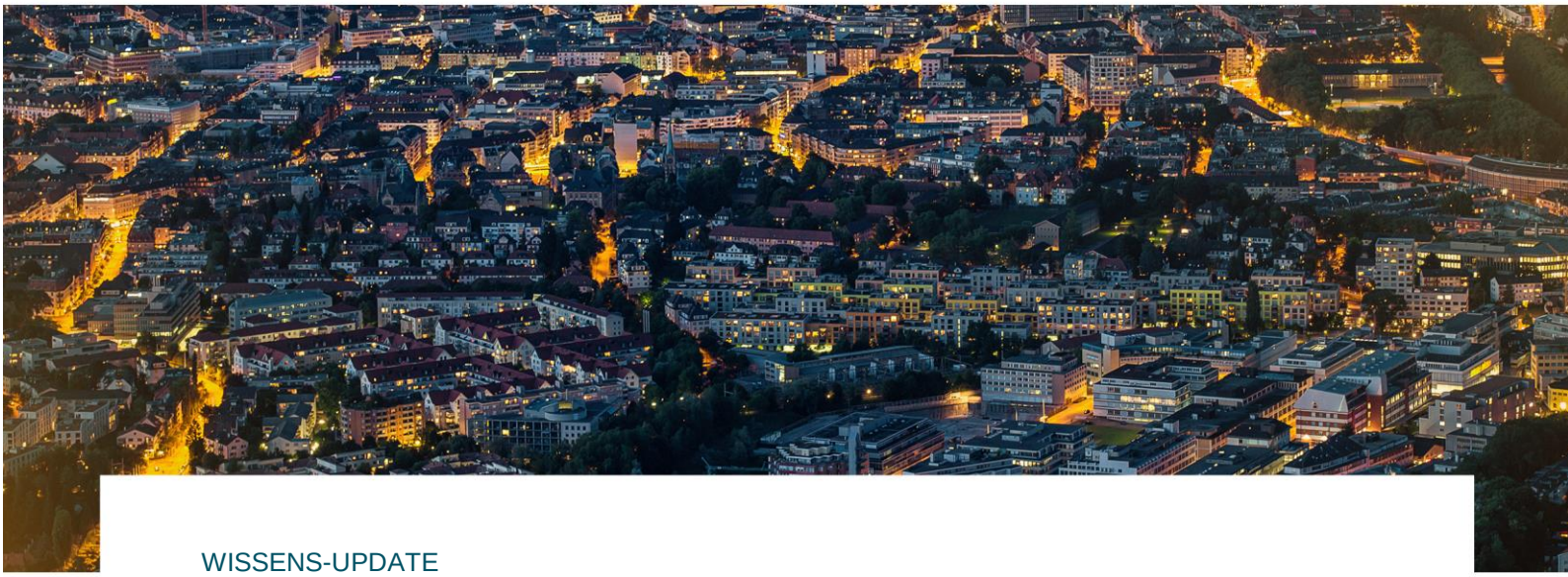
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WISSENS-UPDATE

Malware Trends 2019

Reto Amstad | Senior Security Consultant | Steinhausen, 22. Januar 2019

Cyber-Kriminelle werden auch dieses Jahr versuchen neue Angriffs- und Infizierungs-vektoren für ihre Malware-Produkte zu entwickeln, um noch effektiver und gewinnbringender ihren Geschäftstätigkeiten (bzw. denen ihrer Auftraggeber) nachgehen zu können. In diesem Blog erfahren Sie mehr über die Malware Trends 2019.

Ransomware / Wipers

Ransomware-Attacken werden weiterhin auch 2019 stattfinden. Hier wird der bereits ersichtliche Trend zu dezidierten Angriffszielen (targeted attacks) sich noch mehr akzentuieren. Die Erfolge von 2018 mit «Ryuk», «BitPaymer» und «Dharma» werden die entsprechenden Gruppierungen weiter ermuntern, vermehrt spezifische Ziele aus Industrie, dem Gesundheitswesen und von Stromlieferanten ins Visier zu nehmen. Somit werden auch 2019 nur schwer rückverfolgbare Geldzahlungen innerhalb des Dark Webs von den Geschädigten erpresst.

Bei den Entwicklern der Wiper Malware (z.B. Shamoon, Petya, Black Energy, Olympic Destroyer) andererseits geht es in erster Linie darum, grossen finanziellen Schaden oder einen Reputations-verlust bei den betroffenen Unternehmen zu verursachen. Die Akteure, welche diese Art von Malware einsetzen, wollen meistens politisch motivierte Messages und / oder die physikalische Zerstörung von entsprechenden Daten erreichen. Durch die damit erlangte mediale Aufmerksamkeit werden die entsprechenden Extremistengruppen auch 2019 weiterhin für ihre Sache solche Tools einsetzen. Bereits heute wurden neue Varianten gesichtet (z.B. für Shamoon etc.).

Mehr Vorsicht wird auch 2019 geboten sein, wenn entsprechende Wipers und Ransomware im Bereich der kritischen Infrastrukturen, sowie bei den Rüstungs- und Behörden-nahen Unternehmen zum Einsatz kommen. Hier könnten die wahren Einsatzmotive, die Vertuschung der Tracks und / oder der Datenexfiltration, im Vordergrund stehen. Eine umfassende Untersuchung dieses für dieses

Umfeld «einfachen» Angriffsvektors ist aus unserer Sicht unter solchen Umständen zwingend notwendig.

Emotet

Gestartet als einfacher Banken-Trojaner (im Jahre 2014 von einer Cybercrime Gruppe namens Mealybug) hat Emotet sich heute zu einem umfassenden «full-scale-threat-delivery-service» entwickelt. So existieren heute mittlerweile entsprechende Schnittstellen, um z.B. Drittprodukte vollständig integrieren zu können. Auch verfügt das Framework bereits über umfassende Open Source Libraries, welche zukünftig noch ausgebaut werden können.

Diese Funktionalitäten erlauben es einer weit grösseren Anzahl von Cyber-Kriminellen-Gruppierungen, das Emotet-Framework laufend dem neusten Entwicklungsstand anzupassen resp. neue Funktionen zu implementieren. So wurde z.B. kürzlich ein «Obfuscation-Makro» in Emotet integriert. Dadurch wird Emotet vermutlich auch 2019 in Erscheinung treten, um auch andere (evtl. unbekannte) Malware kostengünstig und zielgerichtet platzieren zu können.

Botnets und Cryptojacking

Letztes Jahr konnten wir sehen, wie Cyber-Kriminelle mittels Bot-Netzen mit mehreren integrierten Cyber-Aktionen den Schaden in ihren Zielen maximieren konnten. So wurden z.B. mit «Wicked» (eine Mirai-Botnet-Variante) drei neue Exploits in das Arsenal aufgenommen, welche gezielt unpatched IoT-Devices angreifen und für eigene Zwecke übernehmen konnten.

Weiter wurden mit «state-sponsored» Botnet mit dem Namen «VPNFilters» gezielt SCADA/ICS-Umgebungen angegriffen und über das MODBUS-SCADA-Protokoll entsprechende Webseiten Credentials exfiltriert. Bis heute wurden damit gemäss Schätzungen von FortiGuard mehr als 500‘000 Router und Netzwerk-Server infiziert.

Erwähnenswert ist auch die Weiterentwicklung der «Anubis»-Variante von der Bankbot-Familie. Diese stellt neu neben Ransomware, RAT-Funktionalität und Keylogging auch eine SMS-Interception und ein Call-Forwarding zur Verfügung.

Für das Jahr 2019 wird darum eine kontinuierliche Weiterentwicklung der Botnets erwartet, welche es den Cyber-Kriminellen erlauben wird, mittels modularer Architektur einerseits weiterhin klassische DDoS-Aktionen ausführen zu können. Andererseits werden vermutlich auch vermehrt intelligente sich selbstorganisierende Bot-Netze (Schwarm-Netze) auftauchen. Diese werden vermutlich weiterhin adaptierte und neue Malware für unterschiedliche Umgebungen, insbesondere aber für OT-Umgebungen, mit neuen Funktionalitäten verbreiten.

Der Trend «Cryptojacking to IoT-Devices in the Home» wird 2019 vermutlich weiter anhalten. Dieser Trend wird jedoch stark abhängig von den finanziellen Entwicklungen der Kryptowährungen sein. Die Cyber-Kriminellen werden sich hier noch stärker auf IoT-Devices (vermutlich vor allem auf Media-Devices) konzentrieren. Sie können so im grossen Stil das Mining der entsprechenden Kryptowährungen billig (weil die Zielinfrastruktur den Strom zahlt) und zuverlässig (weil die Geräte permanent am Netz laufen) dezentral durchführen. Dazu werden die entsprechenden Web-Interfaces der Geräte mittels der verfügbaren Exploits gehackt. Es wird darum auch 2019 für Sicherheitsunternehmen extrem wichtig sein, entsprechende IoT-Devices in Firmenumgebungen frühzeitig abzusichern und entsprechende Netze zu segmentieren.

Fileless Malware und Stegware

Fileless Malware versteckt sich im Memory oder andern schwer zu findenden Lokalitäten auf unterschiedlichsten Systemen und schreibt direkt ins RAM anstelle der Harddisk. Dadurch verursacht sie kaum Spuren (sog. Artifakte). Innerhalb des RAMs führt die Malware dann eine Serie von Aktionen aus wie z.B. Malicious Code Injection in bereits installierte Applikationen. Es ist bekannt, dass Cyber-Kriminelle immer mehr auf agile Entwicklungsmethoden setzen, um rasch auf die entsprechenden Anpassungen der verschiedenen Produkte- und Sicherheitsanbieter reagieren zu können. Dies gilt auch für Fileless Malware, welche als «First level of attack» bezeichnet werden kann.

2018 haben sich die Fileless-Malware-Attacken gemäss SentinelOne fast verdoppelt und das Unternehmen geht davon aus, dass dieser Trend 2019 weiter anhält. Ende 2018 wurde auch bekannt, dass Malware Code in einem Twitter-Bild eingebettet und gepostet wurde. Diese sogenannten Meme-driven Stegware war in diesem Fall ein einfaches RAT. Es zeigt aber eindrücklich auf, dass eine Stegware auch über einen Social-Kanal verbreitet und gesteuert werden kann. Für 2019 wird es sich zeigen, ob und welche neuen kreativen Wege sich Cyber-Kriminelle ausdenken, um Malware mit solchen Methoden an ihre Cyber-Kriminellen-Ziele zu bringen.

Auch wird es 2019 interessant zu beobachten sein, ob und mit welcher Qualität das anlässlich der Blackhat-US 2018 gezeigte «AI-based and target attribute concealment»-Malwaremodell (siehe DeepLocker), auftauchen wird. Es könnte sein, dass diese Art von Malware zukünftig vermehrt auftauchen wird.

APT

Es ist bekannt, dass mehrere APT (z.B. APT-28, APT-30, APT-37, APT-34 etc.) ihre Fähigkeiten und Methoden kontinuierlich verbessern. Dies einerseits, um entsprechende Varianten der APT-Malware weiterhin verborgen halten zu können, und andererseits, um die geforderten Spionage-aktivitäten zuverlässig erfüllen zu können. Der entsprechende Trend, dass sich die APT-Szene vermehrt in kommerzielle Malware bewegt, wurde 2018 bestätigt. An diesem Trend wird sich auch 2019 nichts ändern.

Von Bedeutung ist die Entwicklung von TURLA (welche sich nicht eindeutig APT-28 oder anderen russischen APT-Kampagnen zuordnen lässt). Hier ist ein Trend zur vermehrten Integration in Open Source Tools erkennbar. Zudem wird es interessant sein zu sehen, ob neue Varianten von TURLA auftauchen werden. Die neusten Versionen von TURLA brauchen heute keinen konventionellen C&C Server mehr. Vielmehr kommuniziert und lässt sich die Malware über speziell präparierte PDF-E-Mail Attachments oder über PowerShell commands mittels Empire PSInjects steuern.

Zudem dürfen wir 2019 darauf gespannt sein, ob entsprechende neue 0-Days von TURLA gefunden werden. 2018 war es hier eher trügerisch ruhig.

CyOne Security ist der vertrauensvolle Partner

Setzen Sie dafür auf die langjährige Erfahrung und die 360°-Sicherheitskompetenz der CyOne Security AG. Als rein schweizerisches Unternehmen bieten wir den kundenspezifischen Risiken angepasste, umfassende Sicherheitskonzepte und -lösungen auf höchstem Niveau für Product Security, System Security sowie Operational Security an.

Beginnen Sie heute, Ihre Organisation und somit die Schweiz vor Cyber-Risiken zu schützen.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Experten Ihre aktuellen und zukünftigen Cyber-Sicherheitsbedürfnisse und entsprechende Sicherheitslösungen.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.