**MEDIENINFORMATION**

Hamburg, 20. Dezember 2022

**HTTPS-Unsicherheit: Malware konzentriert sich auf verschlüsselte Verbindungen**

**WatchGuard analysiert im ISR Q3 u.a. kommerzielle Adversary-in-the-Middle-Angriffe, JavaScript-basierte Exploit-Kits und Malware mit Gothic-Panda-Bezug**

**Kurz vor Ende des Jahres hat WatchGuard Technologies seinen neuesten Internet Security Report (ISR) veröffentlicht. In diesem werden in gewohnter Weise die wichtigsten Malware-Trends sowie aktuell relevante Angriffsmethoden auf Netzwerke und Endpunkte ausführlich beschrieben. Die Erkenntnisse der Forscher des WatchGuard Threat Labs zeigen, dass die grösste Malware-Bedrohung für das dritte Quartal 2022 ausschliesslich über verschlüsselte Verbindungen verschickt wurde. Ebenso konnten vermehrt Angriffe auf ICS- und SCADA-Systeme verzeichnet werden. Auch Computerspieler sind gefährdet, denn bei einer Minecraft-Cheat-Engine wurde eine bösartige Nutzlast entdeckt. Der ISR enthält darüber hinaus eine Vielzahl weiterer Informationen und Beispiele zur gegenwärtigen Bedrohungslage.**

„Wir können gar nicht oft genug betonen, wie wichtig die Inspektion von HTTPS-Verbindungen ist: Unternehmen sollten die entsprechende Sicherheitsfunktion unbedingt aktivieren – selbst wenn es einige Anpassungen und Ausnahmeregeln erfordert. Denn der Grossteil der Malware kommt über verschlüsseltes HTTPS. Wird dieser Angriffsvektor nicht überprüft, steht Bedrohungen jeglicher Art Tür und Tor offen“, sagt Corey Nachreiner, Chief Security Officer bei WatchGuard Technologies. „Auch sollte sich das Augenmerk verstärkt auf Exchange-Server oder SCADA-Managementsysteme richten. Sobald für diese ein Patch zur Verfügung steht, ist es wichtig, dieses Update sofort einzuspielen und die Anwendung zu aktualisieren. Angreifer profitieren von jedem Unternehmen, das Schwachstellen noch nicht gefixt hat.“

Weitere wichtige Erkenntnisse aus dem Q3 Internet Security Report sind:

**Die überwiegende Mehrheit der Malware kommt über verschlüsselte Verbindungen** – Obwohl die Malware „Agent.IIQ“ in der Zeit von Juli bis September 2022 den dritten Platz in der regulären Top-10-Malware-Liste belegte, landete sie auf Platz 1 der Aufstellung für verschlüsselte Schadsoftware. Denn alle Agent.IIQ-Erkennungen wurden in HTTPS-Verbindungen gefunden. Wie die Analysen zeigen, kamen 82 Prozent der gesamten Malware über gesicherte Verbindungen, aber nur 18 Prozent unverschlüsselt. Wird der HTTPS-Datenverkehr auf der Firebox nicht überprüft, ist es sehr wahrscheinlich, dass ein grosser Teil der Malware unentdeckt bleibt. In diesem Fall können Unternehmen nur darauf hoffen, dass ein wirksamer Endpunktschutz implementiert ist, um wenigstens die Chance zu haben, die Malware an einer anderen Stelle der sogenannten Cyber Kill Chain abzufangen.

**ICS- und SCADA-Systeme sind weiterhin beliebte Angriffsziele** – Neu in der Liste der zehn häufigsten Netzwerkangriffe im dritten Quartal 2022 ist eine Attacke vom Typ SQL-Injection, die gleich mehrere Anbieter traf. Eines dieser Unternehmen ist Advantech, dessen WebAccess-Portal den Zugriff auf SCADA-Systeme einer Vielzahl von kritischen Infrastrukturen ermöglicht. Ein weiterer schwerwiegender Angriff im dritten Quartal, der ebenfalls zu den Top 5 der einschlägigen Netzwerkbedrohungen gehörte, betraf die U.motion Builder-Software von Schneider Electric, Version 1.2.1 und früher. Dies ist ein deutlicher Hinweis darauf, dass Angreifer weiterhin aktiv versuchen, Systeme zu kompromittieren, wo immer dies möglich ist.

**Schwachstellen in Exchange-Servern stellen weiterhin ein Risiko dar** – Die jüngste CVE-Schwachstelle (CVE-2021-26855), die das Threat Lab entdeckte, betrifft die Remote-Code-Ausführung (RCE) von Microsoft Exchange Server bei On-Premise-Servern. Diese RCE-Schwachstelle, die eine CVE-Bewertung von 9,8 erhielt, wurde bekanntermassen bereits ausgenutzt. Das Datum und der Schweregrad dieser Sicherheitslücke lassen ebenfalls aufhorchen, da es sich um eine von der Gruppe HAFNIUM ausgenutzte Schwachstelle handelt. Auch wenn die meisten der betroffenen Exchange-Server inzwischen gepatcht worden sein dürften, sind manche noch gefährdet und das Risiko besteht weiter.

**Bedrohungsakteure, die es auf Nutzer kostenloser Software abgesehen haben** – Der Trojaner Fugrafa lädt Malware herunter, die bösartigen Code einschleust. Im 3. Quartal 2022 untersuchten die WatchGuard-Analysten eine Variante, die in einer Cheat-Engine für das beliebte Spiel Minecraft gefunden wurde. Die Datei, die hauptsächlich auf Discord geteilt wurde, gibt vor, die Minecraft Cheat Engine Vape V4 Beta zu sein – aber das ist nicht alles, was sie enthält. Agent.FZUW weist einige Ähnlichkeiten mit Variant.Fugrafa auf, doch anstatt sich über eine Cheat-Engine zu installieren, scheint die Datei selbst geknackte Software zu enthalten. Im konkreten Fall zeigten sich zudem Verbindungen zu Racoon Stealer: Dabei handelt es sich um eine Kryptowährungs-Hacking-Kampagne, mit der Kontoinformationen von Kryptowährungsdiensten entwendet werden.

**LemonDuck-Malware ist jetzt mehr als ein Cryptominer** – Auch wenn die Zahl der blockierten oder verfolgten Malware-Domänen im dritten Quartal 2022 zurückgegangen ist, lässt sich unschwer erkennen, dass die Zahl der Angriffe auf ahnungslose Nutzer weiterhin hoch ist. Mit drei Neuzugängen in der Liste der Top-Malware-Domains – zwei gehörten zu ehemaligen LemonDuck-Malware-Domains und der dritte war Teil einer Emotet-klassifizierten Domain – gab es mehr neue Malware-Sites als üblich. Dieser Trend wird sich im Hinblick auf die Kryptowährungslandschaft voraussichtlich weiter verstärken, da Angreifer nach neuen Möglichkeiten suchen, um Nutzer zu täuschen. Ein wirksames Mittel dagegen ist ein aktiver Schutz auf DNS-Ebene. Damit können die Systeme der Benutzer überwacht und Hacker daran gehindert werden, Malware oder andere ernsthafte Probleme in das Unternehmen einzuschleusen.

**JavaScript-Verschleierung in Exploit-Kits** – Die Signatur 1132518 – als Indikator für JavaScript-Verschleierungsangriffe auf Browser – war der einzige Neuzugang in der Liste der am weitesten verbreiteten Signaturen für Netzwerkangriffe. JavaScript ist seit längerem ein gängiger Angriffsvektor und Cyberkriminelle verwenden immer wieder JavaScript-basierte Exploit-Kits, unter anderem für Malvertising und Phishing-Angriffe. Im Zuge verbesserter Verteidigungsmechanismen der Browser intensivieren auch Angreifer ihre Bemühungen, bösartigen JavaScript-Code zu verschleiern.

**Anatomie der standardisierten Adversary-in-the-Middle-Angriffe** – Die Multifaktor-Authentifizierung (MFA) ist zwar unbestreitbar eine immens wichtige Massnahme im Zuge von IT-Sicherheit, aber auch kein Allheilmittel. Bestes Beispiel dafür sind der rasche Anstieg und die Kommerzialisierung von Adversary-in-the-Middle (AitM)-Angriffen. Die Untersuchung des Threat Labs zeigt, wie böswillige Akteure sich auf immer ausgefeiltere AitM-Techniken umstellen. Ähnlich wie beim zunehmend frequentierten Ransomware-as-a-Service-Angebot hat auch die Veröffentlichung des AitM-Toolkits namens EvilProxy im September 2022 die Einstiegshürde für entsprechend ausgeklügelte Angriffe erheblich gesenkt. Deren Abwehr kann nur durch die Kombination aus technischen Tools und einer Sensibilisierung der Benutzer erfolgreich aufgegleist werden.

**Malware-Familie mit Verbindungen zu Gothic Panda** – Bereits im Bericht des Threat Labs für das zweite Quartal 2022 fiel die Sprache auf Gothic Panda – eine Cyberspionage-Gruppe mit enger Verbindung zum chinesischen Ministerium für Staatssicherheit. Interessanterweise enthält die Top-Liste der verschlüsselten Malware für das dritte Quartal eine Malware-Familie namens Taidoor, die nicht nur von Gothic Panda entwickelt wurde, sondern auch nur von Angreifern einschlägig chinesischer Herkunft eingesetzt wurde. Während sich die entsprechende Malware bisher in der Regel auf Ziele in Japan und Taiwan konzentrierte, wurde das analysierte Generic.Taidoor-Beispiel vor allem bei Organisationen in Frankreich gefunden – möglicherweise ein klarer Hinweis auf einen spezifischen, staatlich gesponserten Cyberangriff.

**Neue Ransomware- und Erpressergruppen in freier Wildbahn** – Ab sofort widmet sich das WatchGuard Threat Lab noch stärker dem Aufspüren von Ransomware-Initiativen. Dafür wurden die zugrundeliegenden Threat-Intelligence-Möglichkeiten gezielt erweitert. Im dritten Quartal 2022 führt LockBit die Liste mit über 200 einschlägigen Vorfällen an – fast viermal mehr als die Ransomware-Gruppe Basta, die von Juli bis September 2022 am zweithäufigsten von sich reden machte.

Die vierteljährlichen Forschungsberichte von WatchGuard basieren auf anonymisierten Firebox-Feed-Daten von aktiven WatchGuard-Fireboxen, deren Besitzer sich für die Weitergabe von Daten zur direkten Unterstützung der Forschungsarbeit des Threat Labs entschieden haben. Im dritten Quartal blockierte WatchGuard insgesamt mehr als 17,3 Millionen Malware-Varianten (211 pro Gerät) und mehr als 2,3 Millionen Netzwerkbedrohungen (28 pro Gerät). Der vollständige Bericht enthält Details zu weiteren Malware- und Netzwerktrends aus dem 3. Quartal 2022, empfohlene Sicherheitsstrategien, wichtige Verteidigungstipps für Unternehmen aller Grössen und Branchen und vieles mehr.

Der aktuelle Internet Security Report in englischer Sprache steht online zum Download zur Verfügung: <https://www.watchguard.com/de/wgrd-resource-center/security-report-q3-2022>

Bildmaterial

|  |
| --- |
|  |
| Corey Nachreiner, Chief Security 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=0&searchType=detailed)"). Selbstverständlich schicke ich Ihnen die Datei auch gerne per E-Mail zu. Kontakt: rh@press-n-relations.de

|  |  |
| --- | --- |
| Kontakt:WatchGuard Technologies GmbHPaul Moll – Field Marketing Manager Central EuropeWendenstr. 379, 20537 HamburgTel.: +49 152 31795040paul.moll@watchguard.comwww.watchguard.de | Presse- und Öffentlichkeitsarbeit:Press'n'Relations GmbHRebecca HornMagirusstr. 33, 89077 UlmTel.: +49 731 962 87 15 rh@press-n-relations.dewww.press-n-relations.de |

**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. Auf diesem Fundament wurde speziell für Managed Service Provider die „Unified Security Platform“ entwickelt, mit der diese ihren Kunden erstklassige Sicherheit bieten können, die sich jederzeit an individuelle Bedürfnisse anpassen lässt – bei gleichzeitig hoher betrieblicher Effizienz. Mehr als 17.000 Security-Reseller und 250.000 Kunden weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau und profitieren von einer einheitlichen Sicherheitsplattform, die folgende fünf Elemente vereint: weitreichende, aufeinander abgestimmte IT-Security-Funktionalität, kollektiver Wissensaustausch, Klarheit und Kontrolle, operative Ausrichtung und Automatisierung. 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 deutschsprachige [Unternehmensblog](https://www.watchguard.com/de/wgrd-news/blog) beleuchtet zudem regelmässig aktuelle Trendthemen im Umfeld von IT-Sicherheit. Reinschauen lohnt sich. Oder Sie abonnieren den „443 – Security Simplified“-Podcast bei [Secplicity.org](http://www.secplicity.org/) bzw. wo immer Sie Ihre Lieblings-Podcasts finden.