Besonderheiten der aktuellen Bedrohungslage

Angreifer nutzen verstärkt vorhandene Werkzeuge
Wie kann man sich davor schützen?

Presenter

Thomas Hemker,
CISSP, CISM, CISA

Director Security Strategy, CTO

Date

12.10.17

PITS

Berlin

Thomas Hemker, CISSP, CISM, CISA

#THeSecurity
(LinkedIn, XING, ResearchGate, noFB)

Thomas_Hemker@symantec.com

22 Jahre IT-Security
PGP

CTO Office
CISO Kontakt
Sprecher, Autor

ISF, TeleTrust, Bitkom, ENISA
ISACA, (ISC)2, HDG

Hamburg

Living off the Land

Angreifer nutzen was bereits auf dem System ist

- Ausnutzbare 0-Day Schwachstellen werden immer schwerer zu finden
- Nutzung von Systemtools taucht in Logfiles unter
- Nutzung von Dual-Use Tools und Cloud Services
  - → Ursprung und Gruppe schwerer herauszufinden
- «Filelose» Backdoor z.B. mit PowerShell in Registry, WMI oder GPO

Simple Attacken - aber erfolgreich und kritisch

«Fileless» Attacken

Möglichkeiten (nicht alle komplett dateilos):

MEMORY ONLY ATTACKS	z.B. remote code exploits wie EternalBlue und CodeRed
DUAL-USE TOOLS	Werkzeuge wie PsExec nutzen um schadhafte Dinge zu tun
NON-PE FILES	Dokumente mit Makros, PDFs mit JavaScript Und Skripte (VBS, JavaScript, PowerShell,…)
FILELESS LOADPOINT	Skripte versteckt in Registry, WMI or GPO, z.B.: Poweliks, Kotver

Angriffsablauf

1. INCURSION

- Exploit in memory
  z.B. SMB EternalBlue
- Email mit Non-PE file
  z.B. document macro
- Remote script dropper z.B. LNK
  Mit PowerShell aus der cloud
- Schwache oder gestohlene PW
  z.B. RDP Passwörter

2. PERSISTENCE

Non-persistent

- Memory only malware
  z.B. SQL Slammer

Persistent

- Fileless persistence loadpoint
  z.B. JScript in registry
- Regular non-fileless method

3. PAYLOAD

- Dual-use tools
  z.B. netsh or PsExec.exe
- Memory only payload
  z.B. Mirai DDoS
- Non-PE file payload
  z.B. PowerShell script
- Regular non-fileless payload

Gezielte Angriffe & Dual-Use Tools

Gruppe	Informationsgewinnung	Stehlen von Zugangsdaten	Bewegung	Eigen
Tick	whoami, procdump, VBS	WCE, Mimikatz, gsecdump	PsExec	Ja
Waterbug	systeminfo, net, tasklist, gpresult,…	WCE, pwdump	Open shares	Ja
Suckfly	tcpscan, smbscan	WCE, gsecdump, credentialdumper	-	Ja
Fritillary	PowerShell, sdelete	Mimikatz, PowerShell	PsExec	Ja
Destroyer	Disk usage, event log viewer	kerberos manipulator	PsExec, curl, VNC	Ja
Chafer	network scanner, SMB bruteforcer	WCE, Mimikatz, gsecdump,…	PsExec	Ja
Greenbug	Broutlook	WCE, gsecdump, browdump, …	TeamViewer, PuTTY	Ja
Buckeye	os info, user info, smb enumerator,…	pwdump, Lazagne, chromedump,…	Open shares	Ja
Billbug	ver, net, gpresult, systeminfo, ipconfig, …	-	custom backdoor	Ja
Appleworm	net, netsh, query, telnet, find, …	dumping SAM	RDP bruteforcer, rdclip	Ja

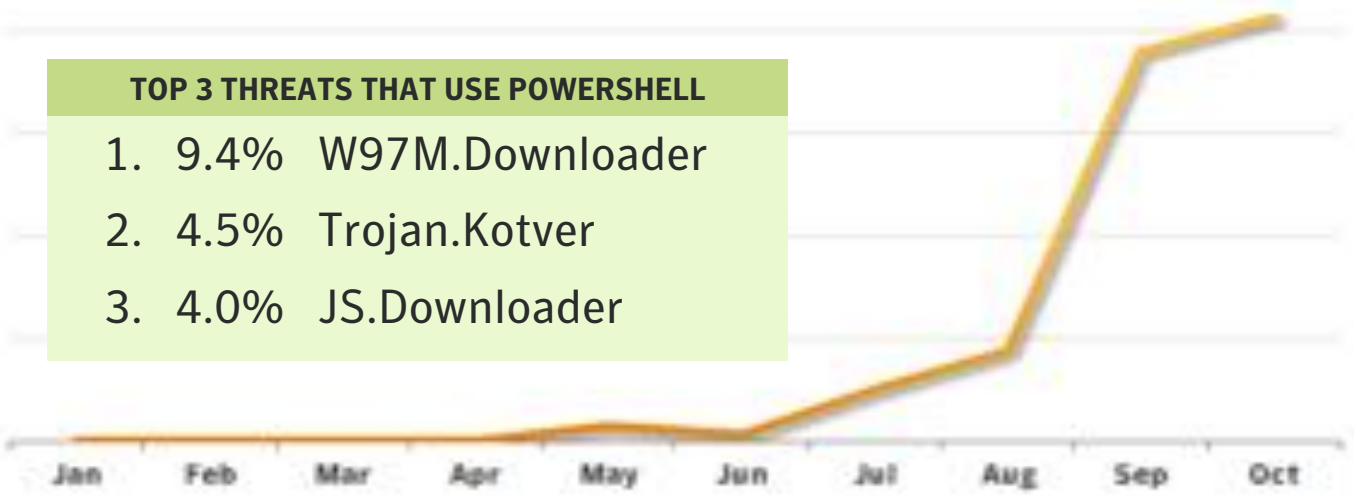
Petya benutzt Dual-use tools

- Angriff ist eine DLL ausgeführt von rundll32.exe
- Benutzt rekompilierte Version von LSADump Mimikatz um an Passwörter zu kommen
- Benutzt PsExec um sich auszubreiten
  - *\\[server_name]\admin$\perfc.dat*
  - psexec rundll32.exe c:\windows\perfc.dat #1 <rand>
- Benutzt WMI zur Ausbreitung wenn PsExec nicht funktioniert
  - *wmic.exe /node:[IP Address] /user:[USERNAME] /password:[PASSWORD] process call create "%System%\rundll32.exe \"%Windows%\perfc.dat\" #1 60"*
- Scheduled task um Neustart in modifizierten MBR zu erzwingen
  - schtasks /RU "SYSTEM" /Create /SC once /TN "" /TR "%system%\shutdown14:42.exe /r /f" /ST
- Löscht Logs um Spuren zu beseitigen
  - wevtutil cl Setup & wevtutil cl System & … & fsutil usn deletejournal /D %C:

PowerShell

- **95.4%** der PowerShell Skripts gesendet an Blue Coat MAA waren schädlich

Volume of PowerShell samples from customers in our sandbox in 2016



TOP 3 THREATS THAT USE POWERSHELL

1. 9.4% W97M.Downloader
2. 4.5% Trojan.Kotver
3. 4.0% JS.Downloader

8

Skript versteckt in der Registry

Bekannt: Windows registry run key verweist auf Malware-Datei

Neu: Windows registry run key beinhaltet ein Skript zur Ausführung

- Skript kann von anderen registry keys Payloads laden und ausführen
- Normale AV-Scans finden diese Skripte wahrscheinlich nicht

Name	Type	Data
(Default)	REG_SZ	rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";eval("epdvnfou/xsjuf)(=tdsjqu!m...
a	REG_SZ	#@~^k4QAAA==n{F+2i@#@&l{xAPzmOk7+p6(L+1O`r?1.rwDRUtnVsE*i@#@&S4k^+cne'c+...

Schwierigkeiten bei der Erkennung

Keine Datei auf Festplatte → Maßnahmen greifen ggf. nicht

Keine Indicators of compromise (IoCs) für den Austausch

Verbreitete Malware braucht nicht unbedingt mehr einen “loadpoint”

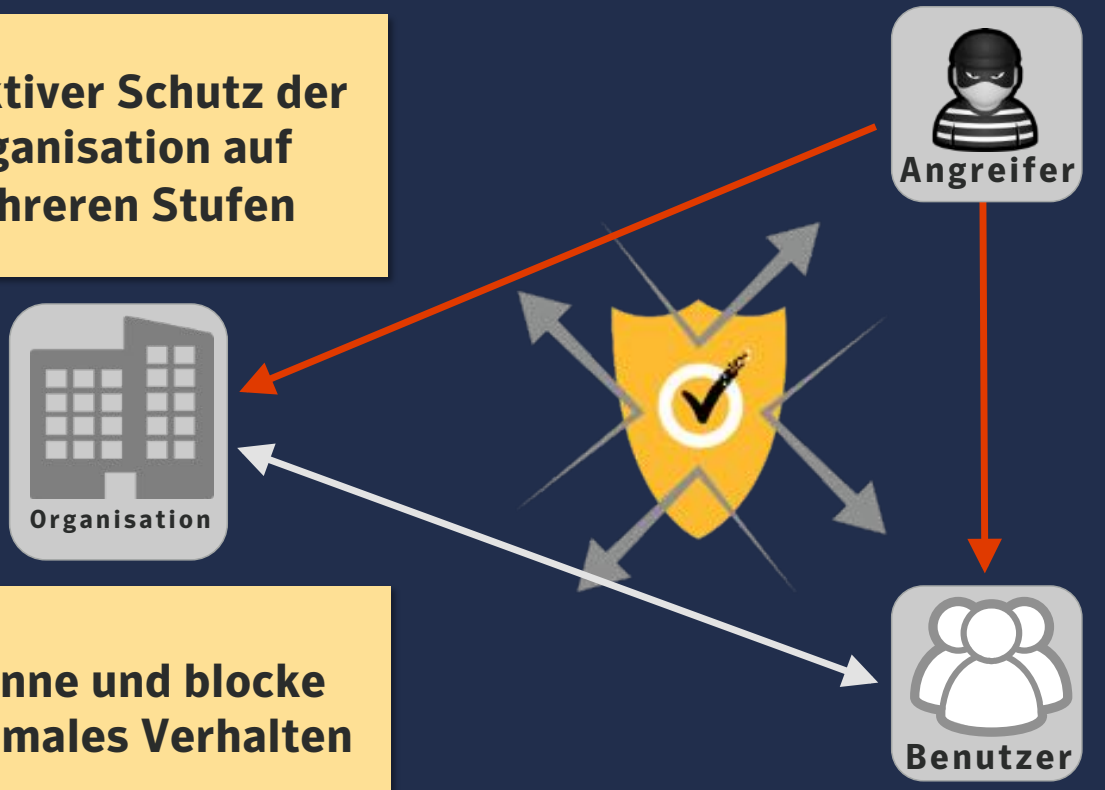
Es gibt aber Erkennungsmöglichkeiten für solche Angriffe

Was kann man tun?

- Nutzung der Dual-Use Werkzeuge überwachen
- Blocken der Remote Execution über PsExec und WMI
- Besseres Logging und Verarbeitung der Information
- Bessere Absicherung der (administrativen) Konton durch z.B. 2FA und Login Benachrichtigung
- Verhaltensbasierte Erkennung kann u.U. das Stehlen von Zugangsdaten und Passwörtern verhindern
- Neue Technologien der Malware-Erkennung zusätzlich einsetzen

Schutzmethoden

Proaktiver Schutz der Organisation auf mehreren Stufen



Informationen zu Angriffstrends

Richtige Konfiguration und Updates

Verhindere Infektionen

Erkenne und blocke abnormales Verhalten

Bericht

https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf