The Threats Are Changing, So Are We.

October 2019
About Me

• Five years as CIO in private industry
• Thirty years at the European Commission
  – IT management
  – Internal and external audit
  – COO, CRO at the Joint Research Centre (3000 scientists)
  – Founder and Head of CERT-EU 2011-2017
• Consultancy
  – Trusted Strategic Advisor
  – Advisor/Board Member in cybersecurity startups
• **Internet of Everything**
  – Increased dependency
  – Everything connected

• **Vulnerability Expanding**
  – Inherently fragile
  – Frequently misconfigured, often unpatchable

• **Agile Adversaries**
  – Determined
  – Industrialized
  – Stealthy
Agenda

• Threats
• Prepare
• Adapt
• Contribute
Threats

- Proliferation of Adversaries
- More Impact
- Proliferation of Techniques
Adversaries: Proliferation

• State-sponsored actors: more of the same and some more
  – Established players not afraid of being called out
  – New kids on the block copycatting established players

• Criminal groups
  – Streamlining operations
  – Specialization
  – Copycatting state-sponsored actors

• More dramatic (potential) impact
• Initial infection using legitimate software
• Spreading using a leaked NSA tool
• Destructive intent: no way to decrypt
• “Targeted”
• Massive collateral damage
10% of all computers in UA destroyed
3 billion € collateral damage
Maersk/APM

• 17 container terminals disrupted for weeks
• Loading and unloading impossible
• Truck chaos
• Reinstallation of 40,000 computers
• Saved by power cut in Ghana...

• More than 300mio€ financial impact
Asco closure after cyber-attack to last another week

Saturday, 22 June 2019

Warning:
Cyber Attack Against the Hydro Network.

Please do not connect any devices to the Hydro network. Do not turn on any device connected to the Hydro Network.

Please disconnect any device (Phone/Tablet etc.) from the Hydro Network.

Await more updates.

-Security

Eurofins Scientific: Forensic services firm paid ransom after cyber-attack

By Danny Shaw
Home affairs correspondent

© 5 July 2019
Intermediate Questions

- Has your company been facing this type of problem?
- Does your company have a cyber insurance in place?
- Would your company pay ransom?
- Is this a Board issue in your company?
- How confident are you in your organisation’s backup?
[~]$ shred
Techniques: Proliferation

- Leaked superweapons
- Blending in
- Broader surface
Leakage of Superweapons

- Espionage & law enforcement tools
  - Three letter agencies
  - Hacking Team
  - NSO

- Penetration and vulnerability testing tools
  - Mimikatz
  - Cobalt Strike
  - Metasploit
  - Bloodhound
Blending In

• Mails appearing as originating from a trusted origin
  - Typo squatting
  - Spoofed
  - Compromised
• Credible content
• Stealthy infection and lateral movements
  - Using legitimate credentials, replicating legitimate behavior
  - Abusing legitimate C&C infrastructure
  - Using legitimate tools (PowerShell, WMI, RDP)
  - Living off the land / file-less
Powershell
Sehr geehrte Damen und Herren,

mit großem Interesse bin ich im Internet auf Ihre ausgesuchte Position aufmerksam geworden. Ich möchte mich gerne einer neuen beruflichen Herausforderung stellen.

Mit mir gewinnt Ihr Unternehmen einen leistungsbereiten Mitarbeiter. Ich widme mich meinen neuen Aufgaben und Herausforderungen stets mit großer Motivation und vollem Einsatz.


Mit freundlichen Grüßen,

Lena Kretschmer

Anlagen: Arbeitszeugnisse, Lebenslauf, Bewerbungsfoto
Broader Surface

- CMS/wiki/webservers
- Cloud, VMs
- Routers, switches
- Control systems, IOT
- Processors, firmware
- Credentials
Your RDP Open?

Sophos - RDP Exposed
Corporate IoT – a path to intrusion

Security Research & Defense / By MSRC Team / August 5, 2019 / Black Hat, IoT, MSTIC, STRONTIUM, Supply chain, Threat intelligence
Cisco Blogs

Cisco Blog > Security

Security

New Forensic Investigation Procedures for First Responder Guides

Lou Ronnau
August 30, 2019 - 1 Comment
Your Credentials Open?

C:\Users\John\Desktop>laZagne.exe browsers

The LaZagne Project

! BANG BANG !

-------------------- Internet Explorer passwords --------------------

Password found ???
Username: zapata@yahoo.com
Password: Zapata_Uive!
Site: https://www.facebook.com/

-------------------- Firefox passwords --------------------

Password found ???
Website: https://accounts.google.com
Username: zapata@gmail.com
Password: LaLuchaSigue!

Password found ???
Website: https://www.facebook.com
Username: che.guevara@gmail.com
Password: hasta_siempre!

[+] 3 passwords have been found.
For more information launch it again with the -v option
elapsed time = 0,1200000,23978
Agenda

- Threats

- *Prepare*

- Adapt

- Contribute
Prepare

• Prevent, detect, respond is not enough
• Gain visibility → ZEEK 😊
• Offline backups of your crown jewels
  ➢ AD, configs, gold images, clients, orders…
• Manual fall backs / resilience
• Incident response plan - BCP
• Insurance / Legal support
Typical APT

- Find a weak entry point
- Scan the internal infrastructure
- Escalate privileges
- Move laterally
- Obtain keys to the Kingdom(s)
- Establish persistence (golden ticket, routers, bios, legit credentials)
- Detonate
- Return when you are kicked out
Agenda

• Threats

• Prepare

• Adapt

• Contribute
Adapt

- Prevent, detect, respond are not static
- APT, the new normal
- Don’t contain too quickly, **assume lateral movement**
- Internal reconnaissance can be noisy -> ZEEK 😊

- Move from Respond into Detect

- Track your adversaries and adapt your approaches
Gap

 Sophistication

 Time

 Dynamic

 Adversary

 Static
## Gaps In Prevention/Detection

<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>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
<tr>
<td>Drive-In Compromise</td>
<td>Appscript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Command And Control</td>
<td>Exfiltration</td>
<td>Impact</td>
</tr>
</tbody>
</table>
Analytics Instead of Indicators

Indicators*

- Detect known bad
- Artifact-driven
- Fewer false positives
- More atomic
- Higher quantity

*good, fresh, indicators are useful too

Analytics

- Detect suspicious events
- Behavior-driven
- More false positives
- Broader
- Lower quantity
- Longer lifetime
TTPs are more stable

Incident 1
Incident 2
Incident 3

Unique TTPs
Yara
Snort
Zeek Scripts
Sigma
Analytics in SIGMA

Sigma Format
Generic Signature Description

Sigma Converter
Applies Predefined and Custom Field Mapping

https://github.com/Neo23x0/sigma
Sample SIGMA Rule

title: Renamed PowerShell
status: experimental
description: Detects the execution of a renamed PowerShell often used by attackers or malware
references:
- https://twitter.com/christophetd/status/1164506034720952320
author: Florian Roth
date: 2019/08/22
tags:
- car.2013-05-009
logsource:
  product: windows
  service: sysmon
detection:
  selection:
    Description: Windows PowerShell
    Company: Microsoft Corporation
  filter:
    Image: '*\powershell.exe'
condition: selection and not filter
falsepositives:
- Unknown
level: critical
SIGMA Rules

Neo23x0 / sigma

Branch: master  sigma / rules / apt /

Latest commit 7bfe5f on 14 Apr

- Create apt_oceanlotus_registry.yml

- apt_apt29_thinktanks.yml  add tags to apt29 thinktanks rule  3 months ago
- apt_apt29_tor.yml  fix tags on apt29 tor rule  3 months ago
- apt_babyshark.yml  add tags to apt babyshark rule  3 months ago
- apt_bear_activity_gtr19.yml  fix and add tags to apt bear activity gtr19 rule  3 months ago
- apt_carbonpaper_turla.yml  fix tags in apt carbonpaper turla rule  3 months ago
- apt_chafer_mar18.yml  Converted to use the new process_creation data source  3 months ago
- apt_cloudhopper.yml  updated to use process_creation  4 months ago
- apt_dragonfly.yml  updated to use process_creation  4 months ago
SIGMA Tools

SIGMA Editor
https://github.com/socprime/SigmaUI

Atomic Threat Coverage
https://github.com/krakow2600/atomic-threat-coverage
Zeek Packages

<table>
<thead>
<tr>
<th>Commit</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oxxon</td>
<td>Rename a few packages from Bro to Zeek</td>
<td>9 months ago</td>
</tr>
<tr>
<td>activecm</td>
<td>Add Bro MongoDB logging writer package</td>
<td>2 years ago</td>
</tr>
<tr>
<td>anthonykasza</td>
<td>add: anthonykasza index</td>
<td>9 months ago</td>
</tr>
<tr>
<td>apache</td>
<td>Add metron-bro-plugin-kafka package</td>
<td>2 years ago</td>
</tr>
<tr>
<td>bricata</td>
<td>Added bricata</td>
<td>last year</td>
</tr>
<tr>
<td>bro</td>
<td>Added the official Bro NETMAP plugin</td>
<td>2 years ago</td>
</tr>
<tr>
<td>corelight</td>
<td>Add the Corelight QUIC protocol analyzer/detector</td>
<td>last year</td>
</tr>
<tr>
<td>cybera</td>
<td>Adding Cybera Sniffpass module</td>
<td>last month</td>
</tr>
<tr>
<td>dopheide</td>
<td>Merge branch ‘master’ of <a href="https://github.com/dopheide/packages">https://github.com/dopheide/packages</a></td>
<td>2 months ago</td>
</tr>
<tr>
<td>dovehawk</td>
<td>added dovehawk anonymized flow collector</td>
<td>17 days ago</td>
</tr>
</tbody>
</table>
Agenda

• Threats
• Prepare
• Adapt
• **Contribute**
• Prevent, detect, respond are can inspire others
• **Provide feedback and contribute analytics** to the Community
• Crowdsourcing behavioral detection libraries
• Sharing TTPs/SIGMA/ZEEK rules is easier than sharing IOCs
• It’s also more useful
  – More context
  – More stable in time

• **Defense: Proliferation**
EU ATT&CK User Community

- Mailing list -> opt in ? -> email to info@circl.lu
- User conference in Brussels 18-19 May 2020

Workshop - EU ATT&CK Community

Next workshop - event for EU ATT&CK Community
Conclusion

• The Threats Are Changing

• And So Are We:
  – Preparing
  – Adapting
  – Contributing
Don’t Hide The Risk, Manage It

www.FreddyDezeure.eu