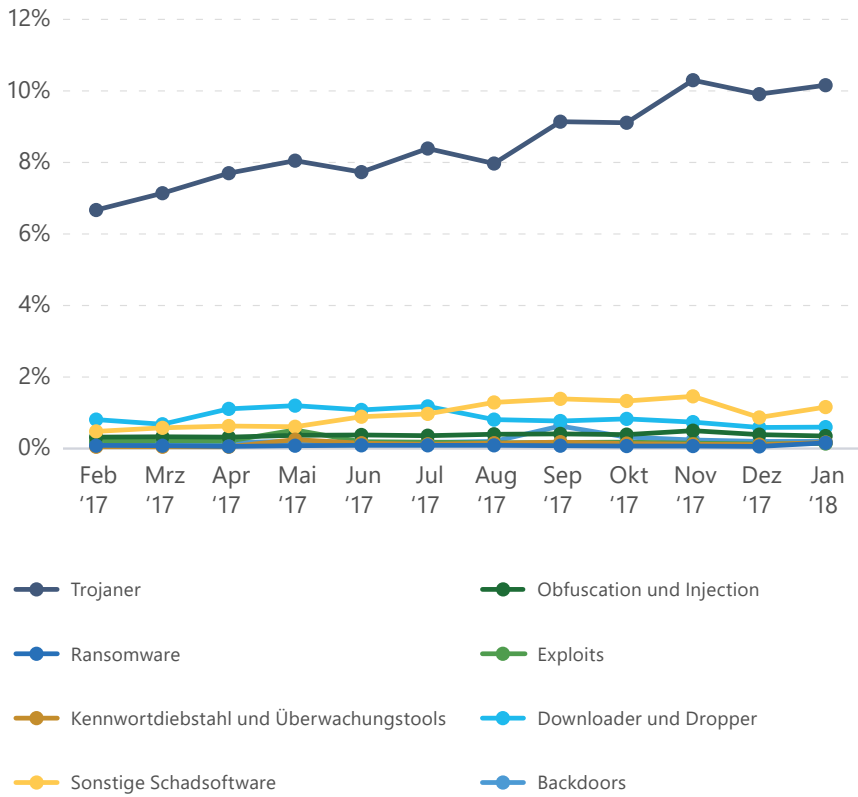


***Abbildung 22**: Auftreten für Kategorien von Schadsoftware, Februar 2017 bis Januar 2018*

- Browser-Modifier waren die häufigste Kategorie unerwünschter Software für den Zeitraum von Februar 2017 bis Januar 2018 und wurden von Win32/Foxiebro und Win32/Obrypser angeführt.
- Software-Bundler waren die zweithäufigste Kategorie unerwünschter Software für den Zeitraum von Februar 2017 bis Januar 2018 und wurden von Win32/Prepscram angeführt.
- Das Auftreten von Adware war signifikant weniger häufig als das der anderen Kategorien unerwünschter Software und wurde von Win32/Adposhel angeführt.

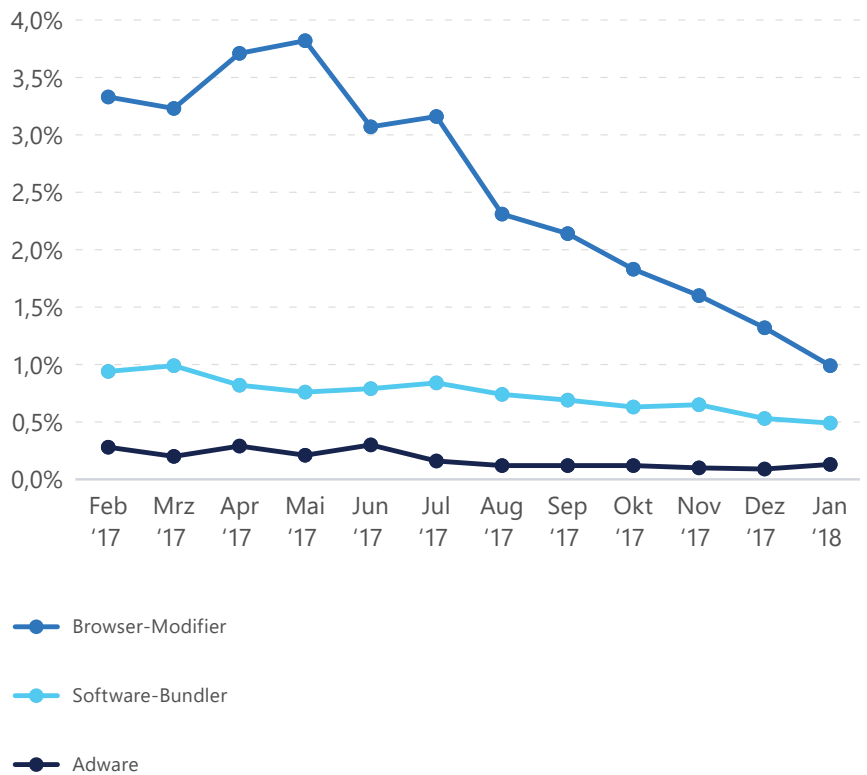


***Abbildung 23**: Auftreten unerwünschter Softwarekategorien, Februar 2017 bis Januar 2018*

Die nächsten beiden Zahlen zeigen Trends für die wichtigsten Familien von Schadsoftware, die von Microsoft-Echtzeit-Antimalware-Produkten weltweit erkannt wurden.

- Win32/Fuery ist eine cloud-basierte Erkennung für Dateien, die von der cloud-basierten Schutzfunktion Windows Defender automatisch als schädlich identifiziert wurden. Weitere Informationen zu der Funktion und Anleitungen für ihre Verwaltung in Netzwerkumgebungen finden Sie im Artikel „Blockieren auf den ersten Blick“ auf technet.microsoft.com und im Eintrag „Windows Defender Antivirus Cloud Protection-Dienst: Erweiterte Echtzeitverteidigung gegen zuvor niemals aufgetretene Schadsoftware“(18. Juli 2017) im Windows-Sicherheitsblog unter blogs.technet.microsoft.com/mmpc.
- Win32/Skeeyah und Win32/Dynamer sind generische Erkennungen für eine Vielzahl von Trojanern, die bestimmte Eigenschaften gemeinsam haben.
- VBS/Mutuodo, in November die am weitesten verbreitete Familie von Schadsoftware weltweit, ist ein Trojaner, der ausführbare Dateien startet, die mit der Win32/Prifou-Familie von Browser-Modifiern in Zusammenhang stehen.
- HTML/Brocoiner ist ein JavaScript-Programm für das Mining von Kryptowährungen, das sich auf böswilligen sowie auf kompromittierten Websites findet. Dazu gehören auch Websites, auf denen Streaming-Videos, Erwachseneninhalte oder Online-Shopping angeboten werden. Wenn eine Webseite mit der JavaScript-Datei geladen wird, wird diese automatisch gestartet, um ein Mining nach Monero oder anderen Kryptowährungen durchzuführen. Diese Mining-Aktivität, die häufig ohne Zustimmung des Benutzers gestartet wird, beansprucht Ressourcen und kann betroffene Computer verlangsamen.

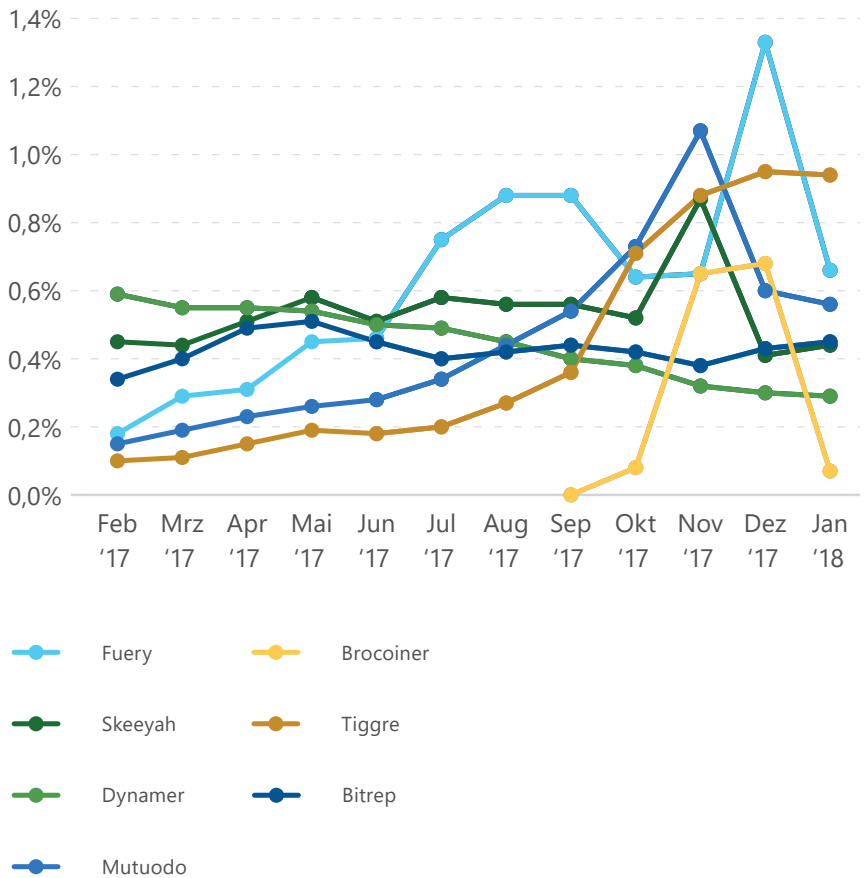


***Abbildung 24**: Trends für das Auftreten der häufigsten Schadsoftwarefamilien, Februar 2017 bis Januar 2018*

- Die häufigsten unerwünschten Softwarefamilien waren Browser Modifier.
- Win32/Prifou ist ein Browser-Modifier, der installiert wird, wenn der Benutzer von bestimmten Drittanbieter-Websites andere Software herunterlädt. Während der Benutzer surft, wird Werbung angezeigt, die „Price Fountain“ zugeschrieben wird.
- Win32/Foxiebro ist ein Browser-Modifier, der Werbung auf Suchergebnisseiten einschleusen kann, Webseiten ändern kann, um Werbung einzufügen, und Werbung in neuen Registerkarten öffnen kann.

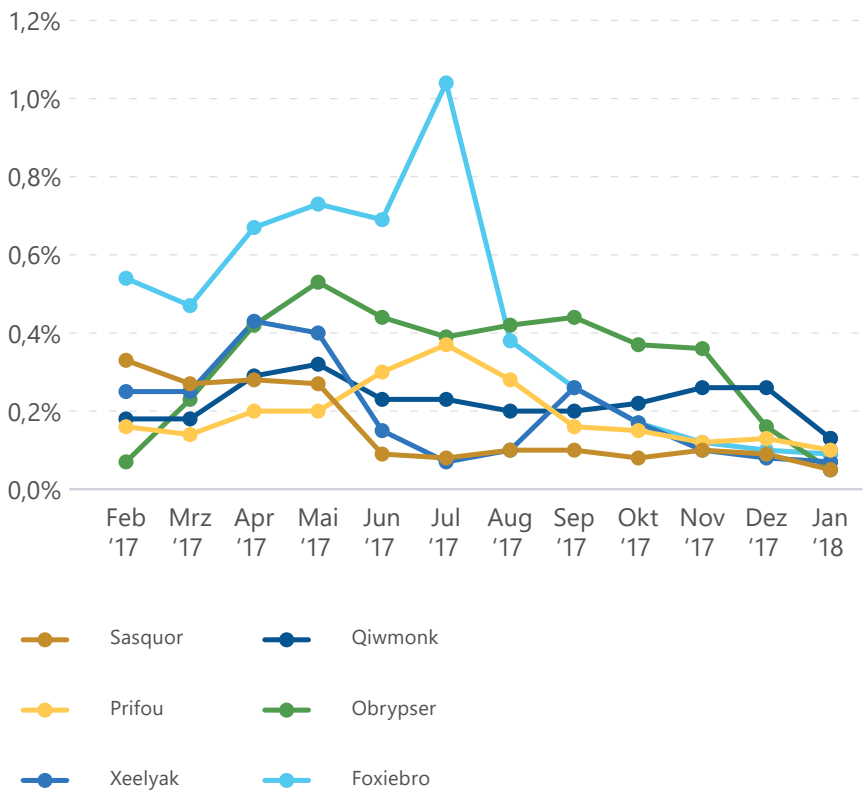


***Abbildung 25**: Trends für das Auftreten der häufigsten unerwünschten Softwarefamilien, Februar 2017 bis Januar 2018*

Bösartige Websites

Microsoft Edge und neuere Versionen von Microsoft Internet Explorer enthalten den SmartScreen-Filter, eine Funktion, die Webanforderungen anhand einer schwarzen Liste bekannter bösartiger Websites überprüft und den Zugriff auf sie standardmäßig blockiert. Bösartige Websites umfassen sowohl Phishing-Sites, die als legitime Websites getarnt sind, um Benutzer zur Eingabe sensibler Informationen zu verleiten, als auch Websites, die Schadsoftware hosten und verbreiten.

Eine Impression ist eine einzelne Instanz eines Benutzers, der versucht, mit aktiviertem SmartScreen-Filter eine bekannte Phishing-Site zu besuchen, und gewarnt wird, wie in Abbildung 26 dargestellt ist.

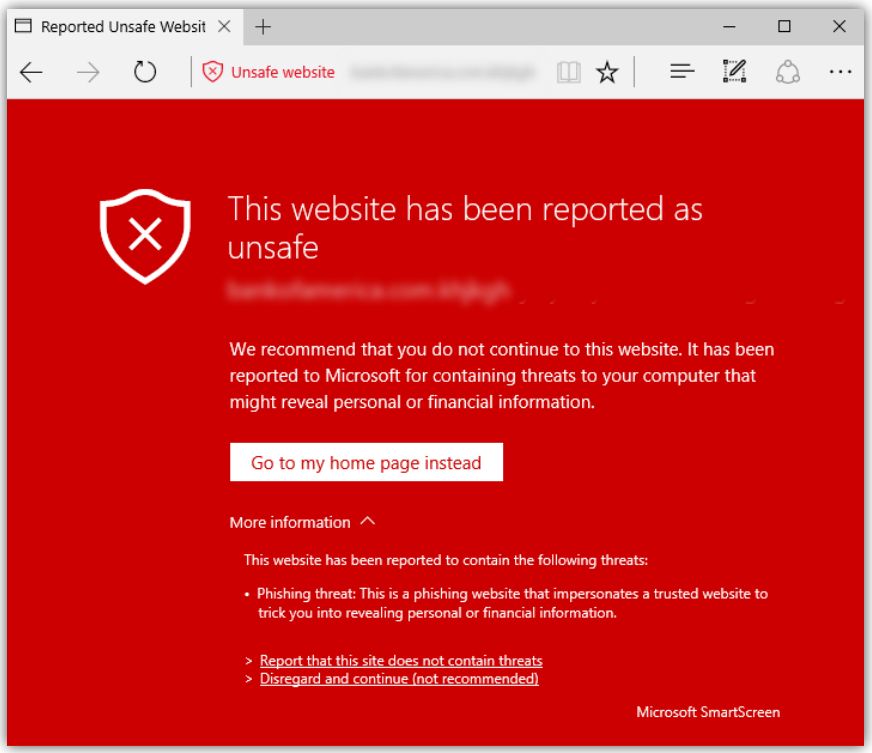


***Abbildung 26**: Zum Schutz der Benutzer werden gemeldete Phishing-Sites und Sites mit Schadsoftware vom SmartScreen-Filter in Microsoft Edge und Internet Explorer blockiert*

- Im zweiten Halbjahr 2017 erkannte SmartScreen weltweit 5,8 Phishing-Sites pro 1.000 Internethosts.
- Zu den Standorten, die eine überdurchschnittlich hohe Konzentration von Phishing-Sites hosten, gehören die Ukraine (19,1 pro 1.000 Internethosts im zweiten Halbjahr 2017), Weißrussland (12,3), Bulgarien (12,2) und Indonesien (10,8). Zu den Standorten mit einer geringen Konzentration von Phishing-Seiten gehörten Taiwan (0,7), China (0,8), Mexiko (0,8) und Korea (1,0).

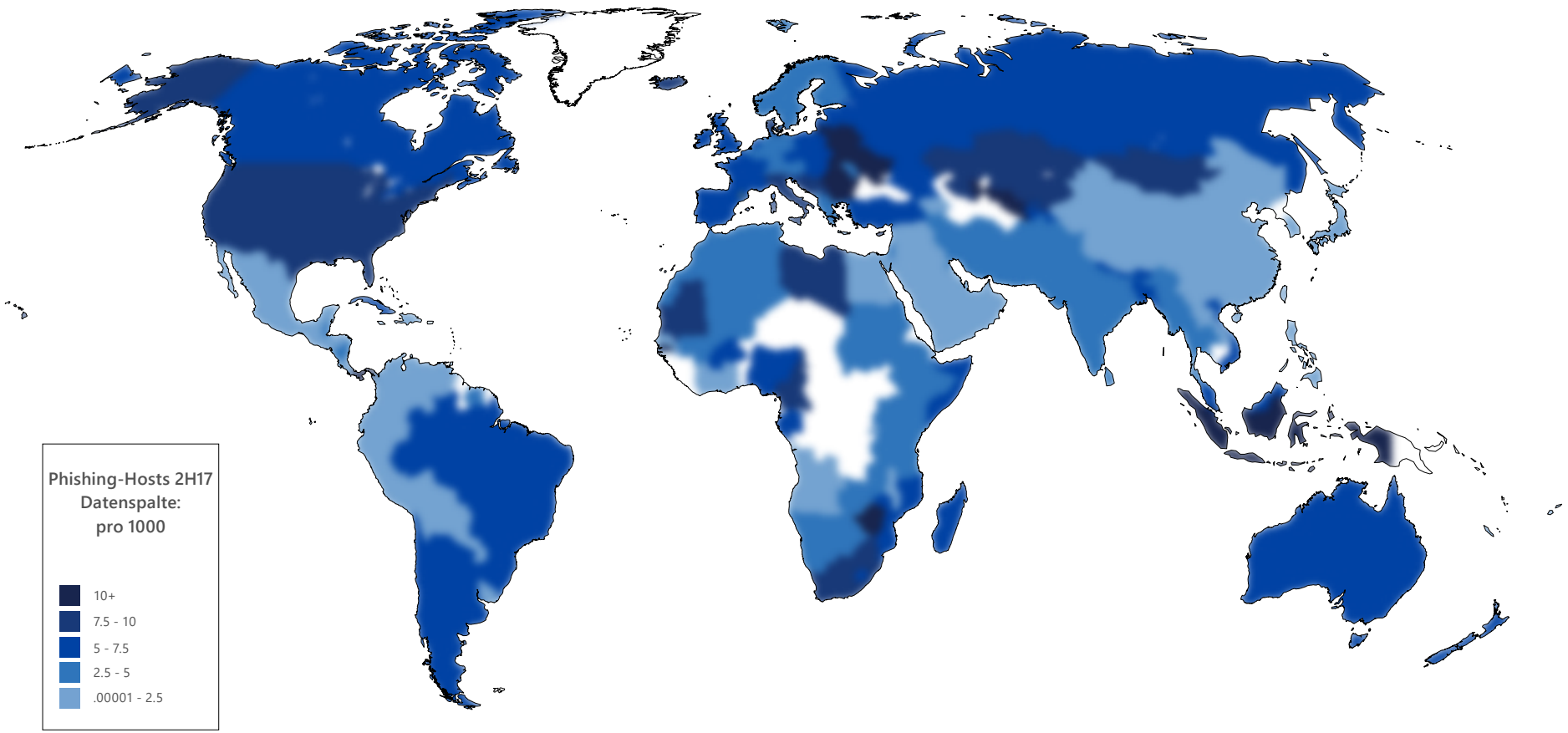


***Abbildung 27**: Phishing-Sites pro 1.000 Internethosts für Standorte weltweit im zweiten Halbjahr 2017*

- SmartScreen meldete 11,7 Phishing-Impressionen pro 1.000.000 Seitenaufrufe im zweiten Halbjahr 2017.
- Zu den Standorten mit ungewöhnlich hohen Phishing-Impressionen gehörten Albanien (188,5 Phishing-Impressionen pro 1.000.000 Seitenaufrufe im zweiten Halbjahr 2017), Armenien (186,5) und Island (77,9).
- Zu den Standorten mit ungewöhnlich niedrigen Phishing-Impressionen gehörten Korea (1,0 Impressionen pro 1.000.000 Seitenaufrufe im zweiten Halbjahr 2017), Japan (1,7) und China (1,9).

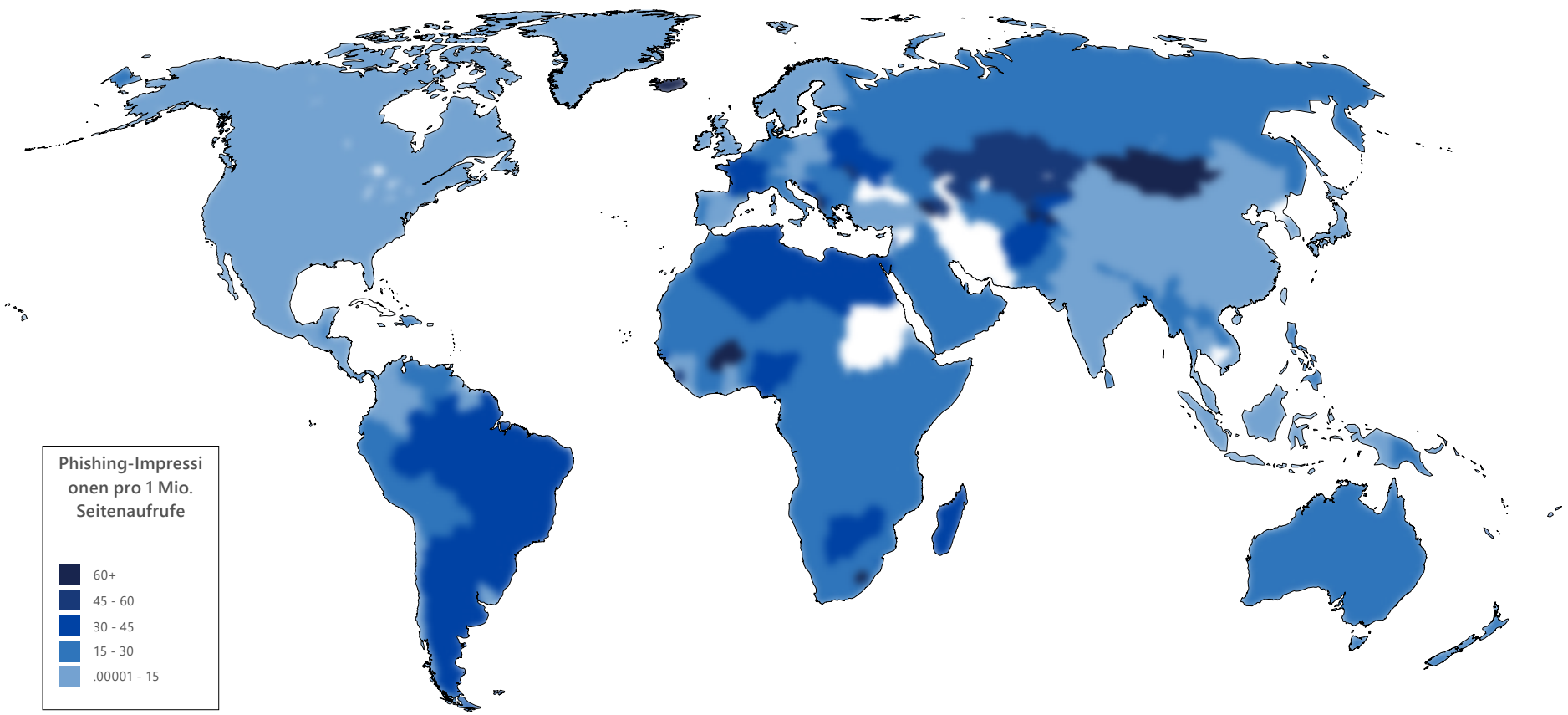


***Abbildung 28**: Phishing-Impressionen nach Clientstandort pro 1.000.000 Seitenaufrufe im zweiten Halbjahr 2017*

- Im zweiten Halbjahr 2017 erkannte SmartScreen weltweit 12,1 Sites, die Schadsoftware hosten, pro 1.000 Internethosts.
- China mit einer der niedrigsten Konzentrationen von Phishing-Sites auf der Welt (0,8 Phishing-Sites pro 1.000 Internethosts im zweiten Halbjahr 2017), wies eine der höchsten Konzentrationen von Sites auf, die Schadsoftware hosten (32,5 Sites, die Schadsoftware hosten, pro 1.000 Hosts im zweiten Halbjahr 2017). Andere Standorte mit einer hohen Konzentration von Sites, die Schadsoftware hosten, umfassten Singapur (21,6), Russland (14,0) und Hongkong (SAR) (14,0). Zu den Standorten mit geringer Konzentration von Sites, die Schadsoftware hosten, gehörten Taiwan (3,4), Österreich (3,4) und Mexiko (3,5).

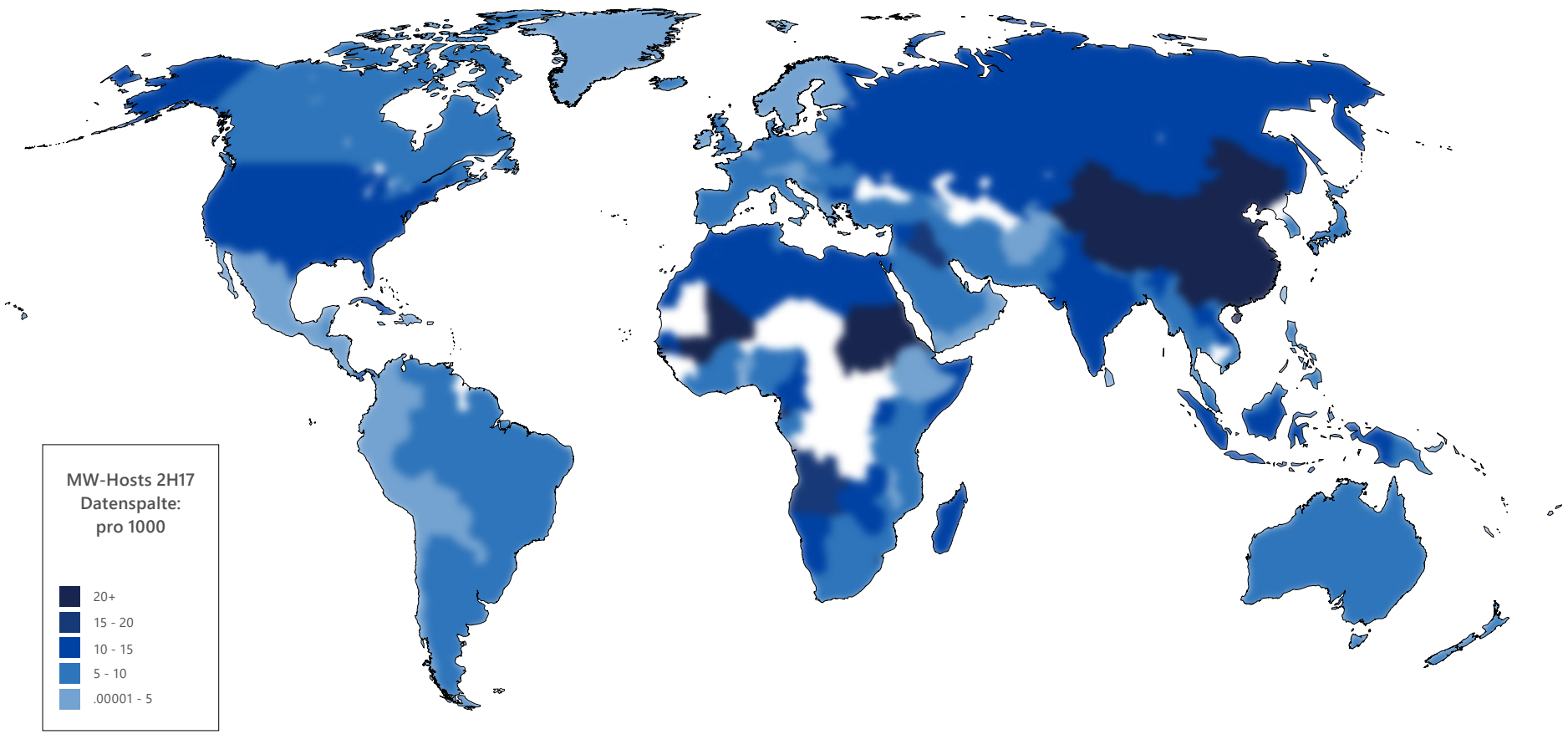


***Abbildung 29**: Sites mit Schadsoftware pro 1.000 Internethosts für weltweite Standorte im zweiten Halbjahr 2017*

- Schadsoftware-Impressionen waren im zweiten Halbjahr 2017 viel häufiger als Phishing-Impressionen. SmartScreen meldete 190,0 Schadsoftware-Impressionen pro 1.000.000 Seitenaufrufe im zweiten Halbjahr 2017, verglichen mit 11,7 Phishing-Versuchen pro 1.000.000 Seitenaufrufe.
- Zu den Standorten, die von Schadsoftware-Impressionen stark betroffen waren, gehörten Ägypten (754,4 Schadsoftware-Impressionen pro 1.000.000 Seitenaufrufe im zweiten Halbjahr 2017), Peru (680,2) und Ungarn (623,5).
- Zu den Standorten mit ungewöhnlich niedrigen Schadsoftware-Impressionen gehörten Korea (20,0), Japan (64,1) und Island (96,3).

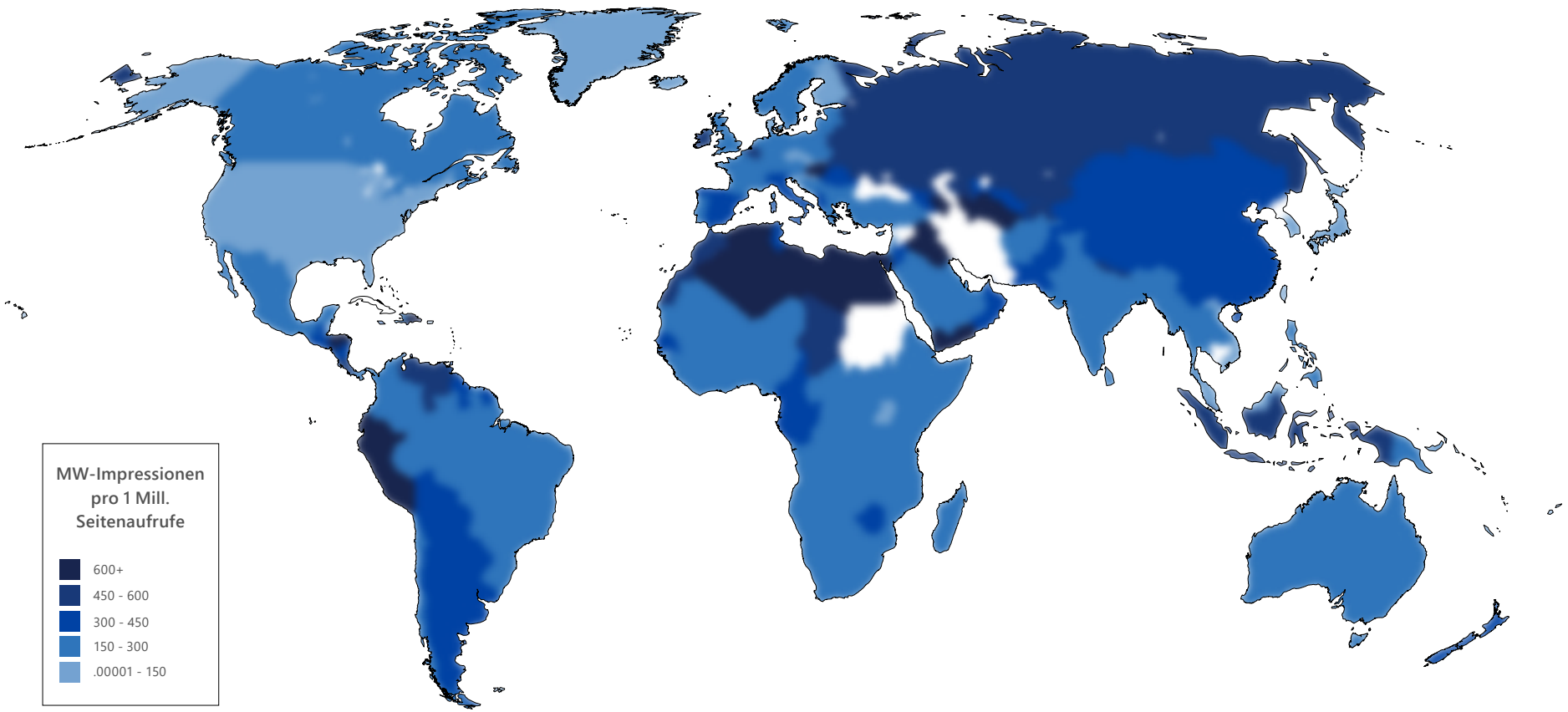


***Abbildung 30**: Schadsoftware-Impressionen nach Clientstandort pro 1.000.000 Seitenaufrufe im zweiten Halbjahr 2017*

Schlussbe-merkungen

Das vergangene Jahr hat uns Folgendes gezeigt: die erheblichen Auswirkungen des Gamarue Botnets auf Computer weltweit, Cyberkriminelle, die weniger anspruchsvolle Methoden nutzen, um Computer zu infizieren und in einigen Fällen Lösegeld von den Opfern erpressen, und Ransomware, die in einem breiten Spektrum von Aktivitäten der Cyberkriminalität eingesetzt wird, darunter E-Mail-Phishing-Kampagnen und destruktiven Angriffe wie WannaCrypt. Organisationen, die Methoden zur Sicherheitspflege, Sicherheitslösungen und bewährte Methoden anwenden, verfügen über Cyberresilienz und über Reaktionspläne für Vorfälle und setzen für den Umgang mit den verschiedenen beschriebenen Bedrohungsszenarien und Angriffen die richtige Mischung von Personen und Prozessen ein, die Schäden und Auswirkungen zumindest minimieren könnte.

Microsoft ist ein vertrauenswürdiger Sicherheitsberater und Partner großer globaler Organisationen. Wenn Sie mehr über unsere Sicherheitsangebote erfahren möchten, besuchen Sie www.microsoft.com/security und rufen Sie den Microsoft-Sicherheitsblog foder unsere Perspektiven zu weiteren wiederkehrenden Bedrohungen und Themen.

Autoren und Mitwirkende

Abhijeet Hatekar
Informationsschutz und Schutz vor Bedrohungen

Abhishek Agrawal
Informationsschutz

Christopher Coy
Digital Crimes Unit

Daniel Kondratyuk
Team für Identitätssicherheit und -schutz

Diana Kelley
Enterprise Cybersecurity Group

Elia Florio
Windows Active Defense

Eric Avena
Windows Defender-Forschungsteam

Eric Douglas
Windows Defender-Forschungsteam

Francis Tan Seng
Windows Defender-Forschungsteam

John Dellinger
Microsoft Threat Intelligence

Jonathan San Jose
Windows Defender-Forschungsteam

Karthik Selvaraj
Windows Defender-Forschungsteam

Kasia Kaplinska
Microsoft Security Marketing

Mark Simos
Enterprise Cybersecurity Group

Matt Duncan
Windows Active Defense Data Engineering und Analytik

Meths Ferrer
Windows Active Defense

Paul Henry
Wadeware LLC

Prachi Rathee
Windows Active Defence Data Engineering und Analytik

Rodel Finones
Digital Crimes Unit

Ryan McGee
Microsoft Security Marketing

Seema Kathuria
Enterprise Cybersecurity Group

Tanmay Ganacharya
Windows Defender-Forschungsteam

Tim Kerk
Windows Defender-Forschungsteam

Tomer Teller
Azure-Sicherheit

Vishant Patel
Digital Crimes Unit

Volv Grebennikov
Bing

Yiftach Keshet
Microsoft Cloud App Security-Forschungsteam

Yinon Costica
Microsoft Cloud App Security-Forschungsteam

Zheng Dong
Windows Defender ATP-Forschung

Datenquellen

Die im Microsoft Security Intelligence Report enthaltenen Daten stammen aus einer Vielzahl von Microsoft-Produkten und-Diensten, deren Benutzer sich für die Bereitstellung von Nutzungsdaten entschieden haben. Dank der Größenordnung und des Umfangs dieser telemetrischen Daten liefert der Bericht die umfassendste und detaillierteste Perspektive für die Bedrohungslandschaft, die in der Softwarebranche verfügbar ist:

- Azure Security Center ist ein Dienst, der Organisationen dabei unterstützt, Bedrohungen zu verhindern, zu erkennen und darauf zu reagieren, indem ein besserer Einblick in die Sicherheit von Cloud-Arbeitslasten ermöglicht wird und fortschrittliche Analysen sowie Threat Intelligence eingesetzt werden, um Angriffe zu erkennen.
- Bing, die Such-und Entscheidungsmaschine von Microsoft, enthält Technologie, die mehrere Milliarden Webseiten pro Jahr scannt, um schädliche Inhalte zu suchen. Nachdem solche Inhalte erkannt wurden, zeigt Bing den Benutzern Warnungen zu den Inhalten an, um Infektionen zu verhindern.
- Exchange Online ist der von Microsoft gehostete E-Mail-Dienst für Unternehmen. Exchange Online-Antimalware-und Antispam-Dienste scannen jedes Jahr mehrere Milliarden Nachrichten, um Spam und Schadsoftware zu identifizieren und zu blockieren.
- Das Tool zum Entfernen bösartiger Software (MSRT) ist ein kostenloses Tool, das von Microsoft entwickelt wurde, um bestimmte verbreitete Schadsoftwarefamilien auf Kundencomputern zu identifizieren und von dort zu entfernen. Das MSRT wird hauptsächlich als wichtiges Update über Windows Update, Microsoft Update und automatische Updates veröffentlicht. Eine Version des Tools ist auch im Microsoft Download Center verfügbar. Das MSRT wurde 2017 in jedem Monat im Durchschnitt mehr als 600 Millionen Mal heruntergeladen und ausgeführt. Das MSRT ist kein Ersatz für eine aktuelle Echtzeit-Antivirus-Lösung.

- Der Microsoft Safety Scanner ist ein kostenloses Sicherheitstool zum Herunterladen, das On-Demand-Scans bereitstellt und das Entfernen von Schadsoftware und anderer bösartiger Software unterstützt. Der Microsoft Safety Scanner ist kein Ersatz für eine aktuelle Antivirus-Lösung, da er keinen Echtzeitschutz bietet und nicht verhindern kann, dass ein Computer infiziert wird.
- Microsoft Security Essentials ist ein kostenloses Produkt für den Echtzeitschutz zum problemlosen Herunterladen, das grundlegenden, effektiven Antivirus-und Antispyware-Schutz für Windows Vista und Windows 7 bietet.
- Microsoft System Center Endpoint Protection (ehemals Forefront Client Security und Forefront Endpoint Protection) ist ein vereinheitlichtes Produkt, das Schutz vor Schadsoftware und unerwünschter Software für Desktops, Laptops und Server-Betriebssysteme von Unternehmen bietet. Es verwendet die Microsoft Malware Protection Engine und die Microsoft-Datenbank für Antivirenprogrammsignaturen, um Echtzeit-, geplanten und On-Demand-Schutz bereitzustellen.
- Office 365 ist der Microsoft Office-Abonnementdienst für Geschäfts- und Privatbenutzer. Ausgewählte Geschäftspläne beinhalten den Zugriff auf Office 365 Advanced Threat Protection.
- Windows Defender in Windows 8, Windows 8.1 und Windows 10 bietet Echtzeitscans sowie die Beseitigung von Schadsoftware und unerwünschter Software.
- Windows Defender Advanced Threat Protection ist ein neuer Dienst, der in das Windows 10 Anniversary Update integriert ist und Unternehmenskunden ermöglicht, hochentwickelte persistente Bedrohungen und Datenschutzverletzungen in ihren Netzwerken zu erkennen, zu untersuchen und zu korrigieren.
- Windows Defender Offline ist ein Tool zum Herunterladen, das zum Erstellen von bootfähigen CDs, DVDs und USB-Flashlaufwerken verwendet werden kann, um einen Computer auf Schadsoftware und andere Bedrohungen zu untersuchen. Es bietet keinen Echtzeitschutz und ist kein Ersatz für eine aktuelle Antimalware-Lösung.
- Windows Defender SmartScreen, eine Funktion in Microsoft Edge und Internet Explorer, bietet Benutzern Schutz vor Phishing-Sites und Sites, die Schadsoftware hosten. Microsoft unterhält eine Datenbank mit Phishing-Sites und Sites mit Schadsoftware, die von Benutzern von Microsoft Edge, Internet Explorer und anderen Microsoft-Produkten und -Diensten gemeldet werden. Wenn ein Benutzer versucht, bei aktiviertem Filter eine Website in der Datenbank zu besuchen, zeigt der Browser eine Warnung an und blockiert die Navigation zu der Seite.

Produkt oder Dienstleistung	URL der Datenschutzerklärung
Azure/Azure Security Center	privacy.microsoft.com/de-de/privacystatement/
Bing	privacy.microsoft.com/de-de/privacystatement/
Exchange Online, Office 365	privacy.microsoft.com/de-de/privacystatement/
Internet Explorer 11	privacy.microsoft.com/en-us/internet-explorer-ie11-preview-privacy-statement
Tool zum Entfernen bösartiger Software	www.microsoft.com/en-us/safety/pc-security/msrt-privacy.aspx
Microsoft Edge	privacy.microsoft.com/de-de/privacystatement/
Microsoft Safety Scanner	www.microsoft.com/de-de/wdsi/products/scanner
Microsoft Security Essentials	windows.microsoft.com/windows/security-essentials-privacy
System Center Endpoint Protection	www.microsoft.com/privacystatement/en-us/SystemCenter2012R2/Default.aspx#tilepspSystemCenter2012R2EndpointProtectionModule
Windows Defender in Windows 10	privacy.microsoft.com/de-de/privacystatement/
Windows Defender Offline	privacy.microsoft.com/en-us/windows-defender-offline-privacy

***Abbildung 31**: US-Datenschutzerklärungen für die in diesem Bericht verwendeten Microsoft-Produkte und-Dienstleistungen*

Glossar der Bedrohungsdefinitionen

Weitere Informationen zu einigen der in diesem Bericht beschriebenen und anderen Bedrohungsfamilien finden Sie unter:

https://www.microsoft.com/de-de/wdsi/threats