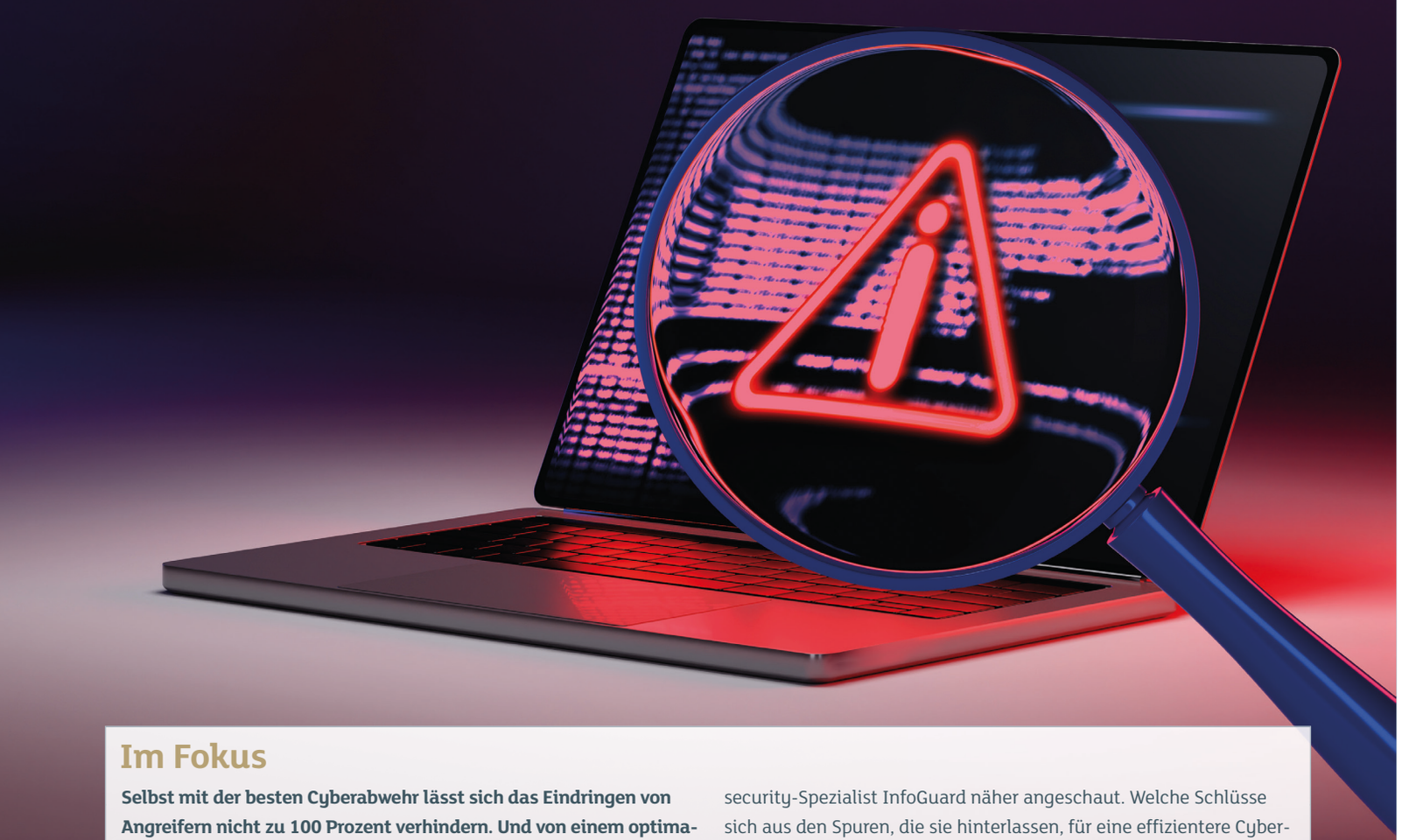
Forensik und Analyse

Die verräterischen Spuren der Top-10-Malware-Familien



Im Fokus

Selbst mit der besten Cyberabwehr lässt sich das Eindringen von Angreifern nicht zu 100 Prozent verhindern. Und von einem optimalen Schutzniveau sind viele Unternehmen mehr oder weniger weit entfernt. Umso mehr kommt es in der IT-Security darauf an, durch Forensik und Analyse die Spuren von Eindringlingen aufzudecken und daraus Erkenntnisse für Abwehrmassnahmen abzuleiten.

- **Analyse:** Viren werden in Familien eingeteilt. Die in der Schweiz am häufigsten vorkommenden Malware-Familien hat sich der Cybersecurity-Spezialist InfoGuard näher angeschaut. Welche Schlüsse sich aus den Spuren, die sie hinterlassen, für eine effizientere Cyberabwehr ziehen lassen, erläutert Stephan Berger, Head of Investigations von InfoGuard.
- **Interview:** Berger wird zu Schweizer Kunden gerufen, wenn es einen Sicherheitsvorfall gegeben hat. Er weiss also ganz genau, mit welchen Angriffen sich die Unternehmen vor allem herumschlagen – und wo sie am besten ansetzen sollten.

Incident Response

Forensische Artefakte der Top-10-Malware-Familien

Forensik und Analyse sind Schlüsselaufgaben von Computer Security Incident Teams. Eine Untersuchung der Top-10-Malware-Familien in der Schweiz identifizierte acht Artefakte zur effektiven Infektionserkennung.

→ **VON STEPHAN BERGER**

Das Lösen von Incident-Response-Fällen ist nur ein Teil der Arbeit von Computer Security Incident Response Teams (CSIRT). Andere wichtige Aufgaben sind Forensik und Analyse. Im Zeitraum von April bis Dezember 2022 wurden die Top-10-Malware-Familien in der Schweiz (gemäss govcert.ch) analysiert, um Muster und Überschneidungen in den forensischen Artefakten zu finden, die nach einer erfolgreichen Infektion auf einem Host zurückbleiben. Diese Untersuchung führte zu acht Artefakten, mit denen Infektionen dieser Malware-Familien mit hoher Wahrscheinlichkeit entdeckt werden können. Diese Artefakte können gezielt überwacht oder für das Threat Hunting im Netzwerk eingesetzt werden. Näher analysiert wurden die Malware-Familien Agent Tesla, Formbook, 404 Keylogger, Loki Password Stealer, Ave Maria RAT, Remcos, Nanocore RAT, QakBot, Redline Stealer und Netwire RAT.

```
Add-MpPreference -ExclusionPath
"C:\Users\user\AppData\Roaming\qLCTUoBHeGs.exe"
# Nanocore RAT
```

Bild 1: Bestimmte Dateien oder Ordner lassen sich vom Scan mit Windows Defender ausklammern.

In vielen Fällen wird eine Ausnahme für Windows Defender von der Malware eingerichtet, damit ein Verzeichnis oder eine Datei nicht gescannt wird (wie in Bild 1 vom Trojaner Nanocore). Die Erstellung dieser Ausnahme wird in einem Event-Log festgehalten (ID 5007, Windows Defender). Wenn (Event-)Logs bereits in einem zentralen SIEM gespeichert werden, sollten auch die Windows Defender Logs gesammelt und überwacht werden, um gezielt nach neuen Ausnahmen Ausschau zu halten. Dadurch können nicht nur Malware-Infektionen entdeckt werden, sondern auch Fehlkonfigurationen oder unsicher geschützte Verzeichnisse.

Eine alternative Möglichkeit, diese Ausnahmen auf Endgeräten zu finden, ist das Auslesen der Registry (HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths). Dieser Weg ist praktikabel, wenn eine Code-Ausführung auf allen Hosts im Netzwerk möglich ist, beispielsweise über ein EDR-Produkt mit dem Befehl req query.

```
New-ItemProperty -Path
'HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run'
-Name 'RZTHXHelper' -Value
'"C:\Users\user\AppData\Roaming\Microsoft\Windows\
Recent\RZTHX\RZTHXHelper.exe"' -PropertyType 'String'
# Ave Maria RAT
```

Bild 2: Manche Malware-Familien haben mit PowerShell eine Persistenz in der Registry erstellt.

Interessanterweise haben diverse Malware-Familien PowerShell verwendet, um beispielsweise eine neue Persistenz einzurichten (Bild 2). Der Vorteil, wenn Malware PowerShell Code ausführt, anstatt die Windows API zu verwenden, besteht darin, dass jeder ausgeführte PowerShell Code in einem eigenen Event-Log gespeichert wird, wenn PowerShell Script Block Logging aktiviert ist. PowerShell Script Block Logging kann über eine Group Policy auf allen Hosts im Netzwerk aktiviert werden. Diese Logs sollten nach Möglichkeit ebenfalls an ein SIEM übermittelt und gezielt überwacht werden.

Die Erstellung von Scheduled Tasks für die periodische Ausführung von Malware kann schon fast als gängige Methode bezeichnet →

DER AUTOR

Stephan Berger
ist Head of Investigations bei InfoGuard.
→ www.infoguard.ch

```
schtasks.exe /Create /RU NT AUTHORITY\SYSTEM /tn
ouqjustt /tr regsvr32.exe -s
"C:\Users\User\Desktop\FIRST\qbot.dll" /SC ONCE /Z
/ST 16:40 /ET 16:52
#QakBot
```

Bild 3: Ein neuer Scheduled Task wird erstellt.

Bild: Shutterstock/Bits And Splits

werden (Bild 3). Mit der Open-Source-Lösung Velociraptor und dem Hunt «TaskScheduler» können alle Tasks von den Hosts gesammelt werden, auf denen Velociraptor installiert ist. Velociraptor bietet neben vordefinierten Suchen («Hunts») auch eine eigene Abfragesprache, mit der Daten in Notebooks innerhalb von Velociraptor aufbereitet werden können. Dadurch ist es relativ einfach, zum Beispiel DLL-Dateien in User-Verzeichnissen zu finden. Neben den Live-Daten auf den Hosts innerhalb der Tasks Files können auch verschiedene Spuren in den Security Event Logs gefunden werden (Task-Erstellung, Löschung etc.). Darüber hinaus gibt es für den TaskScheduler ein eigenes Event-Log, das weitere Spuren zu den ausgeführten Tasks enthalten könnte.

Bild 4: Ein neuer Run-Key in der Registry wird erstellt.

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Fntssqo
"C:\Users\user\AppData\Roaming\Hxkotn\Fntssqo.exe"
# 404 Keylogger
```

Im User-Hive der Registry kann durch das Setzen eines Wertes im Run-Key eine Persistenz erstellt werden (Bild 4). Die eingetragene Datei wird jedes Mal gestartet, wenn sich der Benutzer am System anmeldet (Bild 5). Mit der Open-Source-Software Sysmon kann die Erstellung von Registry-Keys überwacht werden (ID 13). Ebenso können mit Velociraptor alle Run-Keys in den User- und System-Hives ausgelesen werden. Die so gesammelten Daten können wiederum mit der Abfragesprache von Velociraptor durchsucht werden.

Bild 5: Eine Persistenz im Start-up-Folder sorgt dafür, dass die eingetragene Datei stets startet, wenn sich der Nutzer am System anmeldet.

```
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\h2C08rJjFc.exe
# 404 Keylogger
```

Malware kann sich auch klassisch im Startup Folder einnisten. Dateien in diesem Verzeichnis werden ausgeführt, wenn sich ein User am System anmeldet. Zur Untersuchung dieser Persistenz wurde die Software AutoRuns von SysInternals verwendet. AutoRuns wird jedoch wiederum als Velociraptor Hunt gestartet, um Infektionen nicht nur auf einem einzigen Computer, sondern im gesamten Netzwerk zu finden.

Jede Malware-Familie hat während des Untersuchungszeitraums mindestens eine Datei im AppData-Verzeichnis (im Local- oder Roaming-Verzeichnis) abgelegt (Bild 6). Dieser «File Write»-Event kann wiederum mit Sysmon überwacht werden, analog der Registry-Keys. In diesem Fall wird die ID 11 (File created) verwendet. Auch hier eignet sich Velociraptor ideal, um verdächtige Dateien in User-Profilen zu finden. Wenn die Überwachung neu erstellter Dateien im Netzwerk möglich ist, sollte unbedingt auf jede neu erstellte Datei im Verzeichnis C:\Users\Public\ Alarm gegeben werden, da Malware dieses Verzeichnis in vielen Fällen nutzt.

Bild 6: Der Screenshot zeigt eine neu erstellte Datei im AppData-Verzeichnis.

```
File Writte:
"C:\Users\user\AppData\Local\Temp\mnsywlln.exe"

#Loki Password Stealer
```

```
{ "Host:Port:Password":
forwarding2023.ddns.net 18114:1", [..] }
# Remcos RAT
```

Bild 7: Ein Trojaner verwendet eine dynamische Domain als C2-Kanal.

Dynamische DNS-Anbieter wie DDNS.net im Beispiel (Bild 7) sind beliebte Mechanismen, um das Abschalten einer Domain zu erschweren. Diese DNS-Aufrufe sind selten und werden in den meisten Fällen nicht von legitimen Installationen durchgeführt. Es ist empfehlenswert, einen Domänen-Controller im Netzwerk als DNS einzurichten (Install-WindowsFeature -Name DNS) und das DNS-Logging zu aktivieren. Diese Logs können wiederum an ein SIEM für die Weiterverarbeitung gesendet werden. Alternativ könnte ein passiver DNS-Service auf einem Mirror-Port am Netzwerkübergang eingerichtet werden, der den Netzwerkverkehr quasi in Echtzeit mitliest und DNS-Pakete (Anfragen/Antworten) ausliest und speichert. Weiter können DNS-Daten auch live auf den Hosts im Netzwerk abgefragt werden oder bequem mit dem Velociraptor Hunt DNSCache.

```
{ "C2 list":
 [ "tolatilbu.hopto.or :54984 ]}
# Netwire RAT
```

Bild 8: Ein Trojaner verwendet einen High-Port auf einer Domain als C2-Kanal.

Das letzte Artefakt ist die Verwendung eines High-Port (Bild 8). Die Auswertung dieser Informationen auf der Firewall kann jedoch recht aufwendig sein, da die dazugehörigen Services oft nicht eindeutig erkennbar sind. Hierbei empfiehlt sich erneut, auf andere Datenquellen zurückzugreifen wie auf Sysmon, das Netzwerk-Verbindungen mit Destination, Port und dazugehöriger Applikation ausweist.

Die Identifizierung der acht Artefakte ermöglicht es, gezielte Überwachungsmethoden und Threat Hunting im Netzwerk einzusetzen. Dank der Verwendung von Open-Source-Lösungen erfolgt dies effizient und kostensparend, wodurch Aufgaben in Incident Response, Forensik und Analyse erfolgreich bewältigt werden. ←

Bild: InfoGuard/Florian Roth

«Das Missbrauchspotenzial ist gestiegen»

Immer mehr und immer raffinierter – auf diese Formel lässt sich die Entwicklung bei den Cyberangriffen bringen. Stephan Berger, Head of Investigations bei InfoGuard, gibt einen Einblick in die Sicherheitslage und ordnet Technologien wie ChatGPT und KI ein.

→ **INTERVIEW: JOHANN SCHEUERER**

Einen alles entscheidenden Sieg über die Cyberkriminellen wird es nicht geben. Stattdessen liefern sich Angreifer und Verteidiger ein ewiges Wettrüsten mit neuen Technologien und Konzepten. Jüngst haben Fortschritte bei der generativen KI das Spiel verändert. Aber auch dagegen, davon ist InfoGuard-Analyst Stephan Berger überzeugt, können sich die Unternehmen schützen – mit weniger Aufwand, als viele befürchten.

Computerworld: **Wenn Angreifer in ein Unternehmen eindringen können, bleiben sie oft erschreckend lange unentdeckt. Verstecken sie sich zu raffiniert oder wird nicht nach den richtigen Spuren gesucht?**
Stephan Berger: Die meisten Angreifer – abgesehen von staatlichen – gehen nicht besonders raffiniert vor. In Wahrheit setzen viele Firmen zu wenige Überwachungsmittel ein oder suchen gar nach den falschen Spuren. Die vorgestellten forensischen Artefakte können helfen, Kompromittierungen und Infektionen im eigenen Netzwerk schneller und zuverlässiger zu identifizieren.

Computerworld: **InfoGuard hat die in der Schweiz am meisten verbreitete Malware untersucht. Haben diese zehn Malware-Familien etwas gemeinsam oder unterscheiden sie sich sehr?**
Berger: Interessanterweise zeigen die forensischen Spuren der zehn Malware-Familien relativ starke Überschneidungen. Für uns als Sicherheitsexperten und -expertinnen ist das natürlich ein Vorteil: Wir können weniger Alarme für eine grössere Anzahl von Malware-Familien setzen und dadurch die Wahrscheinlichkeit erhöhen, eine Infektion oder einen Angreifer frühzeitig zu erkennen.

Computerworld: **Braucht es zur Abwehr der Top-10-Malware besondere Werkzeuge? Wie kann man sich auf diese Schädlinge vorbereiten?**
Berger: Bei unserer Untersuchung haben wir ausschliesslich Open-Source-Programme zur Suche und Analyse der vorgestellten Spuren eingesetzt. Diese Programme können kostenfrei aus dem Internet heruntergeladen und genutzt werden. Der richtige Einsatz erfordert ein gewisses Know-how, aber grundsätzlich sollten die Kosten kein Hindernis für eine effiziente Cyberüberwachung darstellen.

Computerworld: **Noch herausfordernder wird die Sicherheitslage derzeit durch eine Technik, die seit Monaten die Schlagzeilen beherrscht: künstliche Intelligenz. Wie gross sind die Gefahren, die davon ausgehen?**
Berger: Künstliche-Intelligenz-Modelle, wie ChatGPT, machen es Angreifern einfacher, auf «Befehl» Schadcode generieren zu lassen. Das Missbrauchspotenzial ist daher gestiegen und Angreifer können auch ohne umfassendes Vorwissen potenzielle Angriffe durchführen. Je nach Entwicklung der KI könnte sogar eine vollständig automatisierte Kompromittierung von Netzwerken realisierbar werden.

Computerworld: **Auch wenn KI derzeit alles Interesse auf sich zu ziehen scheint, bleiben die anderen Security-Themen unverändert auf der Tagesordnung. Welche Trends sind aus Ihrer Sicht aktuell denn die wichtigsten? Vielleicht sogar wichtiger als KI?**
Berger: Noch bedeutender als KI – und meiner Ansicht nach am wichtigsten – ist eine Härtung der Betriebssysteme, des Active Directory und allgemein des Netzwerks. Basierend auf meinen Erfahrungen aus Hunderten von Incident-Response-Fällen kann ich sagen, dass viele Unternehmen der Cyberhygiene innerhalb ihrer Netzwerke noch immer ungenügend Beachtung schenken. Dazu zählen klassischerweise Patchmanagement, zu hohe Benutzerberechtigungen und fehlende Multi-Faktor-Authentisierung.

Computerworld: **Worum sollten sich Unternehmen aus Ihrer Sicht grundsätzlich am dringlichsten kümmern?**
Berger: Ein starker Security-Partner, der das Netzwerk 24/7 überwacht, ist unerlässlich. Die aktuelle Bedrohungslage lässt nicht mehr zu, dass kritische Alarme über Nacht oder gar über das Wochenende unbearbeitet bleiben. Viele Angreifer erlangen, sobald sie Zugang zum internen Netzwerk haben, innerhalb weniger Stunden höchste Berechtigungen. Schnelles und professionelles Handeln ist daher zwingend. ←

ZUR PERSON

Stephan Berger ist heute als Head of Investigations bei InfoGuard tätig. Er stiess 2020 als Senior Cyber Security Analyst zu dem Sicherheitsspezialisten aus Baar. Zuvor war er jeweils vier Jahre in ähnlicher Funktion beim Bundesamt für Informatik und Telekommunikation BIT und der Schweizerischen Post beschäftigt. Berger hält einen Master in Engineering mit Vertiefung Computer Science/IT-Security von der Berner Fachhochschule.