McAfee Defender's Blog: Operation Harvest

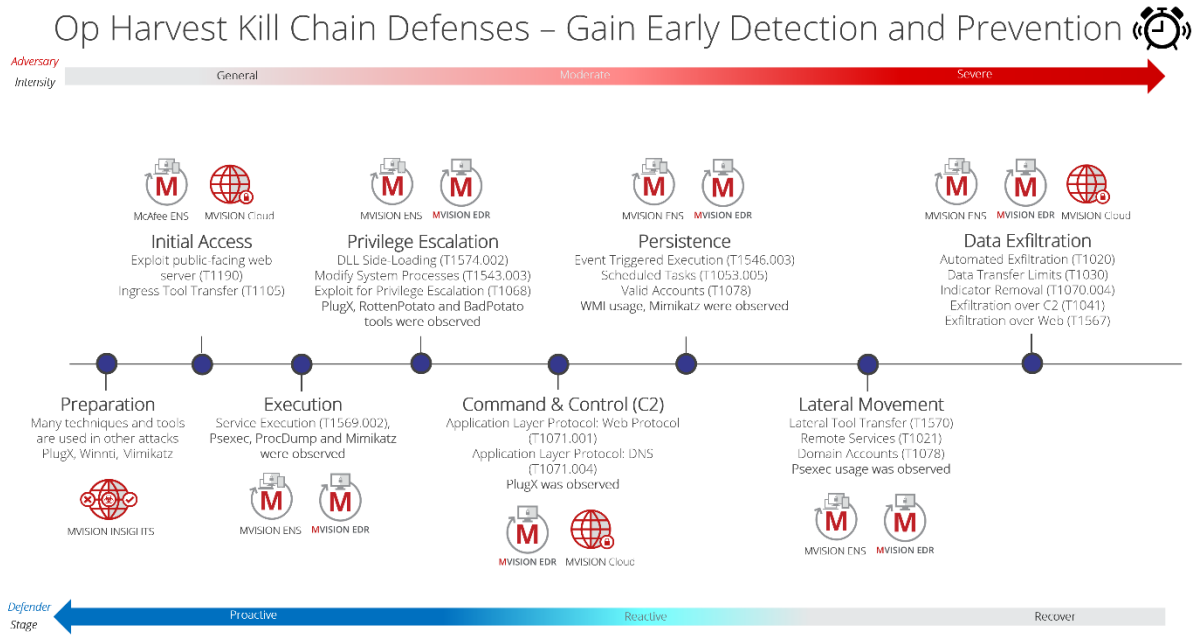
By Mo Cashman, Filippo Sitzia, Taylor Mullins and Nic Stricher

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.

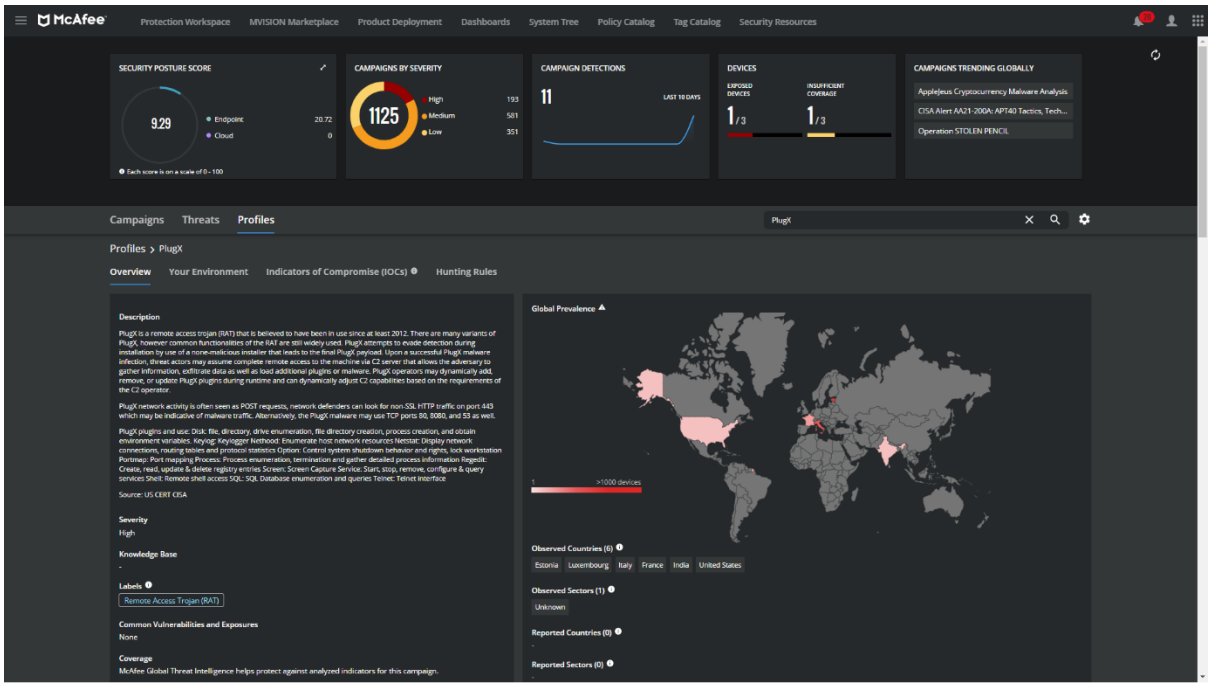


Throughout this blog, we will provide some examples of where MVISION Security Platform could help defend against this type of attack.

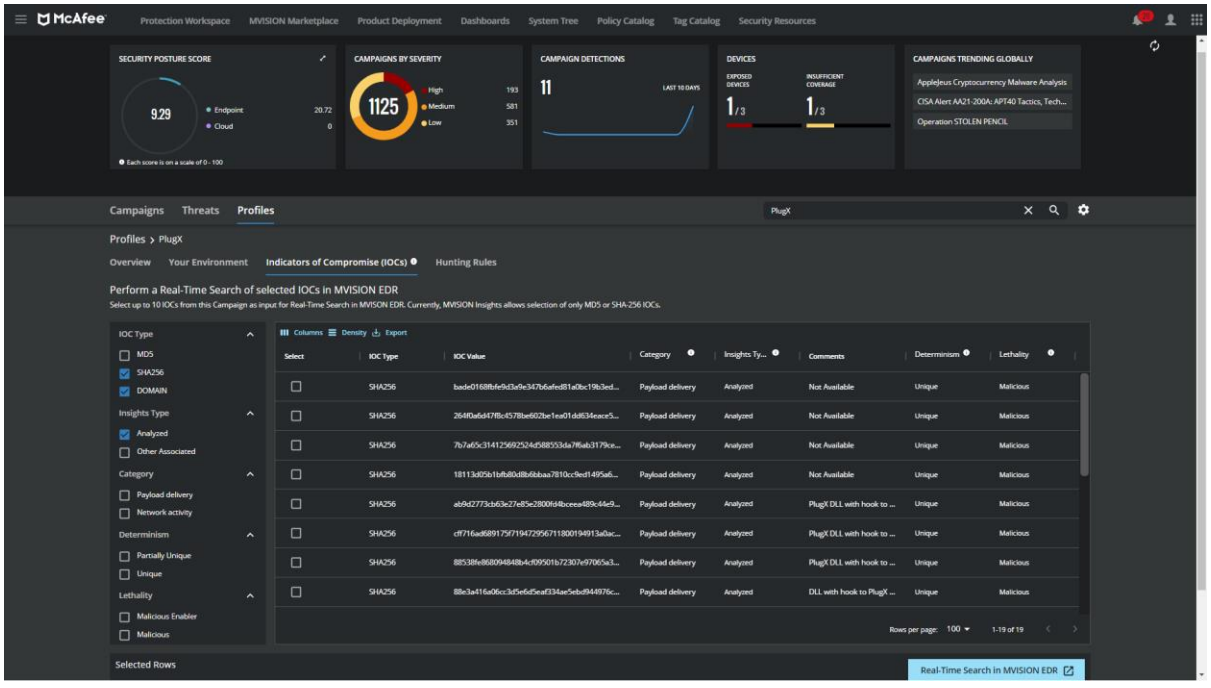
Get Prepared with the Latest Threat Intelligence

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.

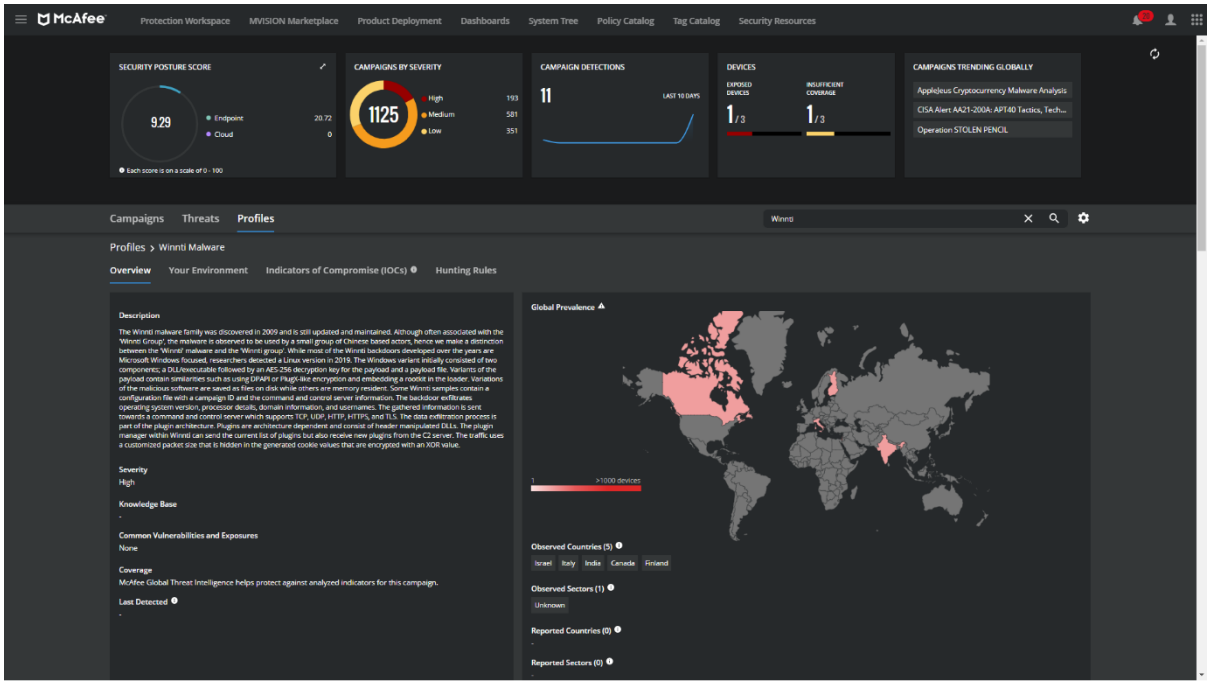
Get a quick overview of the PlugX tool:



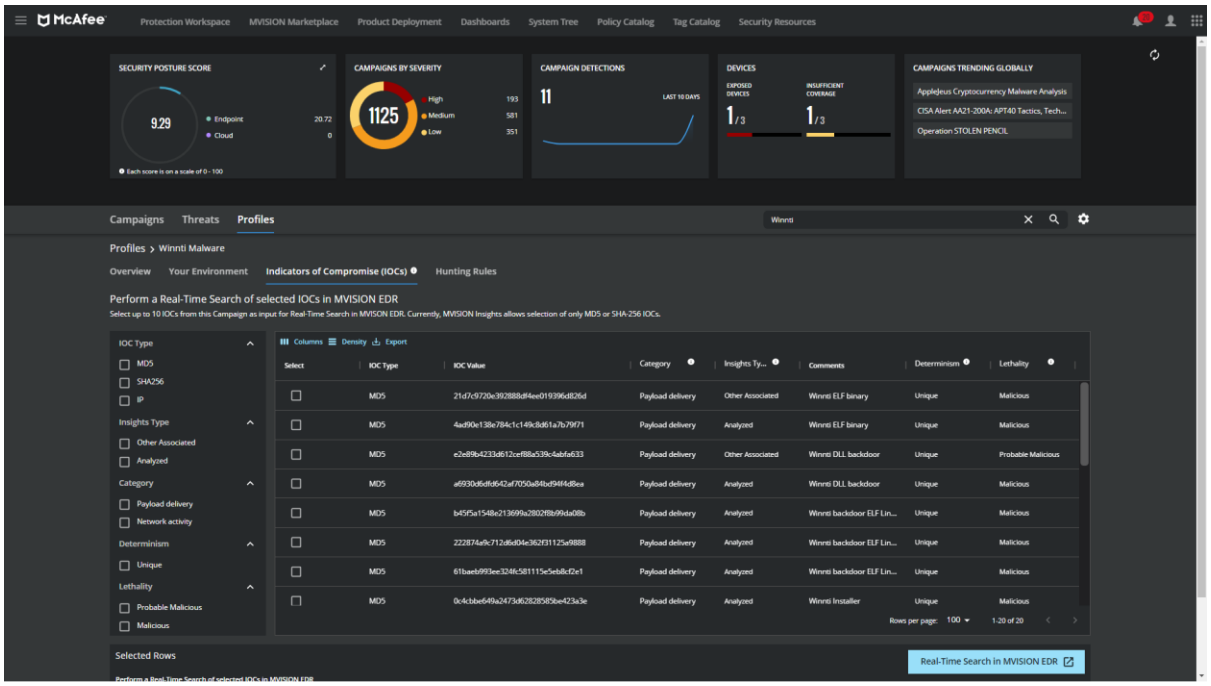
Easily search for or export PlugX IOCs right from MVISION Insights:



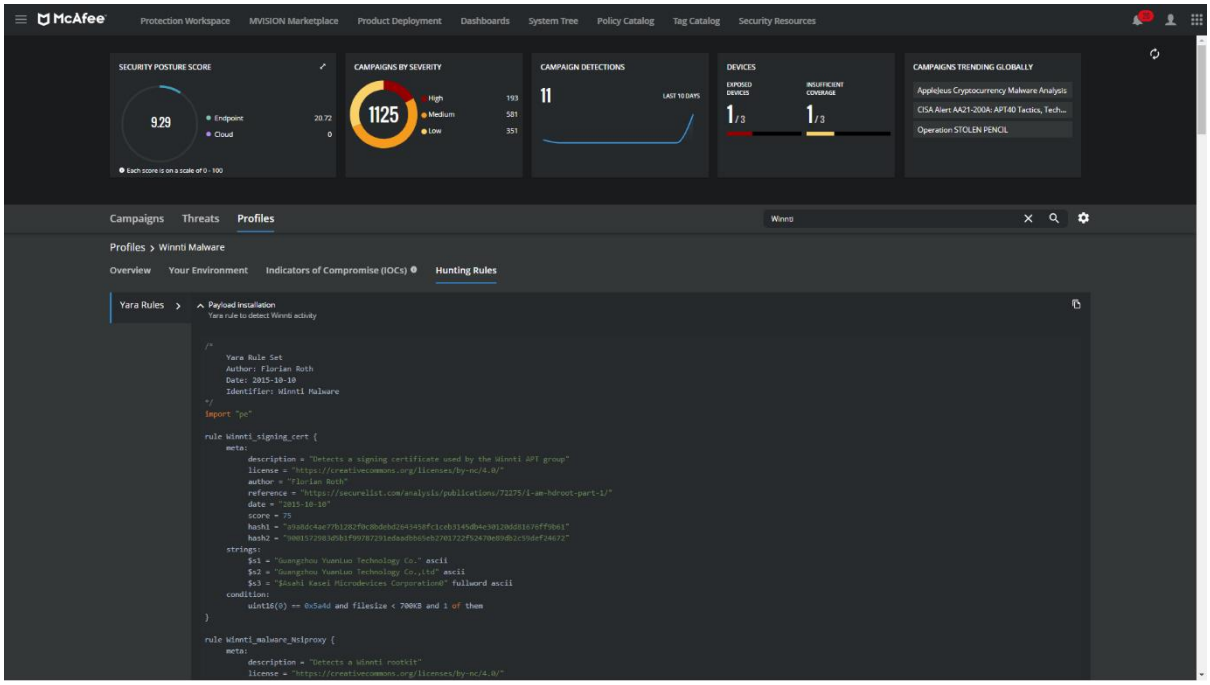
Get a quick overview of the Winnti tool:



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



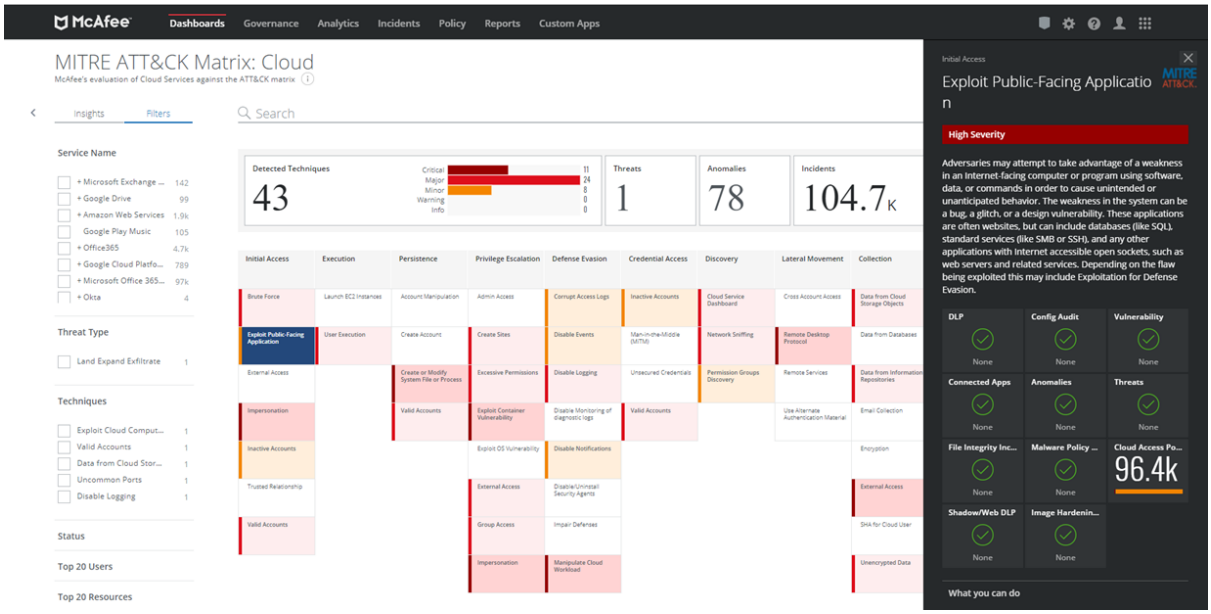
Cross Platform Hunting Rules for Winnti:



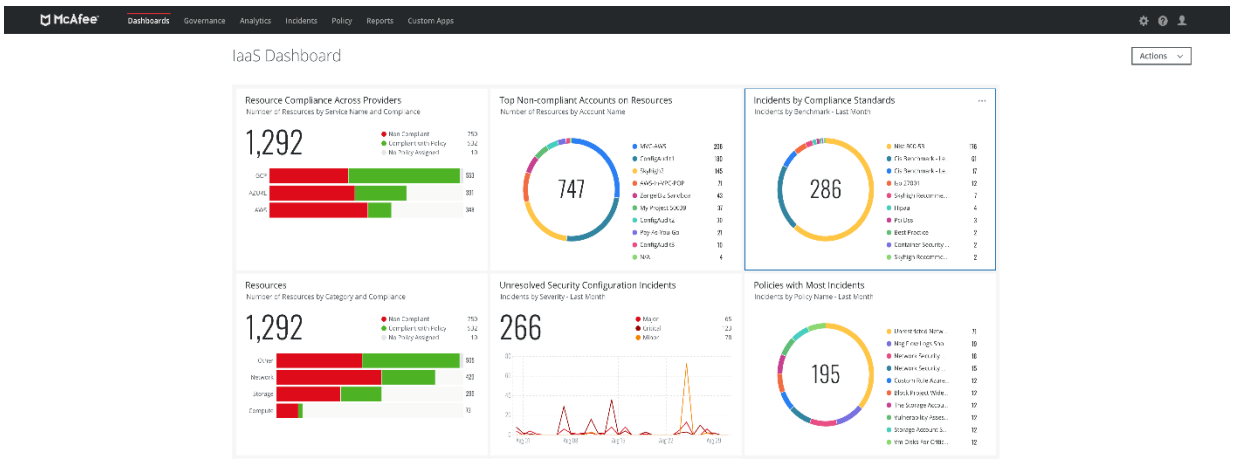
MVISION Insights is also updated with the latest technical intelligence on Operation Harvest including a summary of the threat, prevalence, indicators of compromise and recommended defensive countermeasures.

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.



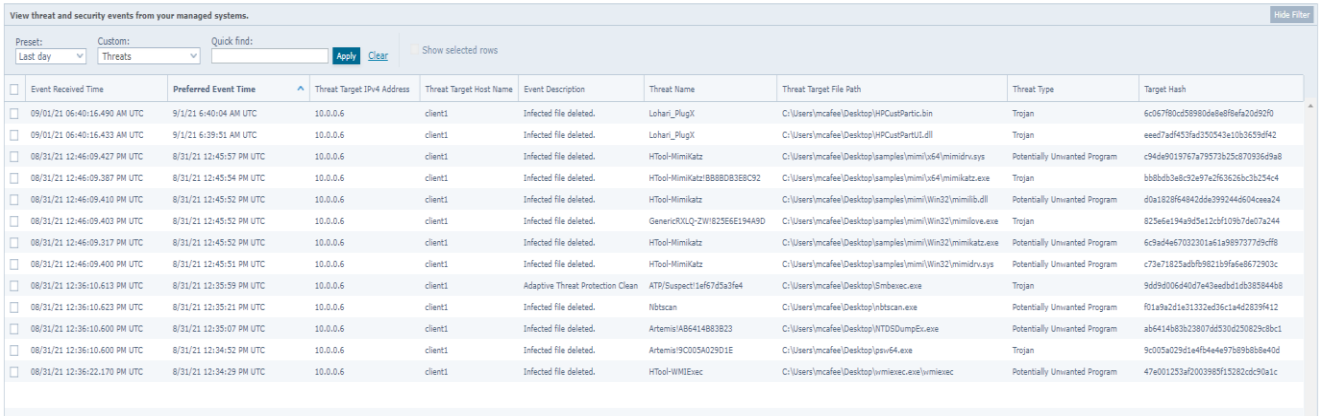
Many customer-facing applications and web servers are hosted on cloud infrastructure. As a Network Defender, gaining visibility and monitoring for misconfigurations on the infrastructure platforms is critical as this is increasingly the entry point for an attacker. MVISION Cloud Native Application Protection 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 Adaptative Threat Prevention Module. The following is a sample of the Threat Event log from ePolicy Orchestrator (ePO) from our testing.

Threat Event Log



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 lsaas

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.

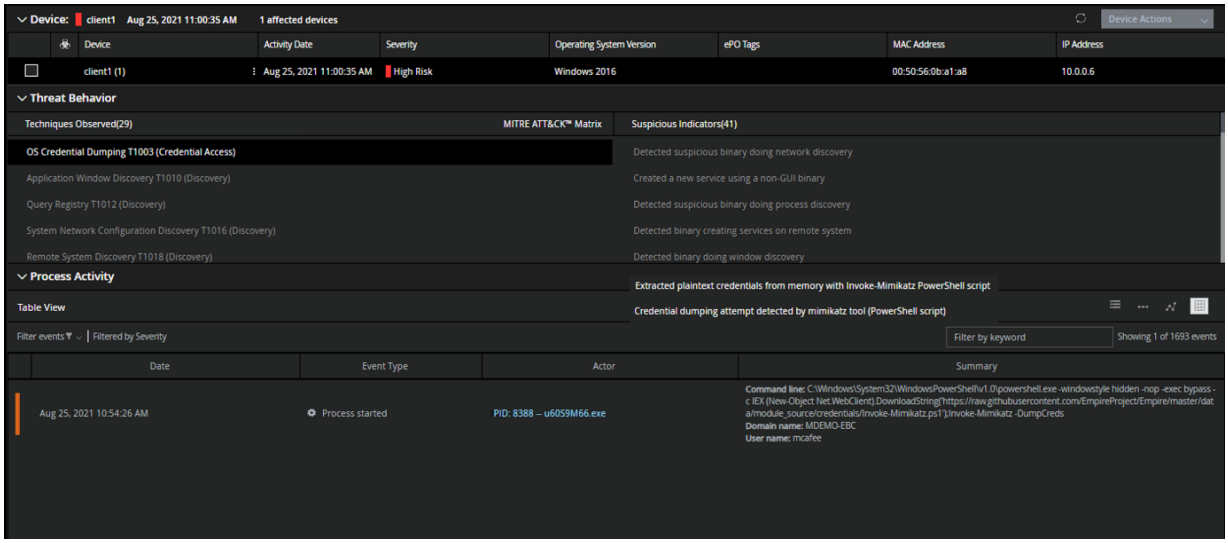
Preventing or Detecting Command and Control

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.

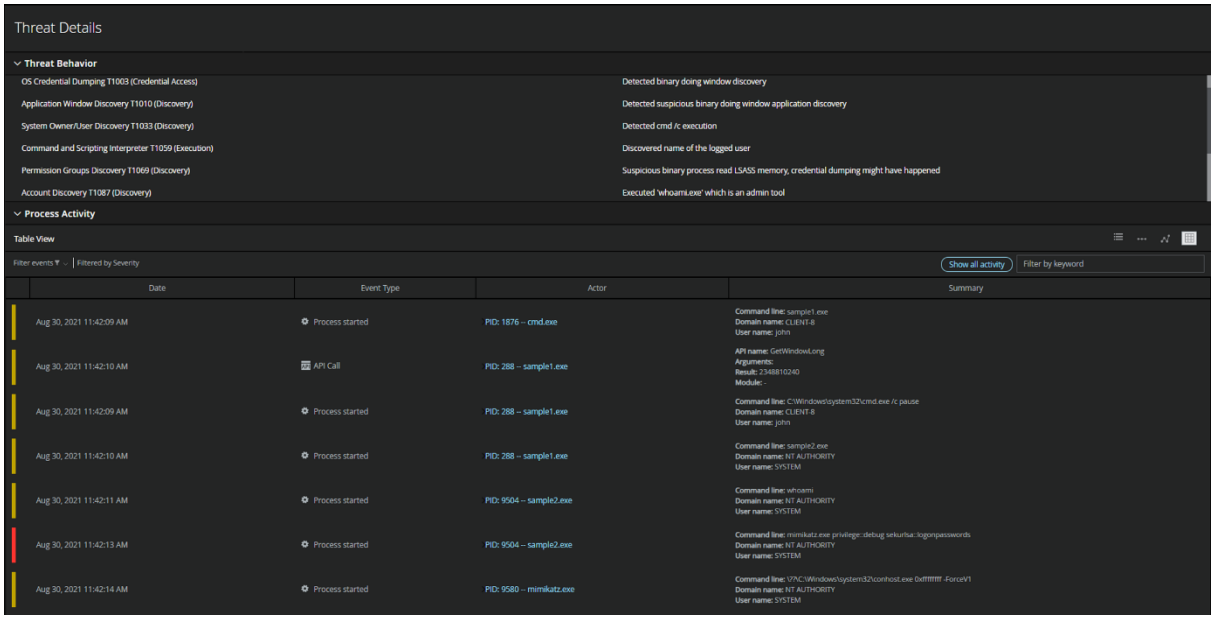
Additionally, Unified Cloud Edge (UCE – SWG) can prevent access to risky web sites using threat intelligence, URL reputation, behaviour analysis and remote browser isolation. Ensure you have a strong web security policy in place and are monitoring logs. This is a great control to identify potentially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

Monitoring for Privilege Escalation

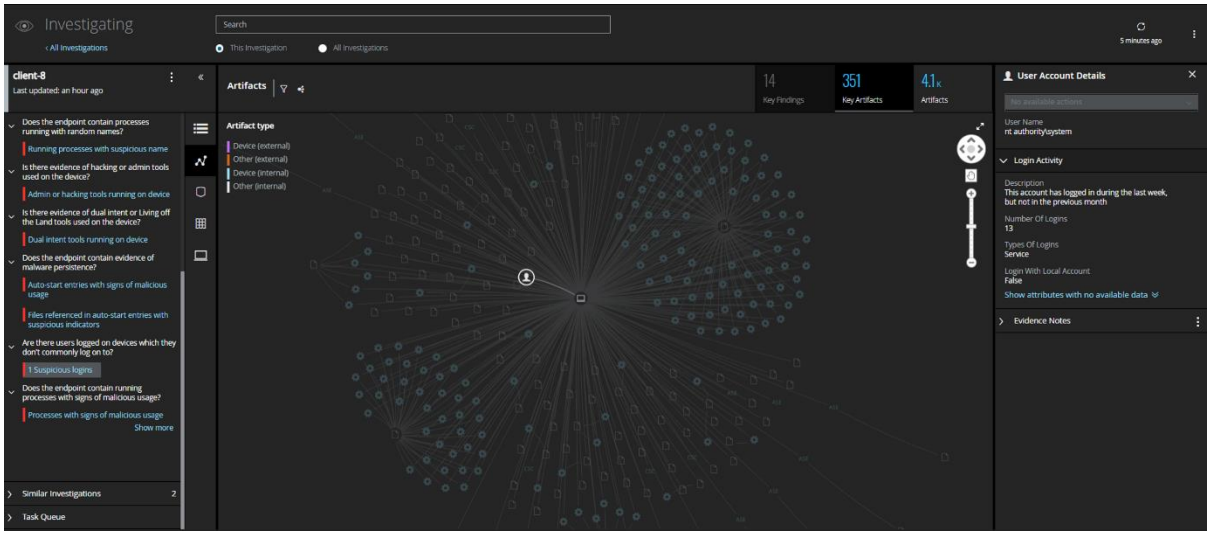
The adversary used several techniques and tools to elevate privileges and run Mimikatz to steal credentials. In our simulation, MVISION EDR proactively identified the attempt to download and execute in memory a Mimikatz PowerShell script.



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."



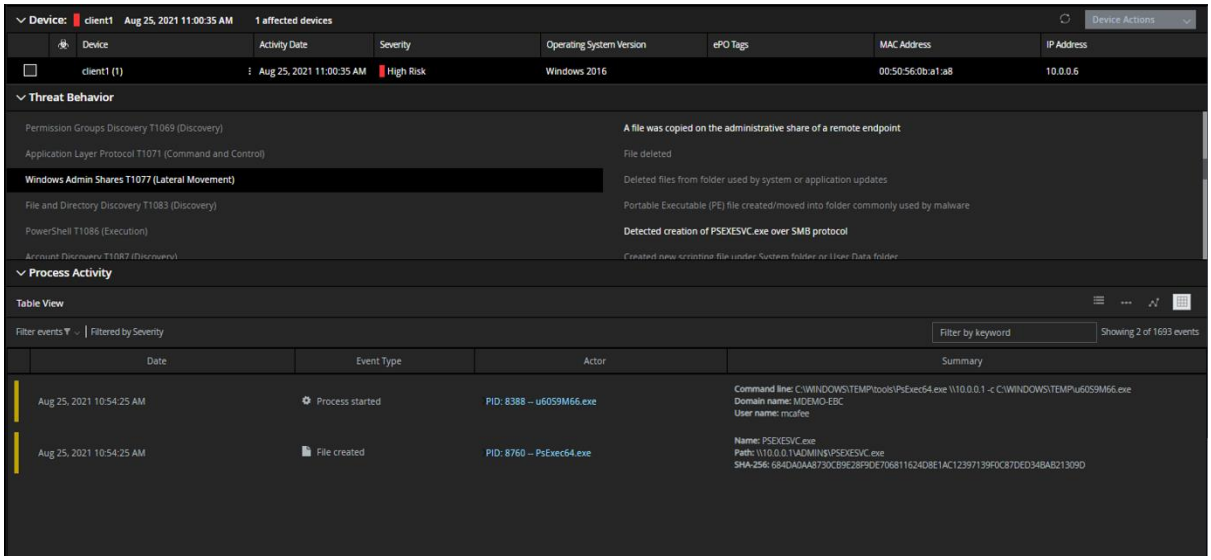
We started a guided investigation on the affected system. Analytics on the data identified anomalies in user behavior. Guided investigations make easier to visualize complex data sets and interconnections between artifacts and systems.



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.

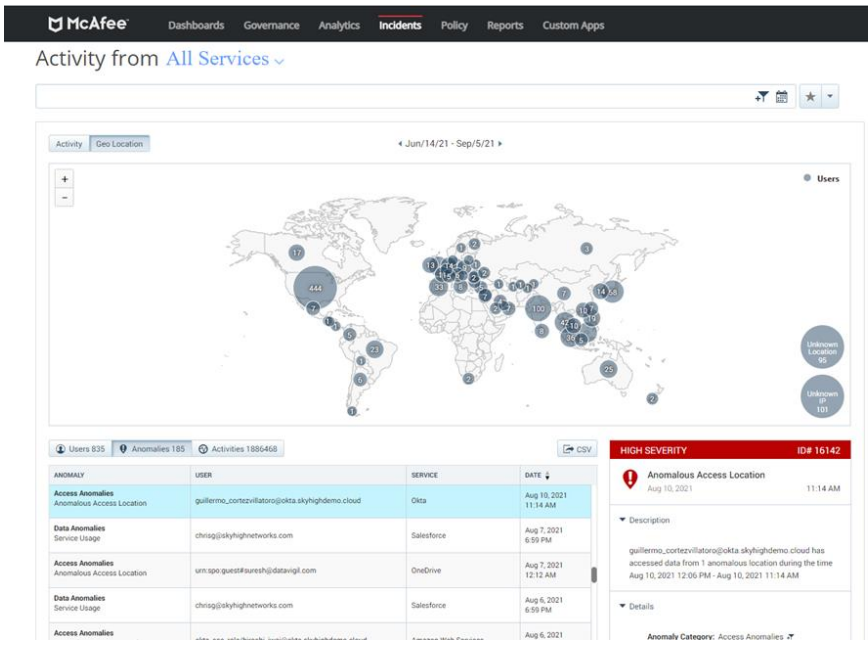
Psexec.exe used for lateral movement:



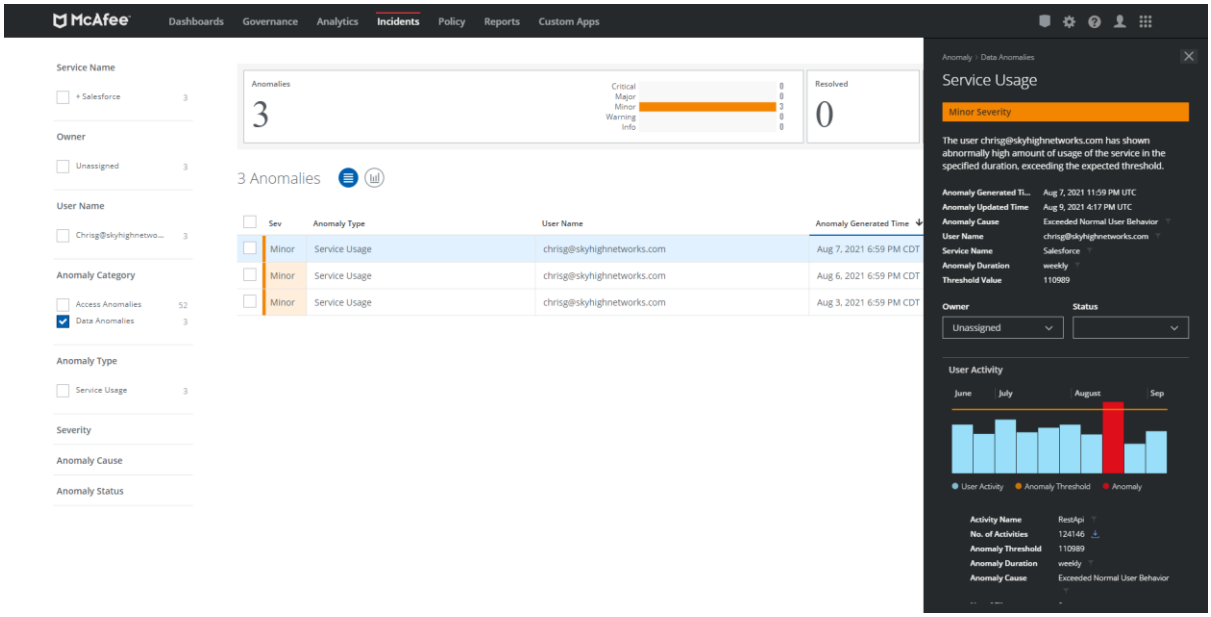
Mapping User and Data Anomalies to Detect Exfiltration

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:



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.