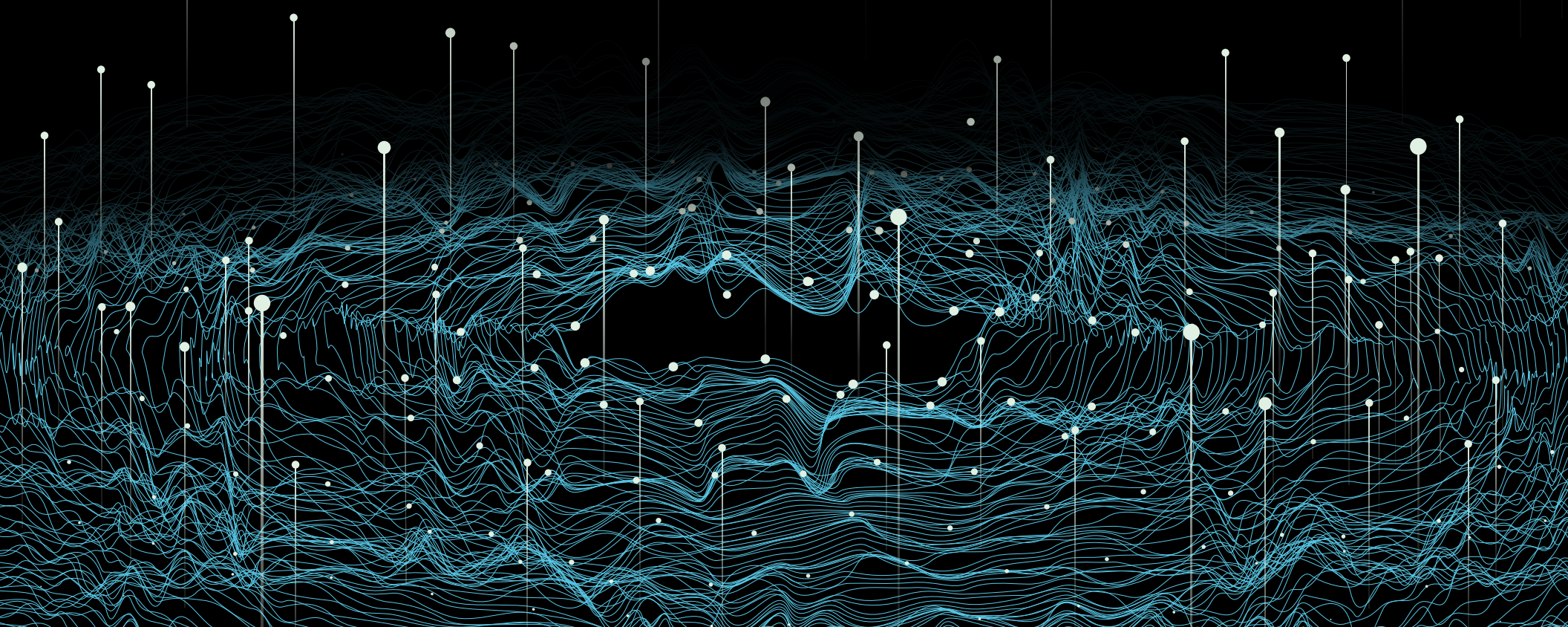
Microsoft

MICROSOFT SECURITY INTELLIGENCE REPORT

AUSGABE 24
JANUAR – DEZEMBER 2018



Inhalt

Autoren und Mitwirkende

Abhishek Agrawal
Schutz von Informationen

David Fantham
Information Protection

Debraj Ghosh
Microsoft Security Marketing

Diana Kelley
Cybersecurity Solutions Group

Elia Florio
Windows Active Defense

Eric Avena
Windows Defender-Forschungsteam

Eric Douglas
Windows Defender-Forschungsteam

Francis Tan Seng
Windows Defender-Forschungsteam

Jonathan Trull
Cybersecurity Solutions Group

Joram Borenstein
Cybersecurity Solutions Group

Karthik Selvaraj
Windows Defender-Forschungsteam

Kasia Kaplinska
Microsoft Security Marketing

Kristina Laidler
Security Incident Response

Matt Duncan
Windows Active Defence Data Engineering und Analytik

Mark Simos
Cybersecurity Solutions Group

Paul Henry
Wadeware LLC

Pragya Pandey
Microsoft Security Marketing

Ram Pliskin
Azure Security

Ryan McGee
Microsoft Security Marketing

Seema Kathuria
Cybersecurity Solutions Group

Steve Wacker
Wadeware LLC

Tanmay Ganacharya
Windows Defender-Forschungsteam

Volv Grebennikov
Bing

Yaniv Zohar
Azure Security

Vorwort

Hallo und herzlich willkommen bei der 24. Ausgabe des Microsoft Security Intelligence Report (SIR). Als Anwenderin und Sicherheitsarchitektin lese ich Berichte dieser Art, in der Hoffnung, die Landschaft etwas besser verstehen zu können und praktische Ratschläge zu erhalten, wie ich dieses Wissen nutzen kann, um Organisationen effektiver zu verteidigen und zu schützen.

Das SIR-Team möchte mit diesem Bericht Aufklärungsarbeit leisten, um eine verbesserte Cyberresilienz zu erzielen. Es hat sich Daten aus einem Jahr angesehen und die wichtigsten Erkenntnisse festgehalten.

Sie lesen Auswertungen aus einem Jahr Sicherheitsdatenanalysen und praktischen Erfahrungen. Die analysierten Daten umfassen die 6,5 Billionen Bedrohungssignale, die täglich die Microsoft-Cloud durchlaufen, sowie Forschungsergebnisse und Praxiserfahrungen von Tausenden unserer Sicherheitsexperten und Mitarbeiter auf der ganzen Welt. Im Jahr 2018 nutzten Angreifer in ihrem fortwährenden Bestreben, Daten und Ressourcen von Kunden und Organisationen zu stehlen, eine Vielzahl von schmutzigen Tricks – sowohl neue (Coin-Mining) als auch alte (Phishing). Hybrid-Attacken wie die Ursnif-Kampagne vereinigen soziale und technische Ansätze. Da sich die Verteidiger nun besser vor Ransomware – einer aufdringlichen, störenden Form des Angriffs – schützen, haben sich Kriminelle den heimlicheren, aber dennoch profitablen Coin-Miner zugewendet.

Diese Wendung kann frustrierend sein, da Angreifer immer einen Schritt voraus zu sein scheinen. Andererseits ist diese Veränderung auch positiv zu bewerten. Denn sie zeigt, dass Verteidiger und Cybersicherheitsexperten wie Sie Abwehrtechniken implementiert haben, die Angreifer dazu zwangen, ihre bevorzugten Nutzlasten zu ändern und sich von der Ransomware wegzubewegen.

Die Lieferkette ist ein weiterer Bereich, in dem Cyberkriminelle ihre Aktivität erhöht haben. Einer der bemerkenswertesten Angriffe, der Ausbruch von Dofoil-Coin-Miner am 6. März 2018, nahm von einer infizierten Peer-to-Peer-App seinen Anfang. Die Bedenken im Bereich der Lieferkette bezogen sich jedoch nicht nur auf Apps, sondern auch auf die Cloud und schädliche Browsererweiterungen, kompromittierte Linux-Repositories und mehrere Instanzen von Modulen mit Hintertüren. Um diese Bedrohung abzuwenden, stellen Organisationen auf ein transparentes und vertrauenswürdiges Lieferkettenmodell um.

Daten sind toll, aber manchmal ist es hilfreicher, herauszufinden, was in einer Organisation wirklich passiert ist. Aus diesem Grund haben wir Erkenntnisse aus der Praxis unseres Detection and Response Team (DART) einbezogen. Dazu gehört beispielsweise, wie ein großes Produktionsunternehmen Kontrollen implementieren konnte, um eine mehrstufige Phishing-Kampagne zu blockieren, die das Unternehmen seit Monaten plagte, und wie Finanzdienstleistungsorganisationen es schließlich schafften, Angreifer mit fortschrittlichen Untersuchungstools und Endpunktüberwachung aus ihren Systemen zu verbannen.

Nicht zuletzt nahmen Phishing-Klicks weiter zu. Modelle des maschinellen Lernens werden jedoch immer besser darin, Phishing-Angriffe abzuwenden, bevor sie in die Benutzerfelder gelangen, und gegebenenfalls Schäden nach einem Klick zu verhindern. Noch mehr gute Nachrichten? Immer mehr Unternehmen implementieren Multi-Faktor-Lösungen, um den Erfolg von Phishing-E-Mails für den Diebstahl von Anmeldeinformationen zu begrenzen.

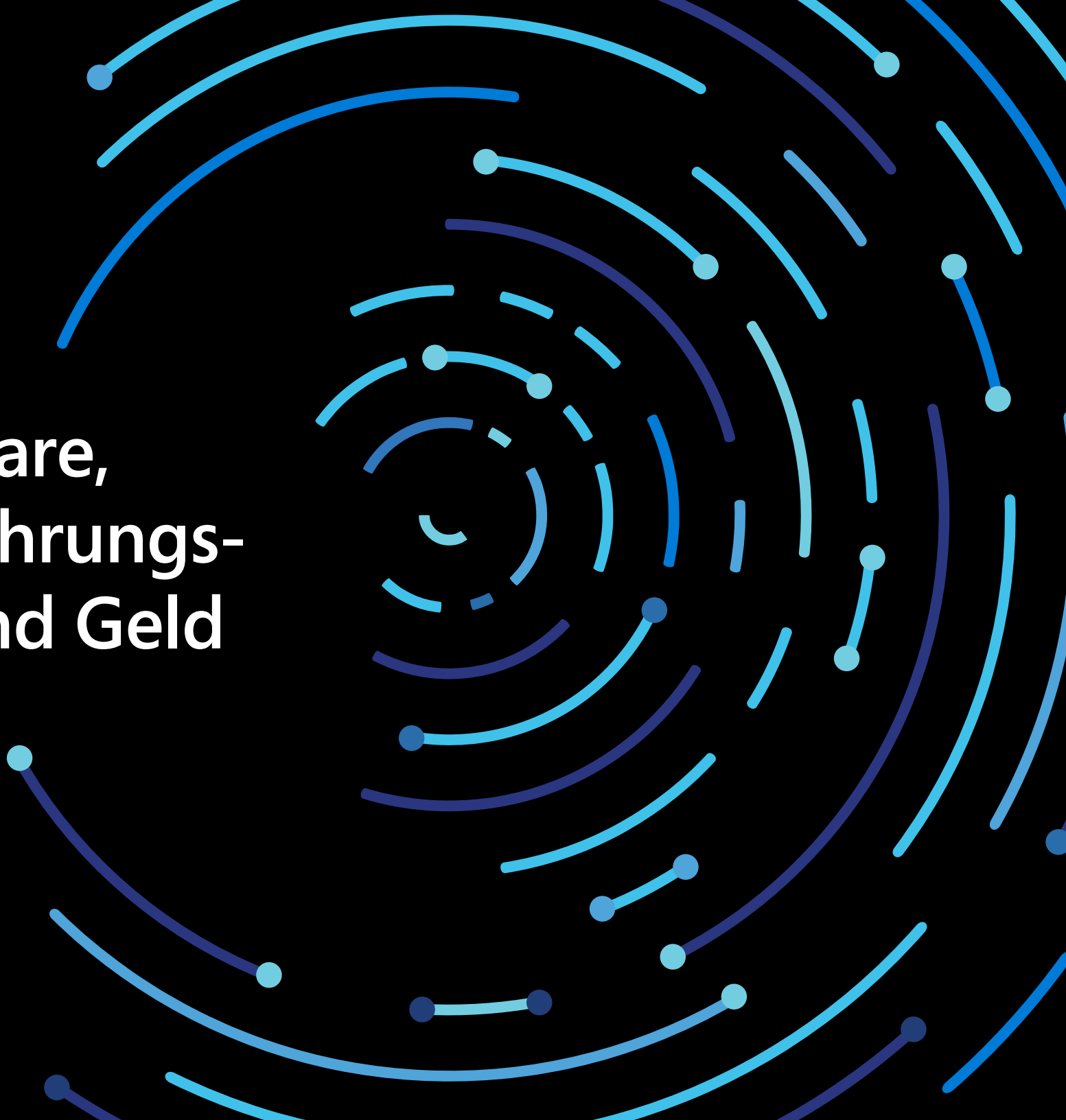
Angreifer suchen nach Möglichkeiten, daher gilt: Je mehr wir über ihre Techniken und ihr Können wissen, desto besser sind wir darauf vorbereitet, Abwehrtechniken zu entwickeln und schnell zu reagieren. Kleine, zielgerichtete Schritte können einen großen Unterschied im Hinblick auf die allgemeine Cybersicherheit einer Organisation machen. Daher finden Sie in diesem Bericht neben tiefgreifenden Einblicken in die sich wandelnde Schadsoftware- und Angriffslandschaft auch empfohlene Schritte und Tipps zu Best Practices. Denn als ich Anwender war, brauchte ich genau das in meinem Kampf gegen Angreifer. Wir hoffen, dass Sie dasselbe brauchen.

Diana Kelley
CTO im Bereich Cybersecurity von Microsoft

P.S. Wir versuchen immer, den SIR zu verbessern. Sollten Sie diesbezüglich Feedback für uns haben, lassen Sie uns dieses bitte zukommen.

ABSCHNITT I

Ransomware, Kryptowährungs-Mining und Geld



Bei den großen Sicherheitsvorfällen im Jahr 2017 ging es meist um Ransomware. Durch bedeutende weltweite Ausbrüche von WannaCrypt und Petya ist Ransomware – eine Art von Schadsoftware, die Computer sperrt oder verschlüsselt und dann Geld verlangt, um den Zugang wieder freizugeben – in das allgemeine Bewusstsein gelangt, und viele haben spekuliert, dass dieses Problem in Zukunft zunehmen würde. Stattdessen gingen die Ransomware-Fälle 2018 deutlich zurück.

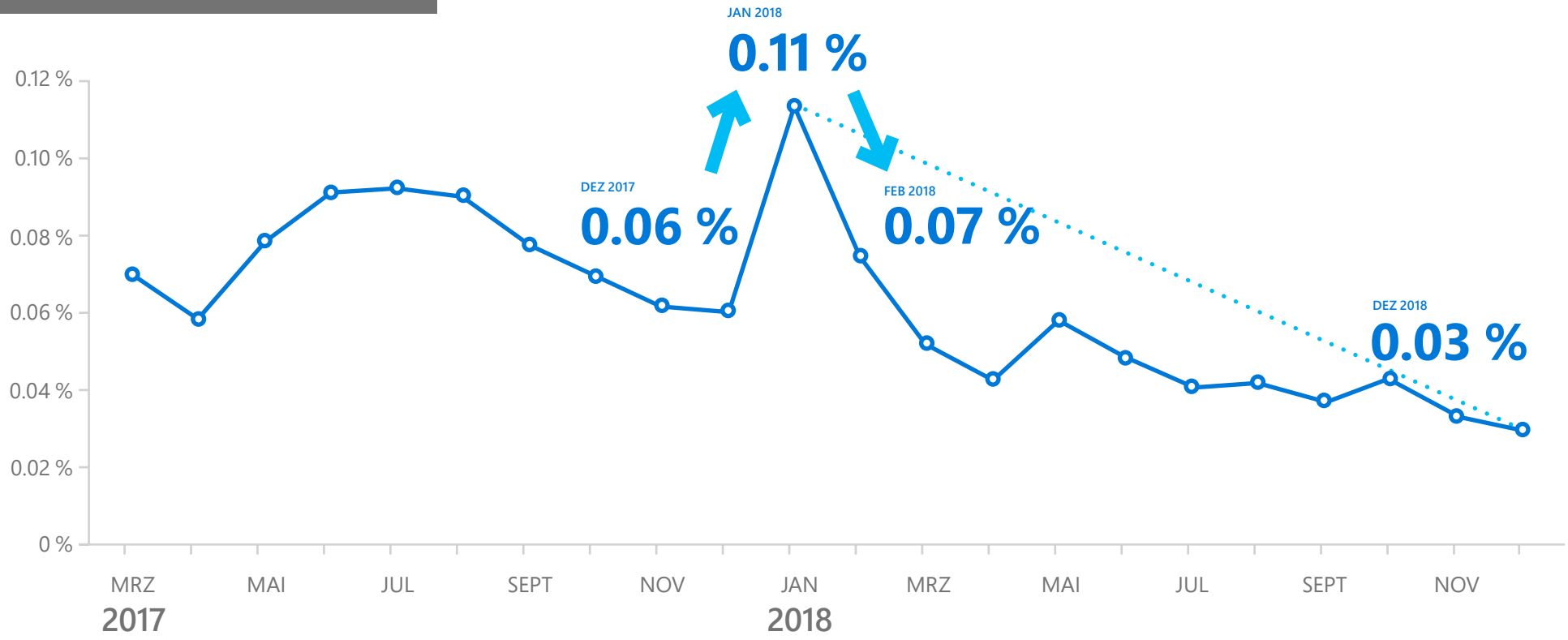
Der Rückgang der Ransomware-Angriffe war zum Teil auf eine verbesserte Erkennung und Aufklärung zurückzuführen, durch die es Angreifern erschwert wurde, dieses Modell profitabel zu betreiben. Infolgedessen begannen sie, der Ransomware den Rücken zu kehren und sich Methoden wie dem Kryptowährungs-Mining zuzuwenden, bei dem Angreifer die Rechenressourcen der Betroffenen nutzen, um digitales Geld zu verdienen. Dieser Wandel zeigt den grundsätzlich opportunistischen Charakter der meisten profitorientierten Cyberkriminellen: Sie neigen dazu, dem am einfachsten verfügbaren Geld hinterherzujagen, und wenn sich die wirtschaftlichen Bedingungen der Cyberkriminalität ändern, orientieren sie sich schnell um.

RANSOMWARE-ANGRIFFE AUF DEM RÜCKZUG

Vor mehr als einem Jahrzehnt wurden die Hacker und Witzbolde, die den frühen Schadsoftware-Untergrund beherrschten, durch organisierte Kriminalität und andere profitorientierte Interessen verdrängt. Während frühe Schadsoftwareausbrüche oft auffällig und offensichtlich waren, operierte gewinnorientierte Schadsoftware eher ruhig und vermied es, Aufmerksamkeit zu erregen, um ihre Funktion – das Versenden von Spam, den Diebstahl sensibler Informationen, die Durchführung von Denial-of-Service-Angriffen und anderer schädlicher Aktivitäten – so lange wie möglich ausüben zu können.

Ransomware steuerte diesem Trend entgegen. Anstatt zu versuchen, unentdeckt zu bleiben, verweigert Ransomware den Betroffenen offen den Zugang zu ihren Computern und wichtigen Dateien, bis sie das Lösegeld bezahlen (und auch nach Zahlung des Lösegelds geben Angreifer ihre Kontrolle über Computer oft nicht ab). Als Ransomware 2017 ihren Höhepunkt erreichte, sah es so aus, als ob dieser Stil des offenen Angriffs eine neue Phase der Angreifertechniken darstellen könnte. Neuere Daten deuten jedoch darauf hin, dass Ransomware auf dem Rückzug sein könnte, wobei Angreifer zunehmend zu der heimlicheren Methode zurückkehren, die sie in der Vergangenheit angewandt haben. Sie versuchen also, unentdeckt zu bleiben, um Angriffe wie Kryptowährungs-Mining effektiver durchführen zu können. Obwohl die Ransomware-Fälle zurückgegangen sind, bedeutet dies nicht unbedingt, dass auch die Schwere der Angriffe abgenommen hat.

Vorkommen von Ransomware



Die Ransomware-Fälle gingen zwischen März 2017 und Dezember 2018 um rund 60 Prozent zurück, wobei in diesem Zeitraum zeitweise auch Anstiege zu verzeichnen waren.

▲ ABBILDUNG 1.

Ransomware-Fälle zwischen März 2017 und Dezember 2018

Es gibt wahrscheinlich viele Ursachen für diesen allgemeinen Rückgang. Microsoft-Sicherheitsexperten vermuten jedoch, dass ein Hauptgrund darin besteht, dass sich sowohl Anwender als auch Organisationen der Ransomware-Bedrohungen stärker bewusst werden und intelligenter damit umgehen. Beispielsweise lassen sie mehr Vorsicht walten und sichern wichtige Dateien, sodass sie im Falle einer Verschlüsselung durch Ransomware wiederhergestellt werden können. Zudem sind Cyberkriminelle, wie bereits erwähnt, opportunistisch.

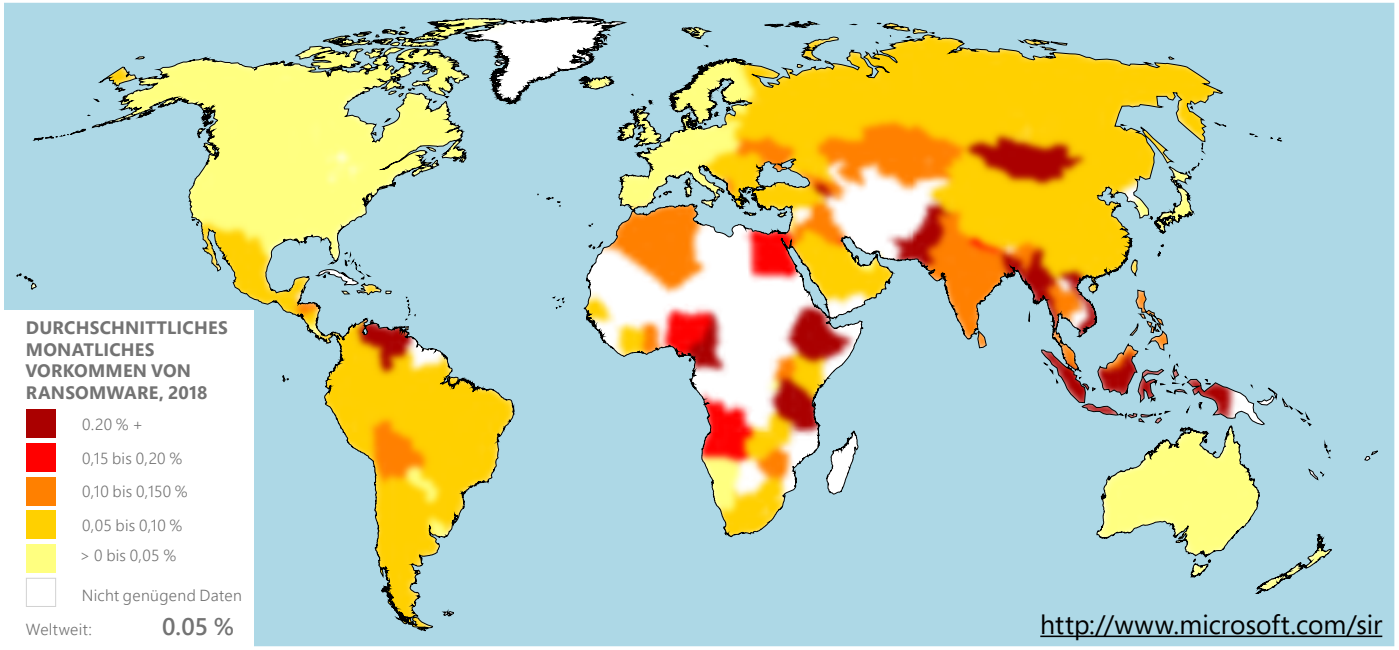
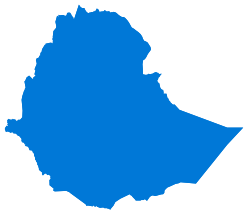


ABBILDUNG 2.

Durchschnittliches monatliches Vorkommen von Ransomware weltweit nach Land/Region im Jahr 2018

AM STÄRKSTEN VON RANSOMWARE BETROFFENES LAND: ÄTHIOPIEN



Durchschnittliches monatliches Vorkommen: **0.77 %**

Die fünf Orte mit durchschnittlich den meisten monatlichen Ransomware-Fällen im Jahr 2018 waren Äthiopien (durchschnittliches monatliches Vorkommen von Ransomware von 0,77 %), Mongolei (0,46 %), Kamerun (0,41 %), Myanmar (0,33 %) und Venezuela (0,31 %), die während des Zeitraums jeweils ein durchschnittliches monatliches Vorkommen von Ransomware von 0,31 Prozent oder höher verzeichneten.1 Vor einigen Jahren konzentrierten sich die Ransomware-Fälle in reichen Ländern und Regionen in Europa und Nordamerika. Seit Ransomware jedoch begann, für Angreifer uninteressanter zu werden, ähnelt das Vorkommensmuster mehr dem von Schadsoftware allgemein.

Die Orte mit den wenigsten Ransomware-Fällen im Jahr 2018 waren Irland (0,01 %), Japan (0,01 %), die Vereinigten Staaten (0,02 %), Großbritannien (0,02 %) und Schweden (0,02 %), mit einem durchschnittlichen monatlichen Vorkommen von Ransomware von jeweils 0,02 Prozent oder niedriger im gleichen Zeitraum. Länder mit wenigen Ransomware-Fällen verfügen in der Regel über eine ausgereifte Cybersicherheitsinfrastruktur und gut etablierte Programme zum Schutz kritischer Infrastrukturen. Außerdem werden dort den Bürgern grundlegende Sicherheitsmaßnahmen kommunikativ vermittelt.

FUSSNOTEN

[1] Das Vorkommen erfasst den Prozentsatz der Computer, auf denen Echtzeit-Sicherheitsprodukte von Microsoft verwendet werden, die das Auftreten von Schadsoftware melden. 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.

KRYPTOWÄHRUNGS-MINING AUF DEM VORMARSCH

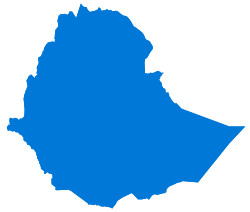
Kryptowährung ist virtuelles Geld, das dazu verwendet werden kann, Waren und Dienstleistungen sowohl online als auch in der realen Welt anonym zu kaufen und zu verkaufen. Es gibt viele verschiedene Arten von Kryptowährungen, sie basieren jedoch alle auf Blockchain-Technologie. Dabei wird jede Transaktion in einem verteilten Ledger aufgezeichnet, das von Tausenden oder Millionen von Computern auf der ganzen Welt gepflegt wird. Neue Coins werden von Computern durch komplexe Berechnungen generiert („mined"), die auch dazu dienen, Blockchain-Transaktionen zu verifizieren.

Das Generieren von Coins kann sehr lukrativ sein – im Jahr 2018 war ein einziger Bitcoin, ein Coin der ältesten und beliebtesten Kryptowährung, mehrere Tausend US-Dollar wert. Die Durchführung der notwendigen Berechnungen kann jedoch sehr ressourcenintensiv sein und wird komplexer, je mehr neue Coins erstellt werden. Bei populären Währungen wie Bitcoin ist es ohne Zugriff auf immense Rechenressourcen, die für die meisten Individuen und kleinen Gruppen vollkommen außer Reichweite liegen, fast unmöglich, auf rentable Weise Coins zu erstellen. Aus diesem Grund haben sich Angreifer, die illegale Gewinne anstreben, zunehmend Schadsoftware zugewendet, die es ihnen erlaubt, die Computer der Betroffenen zu nutzen, um Kryptowährungs-Coins zu erstellen. Auf diese Weise können sie die Verarbeitungsleistung nicht nur von ein oder zwei Computern nutzen, sondern von Hunderttausenden Computern. Selbst wenn eine kleine Infektion entdeckt wird, erschwert es die anonyme Natur der Kryptowährung, die Verantwortlichen aufzuspüren.

Im Jahr 2018 lag das weltweite durchschnittliche monatliche Vorkommen des Kryptowährungs-Coin-Mining bei 0,12 Prozent, verglichen mit nur 0,05 Prozent für Ransomware. Die gestiegene Beliebtheit des Mining als Nutzlast für Schadsoftware hat viele Gründe. Im Gegensatz zu Ransomware ist für das Kryptowährungs-Mining keine Benutzereingabe erforderlich: Es arbeitet im Hintergrund, während der Benutzer andere Aufgaben erledigt oder nicht einmal am Computer ist, und wird unter Umständen gar nicht bemerkt, solange die Leistung des Computers nicht deutlich beeinträchtigt wird. Infolgedessen ist es weniger wahrscheinlich, dass die Nutzer Maßnahmen ergreifen, um die Bedrohung zu beseitigen, und das Mining kann zum Vorteil des Angreifers über einen längeren Zeitraum hinweg fortgesetzt werden.

Für viele Kryptowährungen sind Standardprodukte für das verdeckte Mining verfügbar, was den Trend weiter verstärkt. Die Einstiegshürde ist aufgrund der allgemeinen Verfügbarkeit von Coin-Mining-Software niedrig. Diese Software wird von Cyberkriminellen als Schadsoftware umverpackt, um sie an die Computer ahnungsloser Nutzer zu liefern. Die schädlichen Miner werden dann über viele der gleichen Techniken, die Angreifer anwenden, um andere Bedrohungen zu liefern (wie Social Engineering, Exploits und Drive-by-Downloads), an die Betroffenen verteilt. Nachdem die Mining-Software installiert wurde, wird sie auf den Computern der Betroffenen im Hintergrund ausgeführt und nimmt die Blockchain-Berechnungen vor, von denen der Angreifer profitiert.

DURCHSCHNITTLICHES MONATLICHES VORKOMMEN IN DEN LÄNDERN, DIE AM STÄRKSTEN VON KRYPTOWÄHRUNGS-MINING BETROFFEN SIND



Äthiopien: **5.58 %**

Tansania: **1.83 %**

Pakistan: **1.47 %**

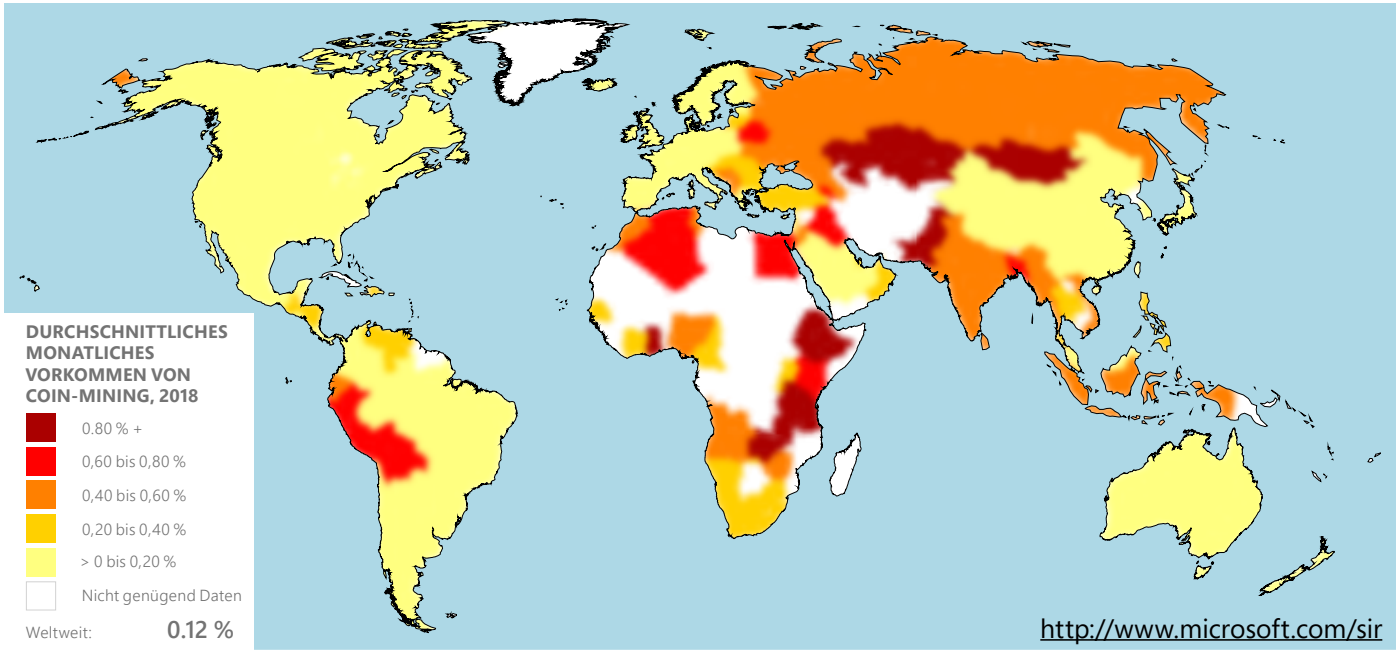


ABBILDUNG 3.

Durchschnittliches monatliches Vorkommen von Coin-Mining weltweit nach Land/Region im Jahr 2018

DURCHSCHNITTLICHES MONATLICHES VORKOMMEN IN DEN LÄNDERN, DIE AM GERINGSTEN VON KRYPTOWÄHRUNGS-MINING BETROFFEN SIND

Irland: 0.02 %

Japan: 0.02 %

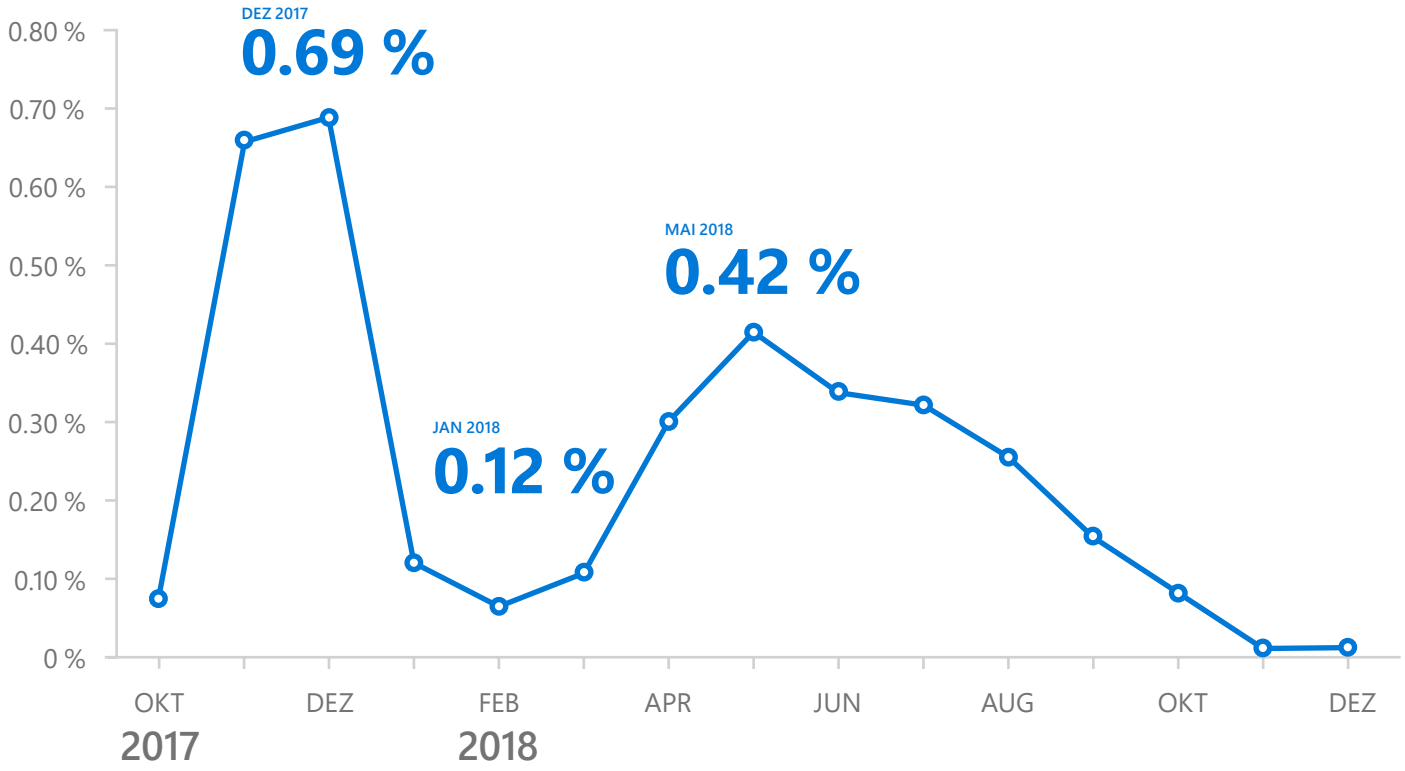
Vereinigte Staaten: 0.02 %

Die fünf Länder mit den meisten Fällen von Kryptowährungs-Coin-Mining im Jahr 2018 waren Äthiopien (5,58 %), Tansania (1,83 %), Pakistan (1,47 %), Kasachstan (1,24 %) und Sambia (1,13 %). Diese Länder verzeichneten während des untersuchten Zeitraums jeweils ein durchschnittliches monatliches Vorkommen von Coin-Mining von ungefähr 1,13 Prozent oder höher. Die Orte mit den wenigsten Fällen von Coin-Mining im Jahr 2018 waren Irland, Japan, die Vereinigten Staaten und China, mit einem durchschnittlichen monatlichen Vorkommen von Coin-Mining von jeweils 0,02 Prozent in diesem Zeitraum.

BROWSERBASIERTE KRYPTOWÄHRUNGS-MINER: EINE NEUE ART DER BEDROHUNG

Die in diesem Abschnitt vorgestellten Statistiken beziehen sich auf schädliche Kryptowährungs-Miner, die so konzipiert sind, dass sie als Schadsoftware auf den Computern der Betroffenen installiert werden. Einige der wichtigsten Kryptowährungs-Mining-Bedrohungen liegen jedoch vollständig innerhalb von Webbrowsern und müssen nicht installiert werden. Verschiedene Dienste werben für browserbasiertes Kryptowährungs-Mining als eine Möglichkeit für Websitebesitzer, den Besucherverkehr auf ihren Websites zu Geld zu machen, ohne sich auf Werbung verlassen zu müssen. Websitebesitzer sollen JavaScript-Code zu ihren Seiten hinzufügen, sodass während des Besuchs der Website

Vorkommen von Brocoiner



durch einen Benutzer im Hintergrund Kryptowährung erstellt wird, wobei der Erlös zwischen dem Websitebesitzer und dem Dienst aufgeteilt wird. Leider haben die Angreifer diese Dienste schnell für sich entdeckt, um Kryptowährung ohne die Zustimmung der Anwender zu erstellen, und zwar häufig durch Kompromittierung legitimer Websites und Einfügen des schädlichen Mining-Codes in ihren Quellcode. Diese browserbasierten Miner müssen den Computer des Anwenders nicht kompromittieren und werden auf jeder Plattform mit JavaScript-fähigem Webbrowser ausgeführt. Genauso wie Kryptowährungs-Mining-Trojaner können auch browserbasierte Miner die Computerleistung erheblich verschlechtern und Strom verschwenden, während ein Nutzer eine infizierte Webseite besucht.

ABBILDUNG 4.

Vorkommen von Brocoiner, dem am weitesten verbreiteten browserbasierten Kryptowährungs-Miner

DIE AUSWIRKUNGEN VON UNERWÜNSCHTEM KRYPTOWÄHRUNGS-MINING

Die offensichtlichste Bedrohung, die für Betroffene von schädlichem Kryptowährungs-Mining ausgeht, ist der Verbrauch von Rechenressourcen, wodurch Strom verschwendet und die Computerleistung erheblich verschlechtert werden kann. Nutzer und Organisationen werden durch Coin-Mining jedoch auch anderen Risiken ausgesetzt, darunter:

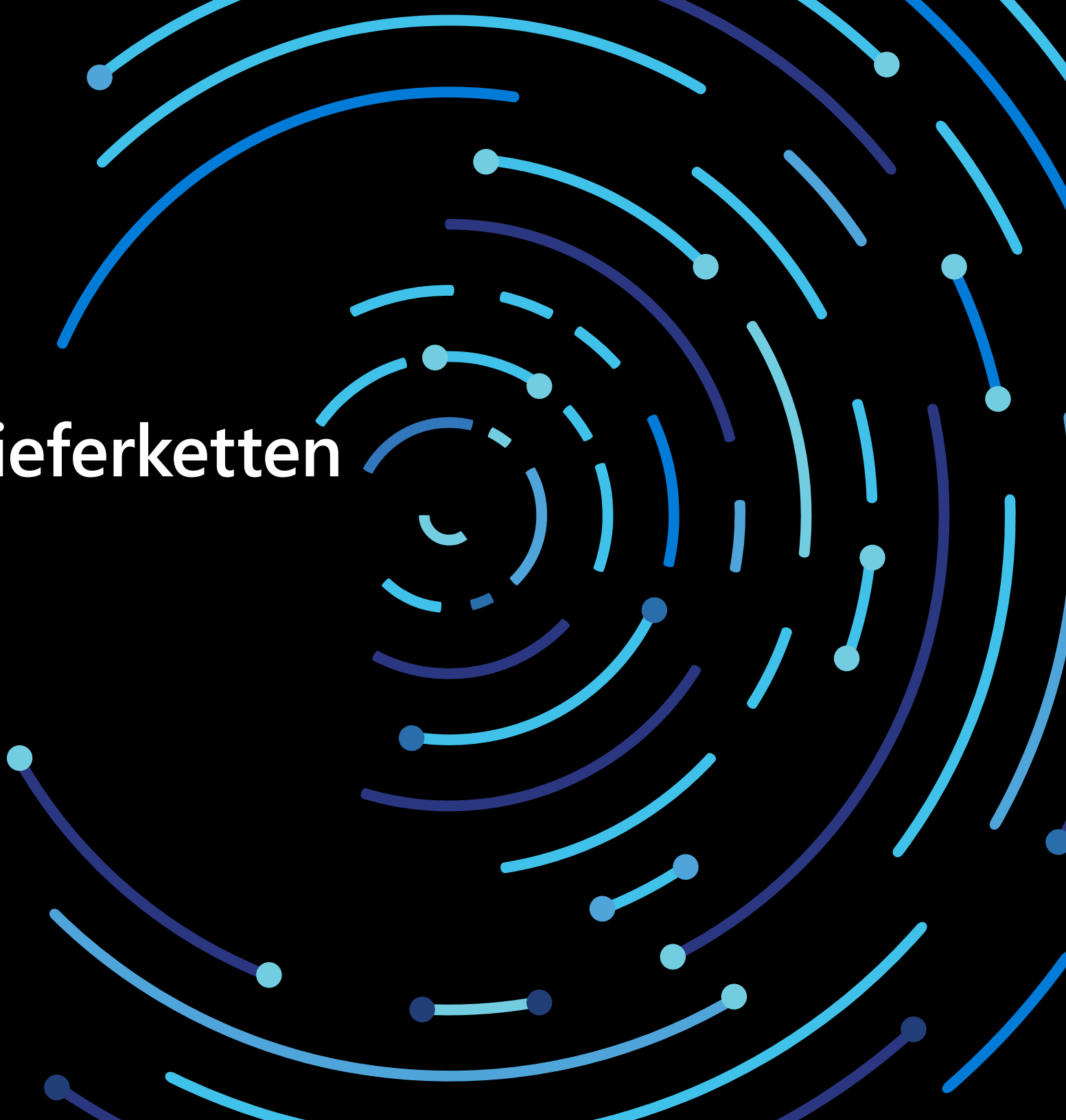
- **Eintrittspforte für größere Schäden in der Zukunft.**
  Wie andere Formen der Schadsoftware kann Kryptowährungs-Mining ein Einstiegspunkt für Angreifer sein. Während der Computer im Hintergrund Kryptowährung erstellt, können Cyberkriminelle Informationen über die Umgebung erfassen und möglicherweise Sicherheitslücken aufdecken, um sie für andere Zwecke auszunutzen.

- **Geräte mit Internetverbindung können kompromittiert und in Bots für Kryptowährungs-Mining verwandelt werden.**
  Vielen solcher Geräte fehlt es an integrierten Sicherheitsfunktionen wie der Erkennung von Schadsoftwarebedrohungen, was sie zu interessanten Zielen für Angreifer machen kann.

- **Beschädigung von Geräten.**
  Software für das Kryptowährungs-Mining, die über Monate oder länger kontinuierlich ausgeführt wird, kann die Leistung beeinträchtigen, und die Hitze, die durch übermäßigen Stromverbrauch und CPU-Auslastung erzeugt wird, kann Computer schädigen.

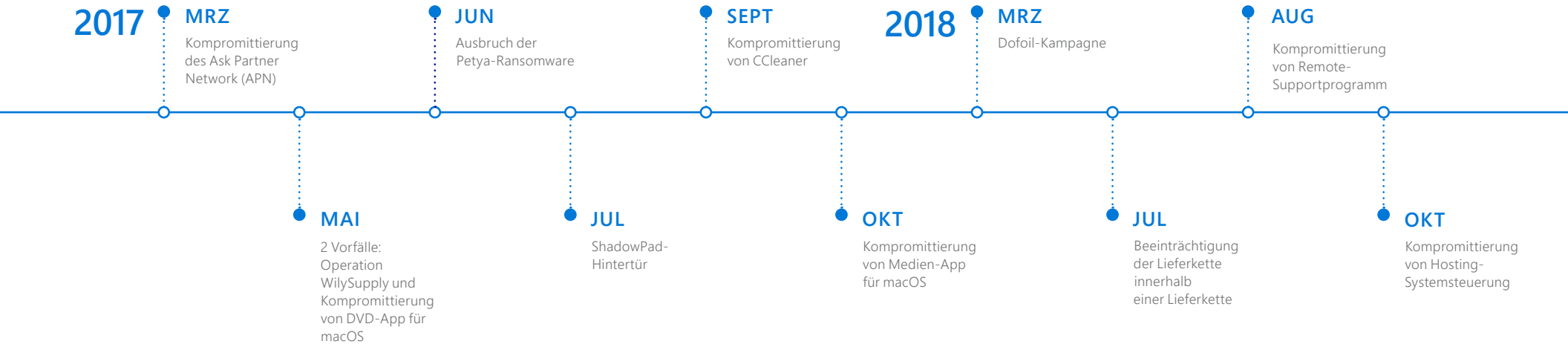
ABSCHNITT II

Softwarelieferketten in Gefahr



Seit Jahren verfolgt Microsoft Angreifer, die die Gefährdung der Lieferkette als Einstiegspunkt für Angriffe nutzen. Bei Angriffen auf die Lieferkette konzentriert sich der Angreifer darauf, den Entwicklungs- oder Update-Prozess eines legitimen Softwareherausgebers zu kompromittieren.

Wenn der Angreifer erfolgreich ist, kann er eine kompromittierte Komponente in eine legitime Anwendung oder ein Updatepaket einspeisen, die dann an die Benutzer der Software verteilt wird. Der schädliche Code wird mit dem gleichen Vertrauen und den gleichen Berechtigungen wie die Software ausgeführt. Die Angriffe auf die Softwarelieferkette haben in den letzten Jahren zugenommen. Dies ist in vielen Gesprächen über die Cybersicherheit zu einem wichtigen Thema geworden und stellt in vielen IT-Abteilungen ein äußerst wichtiges Anliegen dar.



SCHWERWIEGENDE ANGRIFFE AUF SOFTWARELIEFERKETTEN IM JAHR 2017

▲ ABBILDUNG 5.

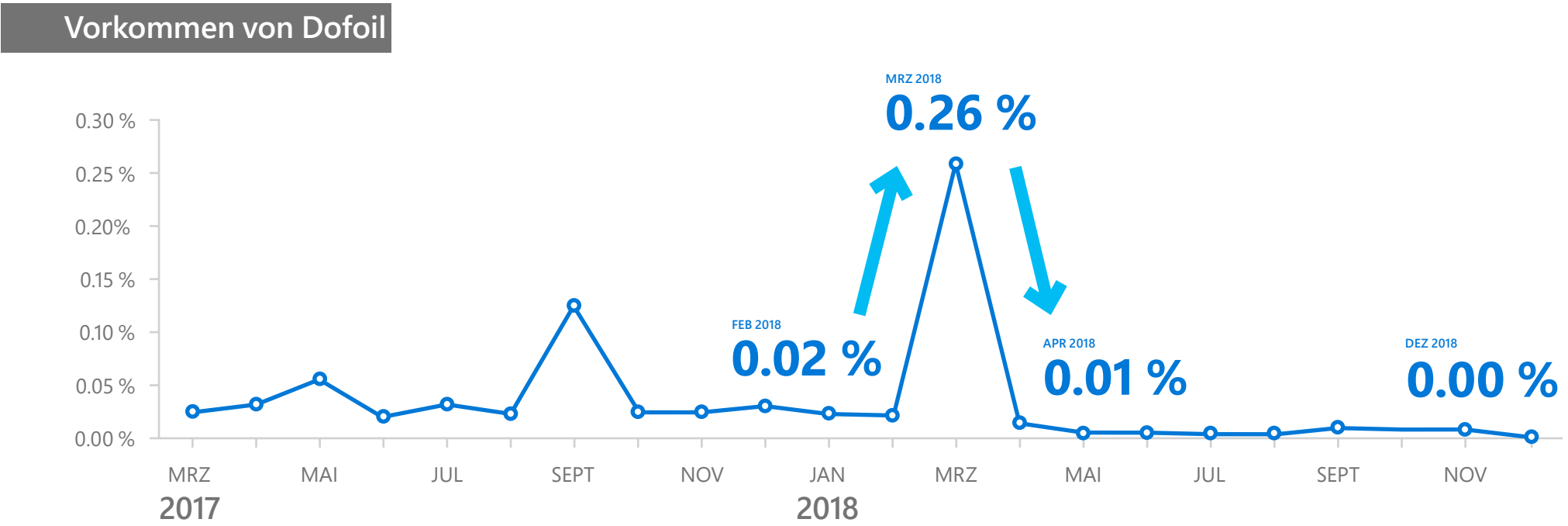
Angriffe auf Softwarelieferketten in den Jahren 2017 und 2018

Im Jahr 2017 waren Lieferkettenangriffe für eine Reihe von bedeutenden Vorfällen verantwortlich, insbesondere für den Ausbruch der Petya-Ransomware im Juni, bei dem die ersten Infektionen auf einen kompromittierten Updateprozess für eine beliebte Steuerbuchhaltungsanwendung in der Ukraine zurückzuführen waren. Im Mai kompromittierte Operation WilySupply den Software-Updater eines Texteditors, um bei Zielorganisationen im Finanz- und IT-Sektor eine Hintertür zu installieren. Im Juli wurde eine Hintertür namens ShadowPad in einem Softwarepaket für die Serververwaltung versteckt und ermöglichte es Angreifern, zusätzliche Schadsoftware-Nutzlasten für Datendiebstahl und andere schädliche Aktivitäten zu installieren. Im September wurde die Infrastruktur des beliebten Freeware-Tools CCleaner kompromittiert und eine Version mit Hintertür an die Benutzerbasis geliefert.

Der erste große Angriff auf eine Softwarelieferkette des Jahres 2018 ereignete sich am 6. März, als Windows Defender ATP eine massive Kampagne zur Lieferung des Dofoil-Trojaners (auch bekannt als „Smoke Loader") stoppte. Die massive Schadsoftwarekampagne konnte auf eine beschädigte Peer-to-Peer-Anwendung zurückgeführt werden. Das Updatepaket der Anwendung wurde durch ein schädliches ersetzt, das kompromittierten Code herunter lud, der später die Dofoil-Schadsoftware installierte. Der ausgeklügelte Trojaner führte eine Coin-Mining-Nutzlast mit und zeichnete sich durch fortschrittliche, prozessübergreifende Einstreuungstechniken, Persistenzmechanismen und Ausweichmethoden aus.

ABBILDUNG 6.

Entwicklung des Vorkommens von Dofoil-Trojanern (Smoke Loader) im Jahr 2018 erreicht im März eine Spitze bei blockierten Instanzen



In den ersten zwölf Stunden der Kampagne blockierte Windows Defender Antivirus weltweit mehr als 400.000 Infektionsversuche. Russland verzeichnete 73 Prozent der weltweiten Fälle, während die Türkei und die Ukraine 18 Prozent bzw. 4 Prozent verbuchten.

Im Jahr 2018 wurden mehrere weitere Angriffe entdeckt, bei denen kompromittierte Softwarelieferketten als Liefermechanismen eingesetzt wurden, darunter die in der folgenden Tabelle beschriebenen:

Zeitraum	Angriff	Beschreibung	Betroffene Software
März 2018	Dofoil-Coin-Mining-Kampagne (berichtet von Microsoft)	Angreifer beschädigten den Updateprozess einer Peer-to-Peer-App, um Dofoil zu installieren, wodurch wiederum Coin-Mining-Schadsoftware installiert wurde.	Peer-to-Peer-App
Juli 2018	Kompromittierung einer Lieferkette innerhalb einer Lieferkette (berichtet von Microsoft)	Angreifer kompromittierten die gemeinsame Infrastruktur zwischen einem PDF-Editor-App-Anbieter und einem seiner Softwareanbieter.	PDF-Editor-App und Drittanbieter
August 2018	Kompromittierung von Remote-Supportprogramm (Operation Red Signature, berichtet von Trend Micro und IssueMakersLab)	Der Updateserver eines Remote-Support-Lösungsanbieters wurde kompromittiert, um ein Remotezugriffstool namens 9002 RAT bereitzustellen.	Remote-Supportprogramm
Oktober 2018	Kompromittierung von Hosting-Systemsteuerungslösung (berichtet von ESET)	Das Installationsskript für eine Hosting-Systemsteuerungslösung wurde abgeändert, um Anmeldedaten zu stehlen.	Hosting-Systemsteuerungslösung

ABBILDUNG 7.

Weitere Angriffe auf Softwarelieferketten im Jahr 2018

VERTRAUEN IN GEFAHR

Angriffe auf Lieferketten sind heimtückisch, weil sie das Vertrauen nutzen, das Anwender und IT-Abteilungen in die verwendete Software setzen. Die kompromittierte Software ist oft vom Anbieter signiert und zertifiziert und enthält möglicherweise keinerlei Hinweis darauf, dass irgendetwas nicht stimmt. Das macht es deutlich schwieriger, die Infektion zu erkennen. Diese Angriffe können das Verhältnis zwischen Lieferketten und ihren Kunden schädigen, egal ob Letztere Firmen- oder Privatnutzer sind. Durch die Beschädigung von Software und die Schwächung von Liefer- oder Aktualisierungsinfrastrukturen können Angriffe auf Lieferketten die Integrität und Sicherheit von Waren und Dienstleistungen beeinträchtigen, die von Organisationen angeboten werden.

Angriffe auf Lieferketten haben bereits eine breite Palette von Software kompromittiert und wurden auf Organisationen in verschiedenen Branchen an unterschiedlichen geografischen Standorten gerichtet. Die Bedrohung durch Angriffe auf Lieferketten ist ein branchenweites Problem, das Aufmerksamkeit von mehreren Stakeholdern erfordert, darunter die Softwareentwickler und -anbieter, die den Code schreiben, die Systemadministratoren, die Softwareinstallationen verwalten, und die Informationssicherheits-Community, die diese Angriffe entdeckt und Lösungen schafft, um Menschen und Software vor ihnen zu schützen.

JENSEITS VON SOFTWARE: LIEFERKETTENKOMPROMITTIERUNG DURCH CLOUD-OBJEKTE

Die Fähigkeit von Lieferkettenangriffen, das Vertrauen zu untergraben, wird in der Cloud verstärkt und noch komplexer. Mehrere Vorfälle mit kompromittierten Cloud-Objekten, Diensten und Infrastruktur im Jahr 2018 unterstreichen diese Komplexität:

- Beschädigte Chrome-Erweiterungen, die Klickbetrug-Schadsoftware installierten (berichtet von ICEBERG)
- Verschiedene kompromittierte Linux-Repositories (berichtet in einigen Onlineforen)
- Schädliche WordPress-Plug-Ins für verschiedene schädliche Aktivitäten verwendet, einschließlich der Möglichkeit für Angreifer, Inhalte auf WordPress-Websites zu veröffentlichen (berichtet von Wordfence)
- Schädliche Docker-Images, die ein Skript zum Herunterladen von Kryptowährungs-Coin-Mining-Schadsoftware enthielten und in Docker-Hub-Konto hochgeladen wurden (berichtet von Fortinet und Kromtech)
- Ein schädliches Typosquatting-Paket im offiziellen Python-Respository; das Paket enthielt ein schädliches Skript, das Schadsoftware herunterlädt, die verwendet wird, um Coin-Mining-Adressen in der Zwischenablage zu rauben (berichtet über Medium)
- Kompromittiertes Skript in StatCounter, das es Angreifern ermöglichte, ein schädliches Skript in Websites einzuschleusen, die StatCounter verwenden (berichtet von ESET)
- Mehrere Fälle von npm-Modulen mit Hintertür (Der npm-Blog, Medium), die bei Nutzung beispielsweise dazu führen können, dass ein Angreifer in der Lage ist, beliebigen Code in einen laufenden Server einzugeben und auszuführen

Diese Vorfälle zeigen, wie die Kompromittierung von Lieferketten Angriffsflächen enorm vergrößern kann. Werden Cloud-Objekte nicht gesichert, können sie unerwartete Einstiegsvektoren sein. Beispielsweise wurden bei dem Docker-Hub-Vorfall Docker-Images mit versteckter Coin-Mining-Hintertür von einem schädlichen Konto hochgeladen. Die Docker-Images wurden fast ein Jahr lang auf dem Docker-Hub gehostet und Millionenfach heruntergeladen und von ahnungslosen Administratoren und Nutzern verwendet.

Die Gefahren für Lieferketten erstrecken sich auch auf Code in der Cloud, Open Source, Webbibliotheken, Container und andere Objekte in der Cloud. Diese Risiken, gepaart mit den großen Unterschieden zwischen den Vorfällen im Bereich der Kompromittierung von Software- und Hardwarelieferketten, die ans Licht gekommen sind, machen Angriffe auf die Lieferkette zu einer breiten Bedrohungskategorie. Zwar gibt es keine einzige Lösung für das gesamte Spektrum dieser Arten von Angriffen, jedoch müssen Organisationen vorbeugenden Schutz und Post-Breach-Erkennung für Lieferkettenangriffe von kompromittierten Hard- und Softwareanbietern, Anbietern und Akquisitionen, Open-Source-Softwareanbietern sowie Cloud-Services und Infrastrukturanbietern vorsehen.

Untersuchung von Cybervorfällen mit DART

Das Microsoft Detection and Response Team (DART) ist ein globales Team aus Cybersicherheitsexperten und für Vorfälle zuständigen Mitarbeitern, die Unternehmen bei der Erkennung und Untersuchung von Cybersicherheitsvorfällen sowie der entsprechenden Reaktion helfen. In diesem Abschnitt werden einige Kundenfälle beschrieben, die DART im letzten Jahr bearbeitet hat. Gezeigt werden gängige Angreifertrends und wie Microsoft und die Kunden diese vereiteln konnten.

UNTERNEHMEN FÜR PROFESSIONELLE DIENSTLEISTUNGEN ERLEBTE NATION STATE ATTACK MIT DATENEXFILTRATION

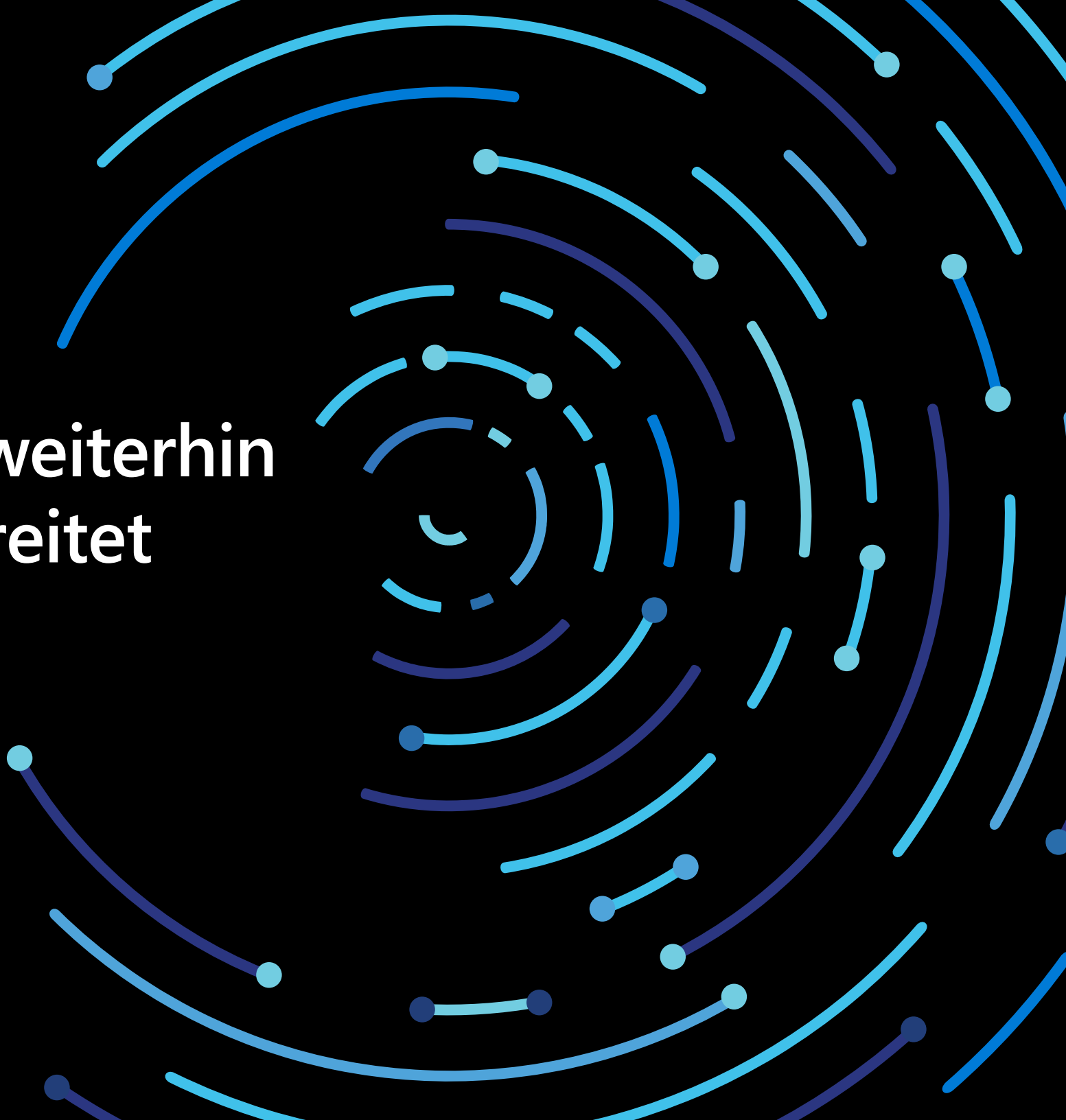
Ein Unternehmen für professionelle Dienstleistungen wurde Opfer eines ausgeklügelten, staatlich geförderten Advanced Persistent Threat(APT)-Angriffs, durch den privilegierte Anmeldedaten der Organisation zugänglich gemacht wurden. Die Angreifer verschafften sich mit einem Passwort-Spray-Angriff Zugang zum Netzwerk. Dabei benutzten sie eine kleine Anzahl schwacher oder weit verbreiteter Passwörter (wie „p@ssword" oder „123456"), um eine große Anzahl von Benutzerkonten anzugreifen und Anmeldedaten für Office 365-Administratorzugänge zu erlangen. (Passwort-Spray-Angriffe werden verwendet, um eine Erkennung zu vermeiden, indem die Anzahl von Anmeldeversuchen für jedes Konto begrenzt wird.) Nach dem Eindringen in das Netzwerk nahm der APT eine aufwendige, automatisierte Exfiltration von Daten aus den Postfächern der Mitarbeiter vor.

Trotz mehrfacher innerbetrieblicher Versuche, den Eindringling zu vertreiben, blieb er mehr als 200 Tage im Netzwerk. Im Rahmen des Angriffs nutzte der Angreifer die Lieferkettensoftware des Unternehmens und die automatisierte Exfiltration von Daten.

Das Unternehmen vermutete eine Verletzung der Sicherheit seiner Kundendaten und beauftragte das DART-Team mit der Untersuchung und Verhinderung weiterer Schäden. DART identifizierte gezielte Office 365-Postfachsuchen, kompromittierte Konten sowie Befehls- und Steuerkanäle für Angreifer. Infolge dieses Vorfalls entschied sich der Kunde für neue Kontrollmechanismen, um Cloud-Dienste vor identitätsbasierten Bedrohungen und Angreifern zu schützen. Die Organisation implementierte Multi-Faktor-Authentifizierung (MFA), bedingte Zugriffsrichtlinien für bestimmte Cloud-Apps und Office 365-Protokollierung. Um sich in Zukunft stärker vor ähnlichen Bedrohungen zu schützen, kann das Unternehmen zudem eine Endpoint Detection and Response(EDR)-Lösung einsetzen, um Angreifer zu erkennen, die versuchen könnten, das Netzwerk auszunutzen. Darüber hinaus haben wir der Organisation empfohlen, eine Stelle für Cloud Governance oder ein globales Identitätsteam aufzubauen, das geeignete Authentifizierungsrichtlinien für Benutzer verwaltet und durchsetzt, sodass das Unternehmen seinen Sicherheitsstatus im Blick behält und Risiken effektiver mindern kann.

ABSCHNITT III

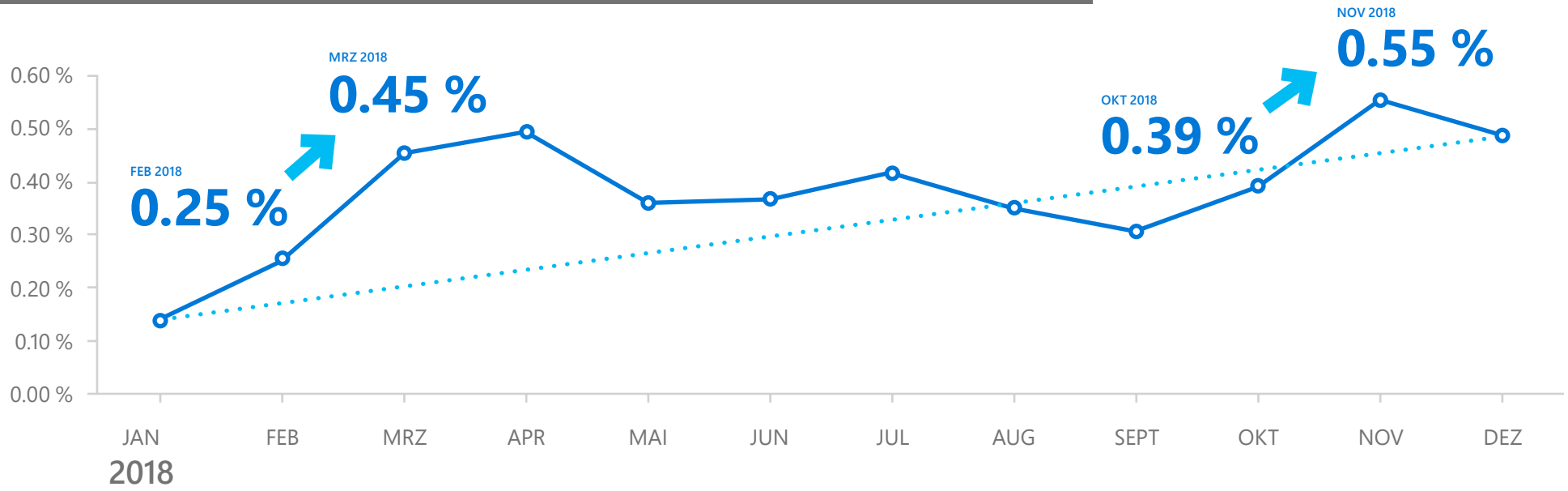
Phishing weiterhin weit verbreitet



2018 haben Microsoft-Bedrohungsanalysten erkannt, dass Angreifer Phishing weiterhin als bevorzugte Angriffsmethode nutzen. Phishing wird vermutlich auch in der absehbaren Zukunft ein Problem darstellen, weil es angesichts der anhaltenden Bemühungen von Cyberkriminellen, Zielobjekte zu finden, menschliche Entscheidungen und Urteile erfordert.

Phishing-Raten nehmen weiter zu

Prozentsatz der insgesamt eingehenden E-Mails, die Phishing-E-Mails sind



PHISHING BLEIBT AUCH 2018 BEVORZUGTER ANGRIFFSVEKTOR

Microsoft analysiert und scannt in Office 365 monatlich mehr als 470 Milliarden E-Mail-Nachrichten auf Phishing und Malware. Dadurch erhalten Analysten einen umfassenden Einblick in die Trends und Techniken von Angreifern. Der Anteil der eingehenden E-Mails, bei denen es sich um Phishing-Nachrichten handelte, hat zwischen Januar und Dezember 2018 um 250 Prozent zugenommen. Phishing bleibt einer der Angriffsvektoren, die am häufigsten verwendet werden, um schädliche Zero-Day-Nutzlasten an die Nutzer zu liefern. Microsoft hat die Verteidigung gegen diese Angriffe mit zusätzlichem Anti-Phishing-Schutz sowie Erkennungs-, Untersuchungs- und Reaktionsfunktionen zum Schutz der Nutzer weiter verstärkt.

▲ **ABBILDUNG 8.**

Phishing-E-Mails im Jahr 2018

Weiterentwicklung von Phishing-Angriffsmethoden

Da die Tools und Techniken zum Schutz von Personen vor Phishing-Angriffen immer ausgeklügelter werden, sind Angreifer gezwungen, sich anzupassen. Phishing-Angriffe sind zunehmend polymorph, was bedeutet, dass Angreifer nicht nur eine einzige URL, Domäne oder IP-Adresse verwenden, um E-Mails zu versenden, sondern eine vielfältige Infrastruktur mit mehreren Angriffspunkten nutzen. Auch die Natur der Angriffe selbst hat sich weiterentwickelt. Moderne Phishing-Kampagnen reichen von kurzzeitigen Angriffen, die nur wenige Minuten lang aktiv sind, bis hin zu deutlich längeren Kampagnen mit hohem Volumen. Bei anderen handelt es sich um Angriffe mit seriellen Varianten, bei denen Angreifer an mehreren aufeinanderfolgenden Tagen eine kleine Menge an E-Mails verschicken.

Darüber hinaus hat Microsoft einen Trend beobachtet, bei dem Angreifer gehostete Infrastruktur und andere Public-Cloud-Infrastruktur nutzen. Auf diese Weise können sie sich einfacher der Erkennung entziehen, indem sie sich zwischen legitimen Websites und Assets verstecken. Beispielsweise nutzen Angreifer zunehmend beliebte Websites und Dienste für Dateienaustausch und Zusammenarbeit, um schädliche Nutzlasten und gefälschte Anmeldeformulare zu verteilen, mit denen Benutzerdaten gestohlen werden. Es war auch eine Zunahme der Nutzung von kompromittierten Konten zu verzeichnen, um schädliche E-Mails innerhalb und außerhalb einer Organisation weiter zu verteilen.

Phishing-Kampagnen: gezielt bis breit angelegt

Wie bei der Schadsoftware-Distribution im Allgemeinen reichen Phishing-Kampagnen von gezielten bis hin zu breit angelegten, generischen Angriffen. Obwohl hoch entwickelte Angriffe zu höheren Geldgewinnen pro ausgespähtem Konto führen, bringen generischere Angriffe zwar weniger Geld pro kompromittiertem Konto, zielen aber auf eine breitere Gruppe von Nutzern ab.

Ein Beispiel für eine ausgeklügelte, zielgerichtete Kampagne ist Ursnif, bei der Angreifer den Namen der Dokumentendatei so lokalisiert haben, dass er den Anschein erweckt, von einer vertrauten Organisation oder aus der Branche des Zielobjekts zu stammen. Solche Angriffe unterscheiden sich deutlich von breit angelegten Kampagnen und scheinen legitimer und vertrauenswürdiger zu sein.

Einige der breit angelegten Kampagnen im Jahr 2018 standen im Zusammenhang mit Business E-Mail Compromise (BEC) und dem Identitätswechsel in Bezug auf bekannte Marken, Domänen oder Nutzer innerhalb der Zielorganisationen sowie ausgeklügelten Spoofing-Kampagnen. Domänenidentitätswechsel ist eine gängige Angriffstaktik, die benutzt wird, um Organisationen vorzutäuschen, dass die E-Mail vertrauenswürdig ist und geöffnet werden sollte.

Phishing-Köder haben viele Formen

Microsoft-Forscher haben herausgefunden, dass viele verschiedene Arten von Phishing-Ködern oder Nutzlasten in Kampagnen eingesetzt werden, darunter:

- **Fälschen von Domänen (Spoofing)** (die Domäne der E-Mail-Nachricht stimmt exakt mit dem ursprünglichen Domänennamen überein)
- **Domänenidentitätswechsel** (die Domäne der E-Mail-Nachricht gleicht dem ursprünglichen Domänennamen)[2]
- **Benutzeridentitätswechsel** (die E-Mail-Nachricht scheint von jemandem zu kommen, dem der Nutzer vertraut)
- **Textköder** (die Textnachricht scheint aus einer legitimen Quelle wie einer Bank, einer staatlichen Behörde oder einem anderen Unternehmen zu stammen, um den Forderungen Legitimität zu verleihen; das Zielobjekt wird in der Regel aufgefordert, sensible Informationen wie Benutzernamen, Passwörter oder vertrauliche Finanzdaten anzugeben)
- **Phishing-Links für Anmeldeinformationen** (die E-Mail-Nachricht enthält einen Link zu einer Seite, die einer Anmeldeseite für eine legitime Website ähnelt, sodass die Nutzer ihre Anmeldedaten eingeben)
- **Phishing-Anhänge** (die E-Mail-Nachricht enthält einen schädlichen Dateianhang, den das Zielobjekt öffnen soll)
- **Links zu gefälschten Cloud-Speicherorten** (die E-Mail-Nachricht scheint aus einer legitimen Quelle zu stammen und soll den Benutzer verleiten, seine Erlaubnis zu erteilen bzw. persönliche Informationen wie Anmeldedaten einzugeben, um auf einen gefälschten Cloud-Speicherort zuzugreifen)

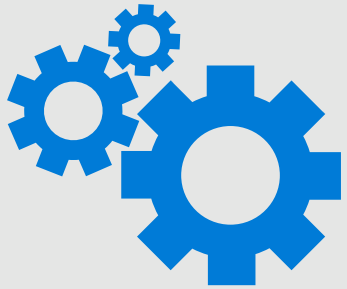
Diese Vielfalt an Ködern, die potenziell von Angreifern eingesetzt werden könnten, erhöht die Komplexität von Phishing-Bedrohungen, mit denen Organisationen zu kämpfen haben.

FUSSNOTEN

[2] Der Domänenidentitätswechsel kann dem Spoofing ähneln (exakte Übereinstimmung mit dem ursprünglichen Domänennamen), wenn die Domäne ausnahmsweise im E-Mail-Anzeigennamen angezeigt wird.

Untersuchung von Cybervorfällen mit DART

GROSSE PRODUKTIONSORGANISATION VON GEZIELTEN PHISHING-ANGRIFFEN BETROFFEN



Eine Produktionsorganisation war über einige Monate hinweg von einer mehrstufigen Phishing-Kampagne betroffen. Dieser Ansatz ist nicht ungewöhnlich. In der ersten Phase führt der Angreifer Ausspähungen durch, in der zweiten Phase nimmt er hochrangige Mitarbeiter ins Visier. In der ersten Phase dieser Kampagne wurde ein bekannter Phishing-Betrug genutzt, bei dem ein Link zu einer Webseite in eine E-Mail eingebettet wurde, die an eine kleine Zielgruppe innerhalb der Organisation gesendet wurde. In der E-Mail wurde behauptet, dass das Zielobjekt ein wichtiges elektronisches Dokument zu überprüfen habe, und sich der Empfänger lediglich mit seinen Domänenanmeldedaten authentifizieren müsse, um darauf zugreifen zu können. Diese gefälschte Zielseite, die für das Zielobjekt eingerichtet worden war, um das angebliche „wichtige Dokument" zu überprüfen, erfasste die Anmeldedaten und ermöglichte dem Angreifer Zugriff auf Office 365-Konten von überall auf der Welt. In der zweiten Phase der Phishing-Kampagne wurden ähnliche Phishing-E-Mails an hochrangige Mitarbeiter innerhalb der anvisierten Produktionsorganisation gesendet, in der Hoffnung, Zugang zu wertvolleren Daten zu erhalten. Microsoft trat dem Kunden in der zweiten Phase der Phishing-Kampagne zur Seite. Die wichtigsten Erkenntnisse des Kunden aus diesem Vorfall: Phishing bleibt eine der effektivsten Angriffsmethoden und Nutzer sind immer noch das schwächste Glied. Die Schulung von Nutzern, um ihnen beizubringen, sich vor Phishing-Betrügereien in Acht zu nehmen, die Implementierung von Tools zur Identifizierung von Angreifern und zum Handeln und das regelmäßige Patchen von Systemen sind wichtig. Wenn die Organisation diese Aspekte nicht berücksichtigt, kann sie angreifbar sein.

In diesem Fall war die größte Sorge des Kunden, den Zugang zu den kompromittierten Konten umgehend zu blockieren. In Zusammenarbeit mit den Teams von Azure Identity und Office 365 hat DART einen Plan entwickelt, um den Angreifer aus dem Netzwerk zu entfernen und sämtlichen Datenverkehr zum Befehls- und Steuerkanal zu überwachen. Dazu wurde die neu implementierte Microsoft Azure Log Analytics-Lösung verwendet. Das Team konnte in nur drei Stunden zur Lösung des Problems beitragen. Der Zugriff des Angreifers wurde gesperrt, und die Organisation konnte ihre Aufmerksamkeit auf Schadensbewertung und Wiederherstellung richten. DART nutzte die Azure Log Analytics-Tools, um das Angreiferverhalten zu analysieren, wodurch viele konfigurationsbezogene Herausforderungen für die Organisation aufgedeckt werden konnten. Beispielsweise identifizierte DART Lücken beim Patchen auf kritischen Servern, entdeckte Computer im Netzwerk, die mit bekannten schädlichen Hosts im Internet kommunizierten, und fand zudem mehrere wichtige Server ohne Schutz vor Schadsoftware.

ABSCHNITT IV

Schadsoftware weltweit

Schadsoftware birgt Risiken für Organisationen und Einzelpersonen in Form von eingeschränkter Nutzbarkeit, Datenverlust, Diebstahl geistigen Eigentums, finanziellen Verlusten, emotionalem Stress und kann sogar menschliches Leben gefährden. Microsoft verwendet eine breite Palette von Tools und Techniken, um Infektionen durch Schadsoftware zu identifizieren, zu blockieren und zu beseitigen.

Das Vorkommen von Schadsoftware bewegte sich 2017 im Bereich von rund 5 Prozent bis hin zu mehr als 7 Prozent. Anfang 2018 stieg diese Rate an, bevor sie während des größten Teils des Jahres auf knapp über 4 Prozent zurückging. Einige mögliche Gründe für die allgemeine Abnahme der Schadsoftwarefälle im Jahr 2018 sind die gestiegene Verwendung von Windows 10 und die verstärkte Nutzung von Windows Defender, um sich zu schützen. Die Vorkommensquote steht für den Prozentsatz der Computer, auf denen Windows Defender Antivirus verwendet wird, über das die Existenz von Schadsoftware im Laufe des Monats gemeldet wurde, darunter Angriffsversuche, die von Defender vereitelt wurden.

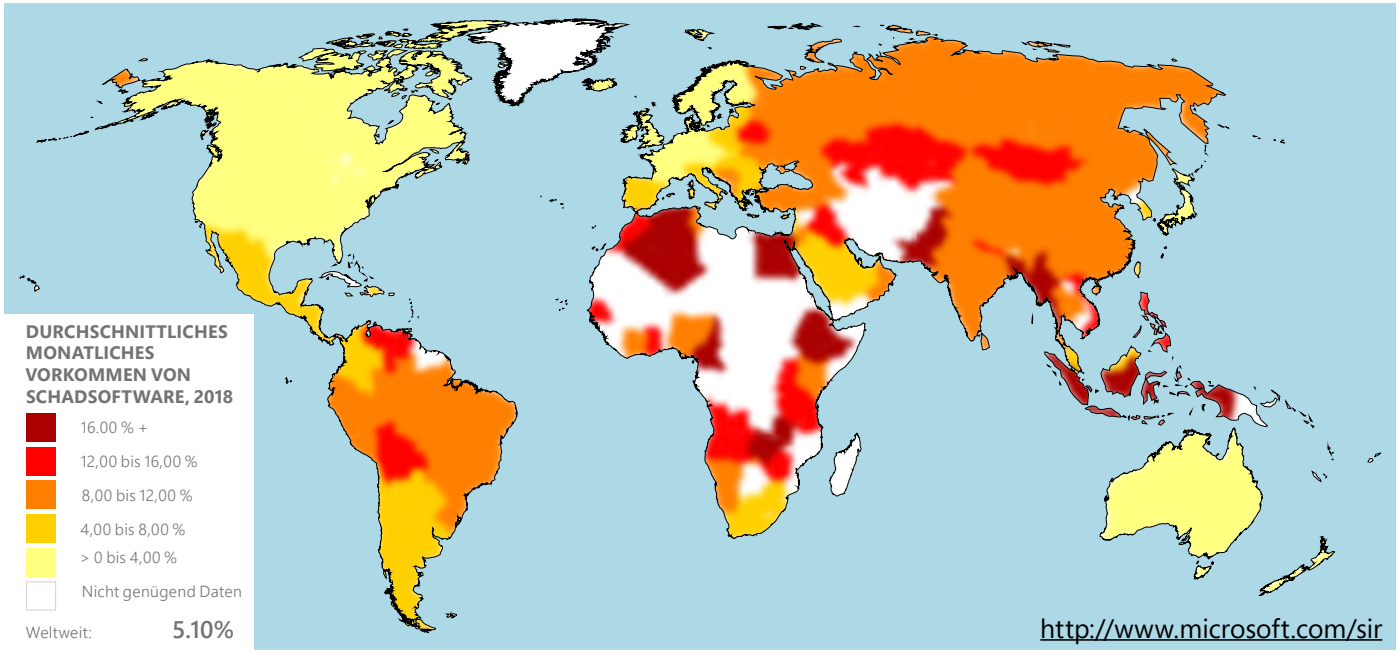


ABBILDUNG 9.

Durchschnittliches monatliches Vorkommen von Schadsoftware weltweit nach Land/ Region im Jahr 2018

Die fünf Länder mit den meisten Schadsoftwarefällen im Zeitraum von Januar bis Dezember 2018 waren Äthiopien (durchschnittliches monatliches Vorkommen von 26,33 %), Pakistan (18,94 %), die Palästinensischen Gebiete (17,50 %), Bangladesch (16,95 %) und Indonesien (16,59 %), die während des Zeitraums jeweils ein durchschnittliches monatliches Vorkommen von etwa 16,59 Prozent oder höher verzeichneten. Infektionsraten korrelieren in der Regel stark mit Faktoren des sozialen Entwicklungsstands und dem technologischen Reifegrad innerhalb einer Gesellschaft. Alle Orte mit dem höchsten Vorkommen im Jahr 2018 befanden sich unter den unteren 40 Prozent der Länder und Regionen im „Information and Communications Technologies Index" für das Jahr 2017, der von der Internationalen Fernmeldeunion der Vereinten Nationen veröffentlicht wird.

Die fünf Orte mit dem niedrigsten Vorkommen von Schadsoftware im gleichen Zeitraum waren Irland (1,26 %), Japan (1,51 %), Finnland (1,74 %), Norwegen (1,79 %) und die Niederlande (1,82 %), die während des Zeitraums jeweils ein durchschnittliches monatliches Vorkommen von 1,82 Prozent oder weniger verzeichneten. Diese Länder verfügen in der Regel über ausgereifte Cybersicherheitsinfrastrukturen und gut etablierte Programme zum Schutz kritischer Infrastrukturen und zur Kommunikation mit ihren Bürgern über grundlegende Sicherheitsmaßnahmen.

DURCHSCHNITTLICHES MONATLICHES VORKOMMEN IN DEN LÄNDERN, DIE AM STÄRKSTEN VON SCHADSOFTWARE BETROFFEN SIND

Äthiopien: **26.33%**

Pakistan: **18.94%**

Palästinensische Gebiete: **17.50%**

Untersuchung von Cybervorfällen mit DART

MEHREREFINANZDIENSTLEISTUNGSORGANISATIONEN ERLEBTEN NATION STATE ATTACKS MIT BETRIEBSSTÖRUNGEN

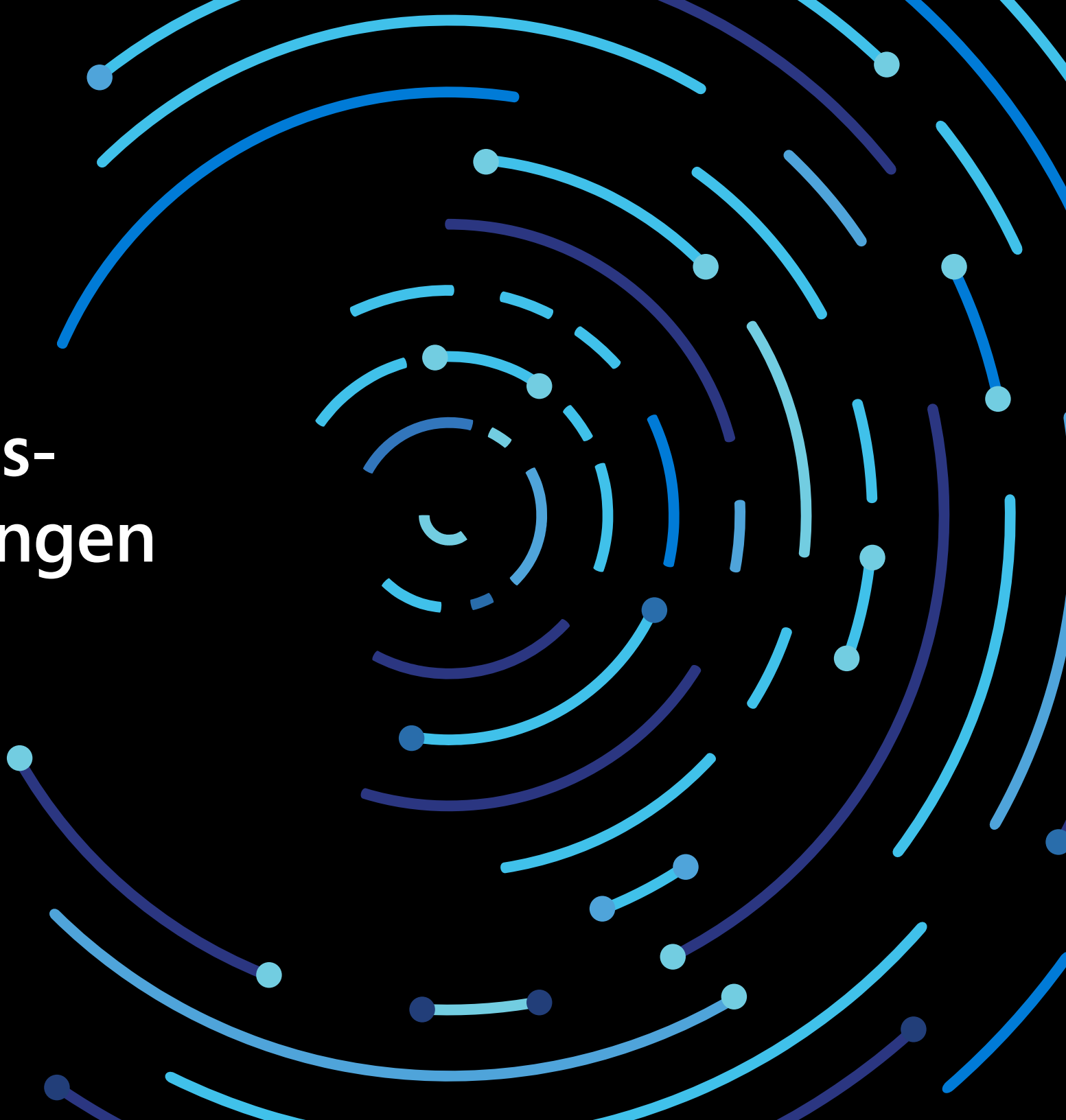
In einem der zerstörerischeren Vorfälle, die DART erlebt hat, wurden mehrere Finanzdienstleister von einem staatlich geförderten APT (eine andere Gruppe als die, die auf das zuvor erwähnte Unternehmen für professionelle Dienstleistungen abgezielt hatte) ins Visier genommen. Der Angriff spielte sich ähnlich ab.

Dieser APT verschaffte sich administrativen Zugang, nachdem er den ersten Rechner („Patient Zero") mit einer sehr gezielten, verschleierten Installation einer Hintertür infiziert hatte, die möglicherweise über eine Spear-Phishing-E-Mail geliefert wurde. Anschließend führte der APT mehrere betrügerische Transaktionen durch und überwies große Summen Bargeld auf ausländische Bankkonten. In einigen Fällen blieb der Angreifer mehr als 100 Tage lang unerkannt. Als der Angreifer erkannte, dass er entdeckt worden war, setzte er rasch einen vorbereiteten Angriff ein, der an mehr als die Hälfte der Systeme in der Umgebung zerstörerische Schadsoftware lieferte. Bei diesen Kunden wurde der Betrieb mehrere Tage lang eingestellt.

Aus diesen Vorfällen konnte der Kunde einige wichtige Erkenntnisse gewinnen. Erstens, dass das Software Lifecycle Management besonders wichtig ist, wozu auch die Sicherstellung gehört, dass die Systeme regelmäßig aktualisiert (Betriebssysteme und Sicherheit), gepatcht und geprüft werden. In einem Fall war die Linux-Systemumgebung einer Organisation, in der eine außergewöhnlich große Anzahl von Workloads ausgeführt wurde, völlig unverwaltet, was ein extrem hohes Angriffsrisiko darstellte. Die zweite Erkenntnis war, dass es wichtig ist, Backups von Systemdaten offline vorzuhalten, falls die Primärdaten verloren gehen. Eine weitere Erkenntnis bestand darin, dass traditionelle Antiviren-Lösungen möglicherweise nicht ausreichen, wenn Sie über gegnerische Aktivitäten Bescheid wissen müssen.

Die Rückkehr zum normalen Betriebsmodus hatte für diese Organisationen höchste Priorität. DART half dabei, Dienste wiederherzustellen, indem zuerst die Auswirkungen untersucht und dann notwendige Abhilfemaßnahmen ergriffen wurden, wie das Entfernen von Schadsoftware aus den betroffenen Systemen und die Wiederherstellung ihrer Integrität. Das Team schulte Kunden auch darin, wie sie Microsoft-Tools zur Untersuchung von Bedrohungen, darunter EDR und andere, zum Aufspüren von anormalem Verhalten und Angreiferaktivitäten in ihrem Netzwerk nutzen können. DART betonte, dass die Endpunktüberwachung entscheidend ist, um sich gegen ausgeklügelte, gezielte Angriffen zu verteidigen, die von traditionellen Antiviren-Lösungen unerkannt bleiben könnten.

Handlungs-empfehlungen



Handlungsempfehlungen

Um organisatorische Resilienz und sinnvolle Risikominderung zu erzielen, bedarf es eines Sicherheitsansatzes, der Prävention, Detektion und Reaktion einschließt. Wir haben die folgenden bewährten Sicherheitsmaßnahmen und -kontrollen in diese Kategorien organisiert.

PRÄVENTION:

Vorbeugende Kontrollen spielen eine Schlüsselrolle für eine allgemeine Verteidigungsstrategie. Denn die richtigen Investitionen können die Kosten der Angriffe für Cyberkriminelle erhöhen und diese erhöhten Angriffskosten im Zeitablauf aufrechterhalten (ohne dass ein professioneller Analyst die Überwachung und Interpretation der Ausgabe übernehmen muss). Investitionen in vorbeugende Kontrollen sollten auf die preisgünstigsten Techniken abzielen, um billige und effektive Angriffstechniken kontinuierlich zu eliminieren.

Die folgenden vier Dinge sind im Hinblick auf die Prävention zu beachten:

1. **Sicherheitshygiene ist entscheidend. Wie bei einigen der in diesem Bericht vorgestellten Cybervorfällen zu sehen ist, können allgemeine Hygieneprobleme fortschrittliche Sicherheitsfunktionen untergraben. Die Einhaltung dieser Tipps kann helfen, Risiken zu verringern:**

- Vermeiden Sie es, unbekannte kostenlose bzw. raubkopierte Software zu verwenden. Verwenden Sie nur Software aus vertrauenswürdigen Quellen.
- Mindern Sie das Risiko eines Diebstahls von Anmeldeinformationen, unter anderem durch die Sicherung privilegierter Administratorkonten. Wie das funktioniert, erfahren Sie in diesem Blog, in dem einige Prinzipien und Tools vorgestellt werden, mit denen Microsoft unseren eigenen Sicherheitsstatus angeleitet und verbessert hat, sowie einige verbindliche Roadmaps, anhand derer Sie Ihre eigenen Initiativen planen können.
- Wenden Sie sichere Konfigurationsleitlinien Ihrer Softwareanbieter an.
- Halten Sie die Computer auf dem neuesten Stand, indem Sie zügig die neuesten Updates für Ihre Betriebssysteme und Anwendungen installieren und sofort kritische Sicherheitsupdates für OS, Browser und E-Mails bereitstellen. Isolieren Sie Computer (oder nehmen Sie sie außer Betrieb), die nicht aktualisiert oder gepatcht werden können.
- Implementieren Sie erweiterte Schutzmaßnahmen für E-Mails und Browser. Stellen Sie ein sicheres E-Mail-Gateway bereit, das über fortschrittliche Bedrohungsschutzfunktionen verfügt, um sich gegen moderne Phishing-Varianten zu verteidigen.
- Aktivieren Sie Antischadsoftware für Hosts und Netzwerkabwehrsysteme, um Sperrreaktionen aus der Cloud nahezu in Echtzeit zu erhalten (sofern diese für Ihre Lösung verfügbar sind).

2. **Implementieren Sie Zugriffskontrollen. Beachten Sie Folgendes:**

- Wenden Sie das Prinzip der geringsten Privilegien an. Dabei wird das Netzwerk segmentiert, Endnutzern werden lokale Administratorenrechte entzogen und Anwendungen, die auf dem Computer ausgeführt werden, werden nur mit Vorsicht Berechtigungen erteilt.
- Beschränken Sie das Herunterladen von Anwendungen auf solche aus zuverlässigen Quellen (offizieller App-Store).
- Stellen Sie starke Codeintegritätsrichtlinien bereit, einschließlich einer Einschränkung der Anwendungen, die Benutzer ausführen können. Setzen Sie wenn möglich eine Sicherheitslösung ein, die den im Systemkern (Kernel) ausgeführten Code einschränkt und nicht signierte Skripte und andere Formen von nicht vertrauenswürdigem Code blockieren kann. Verwenden Sie Whitelists für Anwendungen.
- Um mehr über Angriffe auf Softwarelieferketten zu erfahren und wie Sie sich vor ihnen schützen können, lesen Sie diesen Blog von Microsoft-Forschern.

3. **Bewahren Sie Backups auf.**

- Erstellen Sie zerstörungsfeste Sicherungen Ihrer kritischen Systeme und Daten.
- Nutzen Sie Cloud-Speicherdienste für die automatische Datensicherung online. Sichern Sie im Falle von On-Premises-Daten wichtige Daten regelmäßig anhand der 3-2-1-Regel. Bewahren Sie drei Backups Ihrer Daten auf zwei verschiedenen Speichertypen auf. Mindestens ein Backup sollte offsite aufbewahrt werden.

4. **Seien Sie aufmerksam und handeln Sie, wenn Sie ungewöhnliche Aktivitäten vermuten.**

- Bringen Sie Mitarbeitern bei, sich vor verdächtigen Mitteilungen in Acht zu nehmen, die sensible Informationen anfordern, und weisen Sie sie an, wie sie reagieren und die entsprechenden Mitteilungen sofort an das Sicherheitsteam der Organisation melden können. Schulungen können auch dazu beitragen, Social-Engineering- und Speer-Phishing-Angriffe zu mindern.
- Seien Sie vorsichtig, wenn Sie auf Weblinks klicken. Sichere Webbrowsing-Gewohnheiten und die Verwendung von Lösungen, die vor unsicheren Websites warnen oder diese blockieren, können dazu beitragen, die Wahrscheinlichkeit zu verringern, Websites im Zusammenhang mit Kryptowährungs-Mining aufzurufen.
- Wenn ein Computer außergewöhnlich langsam läuft, suchen Sie nach verdächtigen Dateien, die ausgeführt werden, und senden Sie gerne ein Sample an den Hersteller des Betriebssystems. Unter https://www.microsoft.com/wdsi/filesubmission können Sie Dateien zur Schadsoftwareanalyse an Microsoft senden.

ERKENNUNG UND REAKTION:

Erkennung und Reaktion fördern die Resilienz, indem sie die Dauer begrenzen, während der ein Angreifer Zugriff auf Ihre Ressourcen hat. Dadurch wird der ROI des Angreifers verringert, indem die Kosten für den Angreifer erhöht werden (er muss seinen Angriff erneut versuchen oder ändern) und die Rendite verringert wird (die Wahrscheinlichkeit, sein Ziel zu erreichen, wird begrenzt).

Die gleiche Cloud-Technologie, die es Unternehmen ermöglicht, Marktbedürfnisse besser zu befriedigen, kann auch Sicherheitsdiensten helfen, sich besser gegen Angreifer zu wehren.

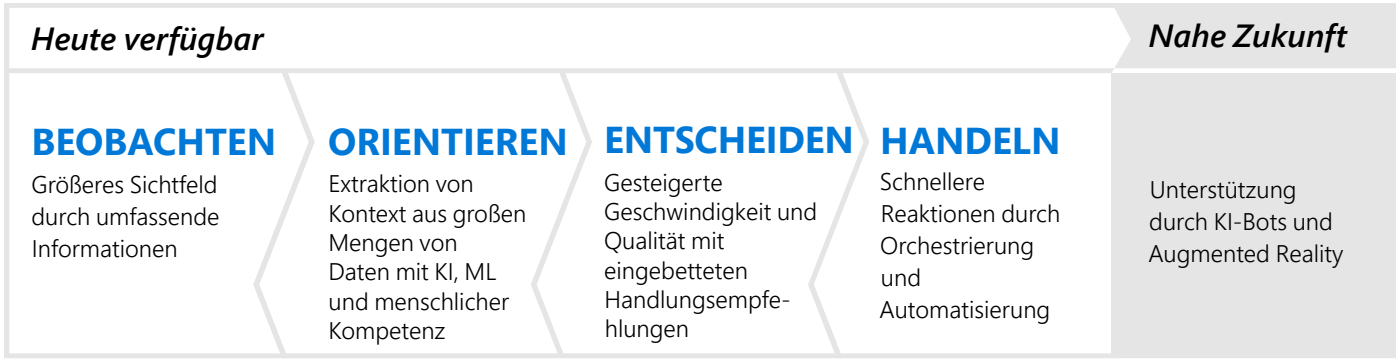


ABBILDUNG 10.

Entwicklungsverlauf von SOCs

Wenn wir uns die Entwicklung von Security Operations Centers (SOCs) ansehen, stellen wir fest, wie technologische Entwicklungen die Geschwindigkeit und Qualität von SOC-Entscheidungen und -Maßnahmen kontinuierlich erhöhen. Viele dieser Innovationen lassen sich den einzelnen Stufen des „Observe Orient Decide Act(OODA)-Loop" zuordnen, der von USAF-Colonel John Boyd dokumentiert wurde.[3]

BEOBACHTEN – SOCs können auf eine große Menge von Sicherheitsdaten zurückgreifen (von Microsoft und aus anderen Quellen), um ihr Sichtfeld innerhalb der Organisation und der externen Umgebung deutlich zu vergrößern.

ORIENTIEREN – In dem Maße, in dem diese neuen Datenquellen bereits überlasteten SOCs verfügbar gemacht werden, wird maschinelles Lernen (eine Teilmenge der künstlichen Intelligenz) zu einem entscheidenden Tool, um diese große Menge an Datensätzen zu analysieren und Anomalien zu identifizieren, die es wert sind, untersucht zu werden. Sicherheitsanbieter (einschließlich Microsoft) haben Machine-Learning-Technologie eingeführt, um Ereignisse schnell priorisieren zu können (und dabei zu helfen, diese einzelnen Ereignisse ganzheitlichen Vorfällen zuzuordnen).

ENTSCHEIDEN – Da Menge und Komplexität der Angriffe ein SOC schnell überlasten können, müssen Analysten und für Vorfälle zuständige Mitarbeiter viele Entscheidungen treffen und schnell auf Warnungen und Erkennungen reagieren. Microsoft und andere Anbieter haben automatisierte Ermittlungsmöglichkeiten sowie Leitlinien integriert, um Analysten dabei zu helfen, schnell richtige Entscheidungen zu treffen (um beispielsweise potenziell infizierte oder kompromittierte Geräte zu isolieren). Im Moment konzentriert sich die Automatisierung auf die schnelle Lösung von Vorfällen mit geringer Priorität, sodass spezialisierte Fähigkeiten zur Lösung komplexerer Probleme angewendet werden können.

HANDELN – Reaktionen erfordern eine schnelle und präzise Ausführung über viele Technologien und Plattformen hinweg, was durch Technologien für Sicherheitsorchestrierung und Reaktionsautomatisierung ermöglicht wird. Microsoft und viele andere investieren weiterhin in diese Technologien, darunter moderne Lösungen für Bedrohungserkennung und automatisierte Reaktionen.

FUSSNOTEN

[3] http://www.militaryhistoryveteran.com/colonel-john-boyd-ooda-loop/

Weitere Trends, die für ein modernes SOC gelten, sind:

- **Qualität über Quantität der Alarm-Feeds** – Wenn Organisationen von der Verwaltung von „zu wenigen Informationen" zur Verwaltung von „zu vielen Informationen" übergehen, wird die Zeit und Aufmerksamkeit hoch spezialisierter SOC-Analysten immer wertvoller. Dies führt zu einem erhöhten Qualitätsbedarf im Hinblick auf die Warnungen, die ein Eingreifen von Tier 1- und Tier 2-Analysten erfordern. Zusätzliche Datenfeeds sind immer hilfreich für Untersuchungen und proaktive Suchen. Das Corporate IT SOC von Microsoft misst jedoch die Richtig-Positiv-Rate von Alarmfeeds, die eine Reaktion der Analysten erfordern (derzeit ist eine Richtig-Positiv-Rate von mindestens 90 % erforderlich).

- Datenträgheit – Analysen an großen Datensätzen (einschließlich Sicherheitsdaten) sind ohne Zugriff auf die zugrunde liegenden Rohdaten nur schwer durchführbar. Wenn mehr Sicherheitsdaten zur Verfügung stehen, ist es wirtschaftlicher und praktischer, die Sicherheitsanalysen in der Cloud durchzuführen, anstatt diese Daten wieder in ein On-Premises-System zu übertragen. Dies wird wahrscheinlich zu einer Weiterentwicklung von SIEM- und SOC-Architekturen führen, die hybride SIEM-Ansätze oder natives cloudbasiertes SIEM-as-a-Service beinhalten können.

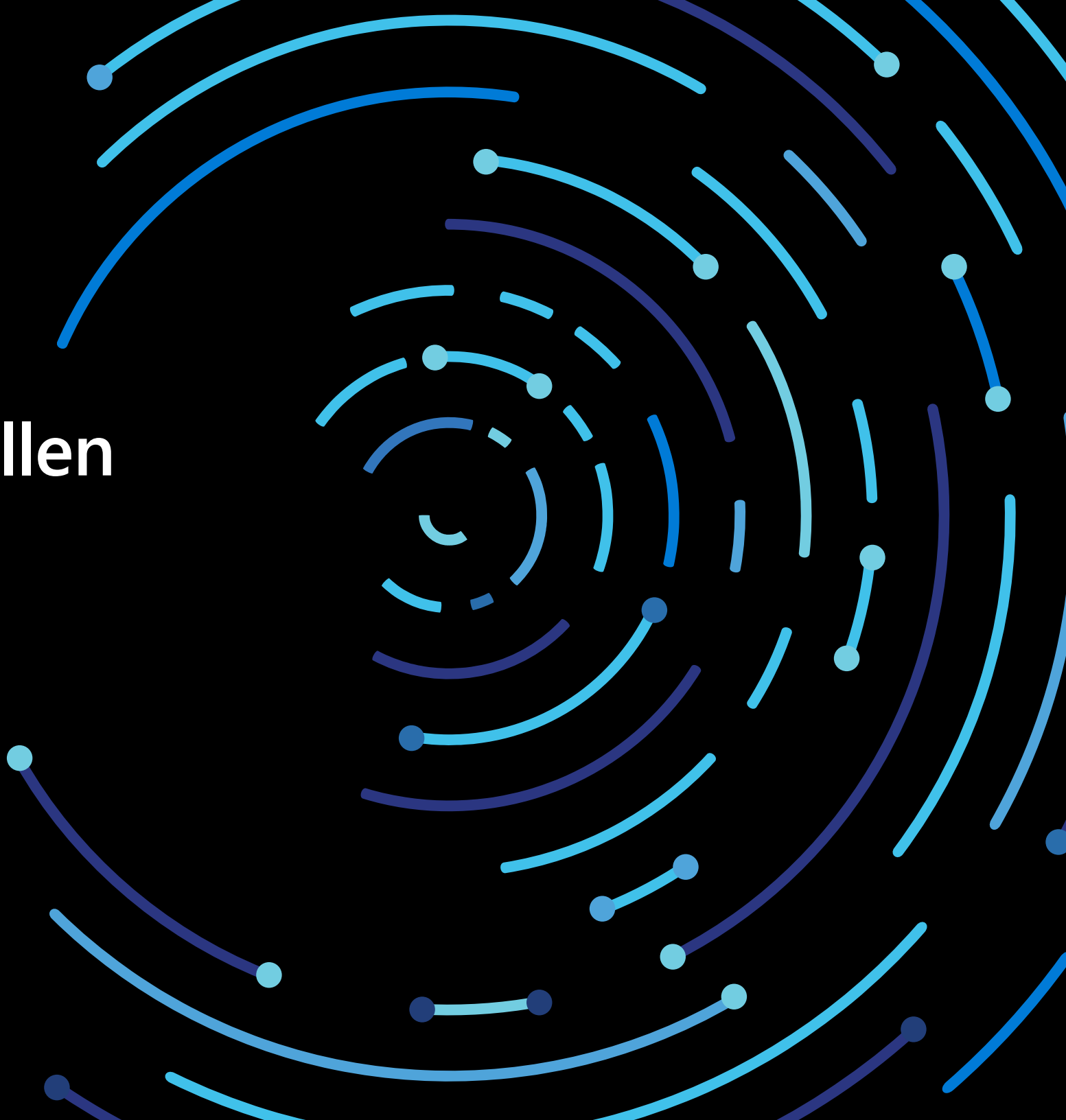
- **Kontextreichtum** – Diese Arten von Erkennungen sind deutlich nützlicher, weil sie Datensätze effektiver korrelieren können. Während herkömmliche Erkennungen auf Grundlage des Netzwerkverkehrs immer noch einen gewissen Sicherheitswert bieten, fehlt es dem rohen Netzwerkverkehr in der Regel an Kontext, um zwischen legitimen Aktivitäten und anomalen Aktivitäten zu unterscheiden. Unserer Erfahrung nach profitieren SOCs deutlich mehr von kontextreichen Erkennungen wie den Folgenden:

  - **Endpoint Detection and Response(EDR)-Lösungen,** die über umfangreichen Kontext zur Host-Aktivität verfügen
  - Identitätsbasierte Erkennungen, die Einblicke in normale Nutzerauthentifizierungsmuster (Standorte, Zeiten, aufgerufene Dienste usw.) umfassen und Verhaltensanalysen anwenden

Diese kontextreichen Erkennungen sind für Angreifer schwieriger zu umgehen, da sie eine viel komplexere Operation nachahmen müssen (im Vergleich zu wenigen technischen Attributen des IP-Verkehrs).

Eine weitere Lektion, die wir aus größeren Angriffen bei Kunden gelernt haben, war die Schwierigkeit, schnell auf Vorfälle zu reagieren, wenn IT-Funktionen teilweise oder vollständig ausgelagert werden. Wir empfehlen Ihnen, Ihre IT-Outsourcing-Verträge und Service Level Agreements (SLAs) sowie Lieferkettenanbieter zu überprüfen, um sicherzustellen, dass sie eine schnelle Reaktion auf Sicherheitsvorfälle ermöglichen. Weitere Erkenntnisse aus unseren Vorfalluntersuchungen bei Kunden finden Sie im Incident Response Reference Guide (IRRG) unter https://aka.ms/IRRG.

Datenquellen



Datenquellen

Microsoft hat die Daten, die im Microsoft Security Intelligence Report enthalten sind, im Zuge der Bereitstellung einer breiten Palette von Microsoft-Produkten und -Diensten gesammelt, worauf in der Microsoft-Datenschutzerklärung hingewiesen wird. Diese Daten liefern uns wertvolle Informationen über die Sicherheit und den Betrieb unserer Produkte und Dienstleistungen sowie Einblicke in die Landschaft der Cybersicherheitsbedrohungen im Allgemeinen. Diese Daten umfassen Analysen aus den folgenden Quellen:[4]

- **Azure Security Center** ist ein Dienst, der Organisationen dabei unterstützt, Bedrohungen zu verhindern, zu erkennen und darauf zu reagieren. Dazu wird die Sicherheit von Cloud-Arbeitslasten transparenter gestaltet und fortschrittliche Analysen sowie Threat Intelligence werden eingesetzt, um Angriffe zu erkennen.

- **Bing** ist die Suchmaschine, die mehrere Milliarden Webseiten pro Jahr scannt, um schädliche Inhalte aufzudecken. Nachdem solche Inhalte erkannt wurden, zeigt Bing den Benutzern Warnungen an, um Infektionen zu verhindern.

- **Exchange Online** ist der von Microsoft gehostete E-Mail- und Produktivitätsdienst. 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 ist kein Ersatz für einen aktuellen Echtzeit-Virenschutz.

- Der **Microsoft Safety Scanner** ist ein als kostenloser Download verfügbares Sicherheitstool, das On-Demand-Scans bereitstellt und das Entfernen von Schadsoftware und anderer bösartiger Software unterstützt. Der Microsoft Safety Scanner ist kein Ersatz für einen aktuellen Virenschutz, da er keinen Echtzeitschutz bietet und nicht verhindern kann, dass ein Computer infiziert wird.

FUSSNOTEN

[4]Wichtig ist, dass diese Daten immer durch strenge Datenschutz- und Compliance-Auflagen geschützt sind, bevor sie zu Sicherheitszwecken verwendet werden.

- **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 durchgängiges 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 Unternehmen und Privatbenutzer. Ausgewählte Abonnementpläne beinhalten Zugriff auf Office 365 Advanced Threat Protection.

- **Windows Security** in Windows 10 bietet Echtzeitscans sowie die Beseitigung von Schadsoftware und unerwünschter Software. Darüber hinaus nutzt die neueste Version von Windows reichhaltige kontextbezogene Daten wie Computerkonfiguration, Geräteleistung und -integrität sowie andere Informationen, um die Sicherheit für Kunden zu erhöhen. Gleichzeitig bieten wir Kunden umfassende Informationen über ihre Privatsphäre in Windows 10. Lesen Sie diesen Blog, um mehr über einige der Methoden zu erfahren, mit denen Microsoft dies erreicht.

- **Windows Defender Advanced Threat Protection** ist ein Dienst, der in das Windows 10 Anniversary Update und höhere Versionen integriert ist und es 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, mit dem bootfähige CDs, DVDs und USB-Flashlaufwerke erstellt werden können, um einen Computer auf Schadsoftware und andere Bedrohungen zu untersuchen. Es bietet keinen Echtzeitschutz und ist kein Ersatz für einen aktuellen Schutz vor Schadsoftware.

- **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.