The Power of Network AND Endpoint Threat Correlation

Danny Banks
Threat Detection & Response SME
Technical Director, Business Development
WatchGuard Technologies

Agenda

- About the Speaker
- BBT
- The Problem Security Teams are Facing Today
  - Current Threat Landscape
  - Simple Malware Evasive Techniques
  - Siloed Defensive Approaches
  - Real-World Customer Examples
- Recommended Solutions to Solving Today's Challenges
  - Definition of Power & Correlation
  - The Network Provides Key Security Information
  - Endpoints Generate Unique Security Events
  - BREAK the Kill Chain
- Summary: Be "Great"
- Q & A

About the Speaker

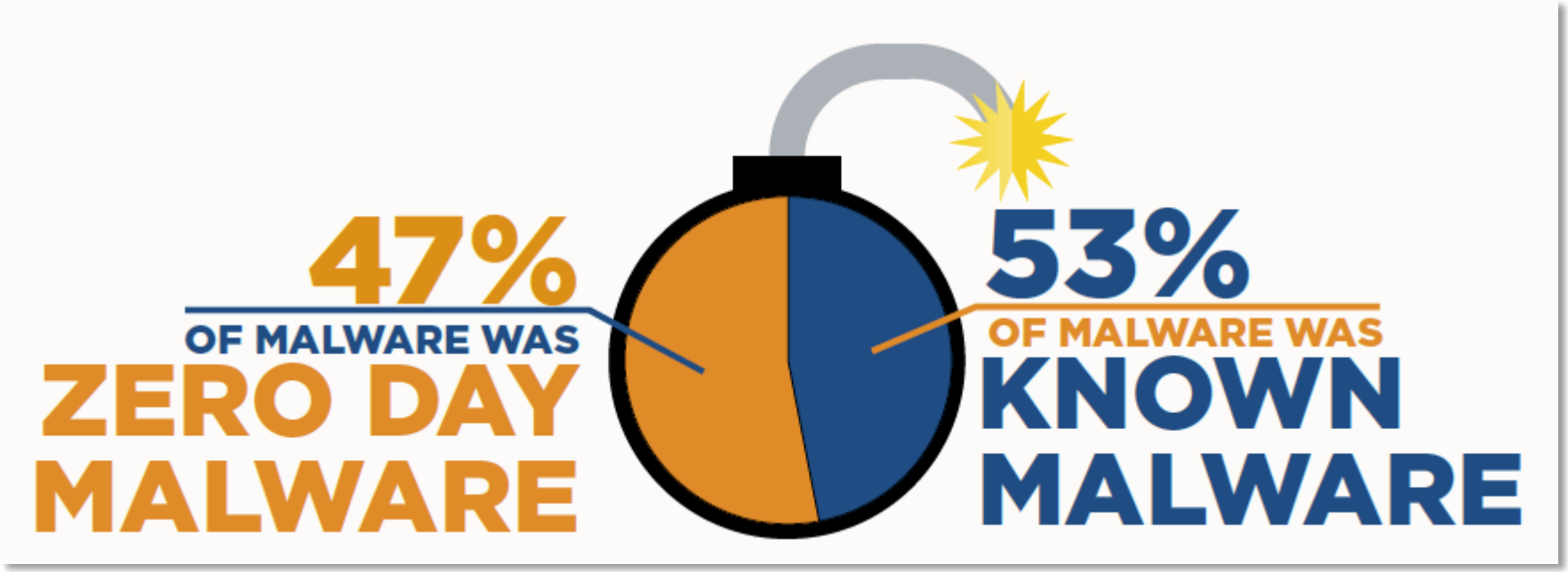
Danny Banks
Threat Detection & Response SME
Technical Director, Business Development
WatchGuard Technologies

As the Threat Detection & Response (TDR) Subject Matter Expert Danny provides market knowledge and field level sales support to WatchGuard partners and customers to assist them with their endpoint related cyber security challenges. Specifically, Danny applies his unique talent and capabilities to evangelize the benefits of WatchGuard's Threat Detection and Response Advanced Security Service to WatchGuard's rapidly expanding partner and customer base. Danny joined WatchGuard Technologies in June 2016 through the acquisition of the HawkEye G Endpoint Detection and Response (EDR) technology that was original developed by Hexis Cyber Solutions in 2013.

Danny holds a BS degree in Physics from the University of California at Davis.


The Big Bang Theory - Shamy's Fort
"Would it alarm you if I told you that I hid this sleep over bag right here (under a chair cushion in Sheldon's apartment) over 2 years ago for an occasion like this?"
The Big Bang Theory - Shamy's Fort
"Who says this one is the only one that I hid?"
3:33 / 4:24

The Problem: Current Threat Landscape



Reference: https://embed.widencdn.net/download/watchguard/iec7lhqo2q/Summary_WG-Threat-Report-Q2-2017.pdf

The Problem: Continued…

- The industry sees anywhere from 300,000 to 1 million new malware ***variants*** each day.
  - Only thousands of truly unique malware families
  - Malware authors use obfuscation techniques to create malware that's: "New to You"

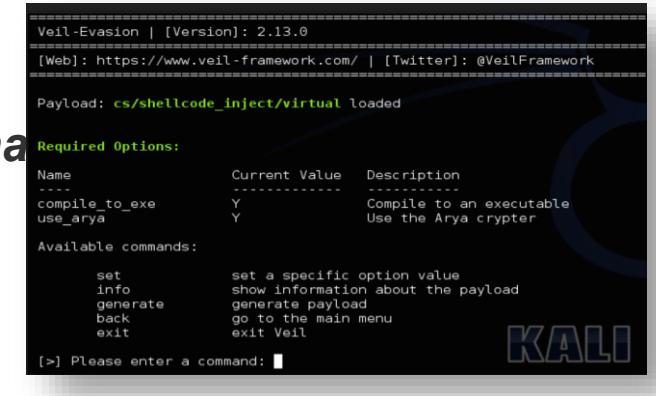
- Simple Malware Evasive Techniques
  - Anti-Security
  - Anti-Sandbox
  - Anti-Analyst

- Siloed Defensive Approaches

Malware Obfuscation

- **Basic Obfuscation:** There are millions of malware variants, and most come from hackers using malware evasion techniques. The four basic methods include packers, crypters, polymorphic malware, and downloaders (also called droppers and staged loaders).
- **Advanced Obfuscation:** Today hackers are moving beyond the basics, using more advanced methods and tactics when hiding malware. This includes anti-disassembly and debugging, rootkits, and code, process and DLL injection.

"Whil… …ha… chang…



Reference: https://www.secplicity.org/2017/08/31/hacker-hide-seek-malware-obfuscation-detect/

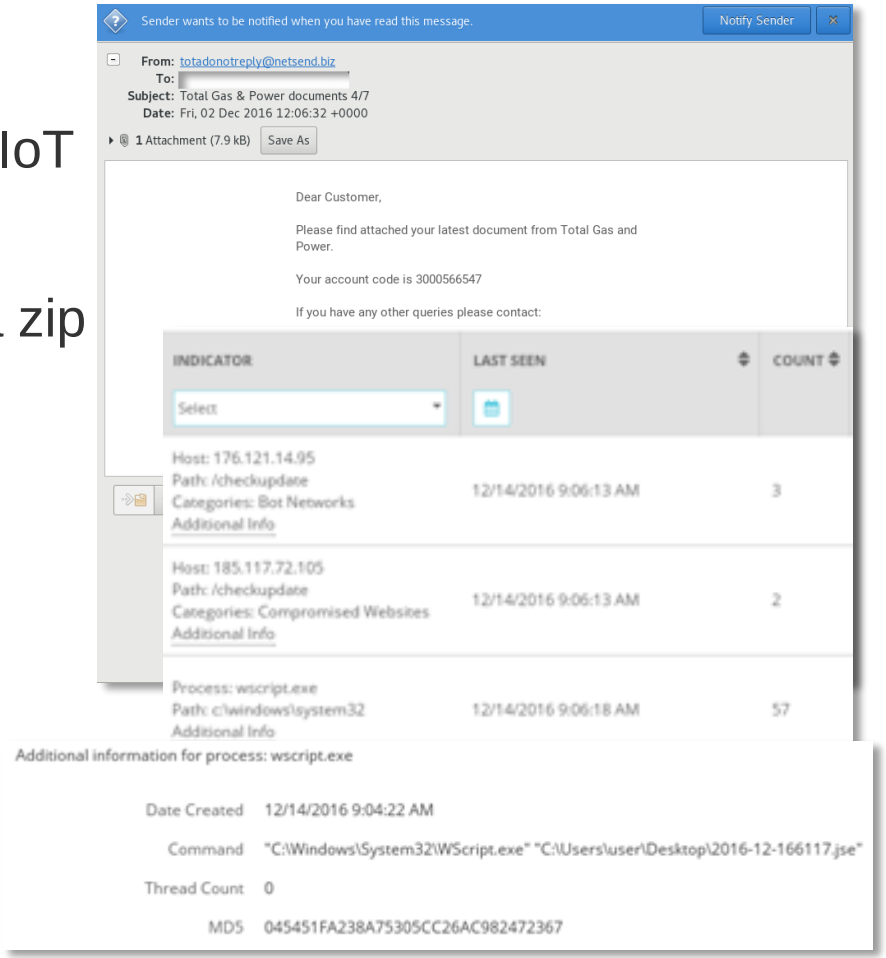
Real World Case Study #1

- Company: [redacted]
  - ~5000 Employees, ~8000 Endpoints/Servers
- **Conficker**
  - ~1000 endpoints infected within 24 hours of initial attack
  - Network Security detected and blocked 50,000 call backs to Conficker C2 sites
  - Identification of endpoints making call outs provided a list of devices to install endpoint detection and response agents
  - Endpoint agents provided automated remediation without having to reimage all the infected machines
- Hundreds of IT man-hours saved $$$
- Workforce productivity uninterrupted $$$
- Brand Protected $$$

Real World Case Study #2

- Company: [redacted]
  - ~4 Employees, ~20 Endpoints/IoT
- **Ransomware**
  - Jscript Encoded Script File in a zip
  - Not detected by Anti-Virus
  - Network Security detected and blocked callbacks to C2
  - Endpoint agents identified responsible malicious process
  - Remediation actions taken
- No precious documents

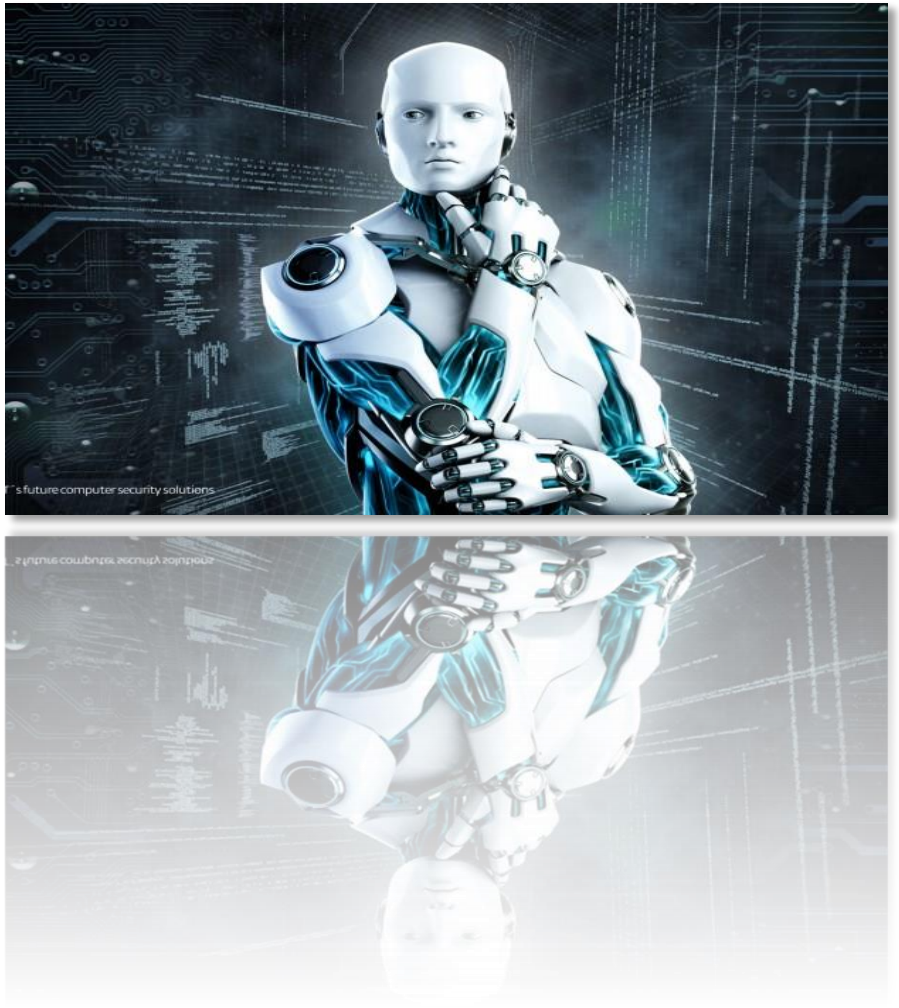
  or family photos encrypted
- Dad is Cyber Security Hero

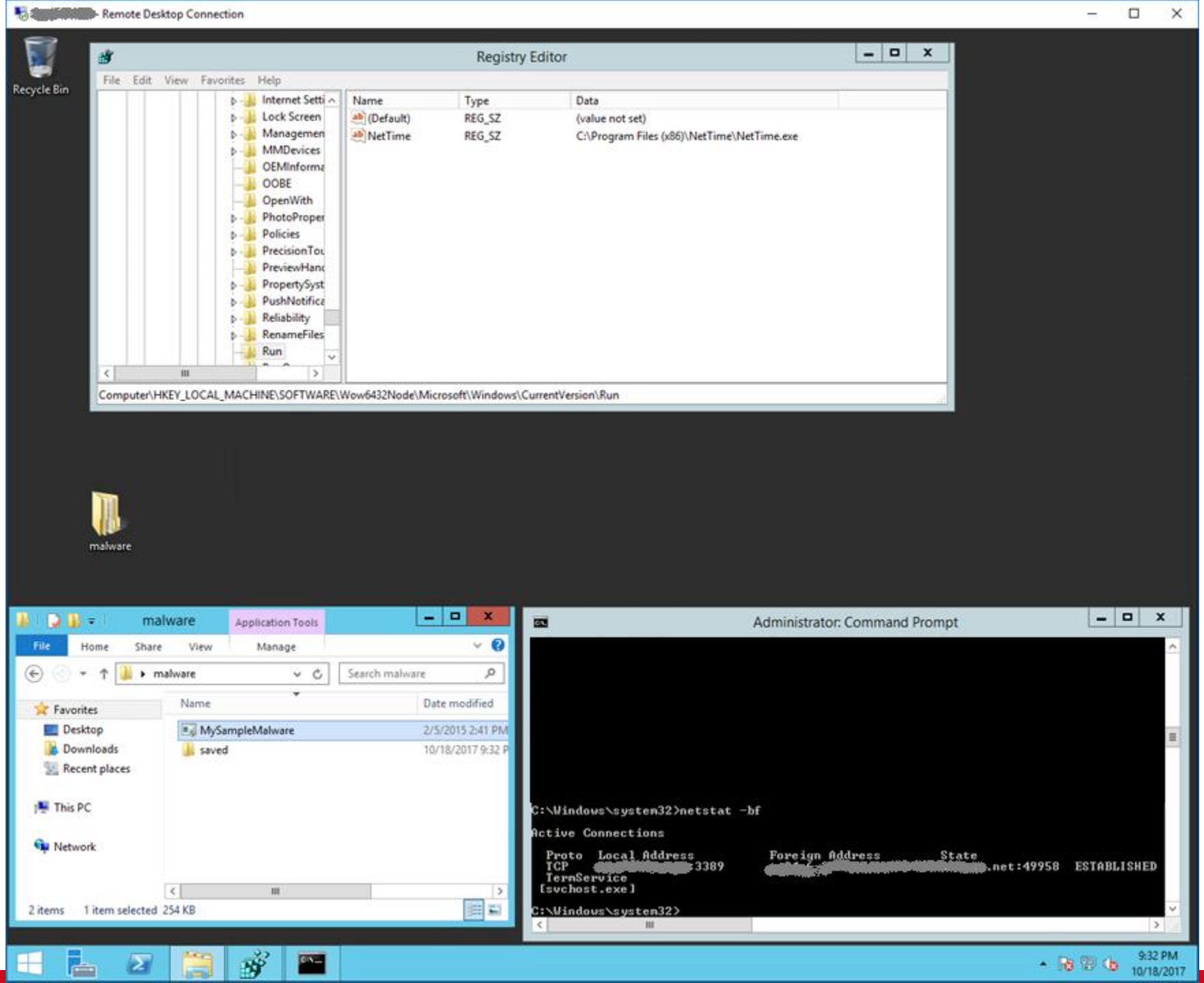


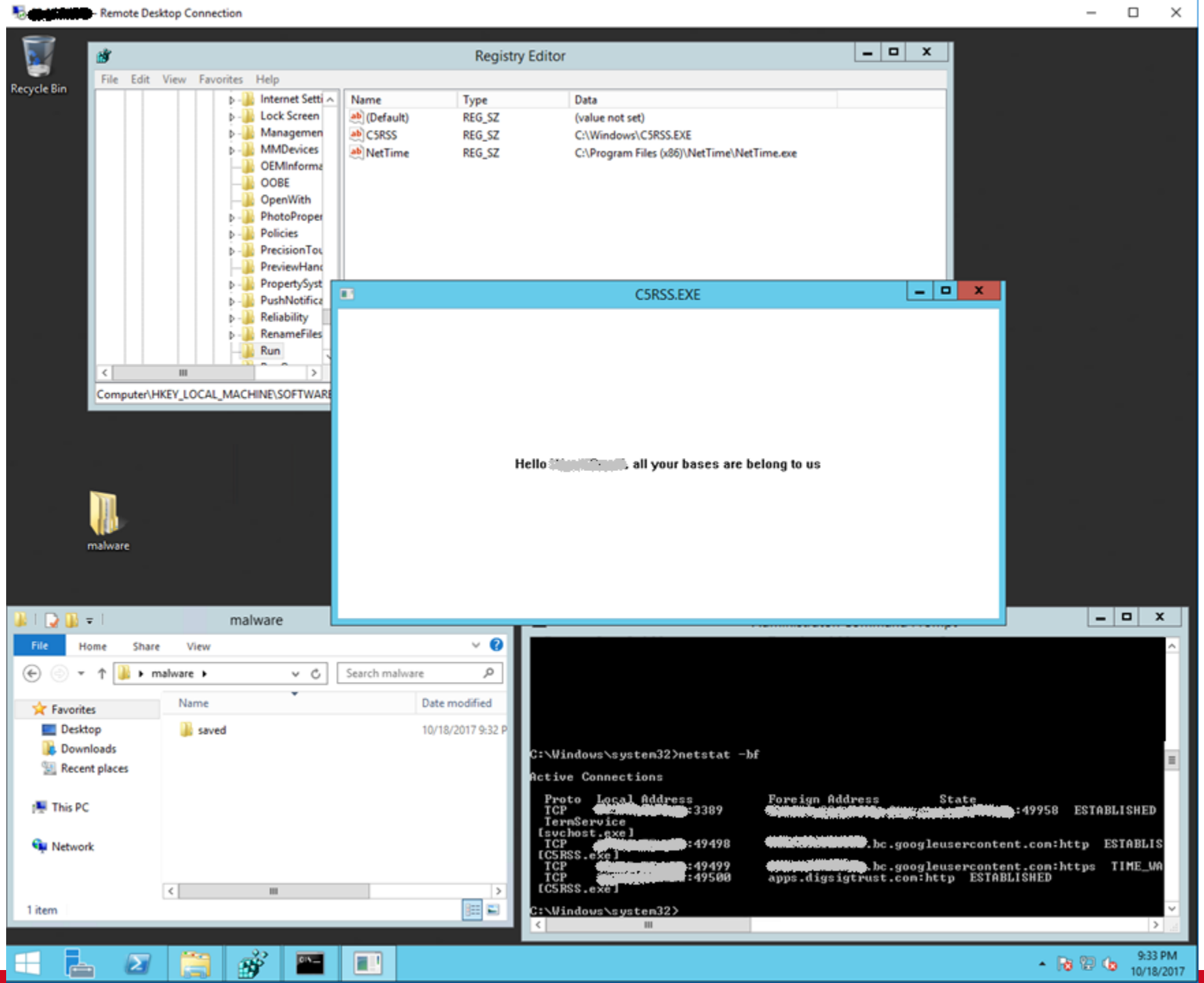
Example Malware with File & Network Indicators

Malware Behaviors in this Example

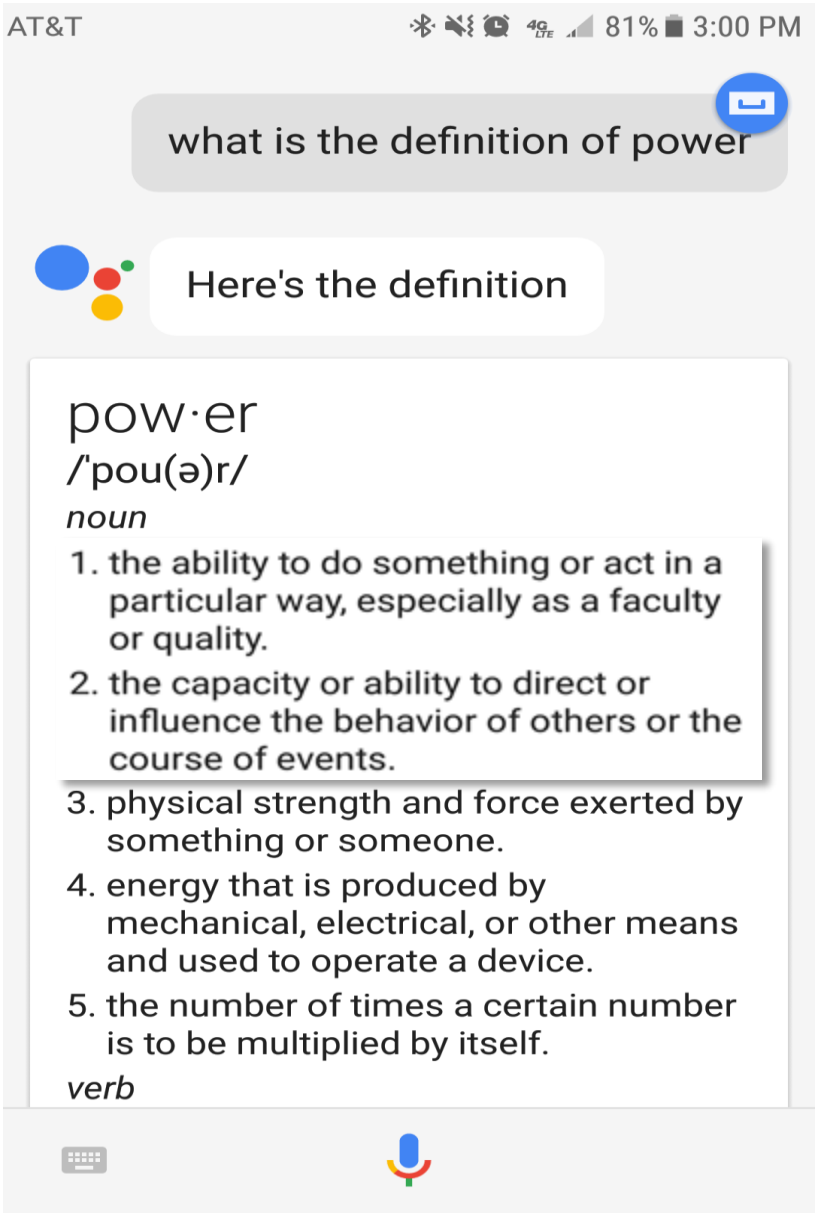
- Small PE file 254kb
- Creates Persistence
- Drops 2nd stage file & executes
- Deletes itself (original dropper)
- Communicates with C2



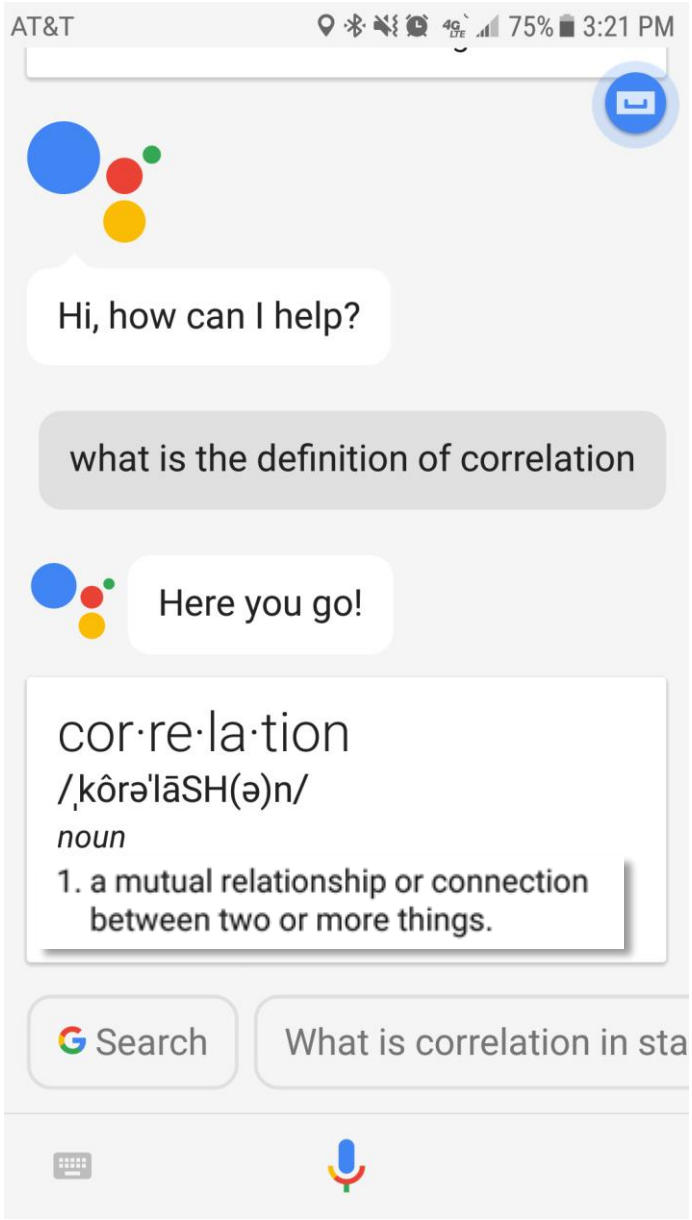

Remote Desktop Connection
Recycle Bin
Registry Editor
File Edit View Favorites Help
Internet Setti
Lock Screen
Managemen
MMDevices
OEMInforma
OOBE
OpenWith
PhotoProper
Policies
PrecisionTou
PreviewHanc
PropertySyst
PushNotifica
Reliability
RenameFiles
Run
Name Type Data
(Default) REG_SZ (value not set)
NetTime REG_SZ C:\Program Files (x86)\NetTime\NetTime.exe
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
malware
malware
Application Tools
File Home Share View Manage
malware
Search malware
Favorites
Desktop
Downloads
Recent places
This PC
Network
Name
Date modified
MySampleMalware 2/5/2015 2:41 PM
saved 10/18/2017 9:32 P
2 items 1 item selected 254 KB
Administrator: Command Prompt
C:\Windows\system32>netstat -bf
Active Connections
Proto Local Address Foreign Address State
TCP [redacted]3389 [redacted].net:49958 ESTABLISHED
TermService
[svchost.exe]
C:\Windows\system32>
9:32 PM
10/18/2017


Remote Desktop Connection
Recycle Bin
Registry Editor
File Edit View Favorites Help
Internet Setti
Lock Screen
Managemen
MMDevices
OEMInforma
OOBE
OpenWith
PhotoProper
Policies
PrecisionTou
PreviewHand
PropertySyst
PushNotifica
Reliability
RenameFiles
Run
Computer\HKEY_LOCAL_MACHINE\SOFTWARE
Name Type Data
(Default) REG_SZ (value not set)
C5RSS REG_SZ C:\Windows\C5RSS.EXE
NetTime REG_SZ C:\Program Files (x86)\NetTime\NetTime.exe
C5RSS.EXE
Hello [redacted], all your bases are belong to us
malware
malware
File Home Share View
malware
Search malware
Favorites
Desktop
Downloads
Recent places
This PC
Network
Name
Date modified
saved
10/18/2017 9:32 P
1 item
C:\Windows\system32>netstat -bf
Active Connections
Proto Local Address Foreign Address State
TCP [redacted]:3389 [redacted]:49958 ESTABLISHED
TermService
[svchost.exe]
TCP [redacted]:49498 [redacted].bc.googleusercontent.com:http ESTABLIS
[C5RSS.exe]
TCP [redacted]:49499 [redacted].bc.googleusercontent.com:https TIME_WA
TCP [redacted]:49500 apps.digsigtrust.com:http ESTABLISHED
[C5RSS.exe]
C:\Windows\system32>
9:33 PM
10/18/2017

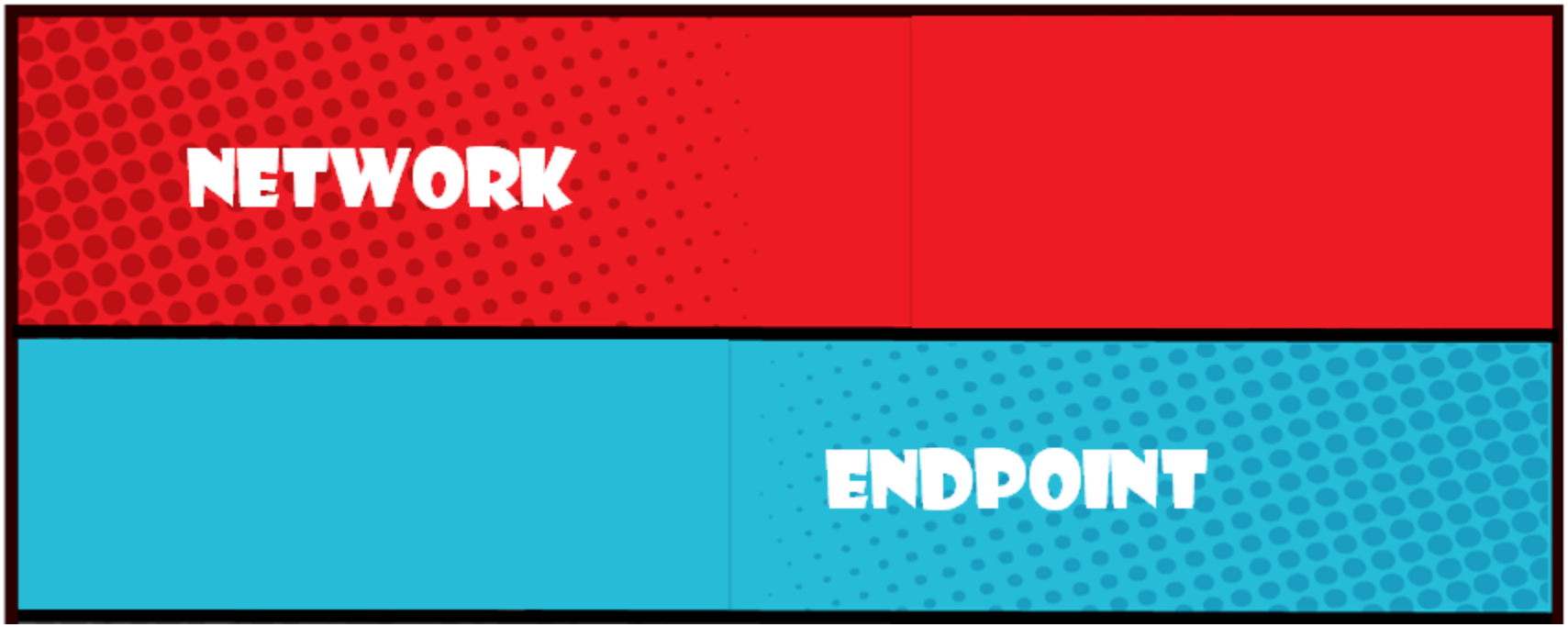
Solution: The Definition of POWER



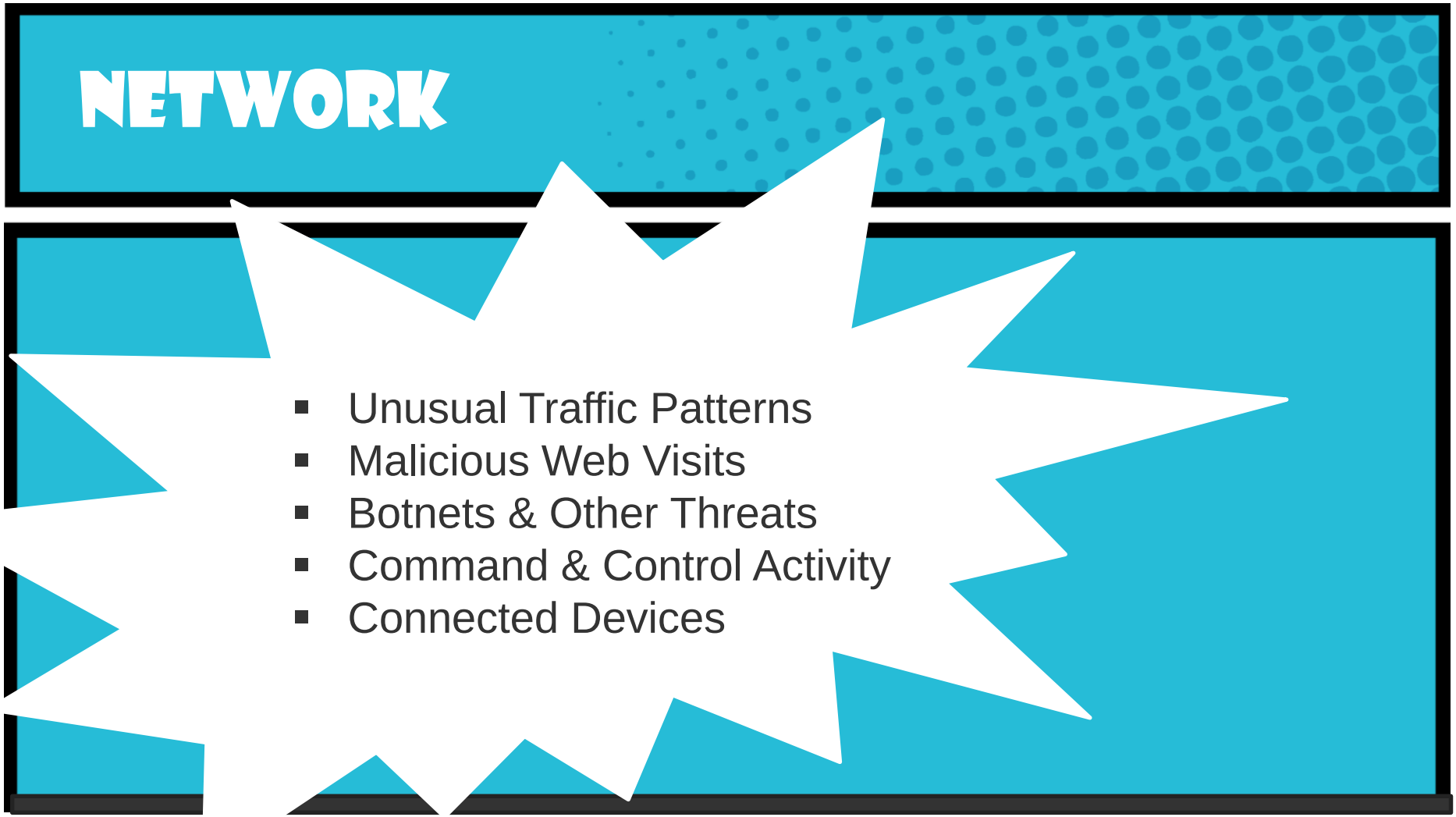
Solution: The Definition of Correlation



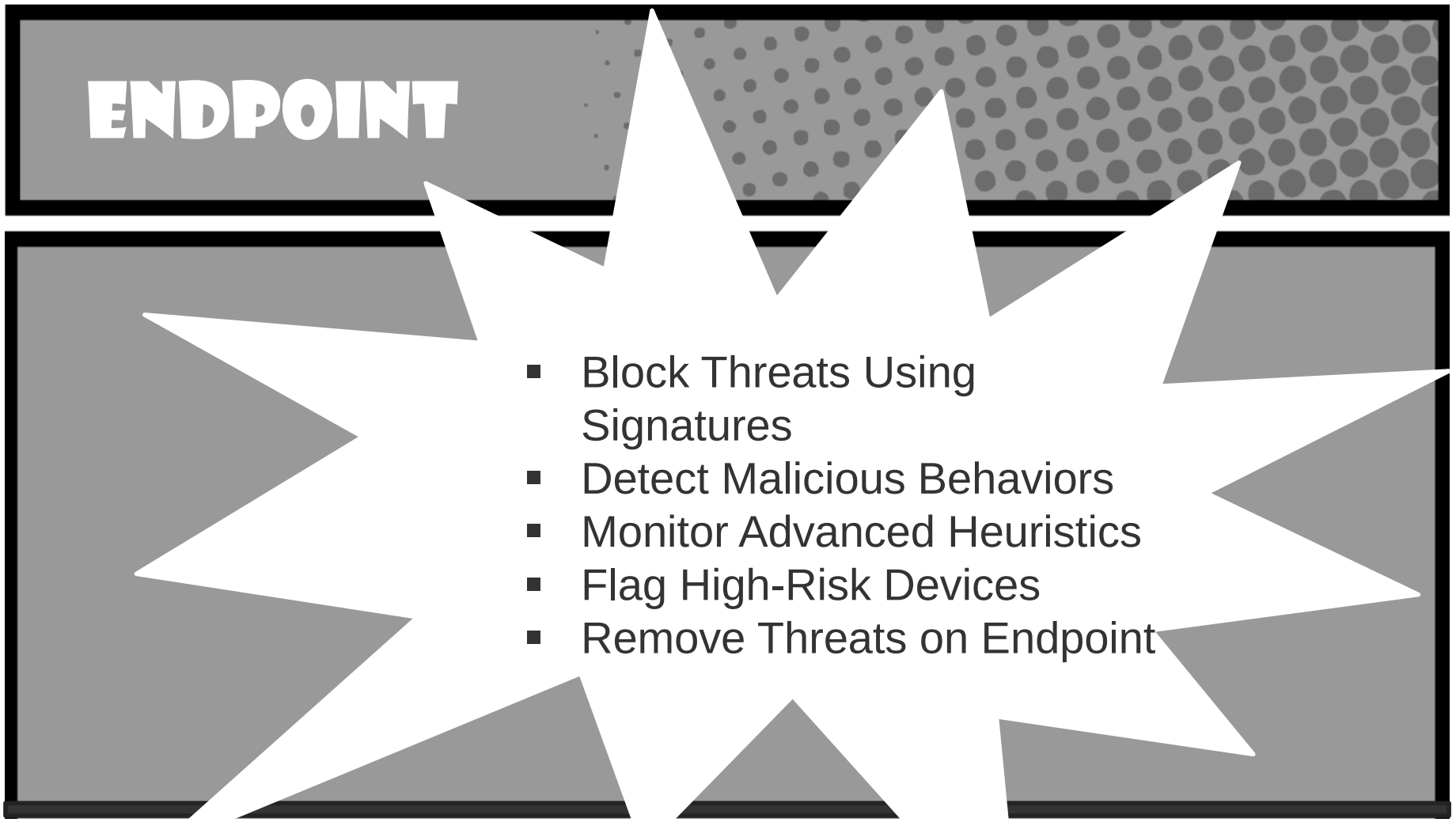
It’s Time to Bring this Information Together



The Network Provides Key Security Information



Endpoints Generate Unique Security Events



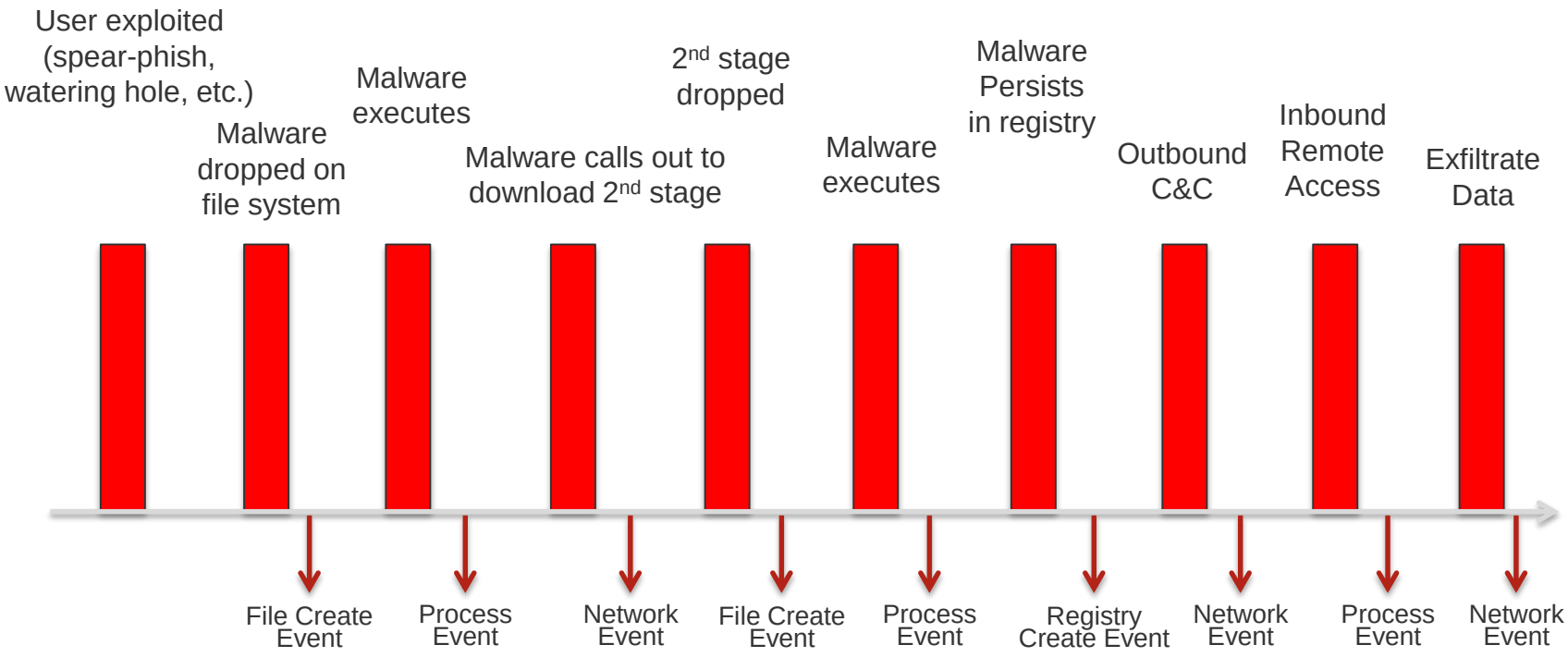
Better Together

"Machine learning, antivirus, intrusion prevention, and enterprise detection and response (EDR) are all examples of technologies that work better together than alone."

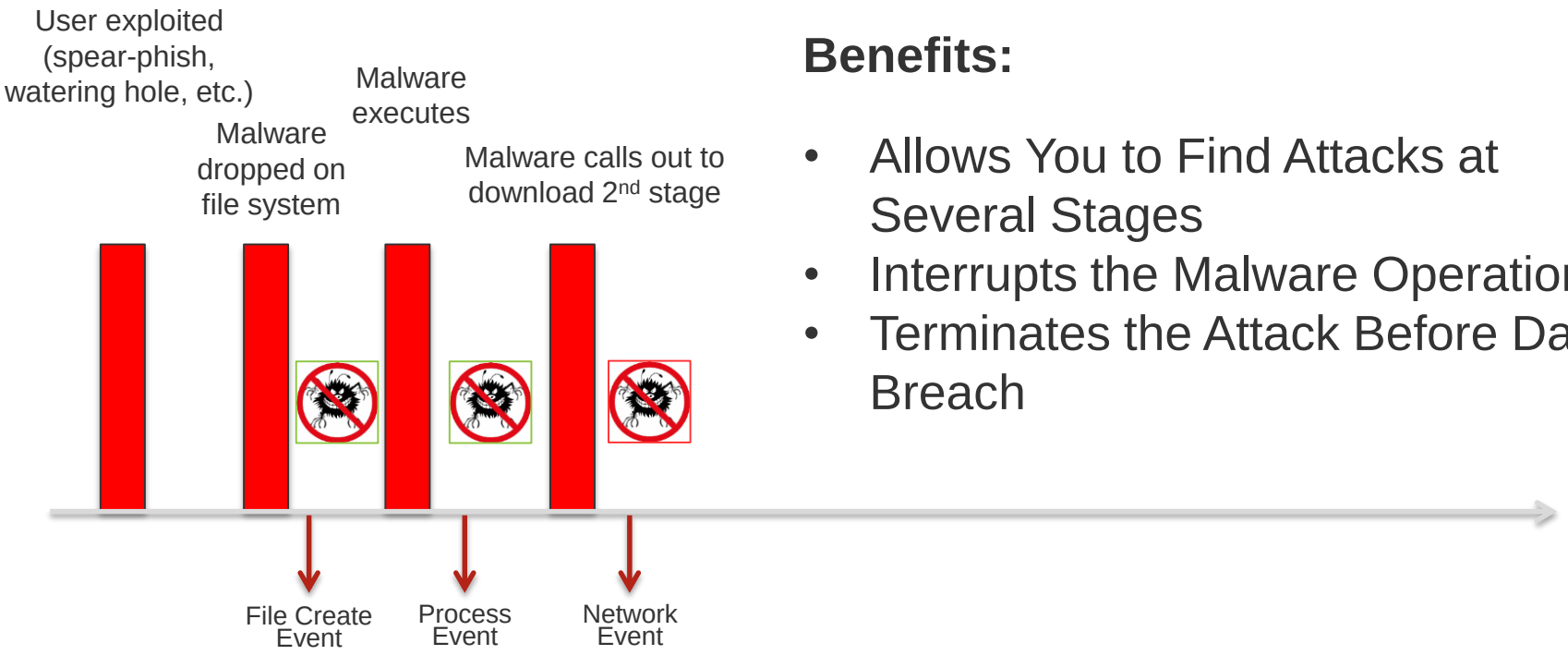
"To make endpoint work, you need a platform…[that] needs to combine the strengths of many different technologies so you account for the weaknesses of those [individual] technologies."

- Kelly Sheridan, *Dark Reading*

Cyber Kill Chain: Endpoint AND Network Events



Cyber Kill Chain: Endpoint AND Network Events
GOAL: BREAK the Kill Chain



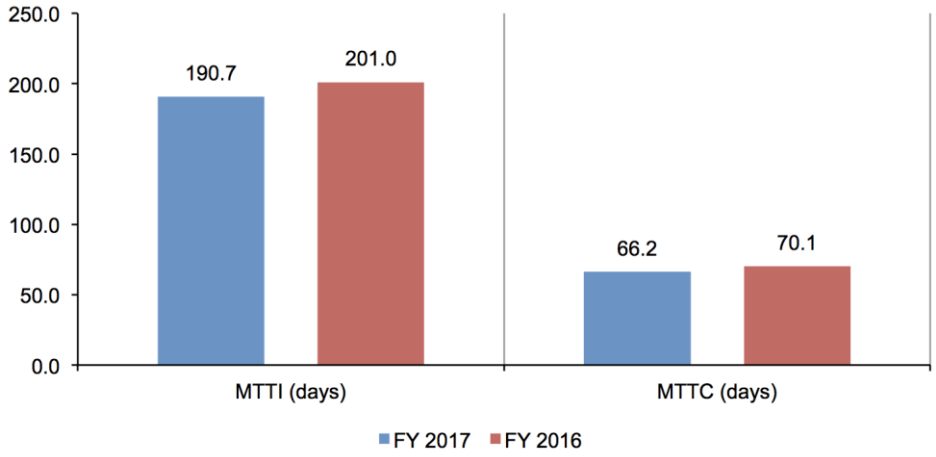
Benefits:

- Allows You to Find Attacks at Several Stages
- Interrupts the Malware Operation
- Terminates the Attack Before Data Breach

With Correlation - You Can Act On Threats Faster

- Correlation Provides Confirmation/Verification of Individual Threats
- Correlation Helps Prioritize (POWER) the Threats That Really Matter
- Correlation Helps Reduce False Positives
- Correlation Dramatically Reduces the Time it Takes to Detect and Respond to an Attack

Figure 21. Days to identify and contain the data breach over the past year



** Ponemon's 2017 Cost of a Data Breach Report*

Summary: Be “Great” Security Practitioners

The vast majority of cyber threats are delivered **via the network**. **Correlating network events and endpoint behaviors** into a single view gives you the insight you need to confidently respond to threats with the appropriate action.


THANK YOU