Responding to Cyber Attacks

On your Mark, Get Set, Go!

September 23rd 2021, Compass Beertalk, cyrill.brunschwiler@compass-security.com

Who

cyrill.brunschwiler@compass-security.com

Nomen est Omen

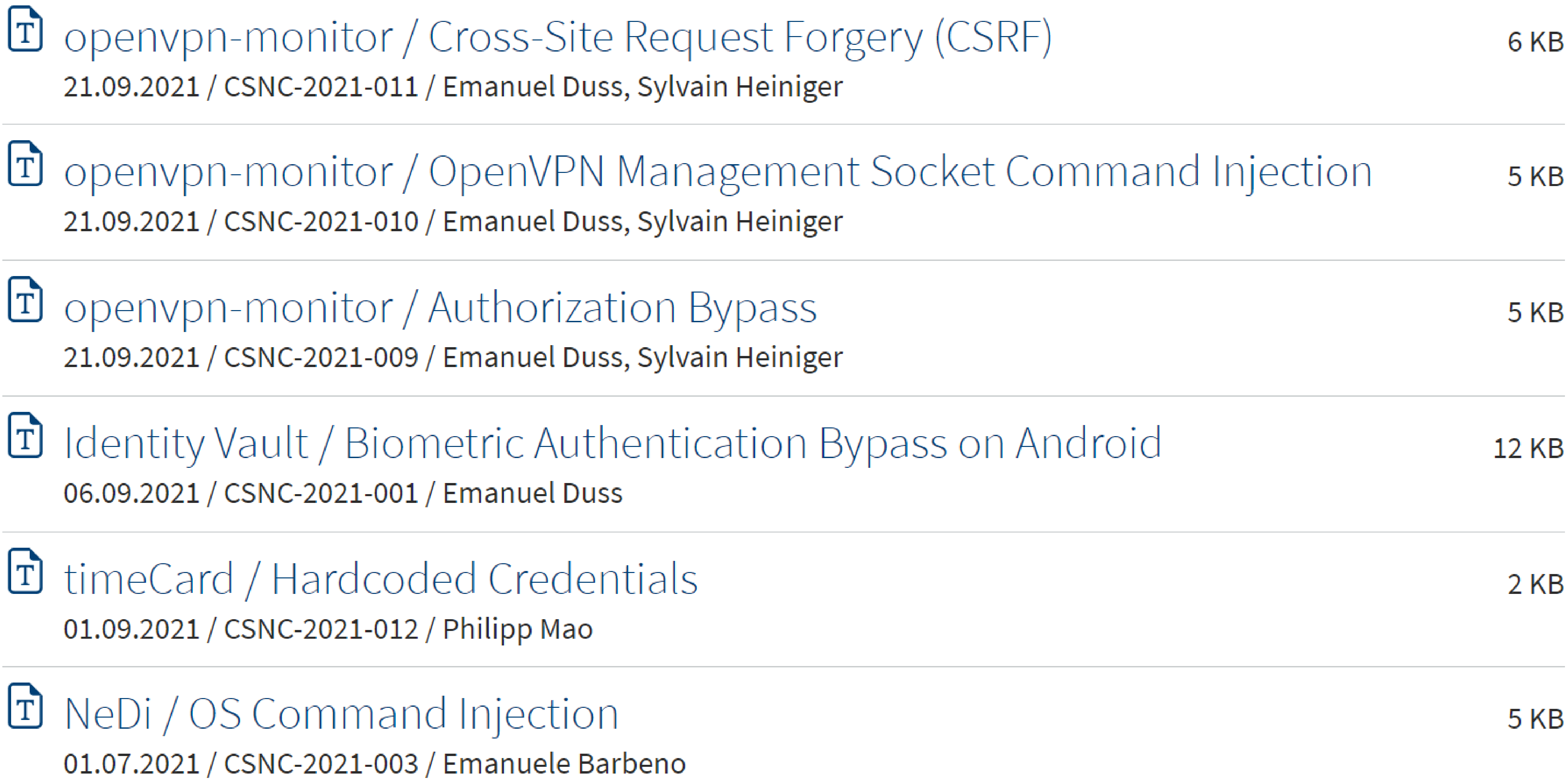
Cyrill **Br**unschwiler

Attack's

Responding to Cyber Attacks Agenda

- Understanding the Attacker
- Response Approaches and Tools
- Recommendations

https://www.compass-security.com/en/research/advisories



openvpn-monitor / Cross-Site Request Forgery (CSRF) 6 KB
21.09.2021 / CSNC-2021-011 / Emanuel Duss, Sylvain Heiniger

openvpn-monitor / OpenVPN Management Socket Command Injection 5 KB
21.09.2021 / CSNC-2021-010 / Emanuel Duss, Sylvain Heiniger

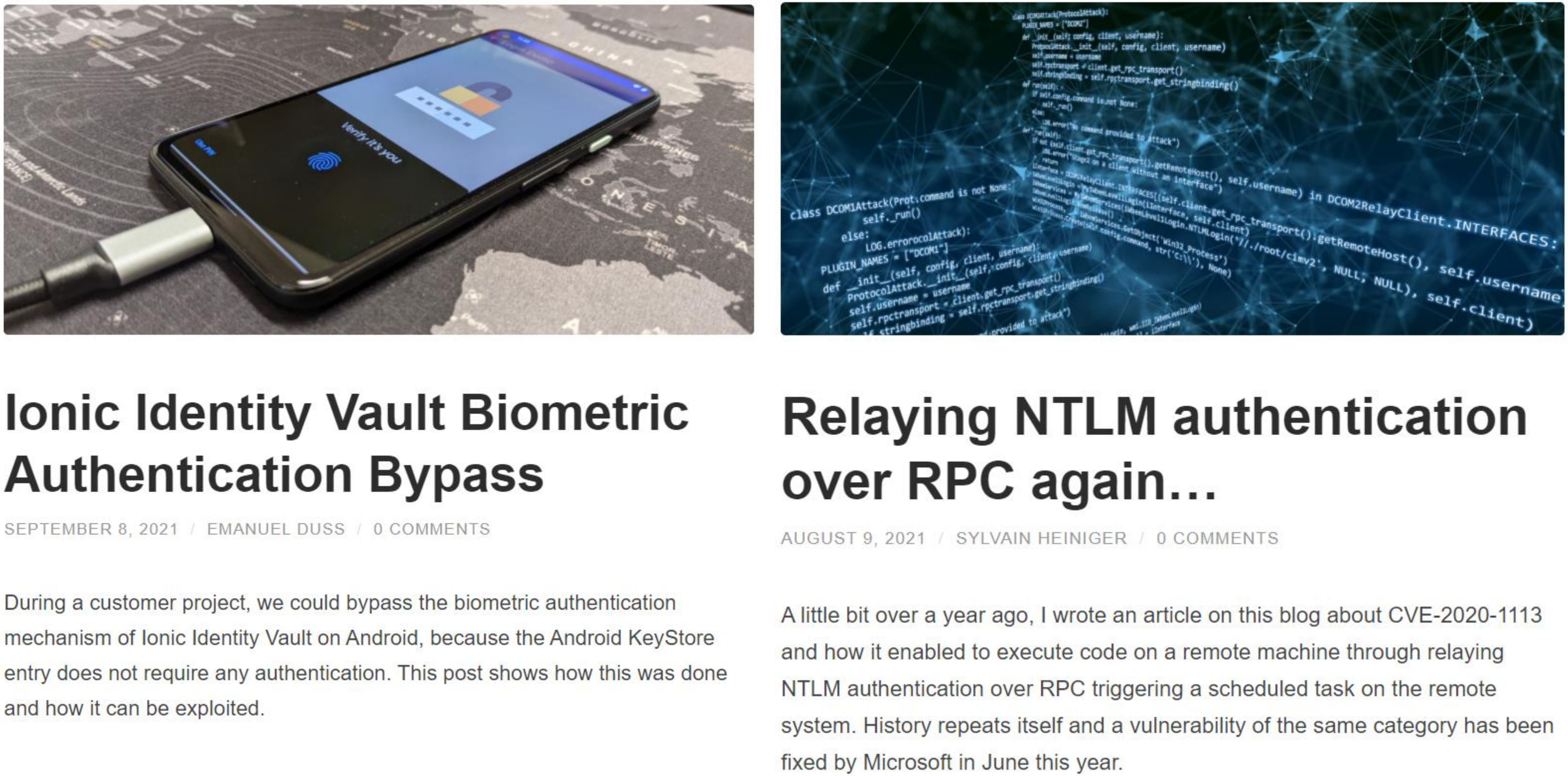
openvpn-monitor / Authorization Bypass 5 KB
21.09.2021 / CSNC-2021-009 / Emanuel Duss, Sylvain Heiniger

Identity Vault / Biometric Authentication Bypass on Android 12 KB
06.09.2021 / CSNC-2021-001 / Emanuel Duss

timeCard / Hardcoded Credentials 2 KB
01.09.2021 / CSNC-2021-012 / Philipp Mao

NeDi / OS Command Injection 5 KB
01.07.2021 / CSNC-2021-003 / Emanuele Barbeno

https://blog.compass-security.com/



Ionic Identity Vault Biometric Authentication Bypass

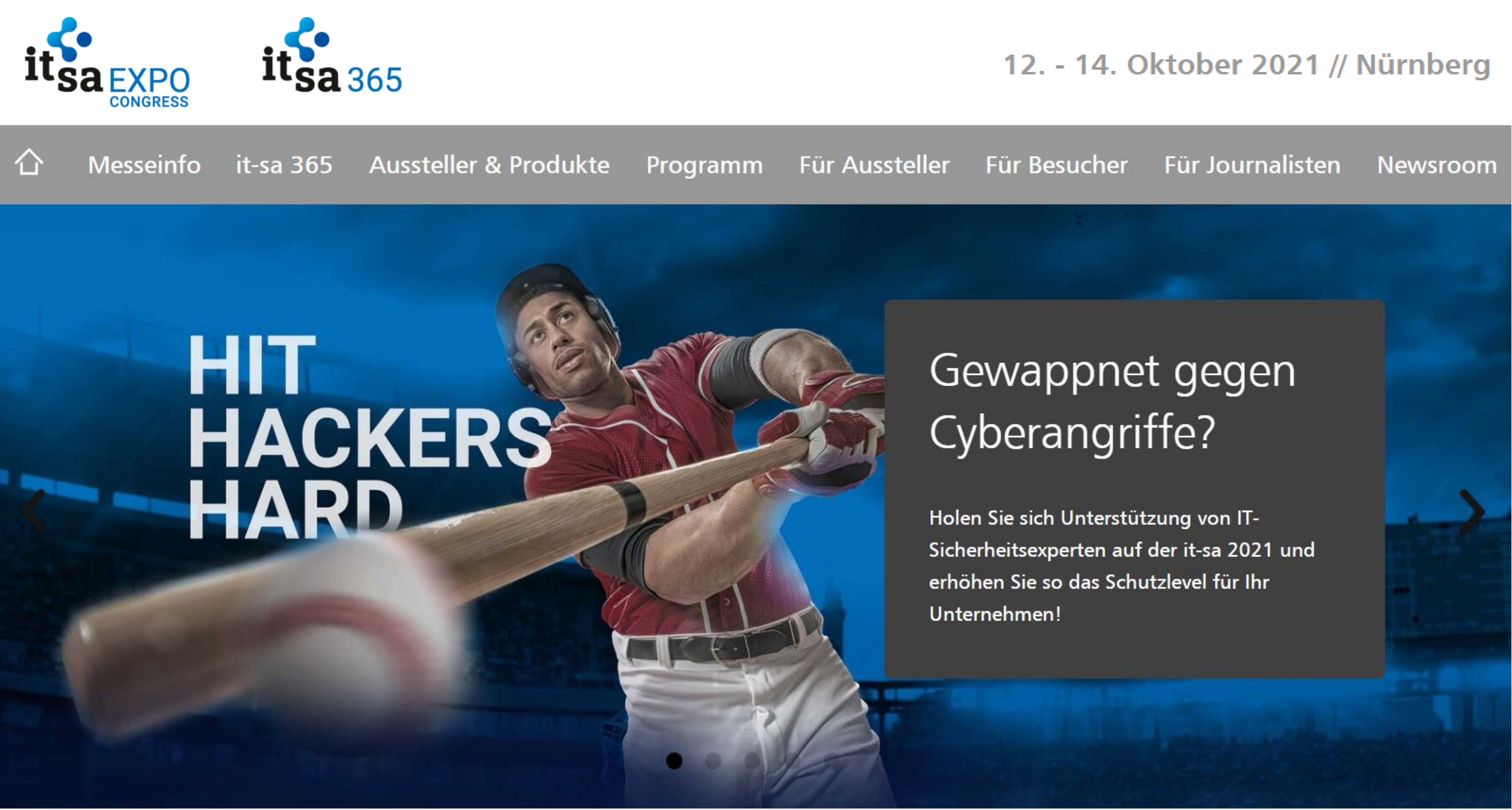
SEPTEMBER 8, 2021 / EMANUEL DUSS / 0 COMMENTS

During a customer project, we could bypass the biometric authentication mechanism of Ionic Identity Vault on Android, because the Android KeyStore entry does not require any authentication. This post shows how this was done and how it can be exploited.

Relaying NTLM authentication over RPC again…

AUGUST 9, 2021 / SYLVAIN HEINIGER / 0 COMMENTS

A little bit over a year ago, I wrote an article on this blog about CVE-2020-1113 and how it enabled to execute code on a remote machine through relaying NTLM authentication over RPC triggering a scheduled task on the remote system. History repeats itself and a vulnerability of the same category has been fixed by Microsoft in June this year.



12. - 14. Oktober 2021 // Nürnberg

Gewappnet gegen Cyberangriffe?

Holen Sie sich Unterstützung von IT-Sicherheitsexperten auf der it-sa 2021 und erhöhen Sie so das Schutzlevel für Ihr Unternehmen!

KURSAAL BERN, SWITZERLAND

12TH OCTOBER 2021

SWISS CYBER STORM 2021

«Securing the Supply Chain»

TICKET VOUCHER CODE 15%
COMPASS-SCS2021-ZZC84

Internal Network and System Security Training

3. und 4. November 2021 in Bern

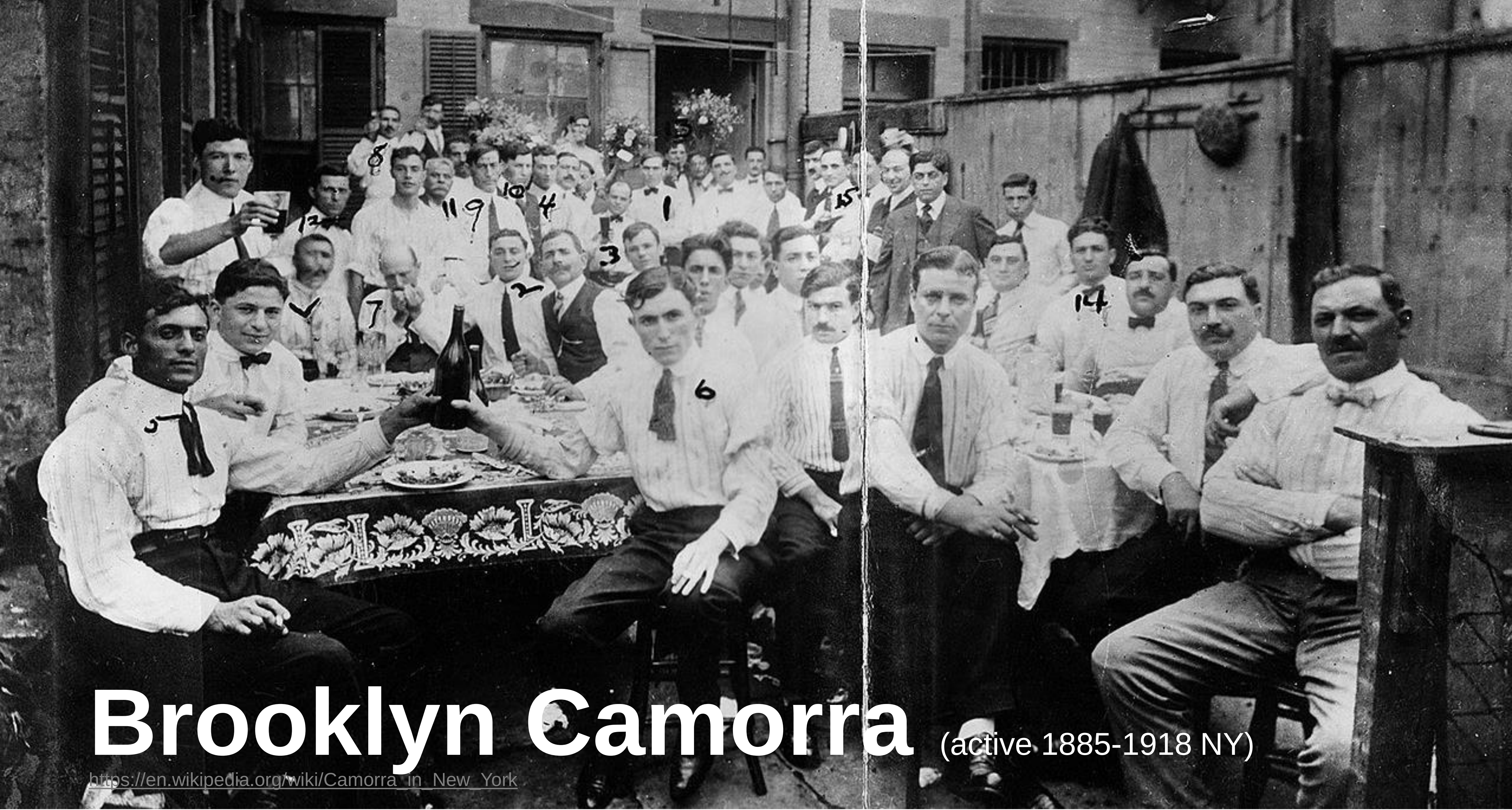
- Info Gathering (Google, whois, Subdomain Enum, Cert. Transparency, DNS)
- Network Discovery mit nmap (Host- und Service Discovery)
- Network Sniffing (tcpdump, Wireshark)
- Vulnerability Scanning (Nessus)
- Exploitation (Shells, Metasploit, ExploitDB)
- Privilege Escalation unter Windows und Linux (PowerSploit, LinEnum, Mimikatz)
- Lateral Movement (Pass the Hash, Responder, NTLM Relay)
- Active Directory Security (BloodHound, PingCastle)
- Command and Control Frameworks

Let’s Respond to Ransomware …

https://en.wikipedia.org/wiki/Wheel_clamp#/media/File:Wheel_clamps_Texas.jpg

Cyber Crime Business Models

- Sell stolen goods
- Commit insider crime
- Extortion



Brooklyn Camorra (active 1885-1918 NY)

https://en.wikipedia.org/wiki/Camorra_in_New_York

DEMO

You became victim of the GOLDENEYE RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   [redacted]

3. Enter your personal decryption code there:

   [redacted]

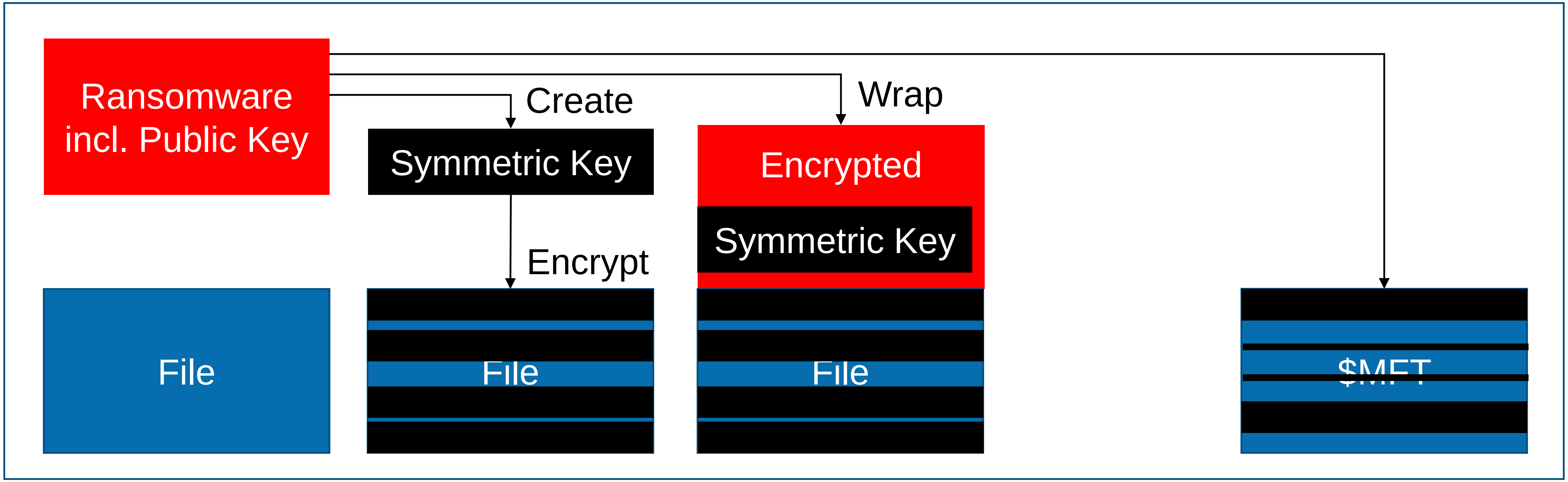
If you already purchased your key, please enter it below.

Applied Crypto in Serious Ransomware

Hybrid Cryptography

1. Create Public/Private Key-Pair (Private Key remains with Creator)
2. Create Symmetric Key
3. Encrypt Symmetric Key using Public Key

Infected Machine



What else? (feat. Nespresso)

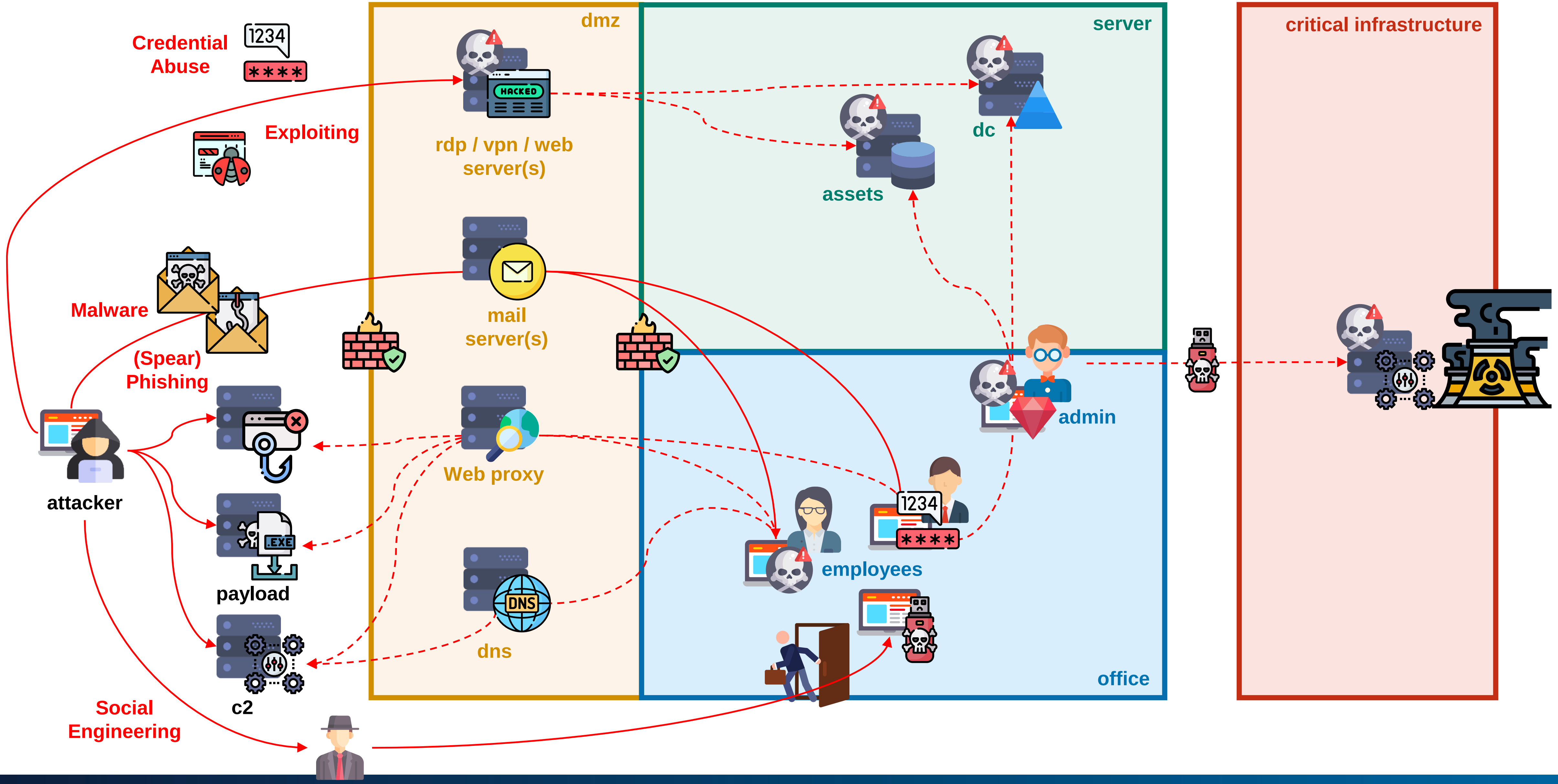
Common Breaches

Not every breach is as super-genius-advanced as the media thinks.

Usually, companies fall for simple things

- Malspam
- Bad Passwords
- 2FA Missing
- Appliance or Software Vulnerability (Patches Missing)

Typical Schemes



Breach Evolvement

Recent breaches involve new techniques or approaches and show threat actor’s evolution

- Manually Escalate Privileges and Kill AV
- Exfiltrate Data to S3 Bucket, Google Drive or MEGA
- Human Operated Ransomware to Target Specific Data
- Send Over and Domain Join a Virtual Machine to Run Crypto Software
- Stop Services and Systems
- Flush Entire File Share
- Delete All Virtual Machines

What’s Up Technically?

MITRE ATT&CK Framework

MITRE ATT&CK Framework

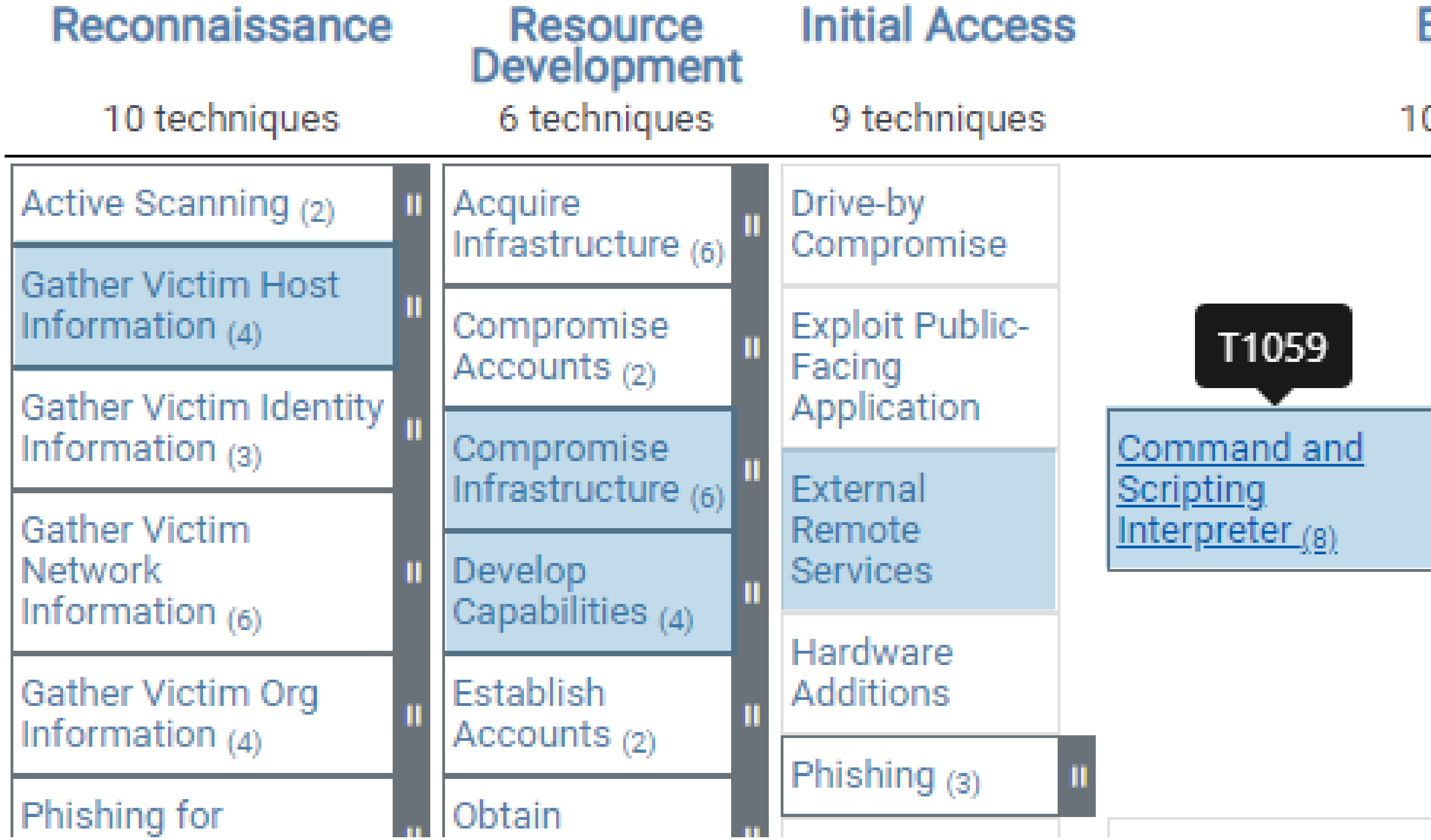
Purpose and Application

Defenders

- Known Bad
- Coverage of Monitoring
- Effectiveness of Monitoring

Attackers

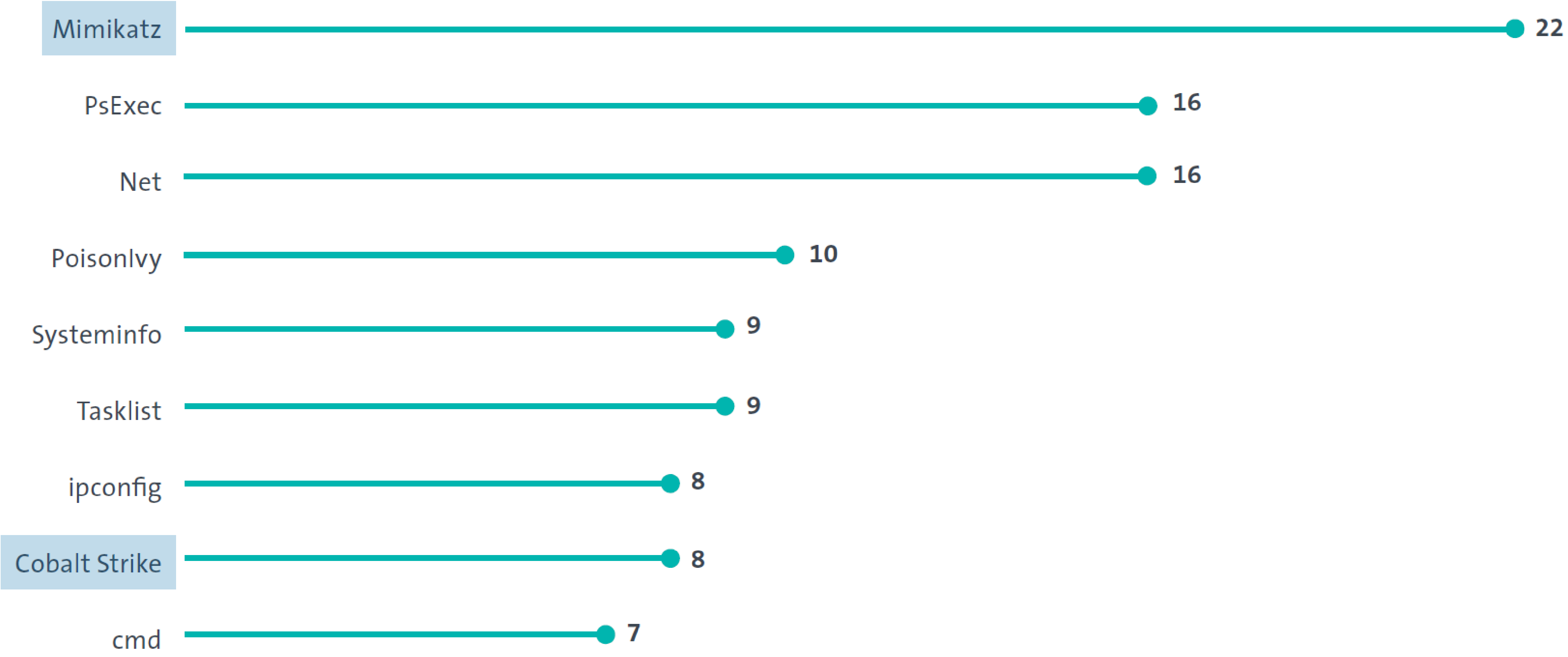
- Ideas on Alternatives
- Avoid getting Trapped
- Simulation (Red Teaming)



Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	E 10
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	T1059
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Command and Scripting Interpreter (8)
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	
Phishing for	Obtain		

MITRE ATT&CK Framework

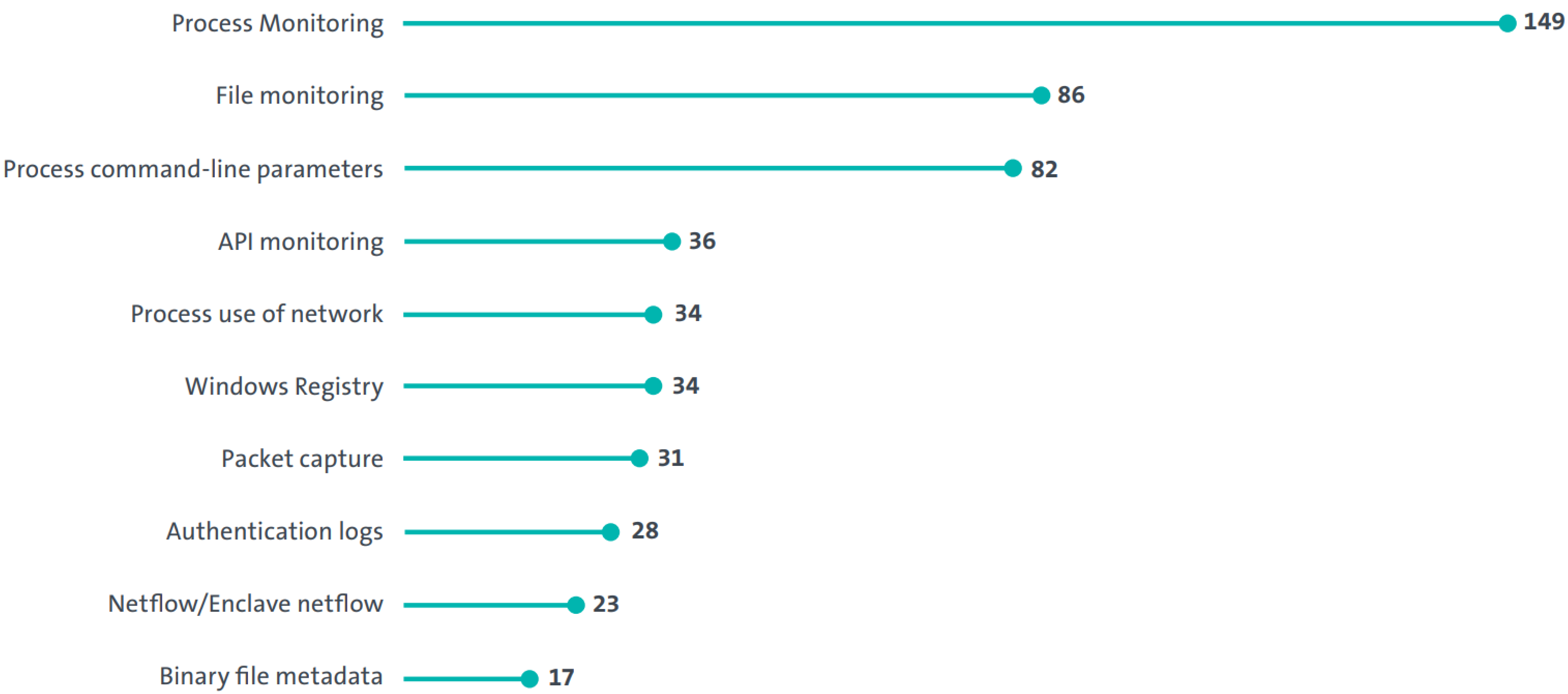
Most used Software



Quelle: http://documents.swisscom.com/product/filestore/lib/7657c513-a231-4725-9d04-eeb343c164e1/Swisscom_Security_Report_2019_EN.pdf

MITRE ATT&CK Framework

Detection Types



Quelle: http://documents.swisscom.com/product/filestore/lib/7657c513-a231-4725-9d04-eeb343c164e1/Swisscom_Security_Report_2019_EN.pdf

Ransomware vs Persistent Threats

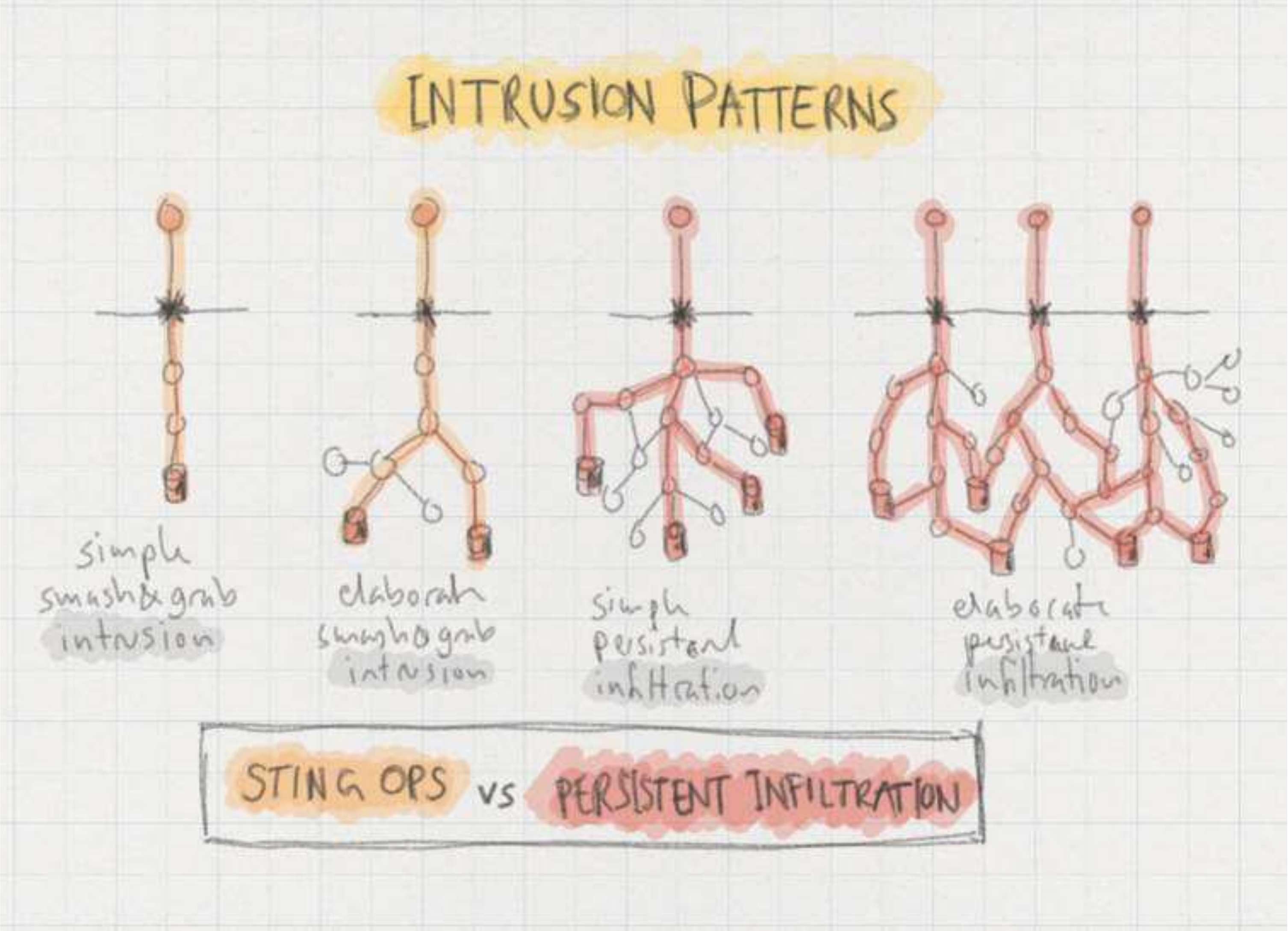
Responding Adequately

Ransomware vs Persistent Threats

Intrusion Patterns

Sting Operation
Also called “smash and grab”. A direct attack to get a specific piece of information.

Persistent Infiltration
A long running campaign against you, where your adversary will gain and sustain unauthorized access to your infrastructure for a long period of time.


INTRUSION PATTERNS
simple smash & grab intrusion
elaborate smash & grab intrusion
simple persistent infiltration
elaborate persistent infiltration
STING OPS vs PERSISTENT INFILTRATION

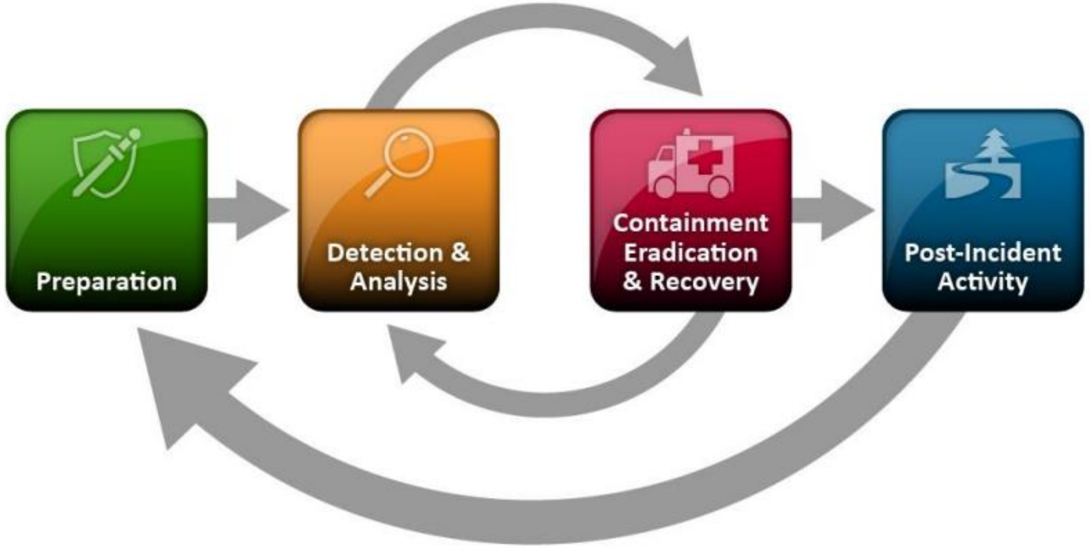
[Quelle]: https://www.slideshare.net/FrodeHommedal/taking-the-attacker-eviction-red-pill
https://www.youtube.com/watch?time_continue=3&v=WAvO0Y0nOws

Bad boys, whatcha gonna do when we come for you? (feat. Burp is not Beef)

Industry Standard Processes

NIST

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident Activity



Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

SANS

1. **P**reparation
2. **I**dentification and Scoping
3. **C**ontainment / Intelligence Development
4. **E**radication / Remediation
5. **R**ecovery
6. **L**essons Learned / Threat Intel Consumption

Source: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NIST Incident Response Process

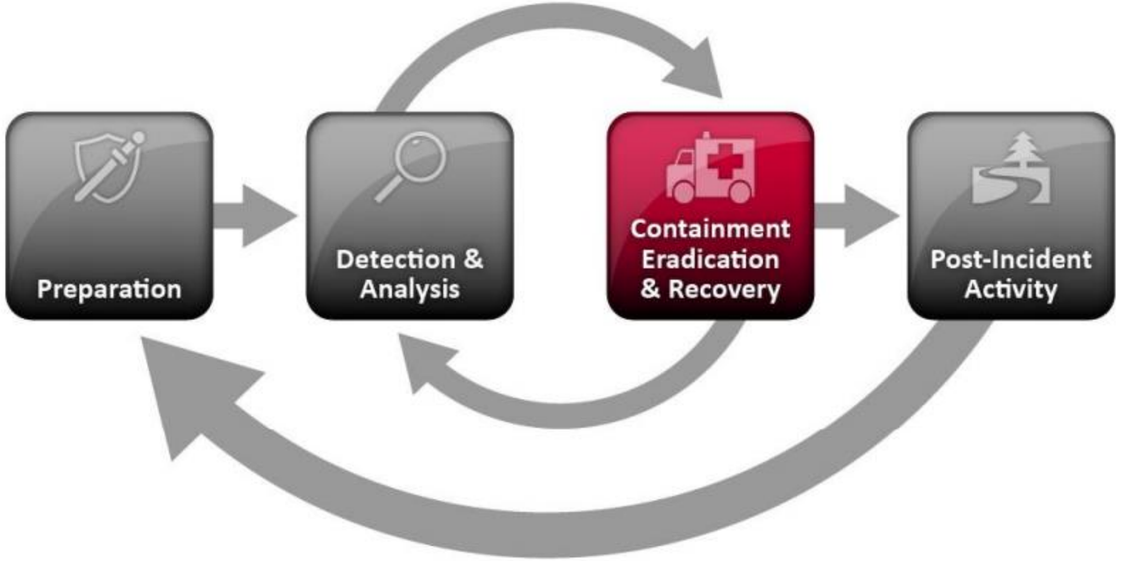
Containment

Choosing a Containment Strategy based on the type of incident

- Avoid just pulling the plug
- Use Adversary network segmentation or similar
- No containment → adversary starts to change TTPs

Intelligence Development:

- Identifying the Attacking Hosts
- Identify Covert Channels
- Document how all evidence, including compromised systems, has been preserved.
- Improve monitoring



Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

“if you want to respond effectively you need to reduce the uncertainty and understand when it’s the right time to act”

Frode Hommedal
@FrodeHommedal
Technical Director PwC.no, former Member NorCERT, Head of Telenor’s CERT

NIST Incident Response Process

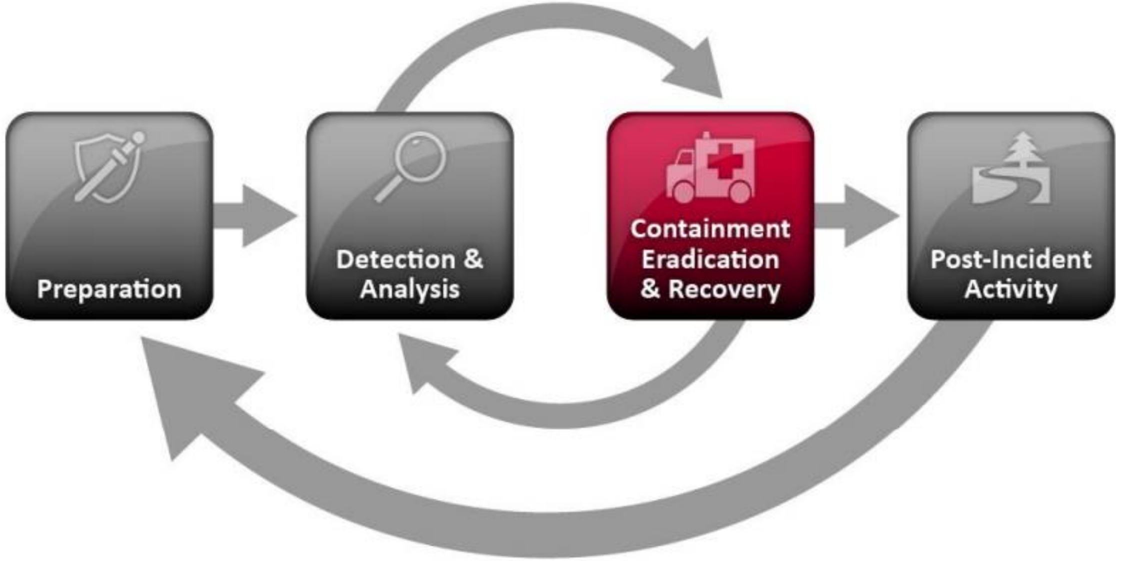
Eradication and Recovery

Eradication

- block network access
- deleting malware and persistence
- disabling breached user accounts
- initiate krbtgt cycling
- mitigating all vulnerabilities that were exploited
- be quick and plan well

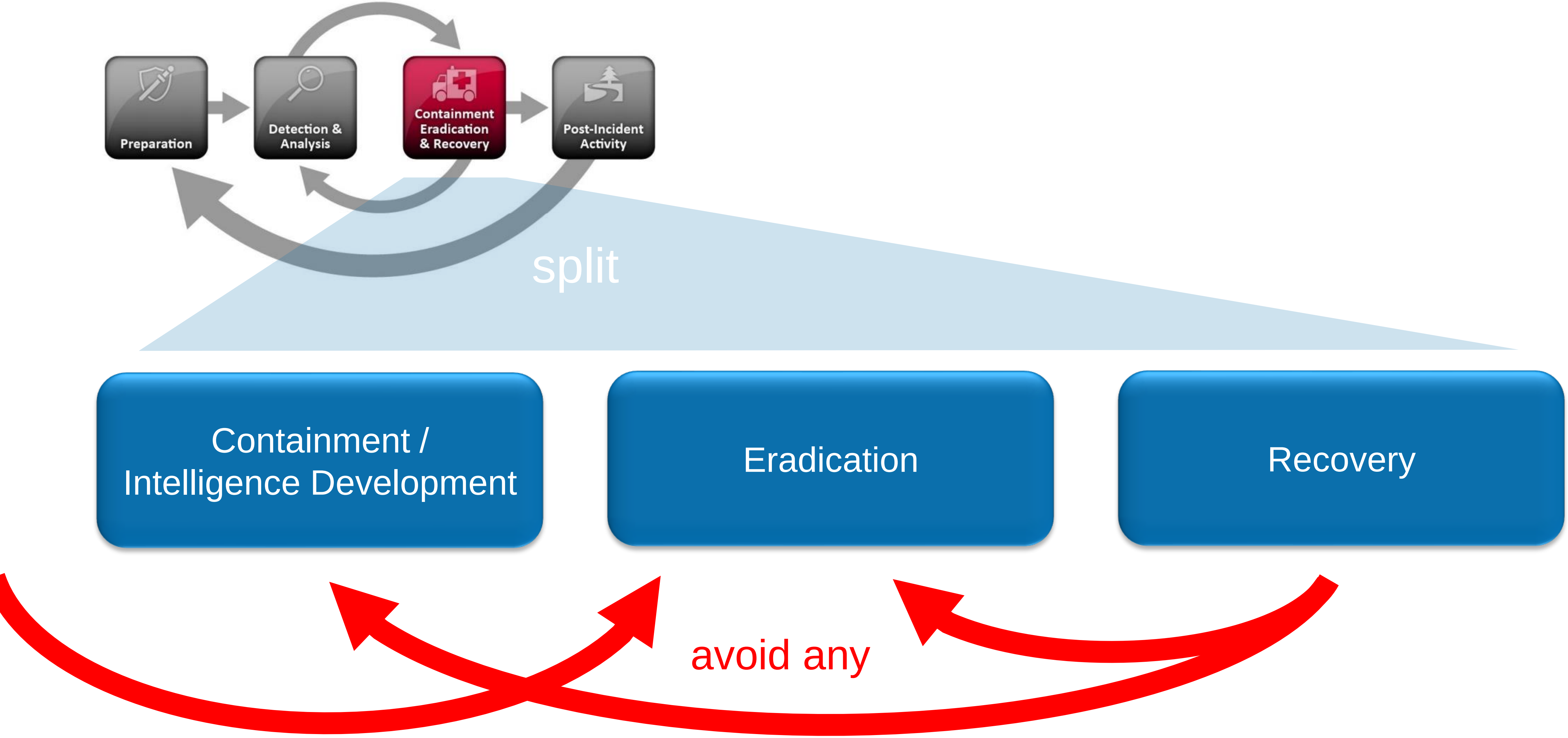
Recovery

- Return to normal business operation
- Implement supplement measures
- Initiate larger projects (segmentation, detection)



Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Advantage of SANS Cycle over NIST Cycle



split

Containment / Intelligence Development

Eradication

Recovery

avoid any

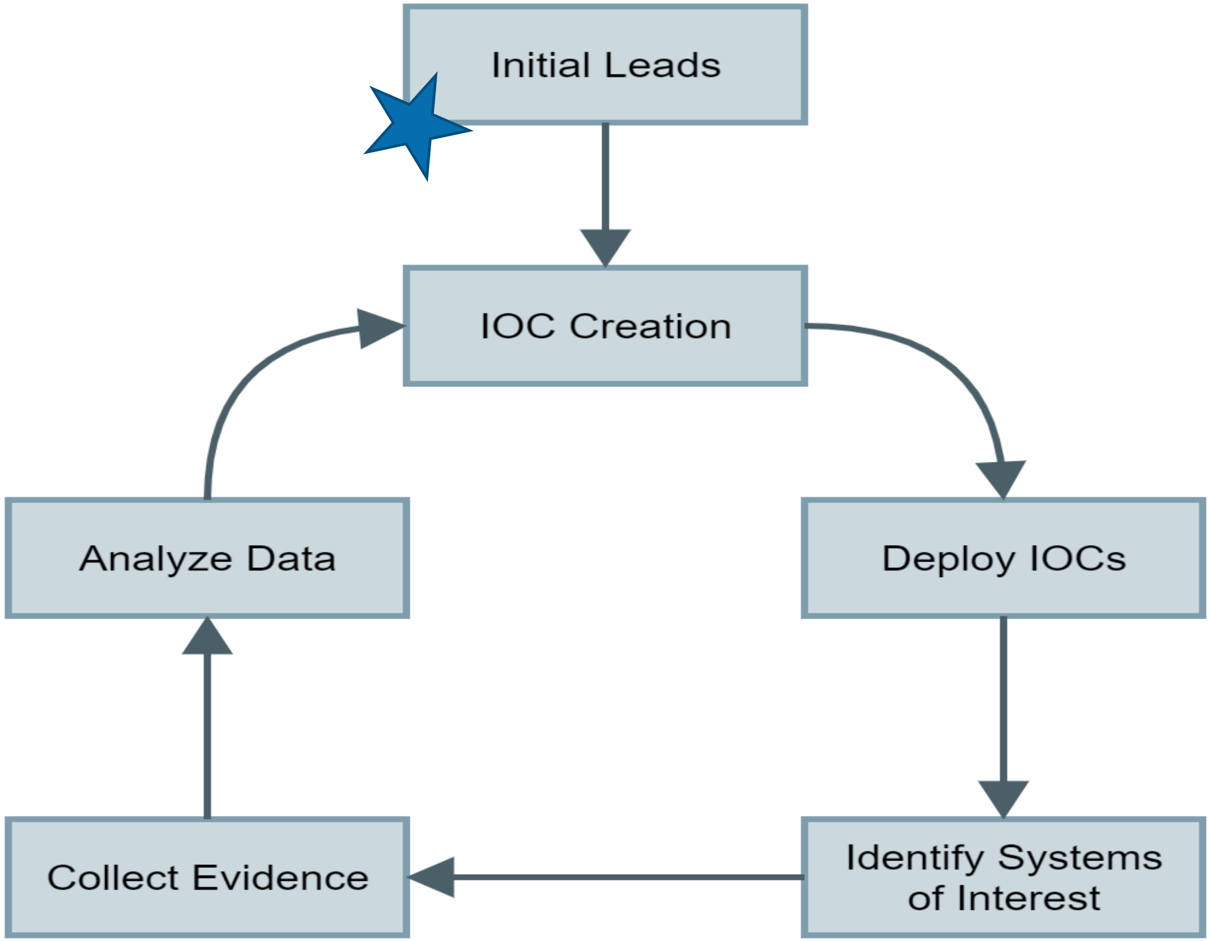
Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, https://www.sans.org/media/score/504-incident-response-cycle.pdf

Detection and Analysis in Detail

Follow the white rabbit…

Detection and Analysis in Detail

Mandiant Investigation Cycle - Initial Leads

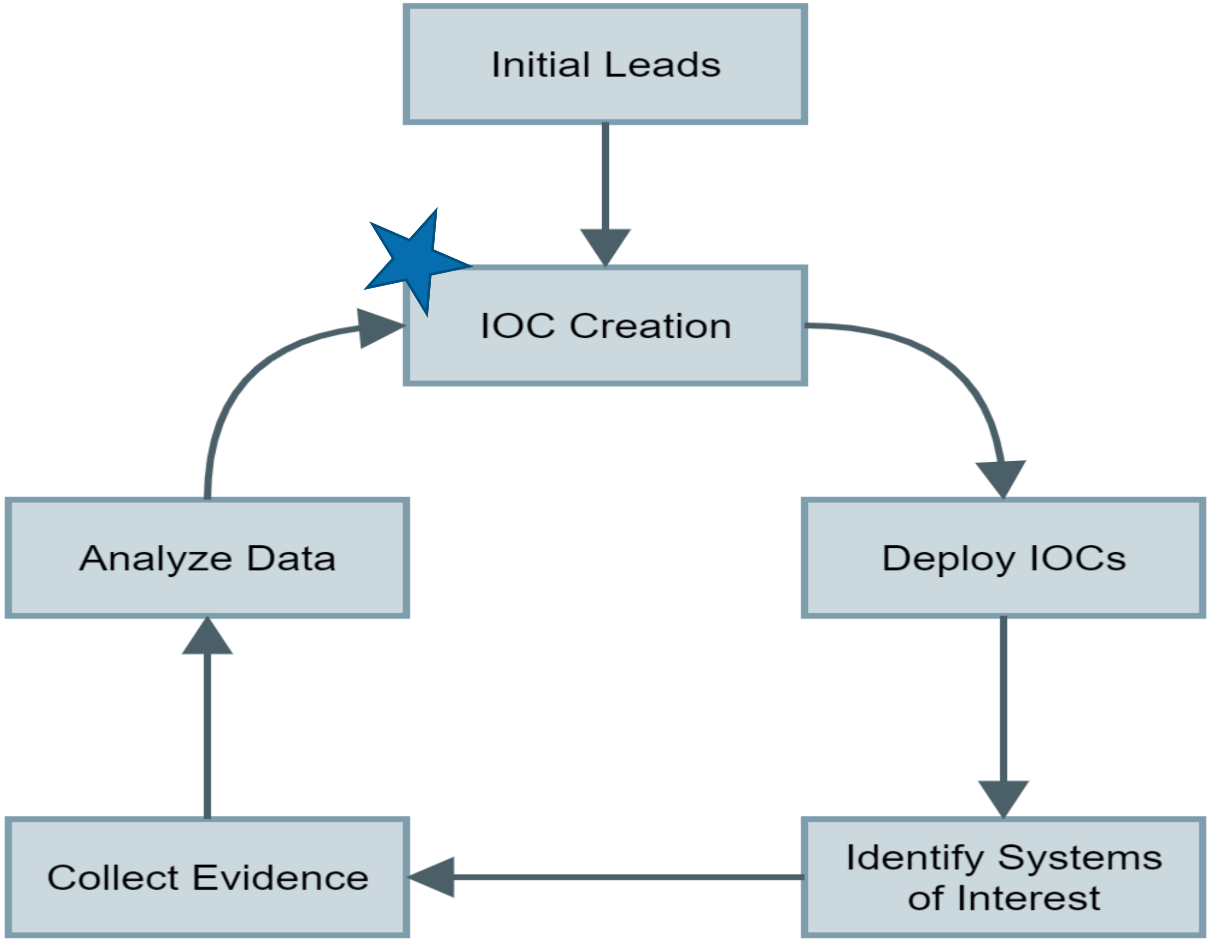


The goal of an analysis is to determine **facts** that describe **what** happened, **how** and **where** it happened, **when** it happened and sometimes, **who** was responsible and **why** it was done.

5-Step Cycle, Incident Response & Computer Forensics, Third Edition, 3rd Edition by Jason Luttgens, Matthew Pepe, Kevin Mandia, ISBN: 9780071798693

Detection and Analysis in Detail

Mandiant Investigation Cycle - IOC Creation



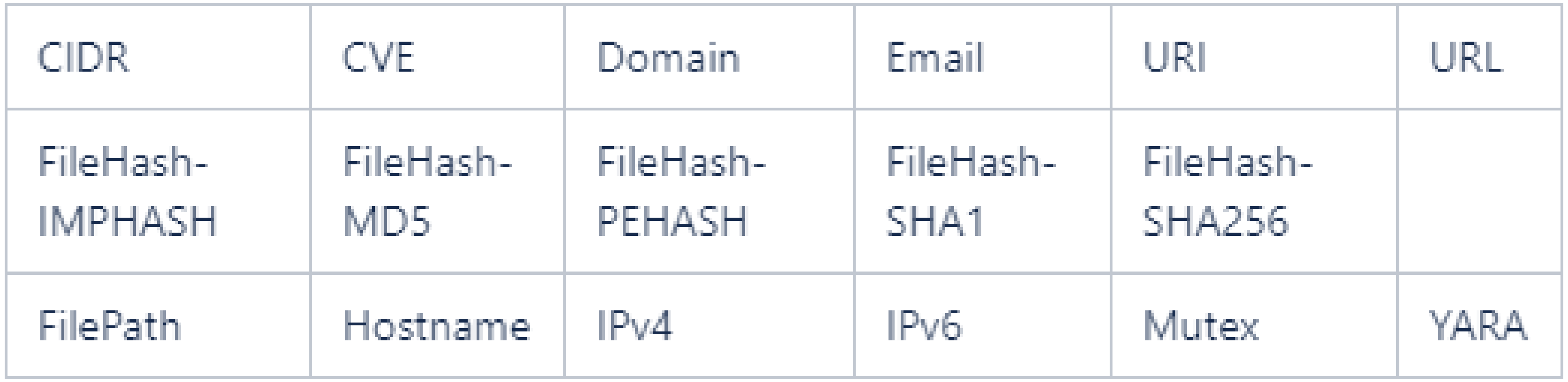
5-Step Cycle, Incident Response & Computer Forensics, Third Edition, 3rd Edition by Jason Luttgens, Matthew Pepe, Kevin Mandia, ISBN: 9780071798693

Detection and Analysis in Detail

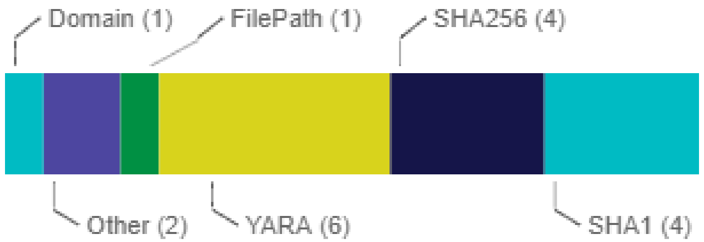
AlienVault OTX Example Petya Ransomware

An IOC might be as simple as a domain or e.g. a slightly more complex YARA rule.

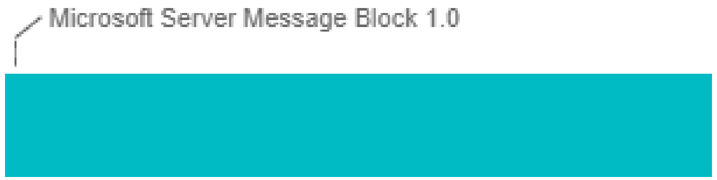
AlienVault's OTX e.g. distinguishes the following IOC types:



CIDR	CVE	Domain	Email	URI	URL
FileHash-IMPHASH	FileHash-MD5	FileHash-PEHASH	FileHash-SHA1	FileHash-SHA256	
FilePath	Hostname	IPv4	IPv6	Mutex	YARA



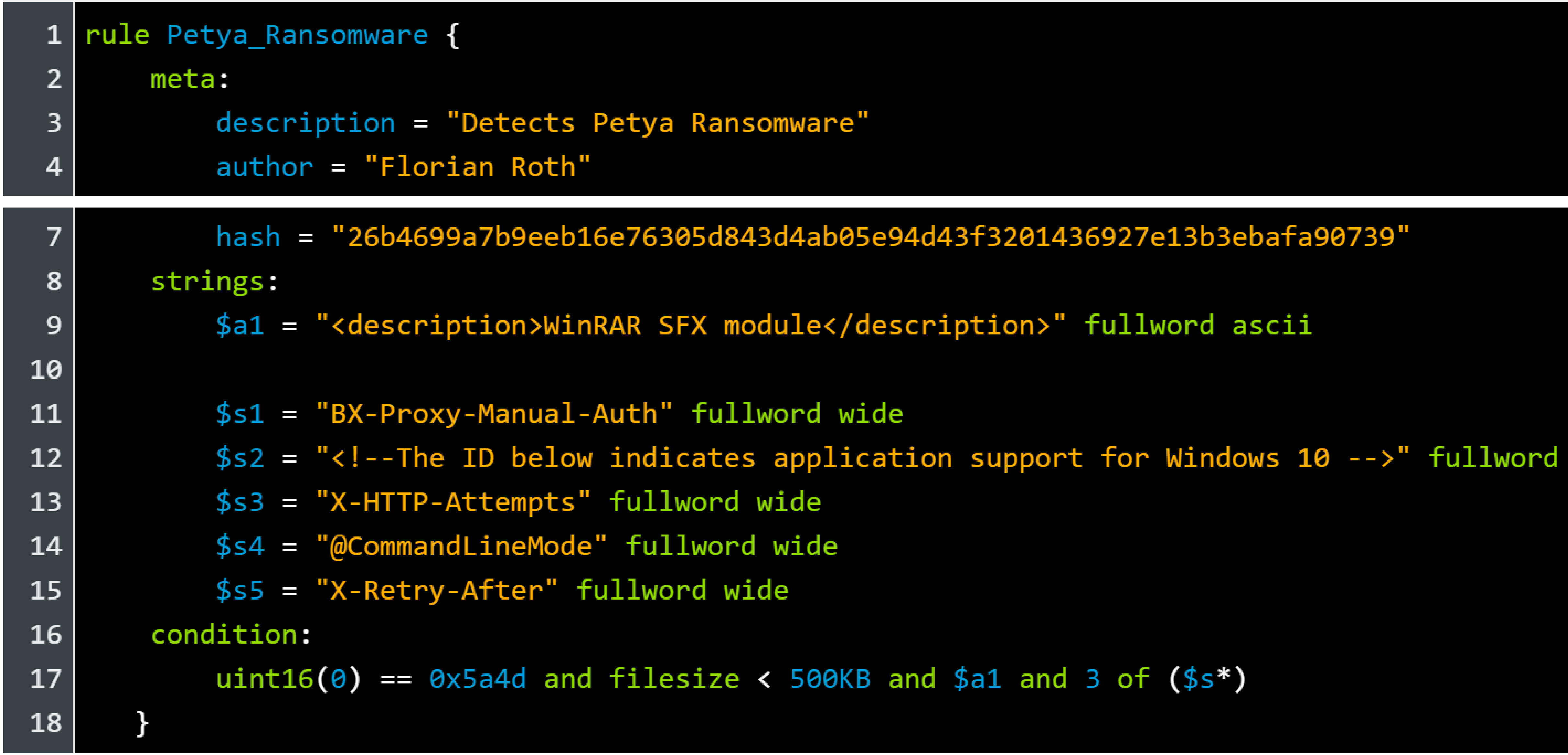
TYPES OF INDICATORS



TARGETED PRODUCTS

IOC Type Domain: wowsmith123456posteo.ne

Detection and Analysis in Detail

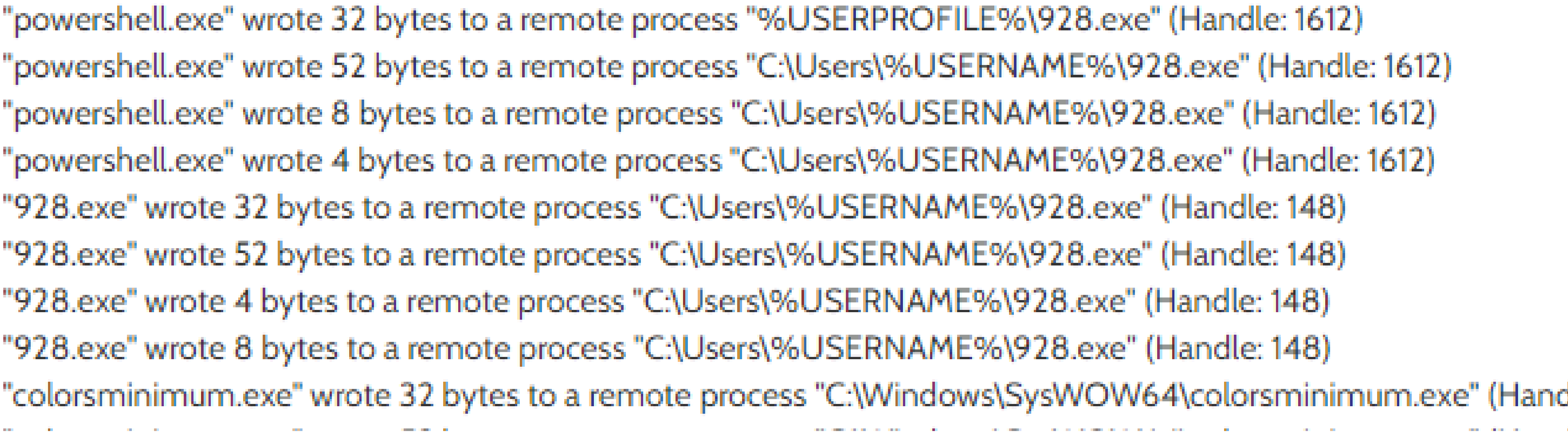


```
rule Petya_Ransomware {
    meta:
        description = "Detects Petya Ransomware"
        author = "Florian Roth"
```

```
        hash = "26b4699a7b9eeb16e76305d843d4ab05e94d43f3201436927e13b3ebafa90739"
    strings:
        $a1 = "<description>WinRAR SFX module</description>" fullword ascii

        $s1 = "BX-Proxy-Manual-Auth" fullword wide
        $s2 = "<!--The ID below indicates application support for Windows 10 -->" fullword
        $s3 = "X-HTTP-Attempts" fullword wide
        $s4 = "@CommandLineMode" fullword wide
        $s5 = "X-Retry-After" fullword wide
    condition:
        uint16(0) == 0x5a4d and filesize < 500KB and $a1 and 3 of ($s*)
   }
```

Emotet Analysis – Sandbox shortcomings II



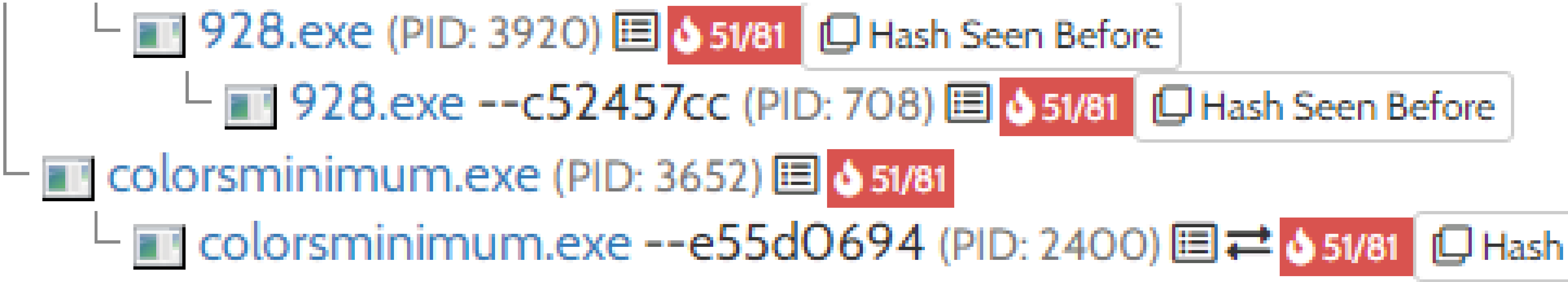
```
"powershell.exe" wrote 32 bytes to a remote process "%USERPROFILE%\928.exe" (Handle: 1612)
"powershell.exe" wrote 52 bytes to a remote process "C:\Users\%USERNAME%\928.exe" (Handle: 1612)
"powershell.exe" wrote 8 bytes to a remote process "C:\Users\%USERNAME%\928.exe" (Handle: 1612)
"powershell.exe" wrote 4 bytes to a remote process "C:\Users\%USERNAME%\928.exe" (Handle: 1612)
"928.exe" wrote 32 bytes to a remote process "C:\Users\%USERNAME%\928.exe" (Handle: 148)
"928.exe" wrote 52 bytes to a remote process "C:\Users\%USERNAME%\928.exe" (Handle: 148)
"928.exe" wrote 4 bytes to a remote process "C:\Users\%USERNAME%\928.exe" (Handle: 148)
"928.exe" wrote 8 bytes to a remote process "C:\Users\%USERNAME%\928.exe" (Handle: 148)
"colorsminimum.exe" wrote 32 bytes to a remote process "C:\Windows\SysWOW64\colorsminimum.exe" (Hand
```

Run as Admin: `%WinDir%\SysWOW64\<MALWARE>.exe`

`%WinDir%\System32\<MALWARE>.exe`

Run as user: `%LocalAppData%/<MALWARE>/<MALWARE>.exe`

Emotet Analysis – Sandbox shortcomings III



928.exe (PID: 3920) 51/81 Hash Seen Before

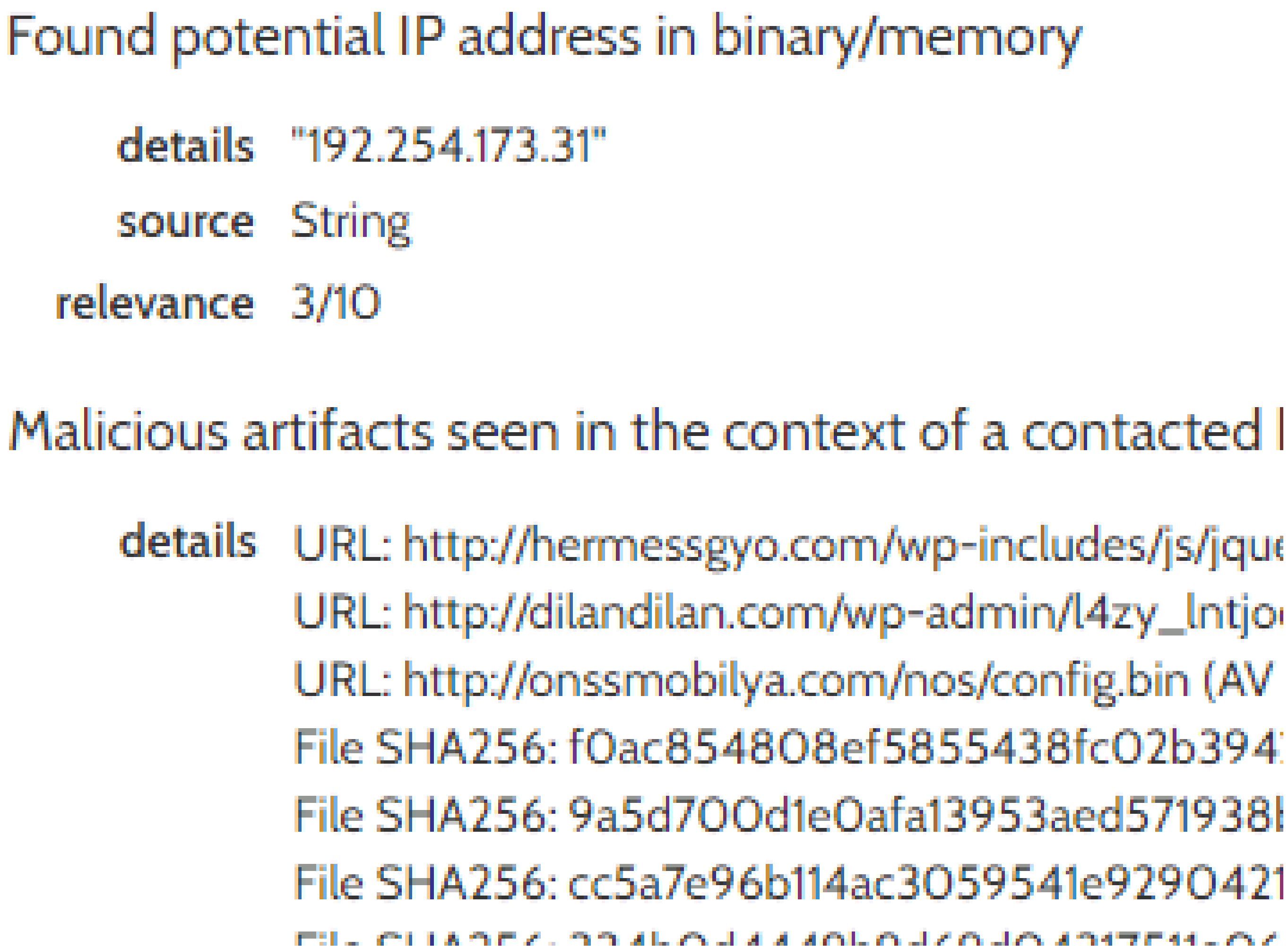
928.exe --c52457cc (PID: 708) 51/81 Hash Seen Before

colorsminimum.exe (PID: 3652) 51/81

colorsminimum.exe --e55d0694 (PID: 2400) ⇄ 51/81 Hash

Name is 2 words from `after, allow, backup, cable, cap, chore, chx, class, cmp, colors, con, cpls, crypto, dasmrc, define, edition, engine, excel, finish, foot, fwdr, generic, hans, kds, keydef, khmer, license, loada, magnify, maker, mferror, minimum, move, mspterm, nop, pen, pink, pixel, play, prep, proc, publish, query, rebrand, resapi, resw, router, shlp, sizes, skip, sms, svcs, syc, tablet, tangent, themes, top, tran, umx, wce, wide, without, wubi, xcl`

Analysis – Sandbox shortcomings IV



Found potential IP address in binary/memory

details "192.254.173.31"

source String

relevance 3/10

Malicious artifacts seen in the context of a contacted I

details URL: http://hermessgyo.com/wp-includes/js/jque

URL: http://dilandilan.com/wp-admin/l4zy_lntjo

URL: http://onssmobilya.com/nos/config.bin (AV

File SHA256: f0ac85408ef5855438fc02b394

File SHA256: 9a5d700d1e0afa13953aed571938

File SHA256: cc5a7e96b114ac3059541e929042

67.225.229.55:8080
185.14.187.201:8080
45.79.188.67:8080
62.75.187.192:8080
41.220.119.246:80
173.212.203.26:8080
80.11.163.139:443
80.11.163.139:443
211.63.71.72:8080
188.166.253.46:8080
115.78.95.230:443
63.142.253.122:8080
95.128.43.213:8080
189.209.217.49:80
149.167.86.174:990
88.156.97.210:80
142.44.162.209:8080
80.11.163.139:21
190.226.44.20:21
186.4.172.5:8080
212.71.234.16:8080
45.33.49.124:443
31.172.240.91:8080
5.196.74.210:8080
104.236.246.93:8080
182.176.132.213:8090
185.94.252.13:443
103.97.95.218:143
200.71.148.138:8080
186.75.241.230:80
201.251.43.69:8080
91.205.215.66:8080
178.254.6.27:7080
190.53.135.159:21
85.104.59.244:20
92.222.216.44:8080

159.65.25.128:8080
88.247.163.44:80
27.147.163.188:8080
149.202.153.252:8080
86.98.25.30:53
83.136.245.190:8080
190.145.67.134:8090
104.131.11.150:8080
103.255.150.84:80
92.233.128.13:143
138.201.140.110:8080
190.18.146.70:80
186.4.172.5:20
144.139.247.220:80
181.143.194.138:443
190.106.97.230:443
85.54.169.141:8080
87.106.136.232:8080
101.187.237.217:20
87.106.139.101:8080
78.188.105.159:21
217.160.182.191:8080
186.4.172.5:443
31.12.67.62:7080
190.228.72.244:53
136.243.177.26:8080
222.214.218.192:8080
45.123.3.54:443
190.211.207.11:443
94.205.247.10:80
187.144.189.58:50000
92.222.125.16:7080
46.105.131.87:80
27.4.80.183:443
178.79.161.166:443
119.15.153.237:80

206.189.98.125:8080
47.41.213.2:22
169.239.182.217:8080
85.106.1.166:50000
78.24.219.147:8080
37.157.194.134:443
190.108.228.48:990
190.186.203.55:80
124.240.198.66:80
182.176.106.43:995
181.143.53.227:21
181.31.213.158:8080
199.19.237.192:80
182.76.6.2:8080
179.32.19.219:22
24.51.106.145:21
217.145.83.44:80
87.230.19.21:8080

Analysis

Automated (Sandbox)

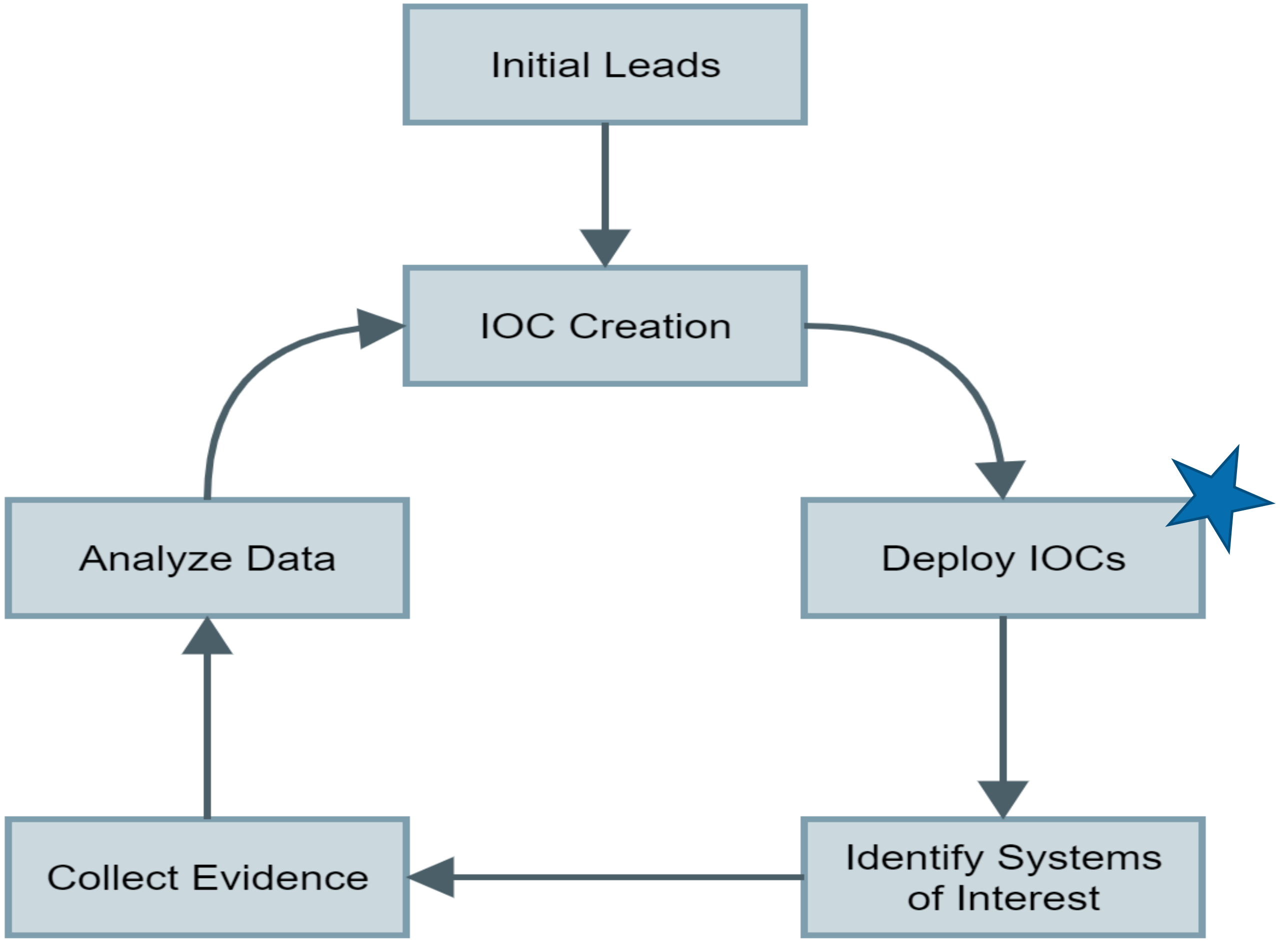
+ Relatively quick (Background time)
+ Results even without knowledge
- Results may not contain all findings
- Victim to anti-analysis techniques

Manual

- Takes more time
- Require some knowledge
+ Findings are more accurate
+ Anti-analysis can be bypassed

Detection and Analysis in Detail

Mandiant Investigation Cycle – Deploy IOCs



5-Step Cycle, Incident Response & Computer Forensics, Third Edition, 3rd Edition by Jason Luttgens, Matthew Pepe, Kevin Mandia, ISBN: 9780071798693

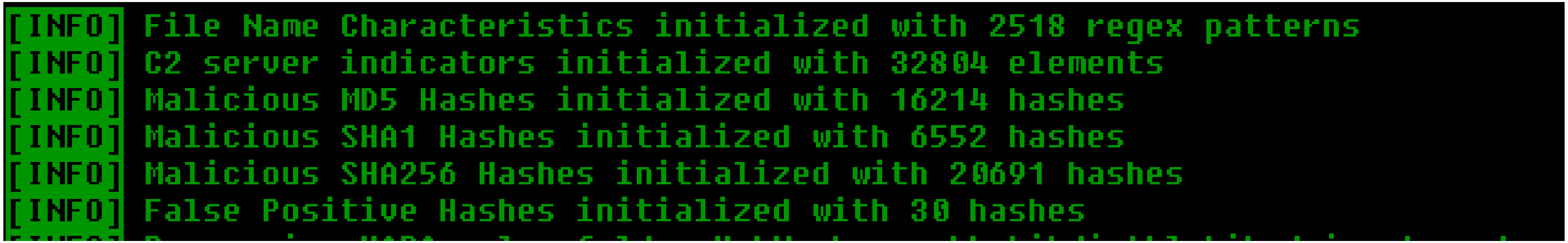
Detection and Analysis in Detail

How to Deploy IOCs (Hosts and Networks)

Possibilities depend on the corresponding victim EDR solution and need to be checked during the onboarding/simulation phases.

Otherwise back-off to

- Open-Source EDR or Orchestration (GRR, OSquery, Velociraptor)
- LOKI or THOR YARA Scanner https://www.nextron-systems.com/loki/
- Mandiant OpenIOC Scanner https://www.fireeye.com/services/freeware/ioc-finder.html
- Snort and Suricata https://snort.org/, https://suricata-ids.org/

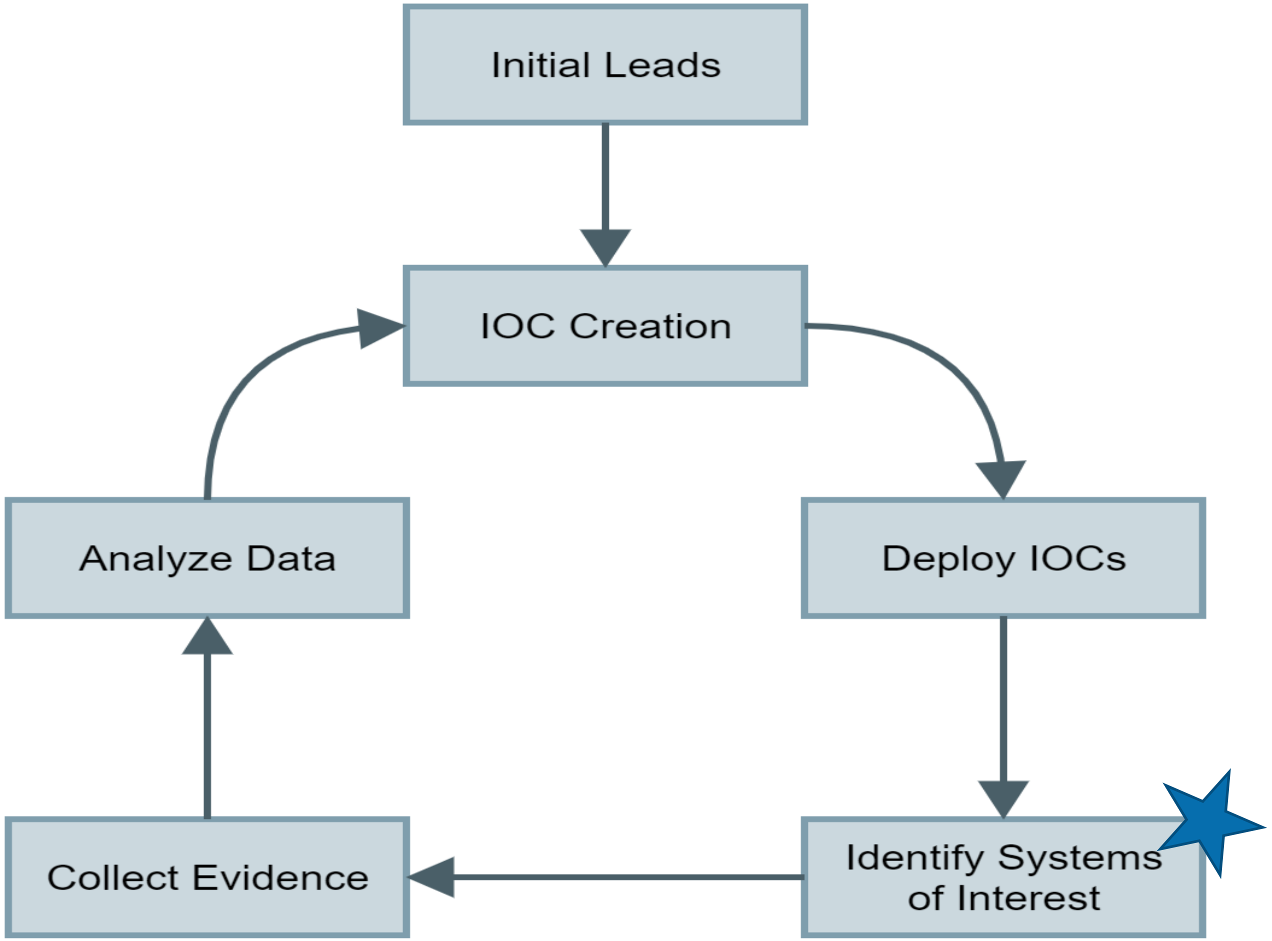


```
[INFO] File Name Characteristics initialized with 2518 regex patterns
[INFO] C2 server indicators initialized with 32804 elements
[INFO] Malicious MD5 Hashes initialized with 16214 hashes
[INFO] Malicious SHA1 Hashes initialized with 6552 hashes
[INFO] Malicious SHA256 Hashes initialized with 20691 hashes
[INFO] False Positive Hashes initialized with 30 hashes
```

Screenshot https://www.nextron-systems.com/loki/

Detection and Analysis in Detail

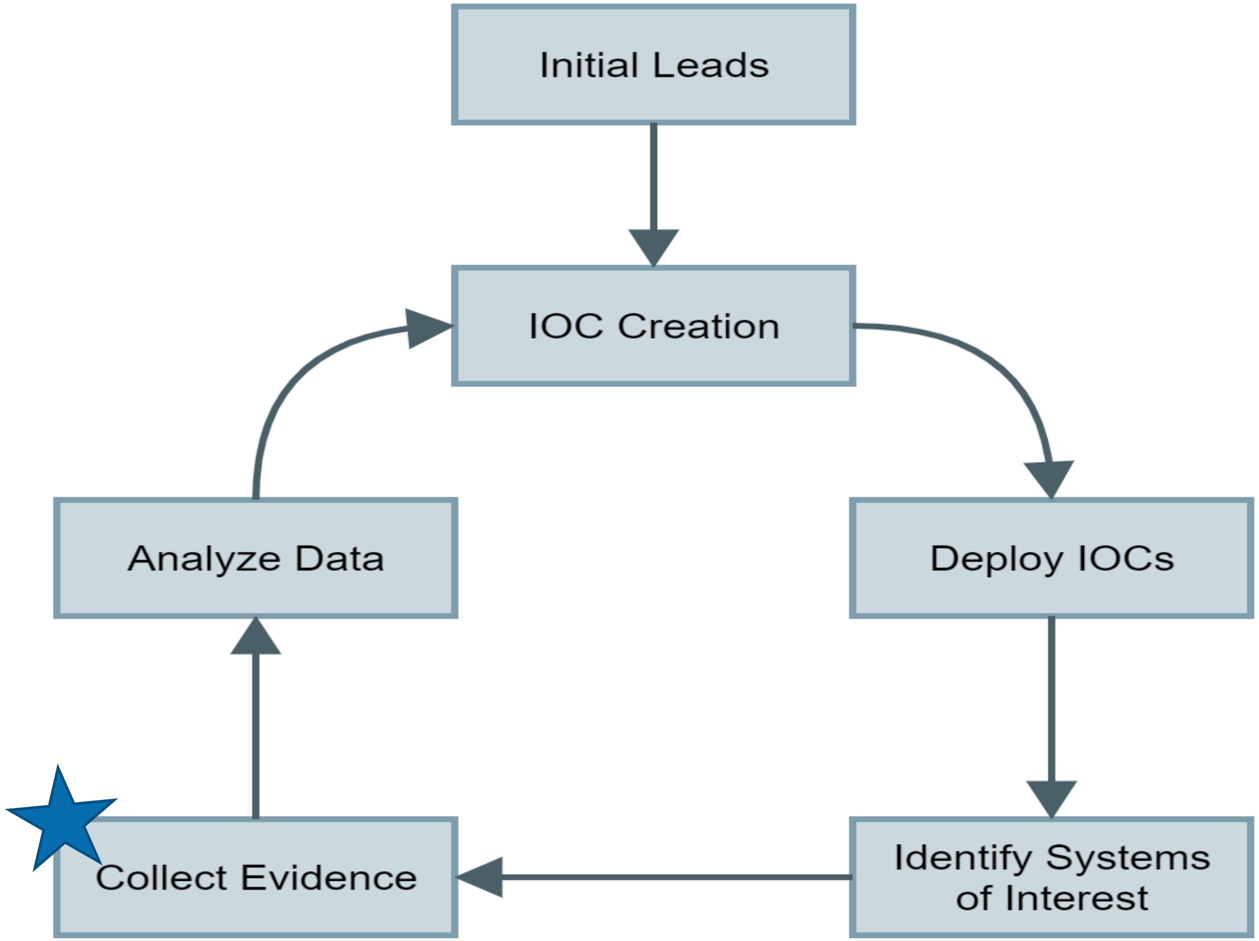
Mandiant Investigation Cycle – Identify Systems of Interest



5-Step Cycle, Incident Response & Computer Forensics, Third Edition, 3rd Edition by Jason Luttgens, Matthew Pepe, Kevin Mandia, ISBN: 9780071798693

Detection and Analysis in Detail

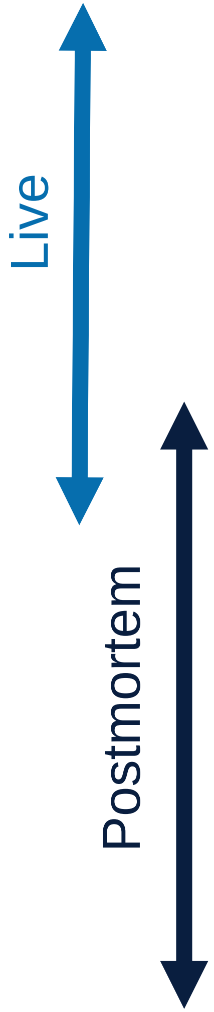
Mandiant Investigation Cycle - Collect Evidence



5-Step Cycle, Incident Response & Computer Forensics, Third Edition, 3rd Edition by Jason Luttgens, Matthew Pepe, Kevin Mandia, ISBN: 9780071798693

Detection and Analysis in Detail

Order of Volatility



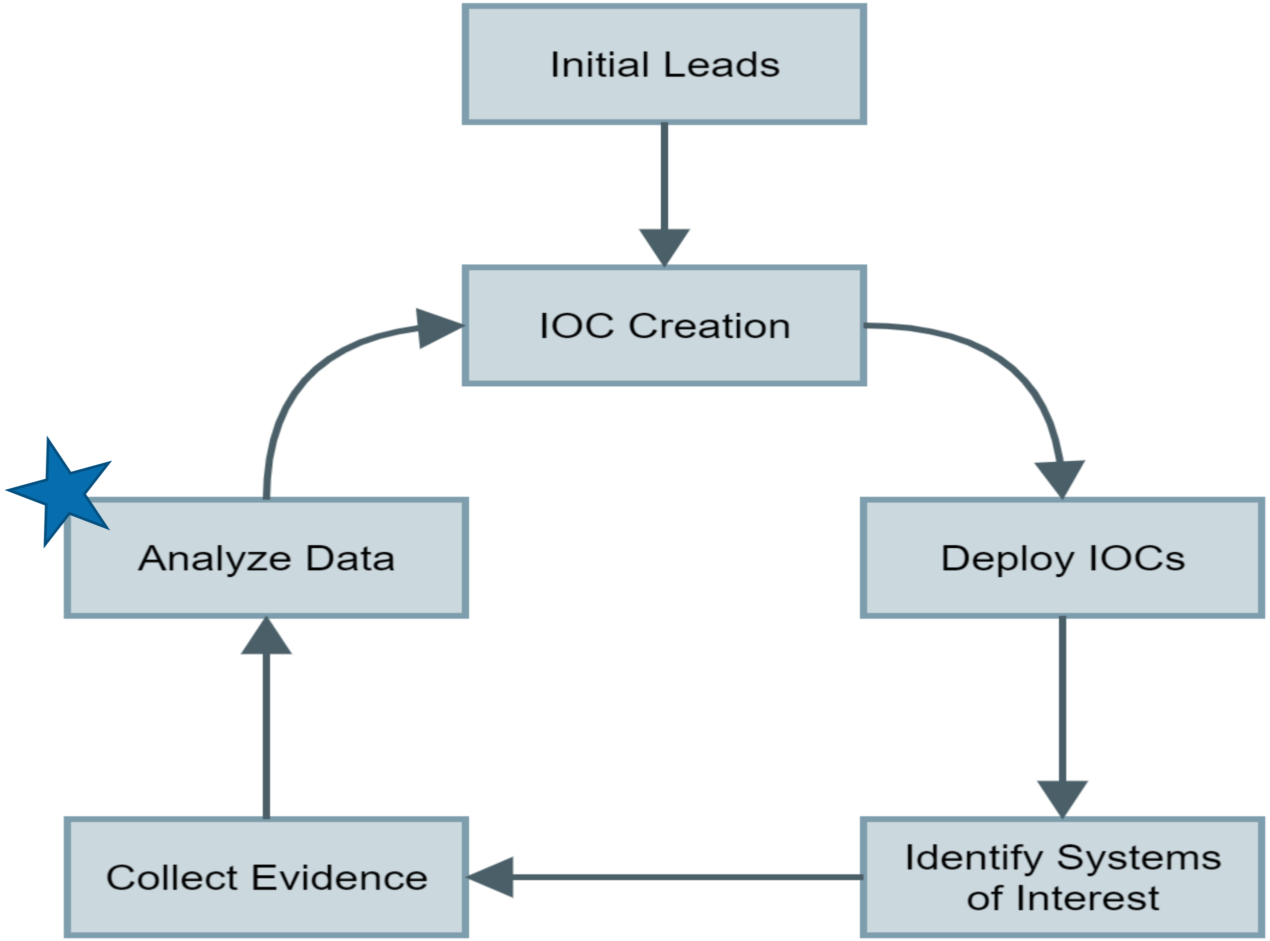
Live

Postmortem

1. Registers, Cache
2. Main Memory, Network State,
   Running Processes
3. Disk
4. Remote logging and monitoring data that is relevant to the system in question
5. Physical Configuration, Network Topology
6. Archival Media

Detection and Analysis in Detail

Mandiant Investigation Cycle - Analyze Data



5-Step Cycle, Incident Response & Computer Forensics, Third Edition, 3rd Edition by Jason Luttgens, Matthew Pepe, Kevin Mandia, ISBN: 9780071798693

List of Best Tools, Guides and Cheat Sheets

Detection and Analysis in Detail

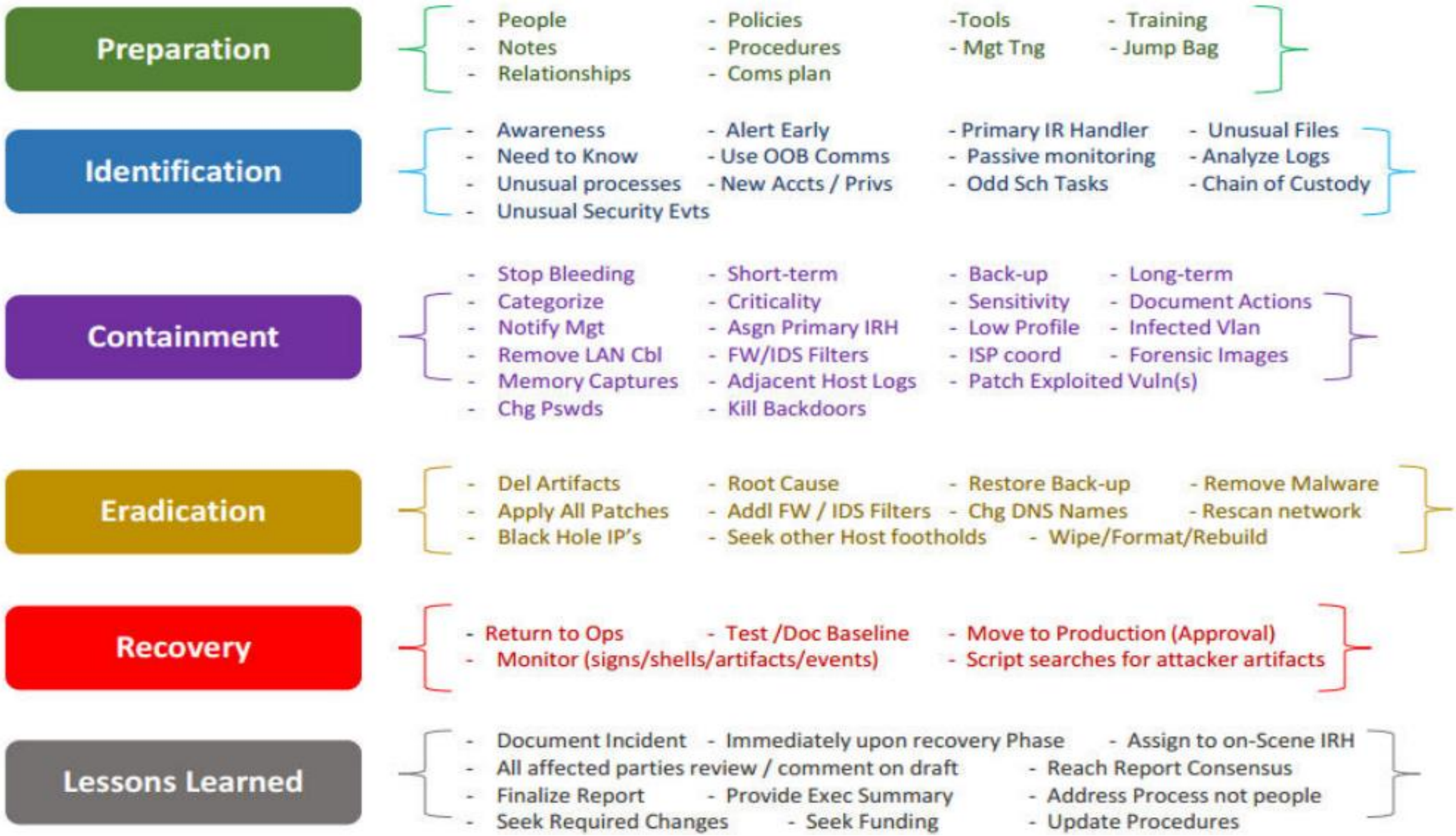
List of Best Tools

«Some of the best tools to use are ones you already have - you are using them right now to read and understand this sentence»

5-Step Cycle, Incident Response & Computer Forensics, Third Edition, 3rd Edition by Jason Luttgens, Matthew Pepe, Kevin Mandia, ISBN: 9780071798693

Guides and Cheat Sheet

SANS PICERL Cheat Sheet. What to do in which phase



Preparation

- People - Policies -Tools - Training
- Notes - Procedures - Mgt Tng - Jump Bag
- Relationships - Coms plan

Identification

- Awareness - Alert Early - Primary IR Handler - Unusual Files
- Need to Know - Use OOB Comms - Passive monitoring - Analyze Logs
- Unusual processes - New Accts / Privs - Odd Sch Tasks - Chain of Custody
- Unusual Security Evts

Containment

- Stop Bleeding - Short-term - Back-up - Long-term
- Categorize - Criticality - Sensitivity - Document Actions
- Notify Mgt - Asgn Primary IRH - Low Profile - Infected Vlan
- Remove LAN Cbl - FW/IDS Filters - ISP coord - Forensic Images
- Memory Captures - Adjacent Host Logs - Patch Exploited Vuln(s)
- Chg Pswds - Kill Backdoors

Eradication

- Del Artifacts - Root Cause - Restore Back-up - Remove Malware
- Apply All Patches - Addl FW / IDS Filters - Chg DNS Names - Rescan network
- Black Hole IP's - Seek other Host footholds - Wipe/Format/Rebuild

Recovery

- Return to Ops - Test /Doc Baseline - Move to Production (Approval)
- Monitor (signs/shells/artifacts/events) - Script searches for attacker artifacts

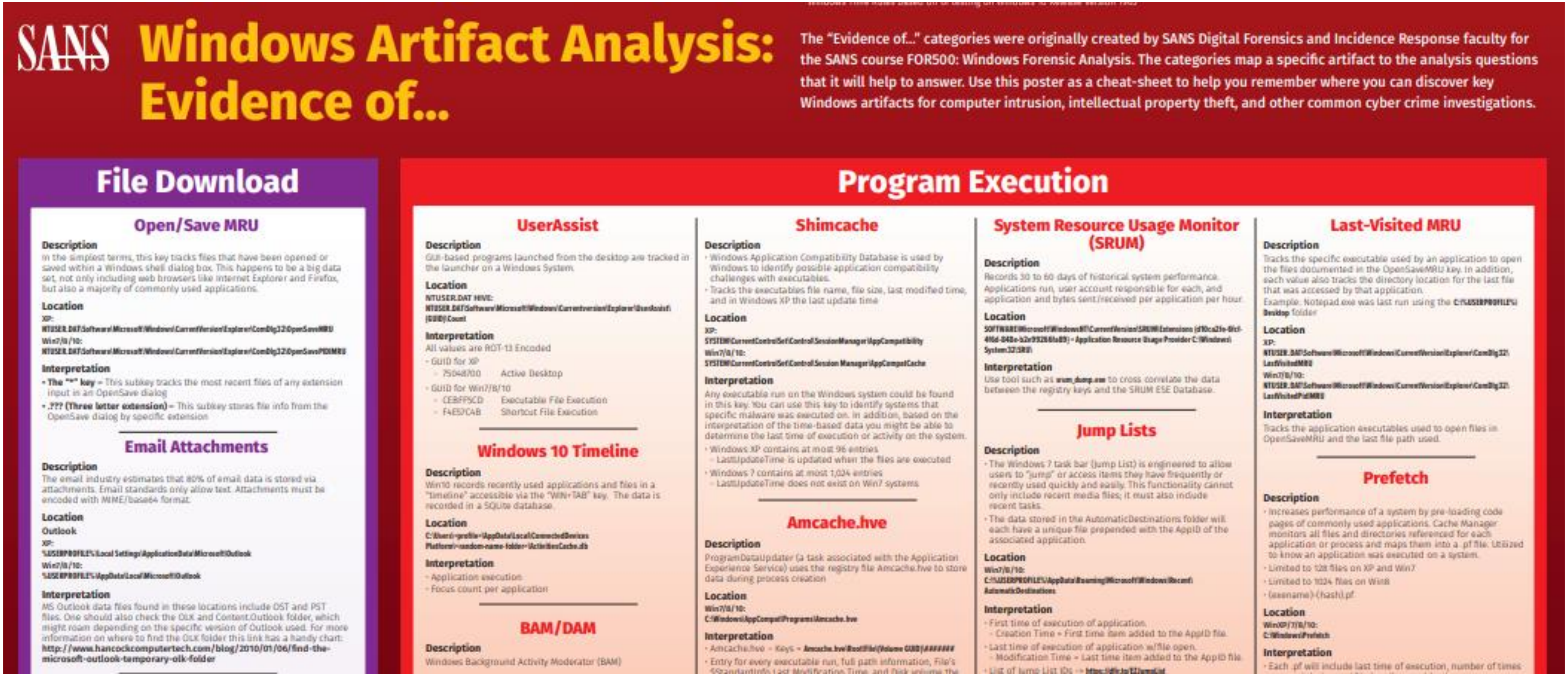
Lessons Learned

- Document Incident - Immediately upon recovery Phase - Assign to on-Scene IRH
- All affected parties review / comment on draft - Reach Report Consensus
- Finalize Report - Provide Exec Summary - Address Process not people
- Seek Required Changes - Seek Funding - Update Procedures

Source https://www.sans.org/media/score/504-incident-response-cycle.pdf

Guides and Cheat Sheet

SANS Windows Forensics is most relevant when doing enterprise cases



SANS **Windows Artifact Analysis: Evidence of...**

The "Evidence of..." categories were originally created by SANS Digital Forensics and Incidence Response faculty for the SANS course FOR500: Windows Forensic Analysis. The categories map a specific artifact to the analysis questions that it will help to answer. Use this poster as a cheat-sheet to help you remember where you can discover key Windows artifacts for computer intrusion, intellectual property theft, and other common cyber crime investigations.

File Download

Open/Save MRU

Description
In the simplest terms, this key tracks files that have been opened or saved within a Windows shell dialog box. This happens to be a big data set, not only including web browsers like Internet Explorer and Firefox, but also a majority of commonly used applications.

Location
XP:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
Win7/8/10:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU

Interpretation
- **The "*" key** – This subkey tracks the most recent files of any extension input in an OpenSave dialog
- **.??? (Three letter extension)** – This subkey stores file info from the OpenSave dialog by specific extension

Email Attachments

Description
The email industry estimates that 80% of email data is stored via attachments. Email standards only allow text. Attachments must be encoded with MIME/base64 format.

Location
Outlook
XP:
%USERPROFILE%\Local Settings\ApplicationData\Microsoft\Outlook
Win7/8/10:
%USERPROFILE%\AppData\Local\Microsoft\Outlook

Interpretation
MS Outlook data files found in these locations include OST and PST files. One should also check the OLK and Content.Outlook folder, which might roam depending on the specific version of Outlook used. For more information on where to find the OLK folder this link has a handy chart:
http://www.hancockcomputertech.com/blog/2010/01/06/find-the-microsoft-outlook-temporary-olk-folder

Program Execution

UserAssist

Description
GUI-based programs launched from the desktop are tracked in the launcher on a Windows System.

Location
NTUSER.DAT HIVE:
NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count

Interpretation
All values are ROT-13 Encoded
- GUID for XP
  - 75048700 Active Desktop
- GUID for Win7/8/10
  - CEBFF5CD Executable File Execution
  - F4E57C4B Shortcut File Execution

Windows 10 Timeline

Description
Win10 records recently used applications and files in a "timeline" accessible via the "WIN+TAB" key. The data is recorded in a SQLite database.

Location
C:\Users\<profile>\AppData\Local\ConnectedDevicesPlatform\<random-name-folder>\ActivitiesCache.db

Interpretation
- Application execution
- Focus count per application

BAM/DAM

Description
Windows Background Activity Moderator (BAM)

Shimcache

Description
- Windows Application Compatibility Database is used by Windows to identify possible application compatibility challenges with executables.
- Tracks the executables file name, file size, last modified time, and in Windows XP the last update time

Location
XP:
SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatibility
Win7/8/10:
SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

Interpretation
Any executable run on the Windows system could be found in this key. You can use this key to identify systems that specific malware was executed on. In addition, based on the interpretation of the time-based data you might be able to determine the last time of execution or activity on the system.
- Windows XP contains at most 96 entries
  - LastUpdateTime is updated when the files are executed
- Windows 7 contains at most 1,024 entries
  - LastUpdateTime does not exist on Win7 systems

Amcache.hve

Description
ProgramDataUpdater (a task associated with the Application Experience Service) uses the registry file Amcache.hve to store data during process creation

Location
Win7/8/10:
C:\Windows\AppCompat\Programs\Amcache.hve

Interpretation
- Amcache.hve – Keys = **Amcache.hve\Root\File\{Volume GUID}\#######**
- Entry for every executable run, full path information, File's $StandardInfo Last Modification Time, and Disk volume the

System Resource Usage Monitor (SRUM)

Description
Records 30 to 60 days of historical system performance. Applications run, user account responsible for each, and application and bytes sent/received per application per hour.

Location
SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SRUM\Extensions {d10ca2fe-6fcf-4f6d-848e-b2e99266fa89} = Application Resource Usage Provider C:\Windows\System32\SRU\

Interpretation
Use tool such as **srum_dump.exe** to cross correlate the data between the registry keys and the SRUM ESE Database.

Jump Lists

Description
- The Windows 7 task bar (Jump List) is engineered to allow users to "jump" or access items they have frequently or recently used quickly and easily. This functionality cannot only include recent media files; it must also include recent tasks.
- The data stored in the AutomaticDestinations folder will each have a unique file prepended with the AppID of the associated application.

Location
Win7/8/10:
C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Interpretation
- First time of execution of application.
  - Creation Time = First time item added to the AppID file.
- Last time of execution of application w/file open.
  - Modification Time = Last time item added to the AppID file.
- List of Jump List IDs -> **https://dfir.to/EZJumpList**

Last-Visited MRU

Description
Tracks the specific executable used by an application to open the files documented in the OpenSaveMRU key. In addition, each value also tracks the directory location for the last file that was accessed by that application.
Example: Notepad.exe was last run using the **C:\%USERPROFILE%\Desktop** folder

Location
XP:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
Win7/8/10:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

Interpretation
Tracks the application executables used to open files in OpenSaveMRU and the last file path used.

Prefetch

Description
- Increases performance of a system by pre-loading code pages of commonly used applications. Cache Manager monitors all files and directories referenced for each application or process and maps them into a .pf file. Utilized to know an application was executed on a system.
- Limited to 128 files on XP and Win7
- Limited to 1024 files on Win8
- (exename)-(hash).pf

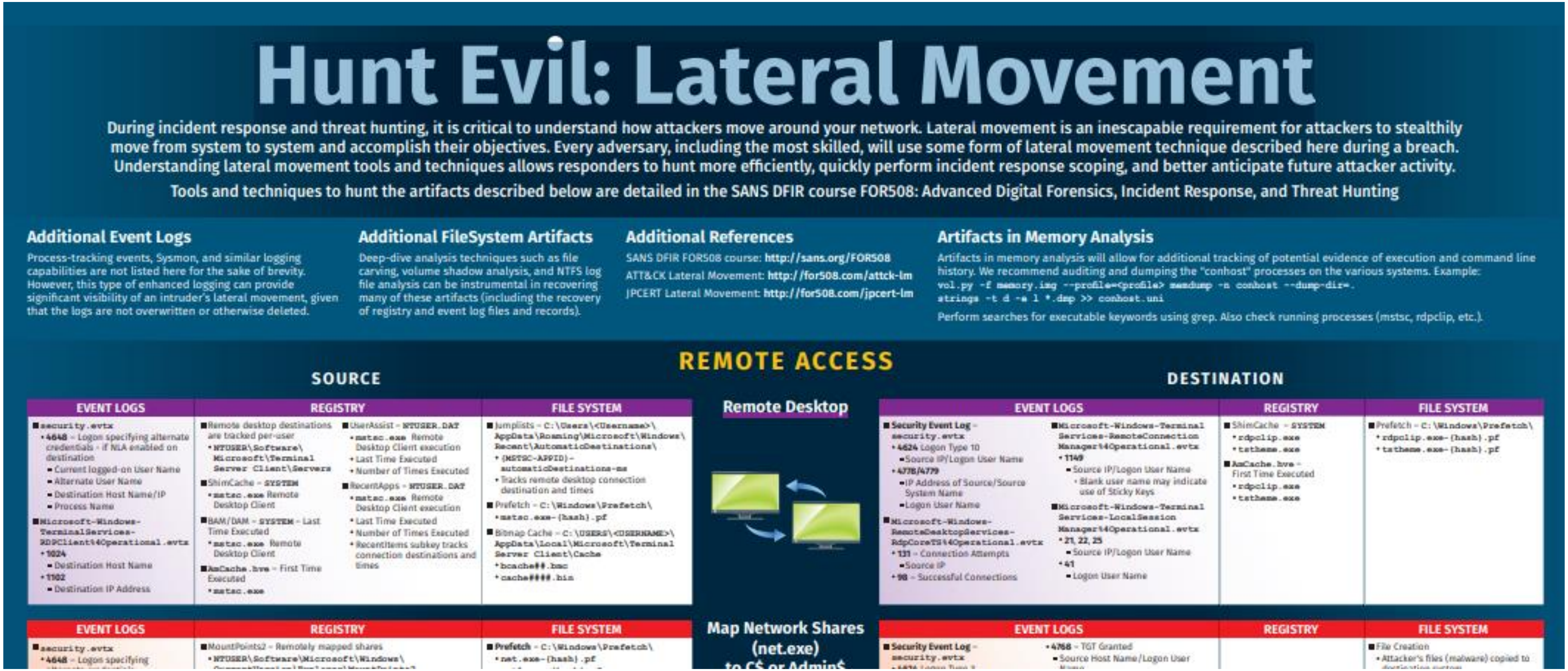
Location
WinXP/7/8/10:
C:\Windows\Prefetch

Interpretation
- Each .pf will include last time of execution, number of times

Source https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download

Guides and Cheat Sheet

SANS Hunt Evil is a great resource for lateral movement artifacts



Hunt Evil: Lateral Movement

During incident response and threat hunting, it is critical to understand how attackers move around your network. Lateral movement is an inescapable requirement for attackers to stealthily move from system to system and accomplish their objectives. Every adversary, including the most skilled, will use some form of lateral movement technique described here during a breach. Understanding lateral movement tools and techniques allows responders to hunt more efficiently, quickly perform incident response scoping, and better anticipate future attacker activity.

Tools and techniques to hunt the artifacts described below are detailed in the SANS DFIR course FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting

Additional Event Logs

Process-tracking events, Sysmon, and similar logging capabilities are not listed here for the sake of brevity. However, this type of enhanced logging can provide significant visibility of an intruder's lateral movement, given that the logs are not overwritten or otherwise deleted.

Additional FileSystem Artifacts

Deep-dive analysis techniques such as file carving, volume shadow analysis, and NTFS log file analysis can be instrumental in recovering many of these artifacts (including the recovery of registry and event log files and records).

Additional References

SANS DFIR FOR508 course: **http://sans.org/FOR508**

ATT&CK Lateral Movement: **http://for508.com/attck-lm**

JPCERT Lateral Movement: **http://for508.com/jpcert-lm**

Artifacts in Memory Analysis

Artifacts in memory analysis will allow for additional tracking of potential evidence of execution and command line history. We recommend auditing and dumping the "conhost" processes on the various systems. Example:

```
vol.py -f memory.img --profile=<profile> memdump -n conhost --dump-dir=.
strings -t d -e l *.dmp >> conhost.uni
```

Perform searches for executable keywords using grep. Also check running processes (mstsc, rdpclip, etc.).

REMOTE ACCESS

SOURCE

Remote Desktop

EVENT LOGS

- **security.evtx**
  - **4648** – Logon specifying alternate credentials - if NLA enabled on destination
    - Current logged-on User Name
    - Alternate User Name
    - Destination Host Name/IP
    - Process Name
- **Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx**
  - **1024**
    - Destination Host Name
  - **1102**
    - Destination IP Address

REGISTRY

- Remote desktop destinations are tracked per-user
  - **NTUSER\Software\Microsoft\Terminal Server Client\Servers**
- ShimCache – **SYSTEM**
  - **mstsc.exe** Remote Desktop Client
- BAM/DAM – **SYSTEM** – Last Time Executed
  - **mstsc.exe** Remote Desktop Client
- **AmCache.hve** – First Time Executed
  - **mstsc.exe**
- UserAssist – **NTUSER.DAT**
  - **mstsc.exe** Remote Desktop Client execution
  - Last Time Executed
  - Number of Times Executed
- RecentApps – **NTUSER.DAT**
  - **mstsc.exe** Remote Desktop Client execution
  - Last Time Executed
  - Number of Times Executed
  - RecentItems subkey tracks connection destinations and times

FILE SYSTEM

- Jumplists – **C:\Users\<Username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\**
  - **{MSTSC-APPID}-automaticDestinations-ms**
  - Tracks remote desktop connection destination and times
- Prefetch – **C:\Windows\Prefetch\**
  - **mstsc.exe-{hash}.pf**
- Bitmap Cache – **C:\USERS\<USERNAME>\AppData\Local\Microsoft\Terminal Server Client\Cache**
  - **bcache##.bmc**
  - **cache####.bin**

DESTINATION

EVENT LOGS

- **Security Event Log** – **security.evtx**
  - **4624** Logon Type 10
    - Source IP/Logon User Name
  - **4778/4779**
    - IP Address of Source/Source System Name
    - Logon User Name
- **Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx**
  - **131** – Connection Attempts
    - Source IP
  - **98** – Successful Connections
- **Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx**
  - **1149**
    - Source IP/Logon User Name
      - Blank user name may indicate use of Sticky Keys
- **Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx**
  - **21, 22, 25**
    - Source IP/Logon User Name
  - **41**
    - Logon User Name

REGISTRY

- ShimCache – **SYSTEM**
  - **rdpclip.exe**
  - **tstheme.exe**
- **AmCache.hve** – First Time Executed
  - **rdpclip.exe**
  - **tstheme.exe**

FILE SYSTEM

- Prefetch – **C:\Windows\Prefetch\**
  - **rdpclip.exe-{hash}.pf**
  - **tstheme.exe-{hash}.pf**

Map Network Shares (net.exe) to C$ or Admin$

EVENT LOGS

- **security.evtx**
  - **4648** – Logon specifying

REGISTRY

- MountPoints2 – Remotely mapped shares
  - **NTUSER\Software\Microsoft\Windows\**

FILE SYSTEM

- **Prefetch** – **C:\Windows\Prefetch\**
  - **net.exe-{hash}.pf**

EVENT LOGS

- **Security Event Log** – **security.evtx**
- **4768** – TGT Granted
  - Source Host Name/Logon User

REGISTRY

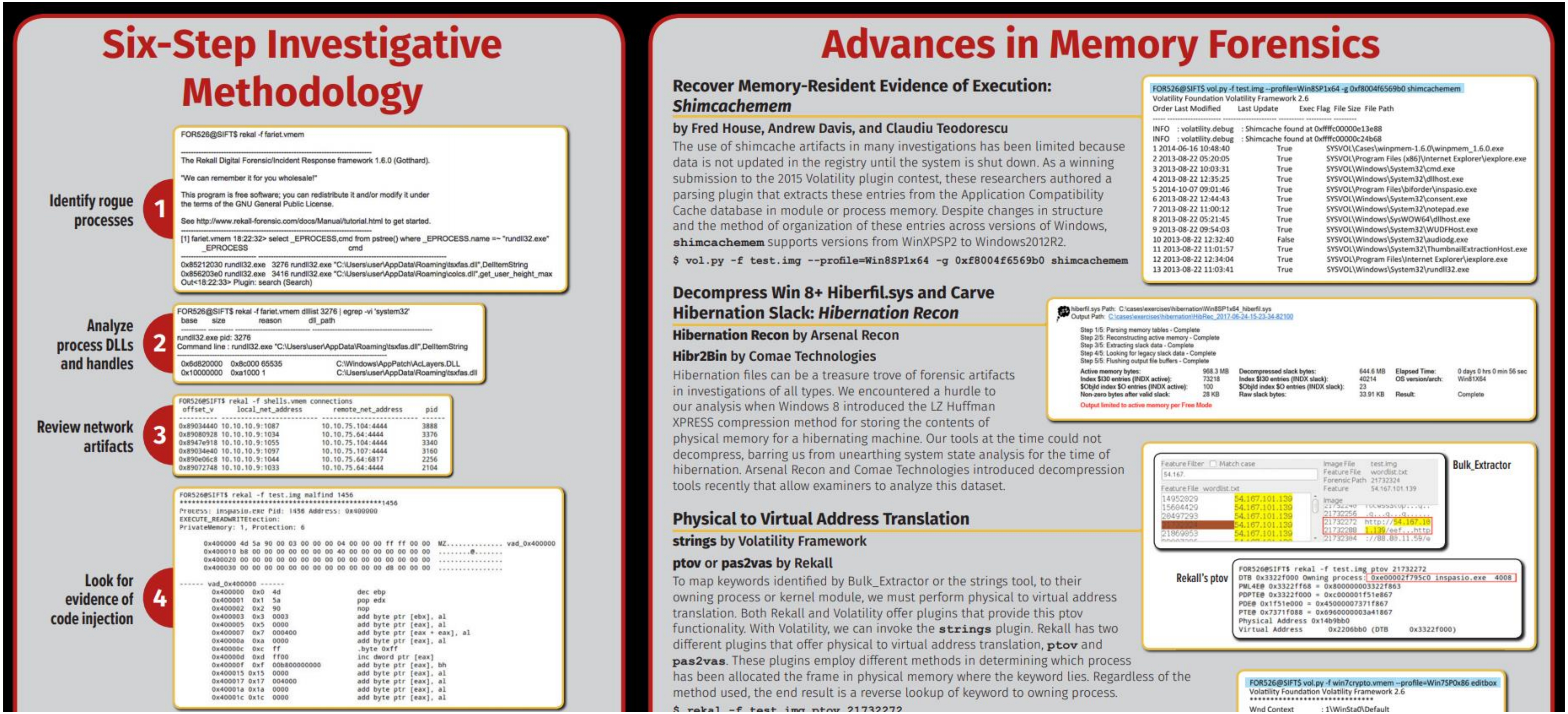
FILE SYSTEM

- File Creation
  - Attacker's files (malware) copied to

Source https://www.sans.org/security-resources/posters/hunt-evil/165/download

Guides and Cheat Sheet

SANS Memory Forensics Analysis Poster provides great condensed know-how



Six-Step Investigative Methodology

1 Identify rogue processes

```
FOR526@SIFT$ rekal -f fariet.vmem

----------------------------------------------------------------------
The Rekall Digital Forensic/Incident Response framework 1.6.0 (Gotthard).

"We can remember it for you wholesale!"

This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License.

See http://www.rekall-forensic.com/docs/Manual/tutorial.html to get started.
----------------------------------------------------------------------
[1] fariet.vmem 18:22:32> select _EPROCESS,cmd from pstree() where _EPROCESS.name =~ "rundll32.exe"
        _EPROCESS                                    cmd
-------------------------- ------------------------------------------------------------
0x85212030 rundll32.exe   3276 rundll32.exe "C:\Users\user\AppData\Roaming\tsxfas.dll",DelItemString
0x856203e0 rundll32.exe   3416 rundll32.exe "C:\Users\user\AppData\Roaming\colcs.dll",get_user_height_max
Out<18:22:33> Plugin: search (Search)
```

2 Analyze process DLLs and handles

```
FOR526@SIFT$ rekal -f fariet.vmem dlllist 3276 | egrep -vi 'system32'
 base       size         reason          dll_path
---------- ---------- ------------------- ------------------------------
rundll32.exe pid: 3276
Command line : rundll32.exe "C:\Users\user\AppData\Roaming\tsxfas.dll",DelItemString
------------------------------------------------------------------------
 0x6d820000  0x8c000 65535            C:\Windows\AppPatch\AcLayers.DLL
 0x10000000  0xa1000 1                C:\Users\user\AppData\Roaming\tsxfas.dll
```

3 Review network artifacts

```
FOR526@SIFT$ rekal -f shells.vmem connections
 offset_v     local_net_address        remote_net_address      pid
---------- ---------------------- ----------------------- ------
0x89034440 10.10.10.9:1087         10.10.75.104:4444       3888
0x89080928 10.10.10.9:1034         10.10.75.64:4444        3376
0x8947e918 10.10.10.9:1055         10.10.75.104:4444       3340
0x89034e40 10.10.10.9:1097         10.10.75.107:4444       3160
0x890e06c8 10.10.10.9:1044         10.10.75.64:6817        2256
0x89072748 10.10.10.9:1033         10.10.75.64:4444        2104
```

4 Look for evidence of code injection

```
FOR526@SIFT$ rekal -f test.img malfind 1456
**************************************************1456
Process: inspasio.exe Pid: 1456 Address: 0x400000
EXECUTE_READWRITEtection:
PrivateMemory: 1, Protection: 6

      0x400000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.............. vad_0x400000
      0x400010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ........@.......
      0x400020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
      0x400030 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00  ................

------ vad_0x400000 ------
       0x400000  0x0  4d                    dec ebp
       0x400001  0x1  5a                    pop edx
       0x400002  0x2  90                    nop
       0x400003  0x3  0003                  add byte ptr [ebx], al
       0x400005  0x5  0000                  add byte ptr [eax], al
       0x400007  0x7  000400                add byte ptr [eax + eax], al
       0x40000a  0xa  0000                  add byte ptr [eax], al
       0x40000c  0xc  ff                    .byte 0xff
       0x40000d  0xd  ff00                  inc dword ptr [eax]
       0x40000f  0xf  00b800000000          add byte ptr [eax], bh
       0x400015 0x15  0000                  add byte ptr [eax], al
       0x400017 0x17  004000                add byte ptr [eax], al
       0x40001a 0x1a  0000                  add byte ptr [eax], al
       0x40001c 0x1c  0000                  add byte ptr [eax], al
```

Advances in Memory Forensics

Recover Memory-Resident Evidence of Execution: *Shimcachemem*

by Fred House, Andrew Davis, and Claudiu Teodorescu

The use of shimcache artifacts in many investigations has been limited because data is not updated in the registry until the system is shut down. As a winning submission to the 2015 Volatility plugin contest, these researchers authored a parsing plugin that extracts these entries from the Application Compatibility Cache database in module or process memory. Despite changes in structure and the method of organization of these entries across versions of Windows, **shimcachemem** supports versions from WinXPSP2 to Windows2012R2.

```
$ vol.py -f test.img --profile=Win8SP1x64 -g 0xf8004f6569b0 shimcachemem
```

```
FOR526@SIFT$ vol.py -f test.img --profile=Win8SP1x64 -g 0xf8004f6569b0 shimcachemem
Volatility Foundation Volatility Framework 2.6
Order Last Modified       Last Update        Exec Flag  File Size  File Path
----- ------------------- ------------------- --------- ---------- ---------
INFO   : volatility.debug   : Shimcache found at 0xffffc00000e13e88
INFO   : volatility.debug   : Shimcache found at 0xffffc00000c24b68
1 2014-06-16 10:48:40              True          SYSVOL\Cases\winpmem-1.6.0\winpmem_1.6.0.exe
2 2013-08-22 05:20:05              True          SYSVOL\Program Files (x86)\Internet Explorer\iexplore.exe
3 2013-08-22 10:03:31              True          SYSVOL\Windows\System32\cmd.exe
4 2013-08-22 12:35:25              True          SYSVOL\Windows\System32\dllhost.exe
5 2014-10-07 09:01:46              True          SYSVOL\Program Files\biforder\inspasio.exe
6 2013-08-22 12:44:43              True          SYSVOL\Windows\System32\consent.exe
7 2013-08-22 11:00:12              True          SYSVOL\Windows\System32\notepad.exe
8 2013-08-22 05:21:45              True          SYSVOL\Windows\SysWOW64\dllhost.exe
9 2013-08-22 09:54:03              True          SYSVOL\Windows\System32\WUDFHost.exe
10 2013-08-22 12:32:40             False         SYSVOL\Windows\System32\audiodg.exe
11 2013-08-22 11:01:57             True          SYSVOL\Windows\System32\ThumbnailExtractionHost.exe
12 2013-08-22 12:34:04             True          SYSVOL\Program Files\Internet Explorer\iexplore.exe
13 2013-08-22 11:03:41             True          SYSVOL\Windows\System32\rundll32.exe
```

Decompress Win 8+ Hiberfil.sys and Carve Hibernation Slack: *Hibernation Recon*

Hibernation Recon by Arsenal Recon

Hibr2Bin by Comae Technologies

Hibernation files can be a treasure trove of forensic artifacts in investigations of all types. We encountered a hurdle to our analysis when Windows 8 introduced the LZ Huffman XPRESS compression method for storing the contents of physical memory for a hibernating machine. Our tools at the time could not decompress, barring us from unearthing system state analysis for the time of hibernation. Arsenal Recon and Comae Technologies introduced decompression tools recently that allow examiners to analyze this dataset.

```
hiberfil.sys Path:  C:\cases\exercises\hibernation\Win8SP1x64_hiberfil.sys
Output Path:  C:\cases\exercises\hibernation\HibRec_2017-06-24-15-23-34-82100

  Step 1/5: Parsing memory tables - Complete
  Step 2/5: Reconstructing active memory - Complete
  Step 3/5: Extracting slack data - Complete
  Step 4/5: Looking for legacy slack data - Complete
  Step 5/5: Flushing output file buffers - Complete
  Active memory bytes:                  968.3 MB   Decompressed slack bytes:             644.6 MB   Elapsed Time:      0 days 0 hrs 0 min 56 sec
  Index $I30 entries (INDX active):     73218      Index $I30 entries (INDX slack):      40214      OS version/arch:   Win81X64
  $ObjId index $O entries (INDX active): 100       $ObjId index $O entries (INDX slack): 23
  Non-zero bytes after valid slack:     28 KB      Raw slack bytes:                      33.91 KB   Result:            Complete
  Output limited to active memory per Free Mode
```

Physical to Virtual Address Translation

strings by Volatility Framework

ptov or **pas2vas** by Rekall

To map keywords identified by Bulk_Extractor or the strings tool, to their owning process or kernel module, we must perform physical to virtual address translation. Both Rekall and Volatility offer plugins that provide this ptov functionality. With Volatility, we can invoke the **strings** plugin. Rekall has two different plugins that offer physical to virtual address translation, **ptov** and **pas2vas**. These plugins employ different methods in determining which process has been allocated the frame in physical memory where the keyword lies. Regardless of the method used, the end result is a reverse lookup of keyword to owning process.

```
$ rekal -f test.img ptov 21732272
```

Bulk_Extractor

```
Feature Filter  □ Match case          Image File      test.img
54.167.                               Feature File    wordlist.txt
                                      Forensic Path   21732324
Feature File  wordlist.txt            Feature         54.167.101.139
14952029          54.167.101.139      Image
15604429          54.167.101.139      21732256  .q...q...q......
20497293          54.167.101.139      21732272  http://54.167.10
[illegible]       54.167.101.139      21732288  1.139/eef...http
21869053          54.167.101.139      21732304  ://88.89.11.59/e
```

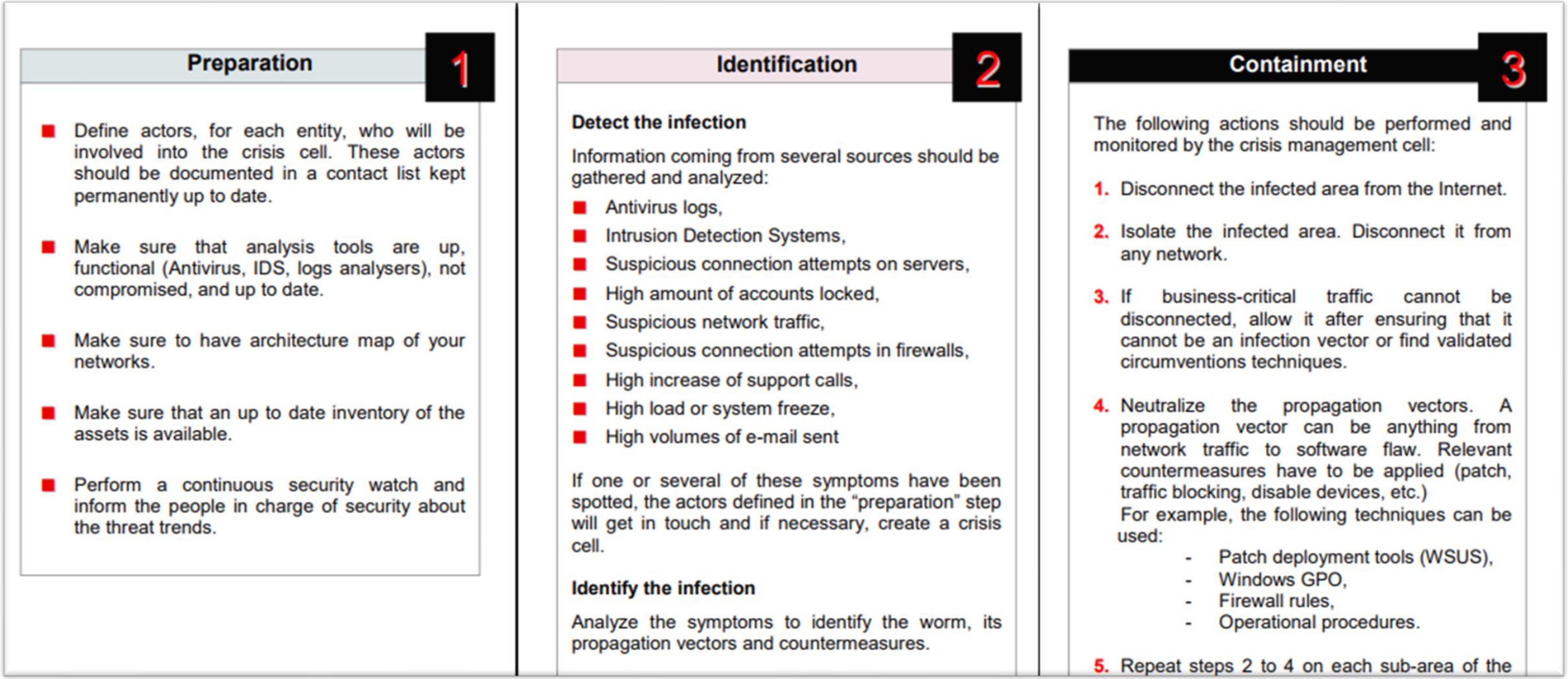
Rekall's ptov

```
FOR526@SIFT$ rekal -f test.img ptov 21732272
DTB 0x3322f000 Owning process: 0xe00002f795c0 inspasio.exe  4008
PML4E@ 0x3322ff68 = 0x800000003322f863
PDPTE@ 0x3322f000 = 0xc000001f51e867
PDE@ 0x1f51e000 = 0x45000007371f867
PTE@ 0x7371f088 = 0x6960000003a41867
Physical Address 0x14b9bb0
Virtual Address      0x2206bb0 (DTB     0x3322f000)
```

```
FOR526@SIFT$ vol.py -f win7crypto.vmem --profile=Win7SP0x86 editbox
Volatility Foundation Volatility Framework 2.6
******************************
Wnd Context           : 1\WinSta0\Default
```

Guides and Cheat Sheet

Societe General generic IR playbooks (e.g. IRM-1-WormInfection)



Preparation 1

- Define actors, for each entity, who will be involved into the crisis cell. These actors should be documented in a contact list kept permanently up to date.
- Make sure that analysis tools are up, functional (Antivirus, IDS, logs analysers), not compromised, and up to date.
- Make sure to have architecture map of your networks.
- Make sure that an up to date inventory of the assets is available.
- Perform a continuous security watch and inform the people in charge of security about the threat trends.

Identification 2

Detect the infection

Information coming from several sources should be gathered and analyzed:

- Antivirus logs,
- Intrusion Detection Systems,
- Suspicious connection attempts on servers,
- High amount of accounts locked,
- Suspicious network traffic,
- Suspicious connection attempts in firewalls,
- High increase of support calls,
- High load or system freeze,
- High volumes of e-mail sent

If one or several of these symptoms have been spotted, the actors defined in the "preparation" step will get in touch and if necessary, create a crisis cell.

Identify the infection

Analyze the symptoms to identify the worm, its propagation vectors and countermeasures.

Containment 3

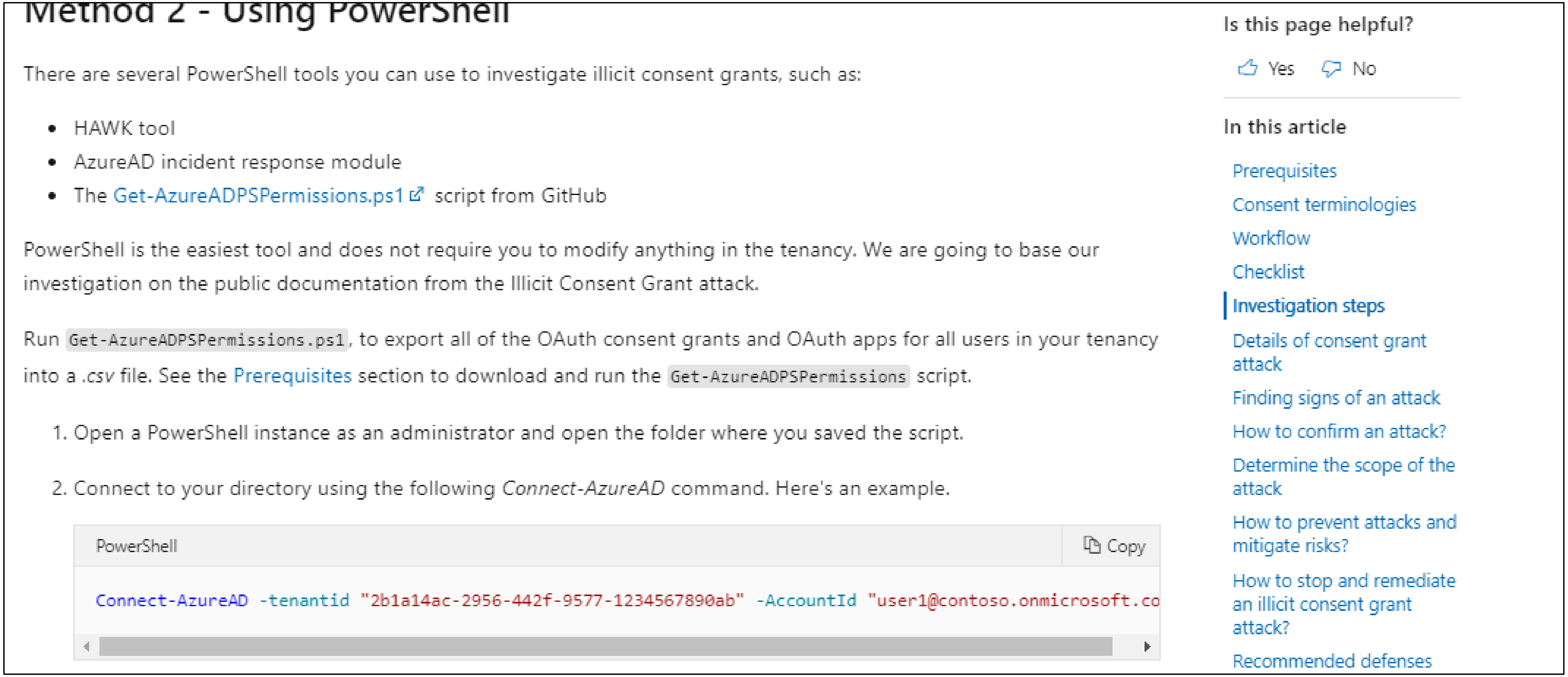
The following actions should be performed and monitored by the crisis management cell:

1. Disconnect the infected area from the Internet.
2. Isolate the infected area. Disconnect it from any network.
3. If business-critical traffic cannot be disconnected, allow it after ensuring that it cannot be an infection vector or find validated circumventions techniques.
4. Neutralize the propagation vectors. A propagation vector can be anything from network traffic to software flaw. Relevant countermeasures have to be applied (patch, traffic blocking, disable devices, etc.)
   For example, the following techniques can be used:
   - Patch deployment tools (WSUS),
   - Windows GPO,
   - Firewall rules,
   - Operational procedures.
5. Repeat steps 2 to 4 on each sub-area of the

https://github.com/certsocietegenerale/IRM/

Guides and Cheat Sheet

Microsoft App Consent Attack IR Playbook



Method 2 - Using PowerShell

There are several PowerShell tools you can use to investigate illicit consent grants, such as:

- HAWK tool
- AzureAD incident response module
- The Get-AzureADPSPermissions.ps1 script from GitHub

PowerShell is the easiest tool and does not require you to modify anything in the tenancy. We are going to base our investigation on the public documentation from the Illicit Consent Grant attack.

Run `Get-AzureADPSPermissions.ps1`, to export all of the OAuth consent grants and OAuth apps for all users in your tenancy into a *.csv* file. See the Prerequisites section to download and run the `Get-AzureADPSPermissions` script.

1. Open a PowerShell instance as an administrator and open the folder where you saved the script.
2. Connect to your directory using the following *Connect-AzureAD* command. Here's an example.

```
Connect-AzureAD -tenantid "2b1a14ac-2956-442f-9577-1234567890ab" -AccountId "user1@contoso.onmicrosoft.co
```

Is this page helpful?

In this article

Source https://docs.microsoft.com/en-us/security/compass/incident-response-playbook-app-consent

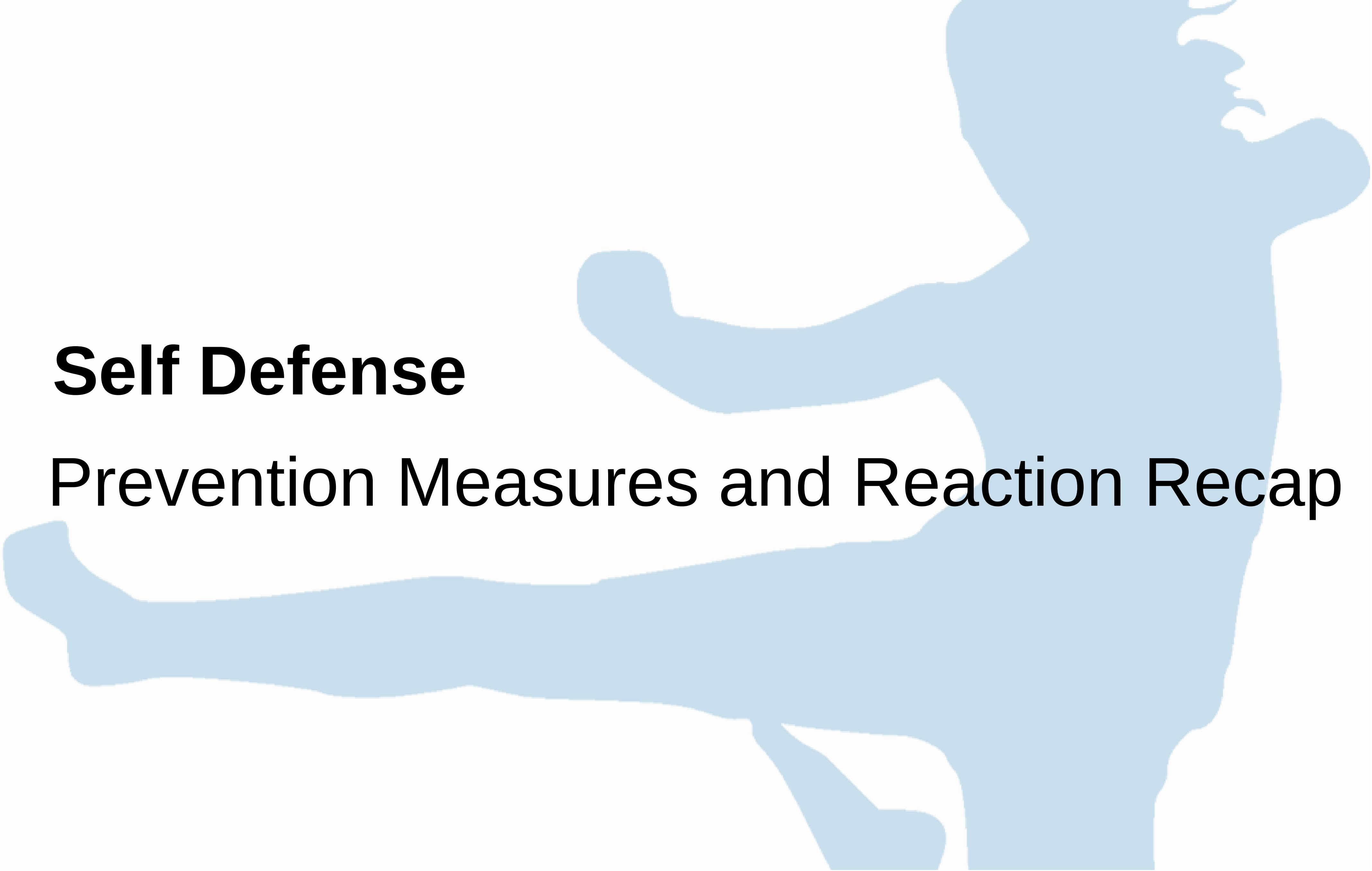
Guides and Cheat Sheets

You will mainly find two sorts of guides and cheat sheets

- How to run the investigation
  - Whom to involve and when
  - Usually generic runbooks / playbooks
  - Must be tailored to the company => Preparation, Forensic Readiness
  - Should be exercised. At least tabletop
- Where to find relevant artifacts
  - Usually, the very technical cheat sheets
  - Do not respect corporate processes

Best Playbooks are a match of both - fit the company crisis management and contain the very specific technical details

… and no, there aren’t any great of-the-shelf playbooks.

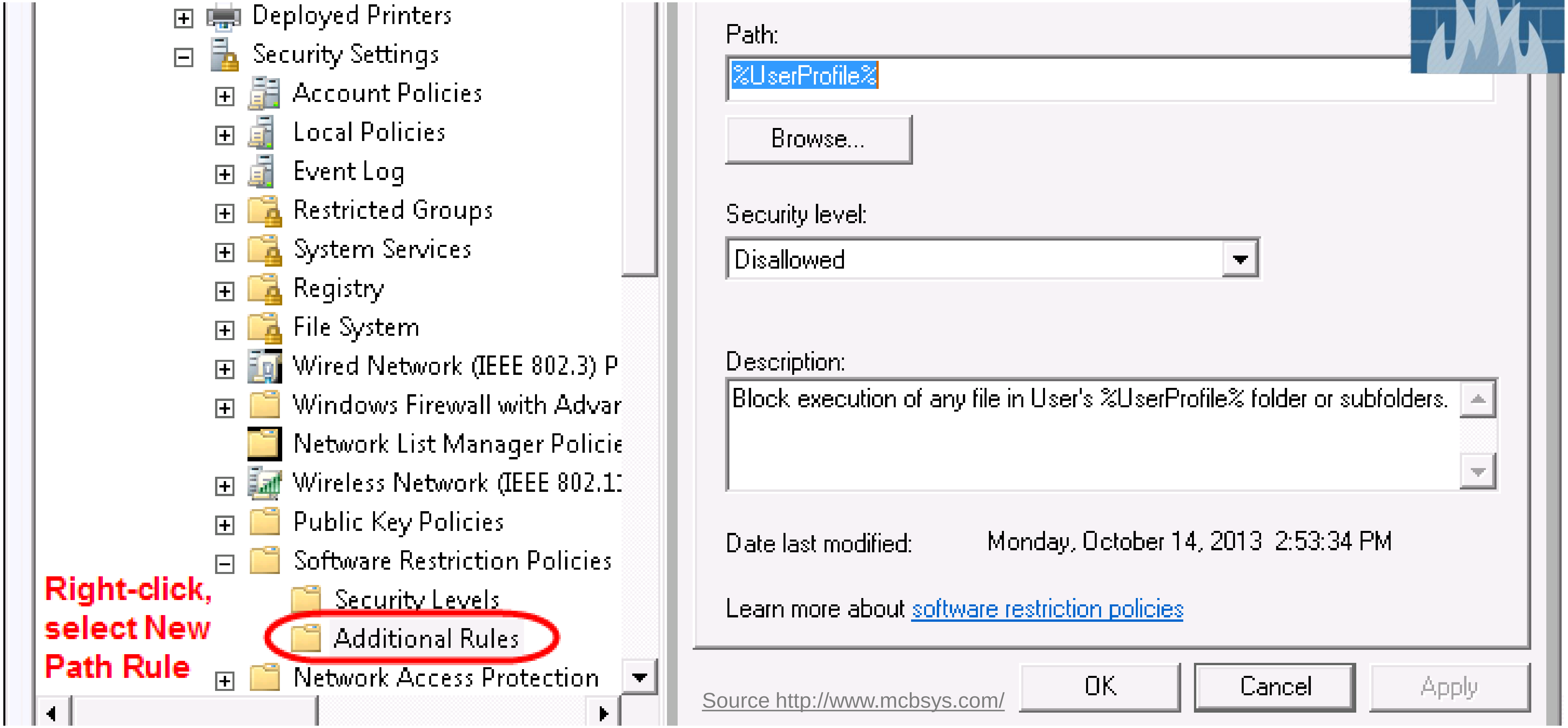


Self Defense

Prevention Measures and Reaction Recap

Protection Mechanisms

Enterprise Measures - Prevent Execution in %UserProfile%



Right-click, select New Path Rule

Path: %UserProfile%

Security level: Disallowed

Description: Block execution of any file in User's %UserProfile% folder or subfolders.

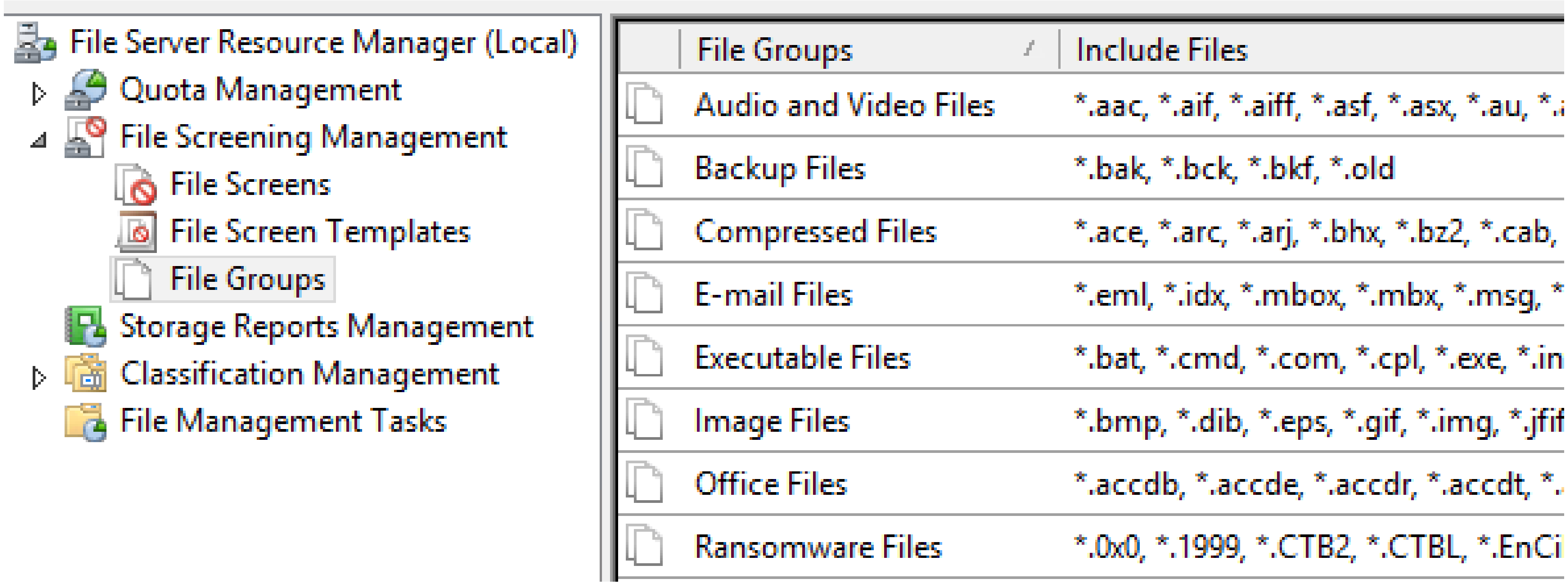
Date last modified: Monday, October 14, 2013 2:53:34 PM

Learn more about software restriction policies

Source http://www.mcbsys.com/

Protection Mechanisms

Enterprise Measures - Detect Ransomware Files and Block Share Access



- File Server Resource Manager (Local)
  - Quota Management
  - File Screening Management
    - File Screens
    - File Screen Templates
    - File Groups
  - Storage Reports Management
  - Classification Management
  - File Management Tasks

File Groups	Include Files
Audio and Video Files	*.aac, *.aif, *.aiff, *.asf, *.asx, *.au, *.
Backup Files	*.bak, *.bck, *.bkf, *.old
Compressed Files	*.ace, *.arc, *.arj, *.bhx, *.bz2, *.cab,
E-mail Files	*.eml, *.idx, *.mbox, *.mbx, *.msg, *
Executable Files	*.bat, *.cmd, *.com, *.cpl, *.exe, *.in
Image Files	*.bmp, *.dib, *.eps, *.gif, *.img, *.jfif
Office Files	*.accdb, *.accde, *.accdr, *.accdt, *.
Ransomware Files	*.0x0, *.1999, *.CTB2, *.CTBL, *.EnCi

Launch Command to Block User Access

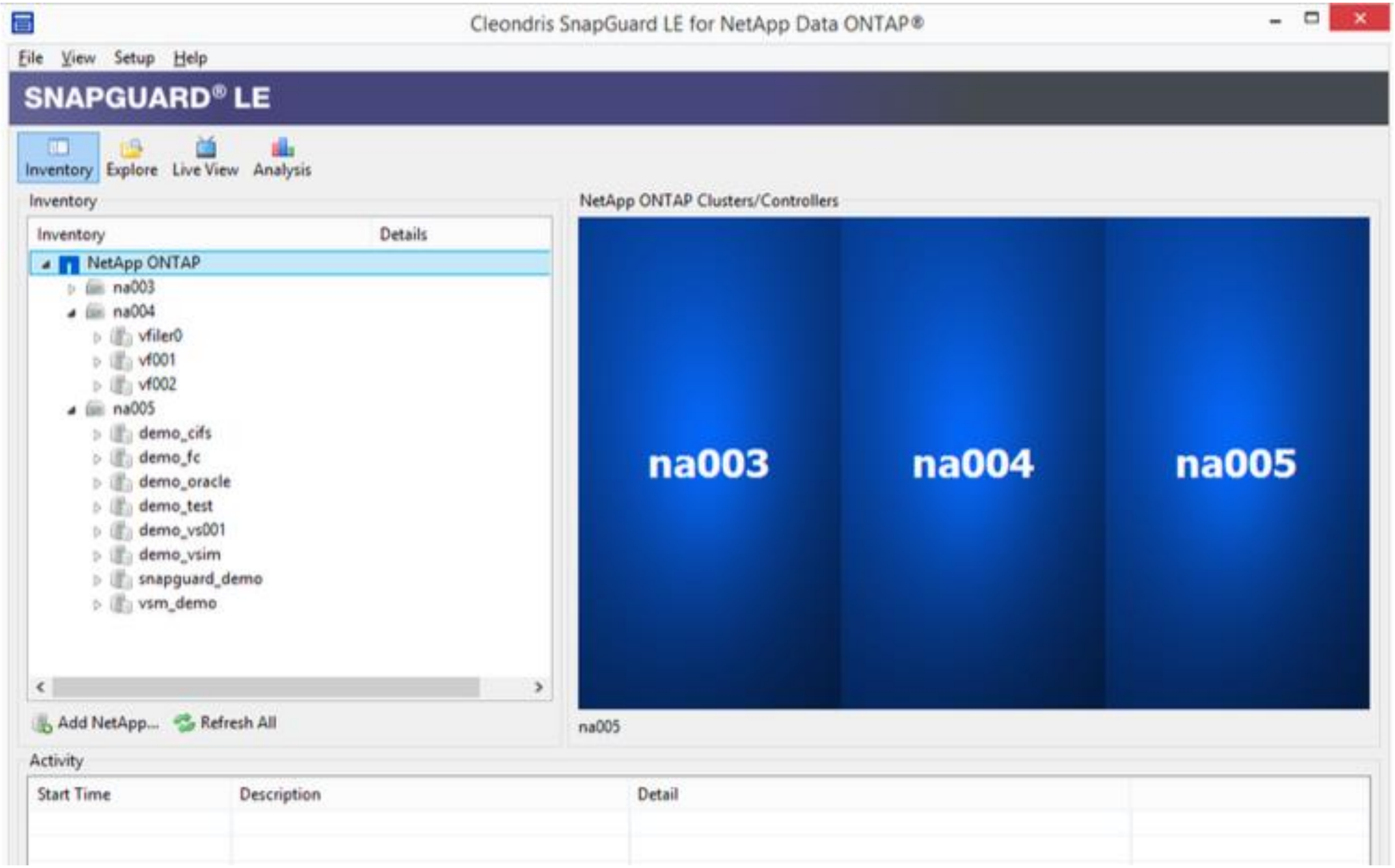
```
-ExecutionPolicy Unrestricted -NoLogo -Command "& { Get-SmbShare -Special $false
| ForEach-Object { Block-SmbShareAccess -Name $_.Name -AccountName '[Source Io
Owner]' -Force } }"
```

https://blog.netwrix.com/2016/04/11/ransomware-protection-using-fsrm-and-powershell/

Protection Mechanisms

Enterprise Measures - Storage Snapguard

Monitors shares and immediately creates snapshots on detection of malicious activity



Protection Mechanisms

Enterprise Measures

- DeviceGuard and Applocker
  - Enforce software and OS integrity and authenticity
  - Enforce application whitelisting

  https://technet.microsoft.com/de-de/library/hh831440.aspx

- E-Mail Enhancements
  - Assure Authenticity of E-Mails by S/MIME Signatures
  - Implement and enforce SPF, DKIM, DMARC
  - Mark external E-Mails as [EXTERNAL] in Subject

Immediate Reaction for Ransomware Cases

Get Offline

- no more Internet, WLAN
- no remote access
- no DNS
- no Internet surfing
- no e-mail

Safe Your Backups

- Get them offline
- Change credentials, enable 2FA

Keep Evidence

- Encrypted files and ransom note, URLs
- VMs, Disks, Memory, Network Dumps
- Work on copies

Recover

- Get Systems isolated and cleaned
- Assure Integrity before re-enabling
- Change Domain, Service and Local Admins
- Cycle krbtgt Account

Guides and Cheat Sheat

How do you keep hashes and tickets for yourself ;)

Connection method	Logon type	Creds	Comments
Log on at console	Interactive	y	Includes hardware remote access / lights-out cards and network KVMs.
RUNAS	Interactive	y	
RUNAS /NETWORK	NewCredentials	y	Clones current LSA session for local access, but uses new credentials when connecting to network resources.
Remote Desktop (success)	RemoteInteractive	y	If the remote desktop client is configured to share local devices and resources, those may be compromised as well.
Remote Desktop (failure - logon type was denied)	RemoteInteractive	-	By default, if RDP logon fails credentials are only stored very briefly. This may not be the case if the computer is compromised.
Net use * \\SERVER	Network	-	
Net use * \\SERVER /u:user	Network	-	
MMC snap-ins to remote computer	Network	-	Example: Computer Management, Event Viewer, Device Manager, Services
PowerShell WinRM	Network	-	Example: Enter-PSSession server
PowerShell WinRM with CredSSP	NetworkClearText	y	New-PSSession server -Authentication Credssp -Credential cred
PsExec without explicit creds	Network	-	Example: PsExec \\server cmd
PsExec with explicit creds	Network + Interactive	y	PsExec \\server -u user -p pwd cmd Creates multiple logon sessions.
Remote Registry	Network	-	
Remote Desktop Gateway	Network	-	Authenticating to Remote Desktop Gateway.
Scheduled task	Batch	y	Password will also be saved as LSA secret on disk.
Run tools as a service	Service	y	Password will also be saved as LSA secret on disk.
Vulnerability scanners	Network	-	Most scanners default to using network logons, though some vendors may implement non-network logons and introduce more credential theft risk.

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Final Conclusion

- we need 2FA!
- keep a copy of what you have => maybe its restorable later on
- how do you restore portions and not to kill latest changes
- need agent based backup with strong protected access
- we need 2FA!
- mind hyper-v domain accounts
- have hunting capabilities?
- how about the correct logs for sufficient long time frame?
- lateral movement detection?
- we need 2FA!

No Ransomware, No Cry (feat. Bob Marley)

COMPASS
SECURITY