**PRESSEINFORMATION**

Hamburg, 30. März 2021

**Fileless Malware: Darf’s ein bisschen mehr sein?**

**Anteil dieser besonders trickreichen Angriffsvariante steigt laut Internet Security Report von WatchGuard Technologies auf das Neunfache an**

Wie der gerade veröffentlichte [Internet Security Report von WatchGuard Technologies für das vierte Quartal 2020](https://www.watchguard.com/wgrd-resource-center/security-report-q4-2020) offenbart, ist die Gefahr, der sich Unternehmen aktuell gegenübersehen, immer weniger „greifbar“. 2020 gab es insgesamt neunmal mehr Angriffe durch sogenannte „[Fileless Malware](https://pandanews.de/fileless-malware-auf-den-zahn-gefuehlt/)“ als noch im Vorjahr. Dieses einschlägige „Durch-die-Decke-gehen“ der Statistik bedeutet nicht Gutes. Denn das Gefährliche an dieser dateilosen Malware-Variante ist die Tatsache, dass sie von klassischen Lösungen zum Schutz von Endpunkten, wie sie vielerorts noch ausschließlich im Einsatz sind, nicht erkannt wird. Dabei reicht es schon, wenn ein Anwender auf einen bösartigen Link klickt oder unwissentlich eine kompromittierte Website besucht. Mit gängigen Werkzeugen wie PowerSploit und CobaltStrike sind Cyberkriminelle in der Lage, auf einfache Weise bösartigen Code in andere laufende Prozesse einzuschleusen. Und selbst wenn die vorhandenen Verteidigungsmaßnahmen des Opfers das ursprüngliche Skript identifizieren und entfernen, arbeitet die Bedrohung weiter. Der Paralleleinsatz von modernen EDR-Lösungen (Endpoint Detection and Response) und vorausschauenden Anti-Malware-Komponenten kann hier Abhilfe schaffen, da sich fortschrittliche Angriffsmuster auf diese Weise leichter erkennen und ausbremsen lassen.

Darüber hinaus liefert der Report viele weitere spannende Erkenntnisse im Hinblick auf Kryptominer, verschlüsselte Malware und sonstige Netzwerkübergriffe. Die gute Nachricht dabei gleich vorweg: Die Analysten des WatchGuard Threat Labs verzeichneten erstmals deutlich weniger Ransomware-Vorfälle.

Wichtige Ergebnisse des Internet Security Reports Q4 2020 im Überblick:

* Nach kurzer Flaute 2019 sind Kryptominer wieder im Kommen: Nachdem sich Anfang 2018 praktisch alle Kryptowährungen im Sinkflug befanden, wurden auch einschlägige Kryptominer-Infektionen deutlich seltener beobachtet. Diese erreichten im Jahr 2019 einen Tiefstand von insgesamt 633 identifizierten Einzelvarianten. Dennoch wurden die Angreifer in dem Zusammenhang nie ganz müde und fügten weiterhin Kryptominer-Module zu bestehenden Botnet-Infektionen hinzu, um an die virtuelle Währung zu kommen und gleichzeitig anderweitigen Schaden in den Netzwerken der Opfer anzurichten. Daran anknüpfend – und im Zuge des erneuten Aufwärtstrends der Kryptowährungen im vierten Quartal 2020 – stieg das Volumen der Kryptominer-Malware-Erkennungen gegenüber 2019 um mehr als 25 Prozent: 850 eindeutige Varianten wurden erkannt.
* Zahl der Ransomware-Angriffe halbiert sich: Das zweite Jahr in Folge wurden 2020 insgesamt weniger Ransomware-Vorfälle verzeichnet. In Zahlen spiegelt sich der Trend wie folgt: 2020 schlagen 2.152 Varianten zu Buche, 2019 waren es noch 4.131. Der Rekord liegt weiterhin bei 5.489 Ransomware-Payloads im Jahr 2018. Der Großteil der erkannten Signaturen reicht ins Jahr 2017 zurück und steht im Zusammenhang mit der Malware „WannaCry“ sowie verwandten Arten, was unterstreicht, dass diese einschlägigen Ransomworm-Taktiken selbst drei Jahre später noch Popularität genießen. Der stetige Rückgang des Ransomware-Volumens deutet darauf hin, dass sich die Konzentration der Angreifer verlagert. Anstelle weitverbreiteter Kampagnen nach dem Gießkannenprinzip – wie sie in der Vergangenheit beobachtet wurden – rücken mittlerweile gezielte Angriffe auf Organisationen des Gesundheitswesens, produzierende Unternehmen oder andere potenzielle Opfer, die extrem sensibel im Hinblick auf Ausfallzeiten sind, in den Fokus.
* Verschlüsselte Malware auf der Überholspur: Obwohl Malware am Netzwerkperimeter in Summe weiter abnimmt, befinden sich die verschlüsselten Varianten nach wie vor im Aufwind: Im vierten Quartal 2020 machten sie 47 Prozent des Gesamtvolumen aus. In dem Zusammenhang stieg der Anteil von Malware, die HTTPS-Verbindungen zur Verbreitung nutzt, um 41 Prozent. Und last but not least konnte auch verschlüsselte Zero-Day-Malware weitere 22 Prozent gegenüber dem Vorquartal zulegen.
* Botnet-Malware, die es auf IoT-Geräte und Router abgesehen hat, wird zur Belastung: Im vierten Quartal debütierte der Virus „Linux.Generic“ (auch bekannt als "The Moon") auf der WatchGuard-Liste der Top-10-Malware. Diese Malware-Variante gehört zu einem Server-Netzwerk, das konkret offene Schwachstellen von in Netzwerken eingesetzten IoT-Geräten und Routern des Consumer-Segments ins Visier nimmt. In Verbindung mit diesem Angriffsnetzwerk brachte die WatchGuard-Analyse eine für ARM-Prozessoren entwickelte Linux-spezifische Malware sowie eine auf MIPS-Prozessoren ausgerichtete Variante ans Licht. Es deutet alles darauf hin, dass die Angreifer damit Evasion-Angriffe auf IoT-Geräte verfolgen.
* SolarWinds-Affäre untermauert Gefahr sogenannter „Supply-Chain-Angriffe“: Der ausgeklügelte, angeblich von staatlicher Seite initiierte Angriff auf die SolarWinds-Lieferkette wird in den kommenden Jahren weitreichende Auswirkungen auf die gesamte IT-Sicherheitsbranche haben. Betroffen waren neben SolarWinds selbst fast 100 Firmen, darunter etliche Fortune 500-Konzerne, bekannte Security-Unternehmen und sogar die US-Regierung. Die detaillierte Aufschlüsselung des Vorfalls zeigt, dass es heutzutage mehr denn je auf Abwehrmechanismen ankommt, die einem vernetzten digitalen Ökosystem Rechnung tragen.
* Neuer Trojaner überlistet E-Mail-Scanner mit Multi-Payload-Ansatz: „Trojan.Script.1026663“ schaffte es im vierten Quartal 2020 auf die WatchGuard-Liste der fünf am weitesten verbreiteten Malware-Varianten. Der Angriff beginnt mit einer E-Mail, in der die Opfer aufgefordert werden, einen Anhang mit einer Bestellliste zu prüfen. Dies setzt eine ganze Reihe schädlicher Aktivitäten in Gang und führt in vielfältiger Weise zur Ausführung von Schadcode, um am jeweiligen Endpunkt schließlich die finale Phase des Angriffs einzuleiten: das Laden des Keyloggers und Remote-Access-Trojaners (RAT) „Agent Tesla“.
* Anzahl der Netzwerkangriffe nähert sich der Bestmarke aus dem Jahr 2018: Die Gesamtzahl der erkannten Netzwerkangriffe stieg im vierten Quartal 2020 um fünf Prozent und erreichte damit den höchsten Stand seit über zwei Jahren. Auch die Summe der identifizierten, individuellen Angriffsmuster wuchs um vier Prozent gegenüber dem Vorquartal. Selbst wenn sich der Arbeitsalltag vieler Unternehmen pandemiebedingt nach wie vor dezentral gestaltet, flauen die Angriffe am klassischen Netzwerkperimeter also nicht ab, sondern liegen weiter auf hohem Niveau.

Fazit: Zusammenspiel einzelner IT-Security-Disziplinen immer wichtiger

Angesichts dieser beobachteten Entwicklungen fällt das Fazit von Corey Nachreiner, Chief Technology Officer bei WatchGuard Technologies, eindeutig aus: „Der im letzten Quartal und dem ganzen Jahr 2020 verzeichnete Anstieg der Bedrohungsvarianten, bei denen besonders raffiniert ans Werk gegangen wird, zeigt, wie wichtig es ist, mehrschichtige und umfassende Sicherheitsmaßnahmen zu implementieren. Angriffe erfolgen an allen Fronten: Cyberkriminelle setzen verstärkt auf dateilose Malware, Kryptominer oder verschlüsselte Angriffe und nehmen sowohl Anwender an dezentralen Standorten als auch Unternehmensressourcen hinter dem traditionellen Netzwerkperimeter ins Visier. Effektive Sicherheit baut daher auf dem Zusammenspiel von leistungsstarker Endpoint-Protection, moderner Netzwerkabsicherung und nicht zuletzt grundlegenden Vorsichtsmaßnahmen wie IT-Security-Schulungen zur Sensibilisierung der Mitarbeiter sowie konsequentem Patch-Management auf.“

Datenbasis des Internet Security Reports

Alle im Report ausgewiesenen Erkenntnisse basieren auf den anonymisierten Firebox-Feed-Daten von über 45.000 aktiven WatchGuard UTM-Appliances weltweit, deren Anwender dem Daten-Sharing zur Unterstützung des WatchGuard Threat Labs zugestimmt haben. In Summe blockierten die Appliances im vierten Quartal 2020 über 20,6 Millionen Malware-Varianten (durchschnittlich 456 pro Gerät) und mehr als 3,5 Millionen Netzwerkangriffe (durchschnittlich 77 pro Gerät). Zudem wurden insgesamt 455 bisher unbekannte Angriffssignaturen identifiziert und abgewehrt, ein Höchstwert seit Ende 2018 und vier Prozent mehr als im vorangegangenen Quartal. Darüber hinaus liegt inzwischen ein zusätzlicher Fokus auf der Gefahrenlage am Endpunkt. Die Betrachtung umfasste 2,5 Millionen eindeutige Payload-Warnungen, die von 1,7 Millionen Endpunkten in 92 Ländern gesammelt wurden. Dank der umfassenden Datengrundlage ist es den WatchGuard-Analysten möglich, klare Trends aufzuzeigen und detaillierte Einblicke in die Gefahrenlandschaft zu geben, die Unternehmen gezielt dabei unterstützen sollen, ihre Abwehrmaßnahmen an aktuelle Gegebenheiten anzupassen.

Der vollständige Bericht mit vielen weiteren Details und Empfehlungen für adäquate Sicherheitsvorkehrungen auf Unternehmensseite steht online zum Download bereit:

<https://www.watchguard.com/wgrd-resource-center/security-report-q4-2020>.

Der Report beinhaltet nicht zuletzt eine detaillierte Analyse der berüchtigten SolarWinds-Attacke.

Bildmaterial

|  |
| --- |
|  |
| Corey Nachreiner, Chief Technology Officer bei WatchGuard Technologies |

Das Bildmaterial zum Download finden Sie in unserem Medienportal press-n-relations.amid-pr.com (Suchbegriff „[Corey Nachreiner](https://press-n-relations.amid-pr.com/AMID-PR/searchresult/searchresult.xhtml?searchString=Corey+Nachreiner&searchId=1&searchType=detailed)").

|  |  |
| --- | --- |
| Kontakt:  WatchGuard Technologies GmbH  Paul Moll – Field Marketing Manager Central Europe  Wendenstr. 379, 20537 Hamburg  Tel.: +49 152 31795040  paul.moll@watchguard.com  www.watchguard.de | Presse- und Öffentlichkeitsarbeit:  Press'n'Relations Austria GmbH  Georg Dutzi  Lange Gasse 65/16, A-1080 Wien  Tel.: +43 1 907 61 48-10  gd@press-n-relations.at  www.press-n-relations.at |

**Über WatchGuard Technologies**

WatchGuard Technologies gehört zu den führenden Anbietern im Bereich IT-Sicherheit. Das umfangreiche Produktportfolio reicht von hochentwickelten UTM (Unified Threat Management)- und Next-Generation-Firewall-Plattformen über Multifaktor-Authen­tifizierung bis hin zu Technologien für umfassenden WLAN-Schutz und Endpoint Protection sowie weiteren spezifischen Produkten und intelligenten Services rund ums Thema IT-Security. Mehr als 250.000 Kunden weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung neben kleinen und mittelständischen Unternehmen nicht zuletzt auch große, dezentral aufgestellte Organisationen vom Einsatz profitieren. Neben der Zentrale in Seattle im US-Bundesstaat Washington verfügt WatchGuard über Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum.

Aktuelle Informationen, Aktionen und Updates finden Sie auch auf [Twitter](https://twitter.com/sichersein), [Facebook](https://de-de.facebook.com/WatchGuardSichersein/) oder [LinkedIn](https://de.linkedin.com/company/watchguardsichersein). Der WatchGuard-Blog „Secplicity“ berichtet darüber hinaus über die neuesten Bedrohungen und zeigt auf, wie man mit ihnen umgeht: [www.secplicity.org](http://www.secplicity.org/). Oder Sie abonnieren den „443 – Security Simplified“-Podcast bei [Secplicity.org](http://www.secplicity.org/) bzw. wo immer Sie Ihre Lieblings-Podcasts finden.