**MEDIENINFORMATION**

Zürich, 25. September 2019

**Gefahr lauert auf populären Domains**

**WatchGuards Internet Security Report für das zweite Quartal 2019 zeigt dramatische Zunahme an Malware im Jahresvergleich**

**Der WatchGuard Internet Security Report für das zweite Quartal 2019 liegt vor und eröffnet erneut einen detaillierten Blick auf die aktuelle Bedrohungslandschaft. Erstmals wird dabei auch gezeigt, welche Domains von Angreifern am häufigsten für Phishing-Angriffe und zum Hosting von Malware genutzt werden. In der Liste tauchen nicht zuletzt etliche Subdomains legitimer Websites und Content Delivery Networks (CDN) – wie SharePoint, Amazonaws.com und Cloudflare.net – auf. Insgesamt überrascht die Zunahme von Malware: Im Vergleich zum Vorjahreszeitraum stieg die Bedrohung um 64 Prozent. Zudem weisen die Sicherheitsspezialisten darauf hin, dass gleich zwei Module von Kali Linux, einem beliebten Werkzeug für Penetration Tests zur Überprüfung der Sicherheit im Netzwerk, in die Top Ten der Malware eingestiegen sind.**

„Tarnen und täuschen – damit lässt sich das perfide Vorgehen von Hackern beschreiben, die Malware oder Phishing-E-Mails auf legitimen Content-Hosting-Domains verstecken, um sie auf diese Weise in Unternehmensnetzwerke einzuschleusen“, sagt Corey Nachreiner, Chief Technology Officer bei WatchGuard Technologies, und ergänzt: „Glücklicherweise gibt es gleich mehrere Möglichkeiten, um sich dagegen zu wehren: Über einen DNS-Filter lassen sich Verbindungen zu bekannten bösartigen Websites blocken und mittels erweiterter Anti-Malware-Dienste sowie Multifaktor-Authentifizierung können Angriffe, die auf kompromittierten Anmeldeinformationen basieren, verhindert werden. Schulungen helfen den Mitarbeitenden dabei, Phishing-E-Mails zu erkennen. Da Einzelmassnahmen jedoch kein wirksames Verteidigungskonzept darstellen, sollten Unternehmen auf eine einheitliche Sicherheitsplattform mit mehrschichtigen Security-Diensten setzen."

Die Erkenntnisse, Forschungsergebnisse und Sicherheits-Best-Practices im vierteljährlichen Internet Security Report dienen sowohl mittelständischen als auch grossen, dezentral aufgestellten Unternehmen dazu, mehr über aktuelle Gefahren zu erfahren. In Folge können sie sich selbst, ihre Partner und Kunden besser vor Bedrohungen schützen. Zu den wichtigsten Ergebnissen des Berichts zum zweiten Quartal 2019 gehören:

* **Malware- und Phishing-Angriffe missbrauchen legitime Domänen** – Über das Tracking der Meldungen des cloudbasierten Filter-Dienst „WatchGuard DNSWatch“, der potenziell gefährliche Verbindungen auf DNS-Ebene erkennt und zum Schutz von Netzwerken und Mitarbeitenden blockiert, wurde deutlich, dass sich unter den Top-Domains, von denen Malware- und Phishing-Angriffe ausgehen, auch immer wieder Subdomains von bekannten Content Delivery Networks wie CloudFront.net (das zu Amazon gehört) und legitimen File-Sharing-Websites befinden.
* **Kali Linux feiert Premiere in den Top Ten der Malware-Liste** – Erstmals erscheinen gleich zwei Module des beliebten Hacking-Betriebssystems Kali Linux auf der WatchGuard-Malware-Liste. Hinter Trojan.GenericKD verbirgt sich eine ganze Malware-Familie, die darauf ausgelegt ist, Hintertürchen zu einem Command-and-Control-Server zu öffnen. Bei Backdoor.Small.DT handelt es sich um ein Web-Shell-Skript, das Verbindungen zu Webservern ermöglicht. Dies könnte darauf hindeuten, dass entweder immer mehr böswillige Angreifer Kali Linux nutzen oder die Anzahl der Penetrationstests durch White Hat-Hacker im Untersuchungszeitraum im Vergleich zu vorher weit höher lag.
* **Deutlicher Anstieg des Gesamtvolumens an Malware gegenüber dem Vorjahr** – Zwei von drei Malware-Erkennungsdienste von WatchGuard verzeichneten im zweiten Quartal 2019 einen klaren Anstieg von Malware gegenüber dem zweiten Quartal 2018: der eine blockierte 58 Prozent mehr Malware, beim anderen belief sich der Zuwachs auf 68 Prozent – was einem Gesamtanstieg von 64 Prozent gegenüber dem Vorjahr entspricht.
* **Breit gestreute Phishing- und Office-Exploit-Malware nimmt zu** – Zwei Malware-Varianten (ein Phishing-Angriff, der auf der Drohung basiert, gefakte Informationen über das Opfer zu veröffentlichen, sowie ein Microsoft Office-Exploit), die bereits im vierten Quartal 2018 und ersten Quartal 2019 auf der Liste der am weitesten gestreuten Malware standen, haben es jetzt auch volumenmässig in die Top Ten geschafft. Dies zeigt, dass solche Kampagnen, die mit hoher Frequenz auf eine grosse Masse abzielen, auf dem Vormarsch sind. Benutzer sollten Office daher regelmässig aktualisieren und Anti-Phishing- sowie auf DNS-Filtering basierende Sicherheitslösungen einsetzen.
* **SQL-Injections dominieren bei Netzwerkangriffen** – SQL-basierte Angriffe machten 34 Prozent aller im zweiten Quartal 2019 erkannten Netzwerkattacken aus. Der Anstieg ist im Jahresvergleich geradezu dramatisch: In einem spezifischen Fall lag das Aufkommen im zweiten Quartal 2019 verglichen mit dem Vorjahresquartal sogar um 29.000 Prozent höher. Jeder, der eine SQL-Datenbank oder Webserver mit Zugriff auf eine solche pflegt, sollte seine Systeme regelmässig auf den aktuellsten Stand bringen und in eine Web Application Firewall investieren.
* **Malware richtet sich zunehmend gegen Europa und APAC** – Im zweiten Quartal 2019 zielten fast 37 Prozent der Malware auf die EMEA-Region. Zudem wurden spezifische Einzelangriffe auf Grossbritannien, Italien, Deutschland und Mauritius registriert. Auf die Asien-Pazifik-Region (APAC) waren insgesamt 36 Prozent aller Malware-Angriffe gerichtet. Vor allem die Malware-Varianten Razy und Trojan.Phishing.MH wurden hier verortet, 11 Prozent der Trojan.Phishing.MH-Fälle entfielen allein auf Japan.

Die Ergebnisse des Reports basieren auf anonymisierten Firebox-Feed-Daten von 41.229 aktiven WatchGuard UTM-Appliances weltweit, deren Anwender dem Daten-Sharing zugestimmt haben. Insgesamt blockierten diese im zweiten Quartal dieses Jahres 22.619.836 Malware-Varianten (549 pro Gerät) und 2.265.425 Netzwerkangriffe (60 pro Gerät). Letzteres stellt einen deutlichen Gesamtanstieg gegenüber dem ersten Quartal 2019 dar und steht im Gegensatz zu früheren Beobachtungen.

Der vollständige Bericht enthält detaillierte Statistiken zu den wirkungsvollsten Malware- und Netzwerkangriffen im zweiten Quartal 2019. Darüber hinaus wird der RobbinHood-Ransomware-Angriff, der die Stadt Baltimore im Mai 2019 lahmlegte und insgesamt etwa 17 Millionen Dollar Schaden verursachte, näher beleuchtet. Natürlich erhalten Unternehmen in dem Zusammenhang auch wieder zahlreiche Tipps und Best-Practices, wie sie sich und ihre Mitarbeitenden besser schützen können.

**Analyse der Ransomware-Angriffswelle „Sodinokibi“**

Last but not least enthält der aktuelle Internet Security Report auch eine detaillierte Analyse der sogenannten Sodinokibi-Angriffe, die es in erster Linie auf Managed Service Provider (MSP) abgesehen hatten. Hierbei nutzten Angreifer schwache, gestohlene oder durchgesickerte Anmeldeinformationen, um sich administrativen Zugang zu den Verwaltungstools zu verschaffen, mit denen auf MSP-Seite Kundennetzwerke administriert und überwacht werden. Dadurch wurde es ihnen möglich, Sicherheitskontrollen zu deaktivieren und die Sodinokibi-Ransomware via PowerShell zu verbreiten.

Der vollständige Bericht steht hier zum Download zur Verfügung: <https://www.watchguard.com/wgrd-resource-center/security-report-q2-2019>

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"). 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 GmbH, c/o Medianovis AGRebecca HornSchaffhauser. 91, 8057 ZürichTel.: +49 731 962 87 15 rh@press-n-relations.dewww.press-n-relations.com |

**Über WatchGuard Technologies**

WatchGuard Technologies gehört zu den führenden Anbietern im Bereich Netzwerksicherheit. 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 sowie weiteren spezifischen Produkten und Services rund ums Thema IT-Security. Mehr als 80.000 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 InfoSec-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.