A Talos Look into the Evolving Threat Landscape

Earl Carter
Senior Threat Researcher
Today’s Plan

- Threat Landscape
- Attack Techniques
  - An Unexpected Attack Vector
  - Self-Propagation (Worms)
  - Attacking Trust
- Talos Threat Intelligence
THREAT LANDSCAPE - VULNERABILITIES

- Network Accessible
- Low Complexity
- No Authorization
- High Severity

60% Reduction

Low Hanging Fruit on Decline

25%

- Network Accessible
- Low Complexity
- No Authorization
- High Severity
Common Attack Vectors

Security Holes Everywhere

Unpatched Vulnerabilities

IoT

Users

YOUR PHONE TOLD YOUR FITBIT THAT TOLD YOUR NEST THAT TOLD YOUR SONOS THAT TOLD ME THAT YOU OWE YOUR WIFE AN APOLOGY.

TWO DOZEN RED ROSES ARE ONLY $29.99 FOR A LIMITED TIME.
Data is the New Target
An Attack Vector In Plain Site
Covert Channels and Poor Decisions: The Tale of DNSMessenger
Multi Stage

Stage 1

Stage 2
Powershell to Gain Persistence

Stage 3
Powershell to Launch C&C

Stage 4

This document has been secured by McAfee. To view this protected document, click Enable Content.
Stage 4 – DNS Messages

Message Query

SYN Query
Spoofed SEC Emails Distribute Evolved DNSMessenger
Spoofed SEC Emails

- Targeted spear phishing campaign.
- Spoofed from SEC EDGAR system and contained malicious attachment.
DNSMessenger – Stage 4

• Functions as a Remote Access Trojan (RAT) that is implemented using PowerShell.

• Uses DNS for command retrieval from C2.
  – Sample domain: EFA29DD310.stage.0.ns0.pw

• POSTs data to attackers server via HTTP.

• Can be used to execute a variety of commands on infected systems.
2017 – Attack of the Worms
Remember

1988 Morris Worm (Sendmail, finger, rsh)

2001 Code Red Worm (IIS)

2003 Blaster Worm (RPC)

2008 Conficker Worm (RPC, NetBIOS)
Massive ransomware cyber-attack hits nearly 100 countries around the world

More than 45,000 attacks recorded in countries including the UK, Russia, India and China may have originated with theft of ‘cyber weapons’ from the NSA.

"WannaCry" ransomware attack losses could reach $4 billion

Global financial and economic losses from the "WannaCry" attack that crippled computers in at least 150 countries could swell into the billions of dollars, making it one of the costliest single incidents involving so-called ransomware.

Cyber-Safe

Massive cyberattack targeting 99 countries causes sweeping havoc

by Selena Larson  @selenalarson

May 13, 2017, 7:12 AM ET
WannaCry Propagation
More than half of major malware attack’s victims are industrial targets

Ransomware 'Nyetya' behind new global cyber attack: Cisco

Key researchers reclassify Nyetya suspect destruction was true
Bad Rabbit ransomware spread using leaked NSA EternalRomance exploit, researchers confirm

Bad Rabbit used NSA “EternalRomance” exploit to spread, researchers say

EternalRomance exploit was used to move across networks after initial attack.

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If you succeed, you’ll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you’ll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.
Propagation

infpub.dat

- WMI
- SMB/SMB2/SVCCTL
- NTLMSSP brute forcing
- ETERNALROMANCE

Scans IP subnet
139 TCP
This 'Olympic Destroyer' Malware May Have Killed Winter Games Computers -- UPDATED

‘Olympic Destroyer’ Cyberattack Disrupted Pyeongchang Opening Ceremony

Researchers: We Found the Olympic-Disrupting Malware

They're calling the malware 'Olympic Destroyer' and say they have "moderate confidence" that it was used to disrupt the Opening Ceremony.
Olympic Destroy Propagation

WINLOGON.EXE

PSEXEC
WMI

SCANS IP SUBNET
ARP TABLE & WMI

Eternal Romance Artifacts – No execution
Olympic Destroy Workflow

WINLOGON.EXE

- Browser Stealer
- Stealer Stealer
- Patched Winlogon.exe with discovered credential
- Destroyer
- PsExec
Supply Chain Attacks
Exploiting Trust Relationships

New Havex malware variants target industrial control system and SCADA users

Maersk says Nyetya cyberattack cost it $300M in revenue loss

Avast! There’s malware in that CCleaner software update

Avast’s recent acquisition spreads a backdoor signed with its own certificate.

SEAN GALLAGHER - 9/18/2017, 10:08 AM
Nyetya “Ransomware” Attack
JUNE 27TH, 2017

8:59:14 UTC
Malicious actor used stolen credentials and “su” to obtain root privileges on the update server.

BETWEEN 9:11:59 UTC AND 9:14:58 UTC
The actor modifies the web server configuration to proxy to an OVH server.

9:14:58 UTC
Logs confirm proxied traffic to OVH.

12:31:12 UTC
The last confirmed proxy connection to OVH is observed. This marks the end of the active infection period.
Restoring Connections

12:33:00 UTC
The original server configuration is restored.

14:11:07 UTC
Received SSH disconnect from Latvian IP 159.148.186.214

19:46:26 UTC
The OVH server, 176.31.182.167, is wiped using "dd if=/dev/zero", filling the hard drive with 0x00.
The Backdoor

**COMMAND 0** will read in parameters and a timeout in minutes and will then execute “cmd.exe” with those parameters. It will return the result of this command back to the web server.

**COMMAND 1** will write data to a file, potentially using environment variables to write to the correct path (e.g., %SystemRoot%\filename).

**COMMAND 2** will return the information that it retrieved earlier (Proxy and SMTP information, including usernames and passwords) as well as information on the OS version and architecture, whether the user is admin, what token level the process is running as and whether UAC is enabled.

**COMMAND 3** will read any file from the file system and upload it to the server.

**COMMAND 4** is similar to Command 1 in that it will write a file to the filesystem, but it will also immediately execute that file as a new process. When it is done, the file will be overwritten by random data and then deleted.

**COMMAND 5** handled by the function AutoPayload, is similar to command 4, but will start the downloaded file with “rundll32.exe”

Contacts upd.me-doc.com.ua every 2 mins

If finds a proxy:

Retrieves email data from local me-doc

Wait for & execute commands

These commands almost certainly used to distribute Nyetya.
CCleanup: A Vast Number of Machines at Risk

CCleaner Command and Control Causes Concern
Digital Signature of CCleaner 5.33

- presence of a valid digital may be indicative of a larger issue that resulted in portions of the development or signing process being compromised
- this certificate should be revoked and untrusted moving forward

Compilation Artifact

- likely an attacker compromised a portion of development or build environment
- Leveraged access to insert malware into the CCleaner build that was released and hosted by the organization

S:\workspace\ccleaner\branches\v5.33\bin\CCleaner\Release\CCleaner.pdb
Data Collected on Infected Systems

Installed Programs

- Adobe Flash Player 23 ActiveX
- Adobe Flash Player 20 NSAPI
- Adobe Shockwave Player 12.1
- CCleaner
- CutePDF Utility 0.3.3 Rel (x86)
- Windows 显示标准驱动程序 - OLYMPUS IMAGING CORP
- Camera Communication Driver Package 09/09/2009 1.0.0.0
- Google Chrome
- 部份檔案無法使用英語名稱
- LanScape Cat MRT
- Mozilla Firefox 65.0
- Mozilla Maintenance
- 便携式應用程序集 19.0.0.0
- Picasa 3
- TeamViewer 9
- Roxio Central Data
- Google Toolbar for IE
- 疫情期間需要慎用
- Roxio Central Tools
- Java 8 Update 141
- UpdateAdvisor(待測)
- eReg
- Java Auto Updater
- PA-Z8900T
- SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

Process List

- System
- C:\Windows\System32\smss.exe
- C:\Windows\System32\csrss.exe
- C:\Windows\System32\wininit.exe
- C:\Windows\System32\services.exe
- C:\Windows\System32\lsass.exe

- C:\Windows\System32\spoolsv.exe
- C:\Windows\System32\svchost.exe
- C:\Program Files\Common Files\Adobe\ARM\1.0\arm.exe
- C:\Program Files\AglientIO Libraries Suite\AglientIOLibrariesService.exe
- C:\Program Files\AglientIO Libraries Suite\LxMdnsResponder.exe
- C:\Program Files\ESET\ESET Endpoint Antivirus\akm.exe
- C:\Windows\System32\svchost.exe
- C:\Windows\System32\svchost.exe
Targeted to Tech Companies

2\textsuperscript{nd} Stage only delivered to 23 specific domains

- Database Tracked 2\textsuperscript{nd} Stage Delivery
- No Cisco Devices Delivered 2\textsuperscript{nd} Stage
TALOS INTEL BREAKDOWN

THREAT INTEL

- 1.5 MILLION Daily Malware Samples
- 600 BILLION Daily Email Messages
- 20 BILLION Threats Blocked
- 16 BILLION Daily Web Requests
- 1100+ Threat Traps
- 100+ Threat Intelligence Partners
- 1100+ Threat Intelligence Researchers
- MILLIONS Of Telemetry Agents
- Internet-Wide Scanning
- Open Source Communities
- Honeypots
- 3rd Party Programs (MAPP)
- Vulnerability Discovery (Internal)
- Product Telemetry
- OPEN SOURCE INTEL SHARING
- Service Provider Coordination Program
- Industry Sharing Partnerships (ISACs)
- Customer Data Sharing Programs
- 3rd Party Programs (MAPP)
- Open Source Intel Sharing
- 500+ Participants
- 4 Global Data Centers
- 100+ Threat Intelligence Partners
- 250+ Full Time Threat Intel Researchers
- 20 BILLION Threats Blocked
- 600 BILLION Daily Email Messages
- 1.5 MILLION Daily Malware Samples
- 16 BILLION Daily Web Requests
MULTI-TIERED DEFENSE

Cloud to Core Coverage

- **WEB**: Reputation, URL Filtering, AVC
- **END POINT**: Software – ClamAV, Razorback, Moflow
- **CLOUD**: FireAMP & ClamAV detection content
- **EMAIL**: Reputation, AntiSpam, Outbreak Filters
- **NETWORK**: Snort Subscription Rule Set, VDB – FireSIGHT Updates & Content, SEU/SRU Product Detection & Prevention Content
- **GLOBAL** Threat Intelligence Updates