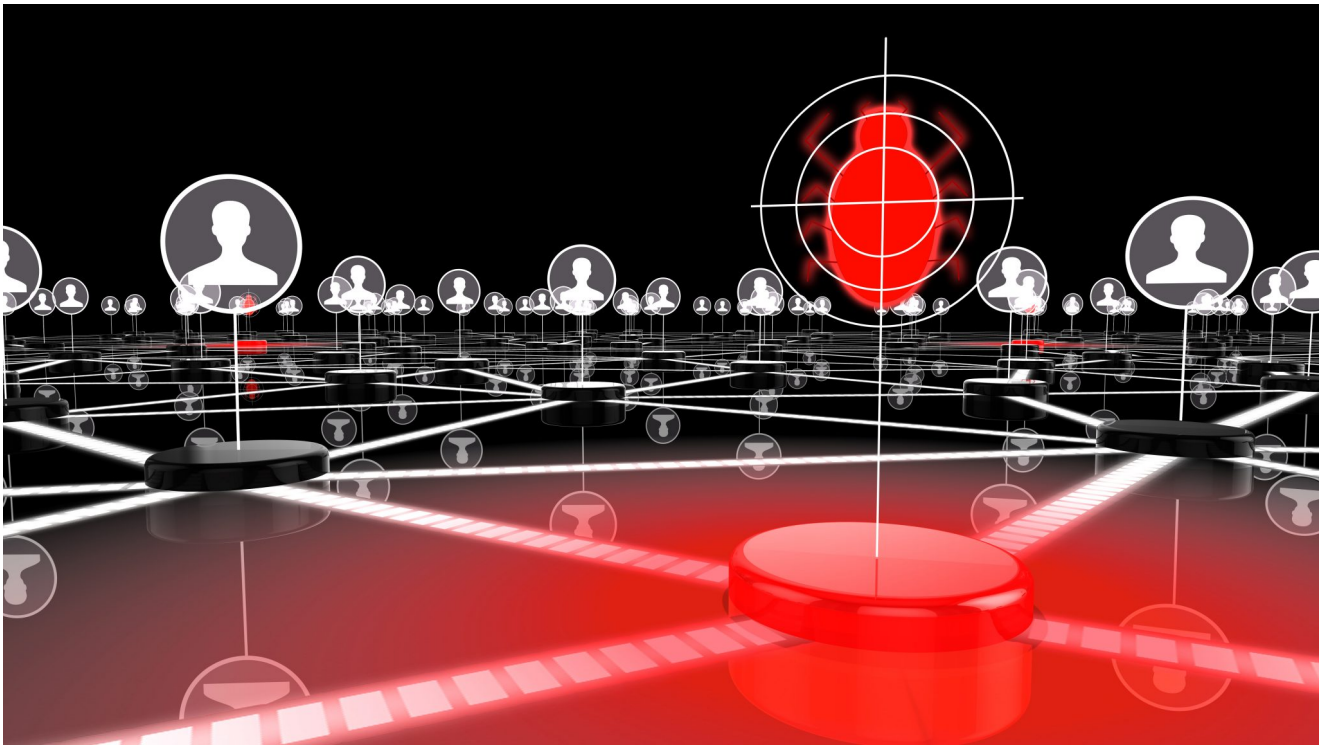
How A Device to Cloud Architecture Defends Against the SolarWinds Supply Chain Compromise

mcafee.com/blogs/other-blogs/mcafee-labs/how-a-device-to-cloud-architecture-defends-against-the-solarwinds-supply-chain-compromise/

December 21, 2020



In a blog post released 13 Dec 2020, FireEye disclosed that threat actors compromised SolarWinds's Orion IT monitoring and management software with a trojanized version of SoalrWinds.Orion.Core.BusinessLayer.dll delivered as part of a digitally-signed Windows Installer Patch. The trojanized file delivers a backdoor, dubbed SUNBURST by FireEye (and Solorigate by Microsoft), that communicates to third-party servers for command and control and malicious file transfer giving the attacker a foothold on the affected system with elevated privileges. From there, additional actions on the objective, such as lateral movement and data exfiltration, are possible. *Since release of the initial blog from FireEye, subsequent additional analysis by McAfee and the industry as well as alerts by CISA, we have seen the attack grow in size, breadth and complexity. We will continue to update defensive recommendation blogs like this as new details emerge.*

The use of a compromised software supply chain as an Initial Access technique (T1195.002) is particularly dangerous as the attack uses assumed trusted paths and as such can go undetected for a long period. This attack leveraged several techniques, such as trusted software, signed code and stealthy hiding-in-plain-sight communication, allowing the attacker to evade even strong defenses and enjoy a long dwell before detection. The sophisticated

nature of the attack suggests that an Advanced Persistent Threat (APT) Group is likely responsible. In fact, FireEye is tracking the group as UNC2452 and has released countermeasures to identify the initial SUNBURST backdoor. McAfee has also provided an intelligence summary within MVISION Insights and mitigation controls for the initial entry vectors are published in KB93861. For additional response actions, please view Part One of this blog series here. If you are using SolarWinds software, please refer to the company guidance here to check for vulnerable versions and patch information.

However, looking beyond the initial entry and containment actions, you should think about how you are prepared for this type of attack in the future. This is a sophisticated actor(s) who may use other techniques such as Spearphishing to gain access, then move around the corporate network and potentially steal intellectual property as was the case with FireEye. They will change techniques and tools, so you need to be ready. Our Advanced Threat Research team tracks over 700 APT and Cyber Crime campaigns so the potential for another threat actor to launch a similar attack is high. In this blog, we will take a specific look at the techniques used in the SolarWinds compromise and provide some guidance on how McAfee solutions could help you respond now and prepare for this type of threat in the future with an adaptable security capability for resilience.

Attack Chain Overview

In our first blog in this series, we provided some initial response guidance designed to disrupt the attack early in the Execution phase or look retrospectively on the endpoints or proxy logs for indicators of compromise. But as you can see in the attack timeline below, it started much earlier with purposeful and detailed preparation and includes multiple other steps. A couple of techniques speak volumes about the sophistication and planning involved in this campaign.

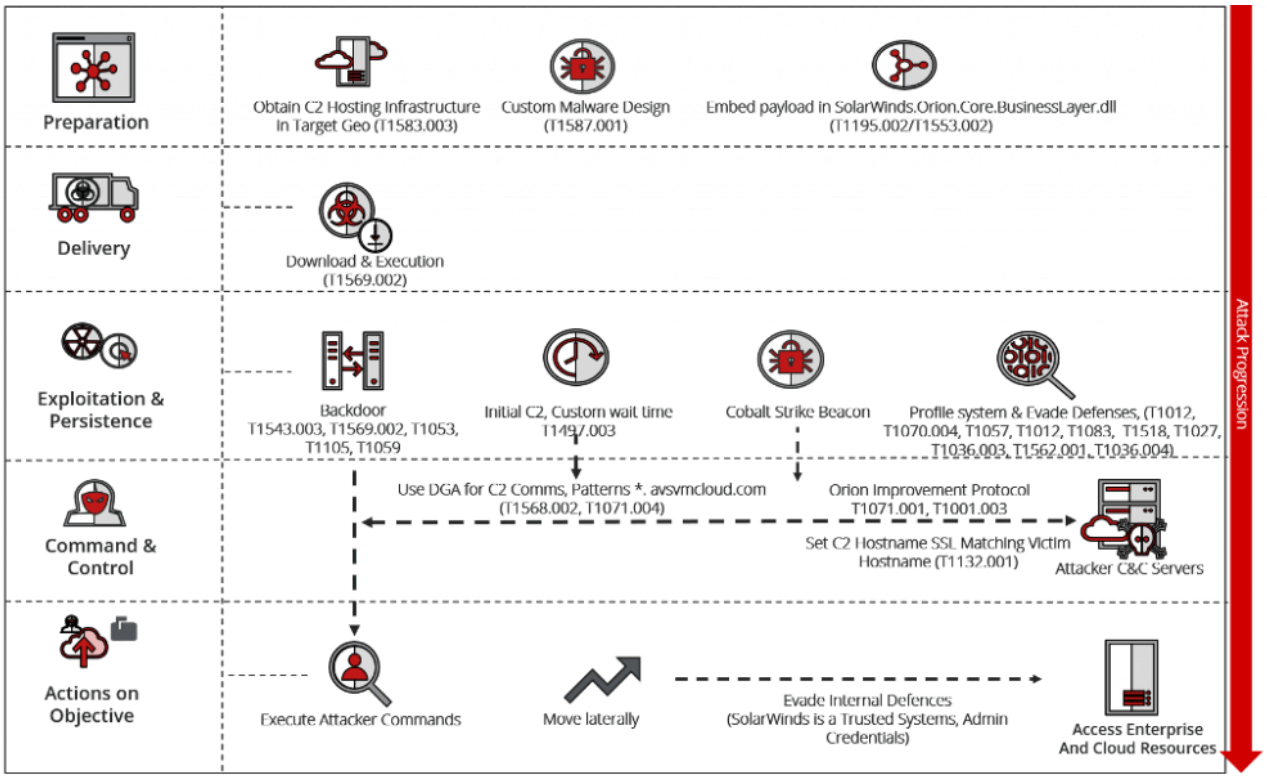


Figure 1: SUNBURST Attack Progression

First is the choice of entry vector. The attacker in this case compromised part of the software supply chain by weaponizing software by SolarWinds, a major brand of IT management software. While software supply chain compromises are not new, like the recent one affecting JavaScript, they are typically on a smaller scale or more quickly detected. More common initial access techniques involve Spearphishing or taking advantage of open remote services like RDP. While both take planning and effort, weaponizing software from a major technology company and going undetected in that process is no easy feat. Secondly, the calculated wait time before external communication and the custom Domain Generation Algorithm (DGA) indicate the attacker has a lot of patience and stealth capability. For more detailed analysis of these advanced techniques, see McAfee Labs additional analysis blog on the SUNBURST backdoor.

The attack also involves numerous post-exploitation actions such as command and control communication masquerading (T1001.003) as normal update traffic, additional payload transfers (T1105), system discovery, credential harvesting and potentially then movement to other systems, even cloud-hosted infrastructure systems. The goal of course is to disrupt or detect any stage of attack before the breakout point and hopefully before any real impact to the business. The breakout point is when an attacker has gained privileges and starts to move laterally within the business. At that point, it becomes very difficult but not impossible to disrupt or detect the activity. But you must act fast. The impact of the attack can vary. In one case, it could be loss of intellectual property, but in another case, destruction of critical systems or data could be the goal. Also, what if the attacker used other initial access techniques, such as Spearphishing (T1566), to deliver a similar backdoor? Would you be able to detect that activity or any of the follow actions? Our point is don't just update the

endpoint with the latest DAT and consider yourself secure. Look for other ways to disrupt or detect an attack throughout the whole attack chain, leveraging both prevention and detection capability and keeping the end goal in mind to reduce impact to the business. Also think about how you prepare. The attackers in this case spent a lot of time in preparation creating custom malware and infrastructure. How about your organization? Do you know what attackers might be targeting your organization? Do you know their tactics and techniques?

Staying Ahead with MVISION Insights

In the first hours of a new threat campaign, if the CIO or CISO asked you, “are we exposed to SUNBURST”, how long would it take you to answer that question? One place to turn is MVISION Insights. MVISION Insights combines McAfee’s Threat Intelligence research with telemetry from your endpoint controls to reduce your attack surface against emerging threats. MVISION Insights tracks over 700 APT and Cyber Crime campaigns as researched by McAfee’s ATR team, including the most recent, FireEye Red Team tool release and SolarWinds Supply Chain Compromise campaigns.

Figure 2: Getting details on the attack

In the beginning hours of a new threat response, you can use MVISION Insights to get a quick summary of the threat, view external resources, and a list of known indicators such as files, URLs, or IP addresses. The campaign summary saves you from some of the time-consuming task of combing multiple sites, downloading reports, and building out the broader picture. MVISION Insights provides critical pieces in one place allowing you to move quicker through the response process. The next question to answer, is this new attack a risk to my business? Insights can help you answer that question as well when you click on “Your Environment”.

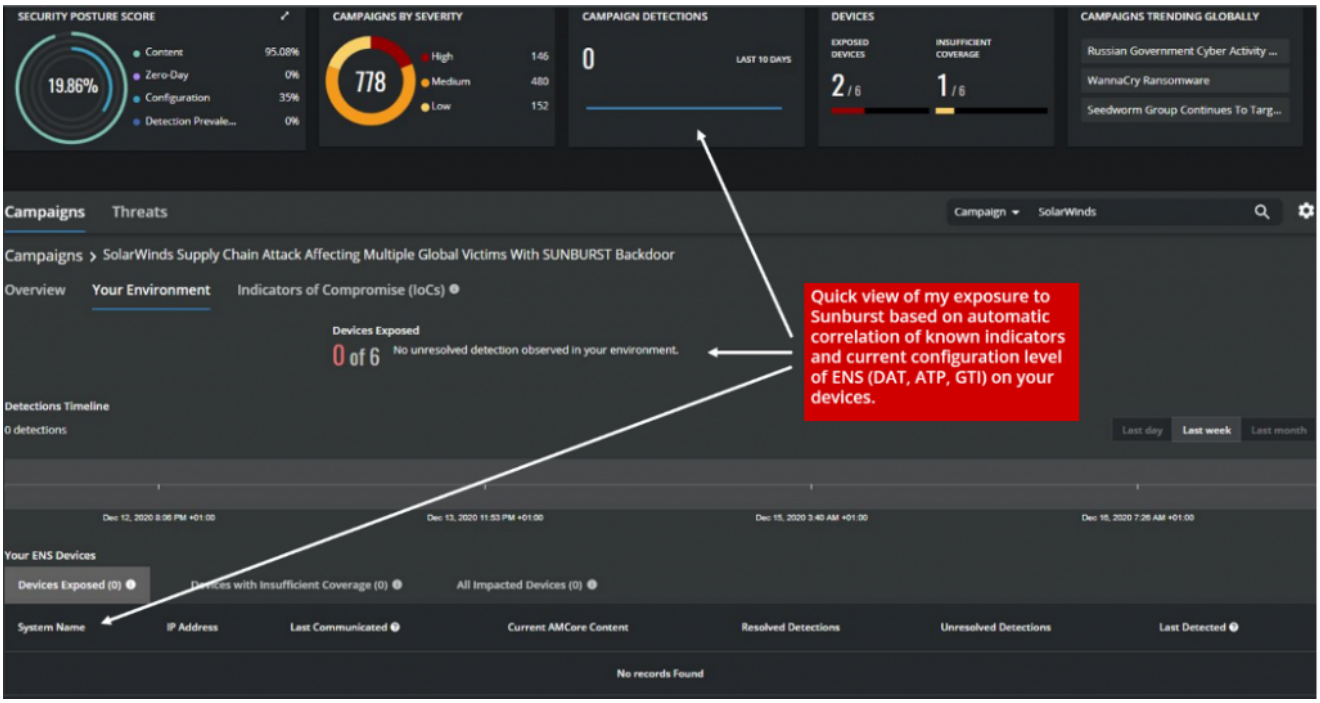


Figure 3: Quick review of your exposure

Insights automatically correlates the indicators of compromise with Threat Events from McAfee ENS, allowing you to quickly asses if there is an immediate problem now. If you had a detection, you should immediately go to incident response. Insights reviews your endpoint control configuration to asses if you have the right content update deployed to potentially disrupt the threat. At this point, you are closer to answer the CIO question of “are we exposed”. I say closer because Insights provides only the endpoint protection view currently so you will need to review other controls you have in place to fully assess risk.

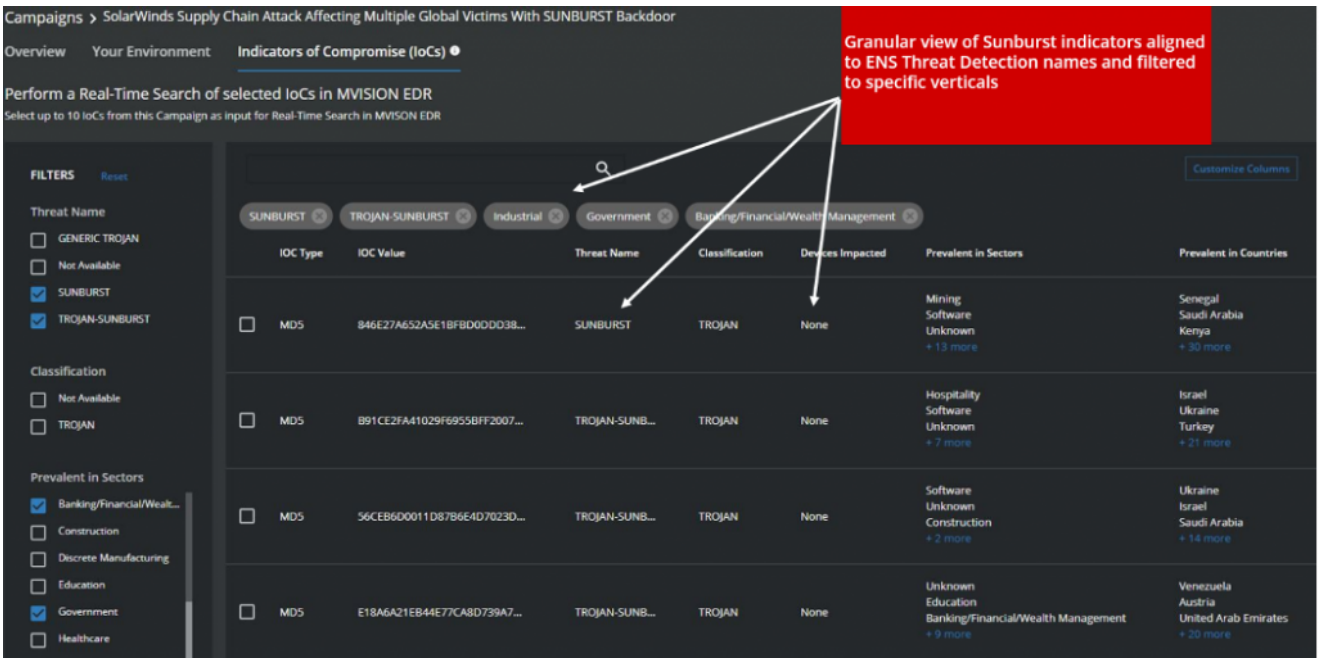


Figure 4: Detail review of your exposure

However, Insights also assesses your endpoint security posture against other advanced threat techniques, looking to see if you are getting the best value from ENS by leveraging signature, intelligence and behavior anomaly detection capability in the solution. This is important because the attackers will change tactics, using new entry techniques and tools, so your security posture must continuously adapt. And this is just one campaign. Insights is summarizing intelligence, surfacing detections and reducing your attack surface continuously, against 700 campaigns!

Review your Defensive Architecture

Mitigating risk from SUNBURST and similar sophisticated APT campaigns requires a security architecture that provides defense in depth and visibility throughout the entire attack chain. You should review your architecture and assess gaps either in technique visibility or protection capability. Below we have outlined where McAfee and partner solutions could be used to either disrupt or detect some of the attack techniques used in SUNBURST based on what we know today.

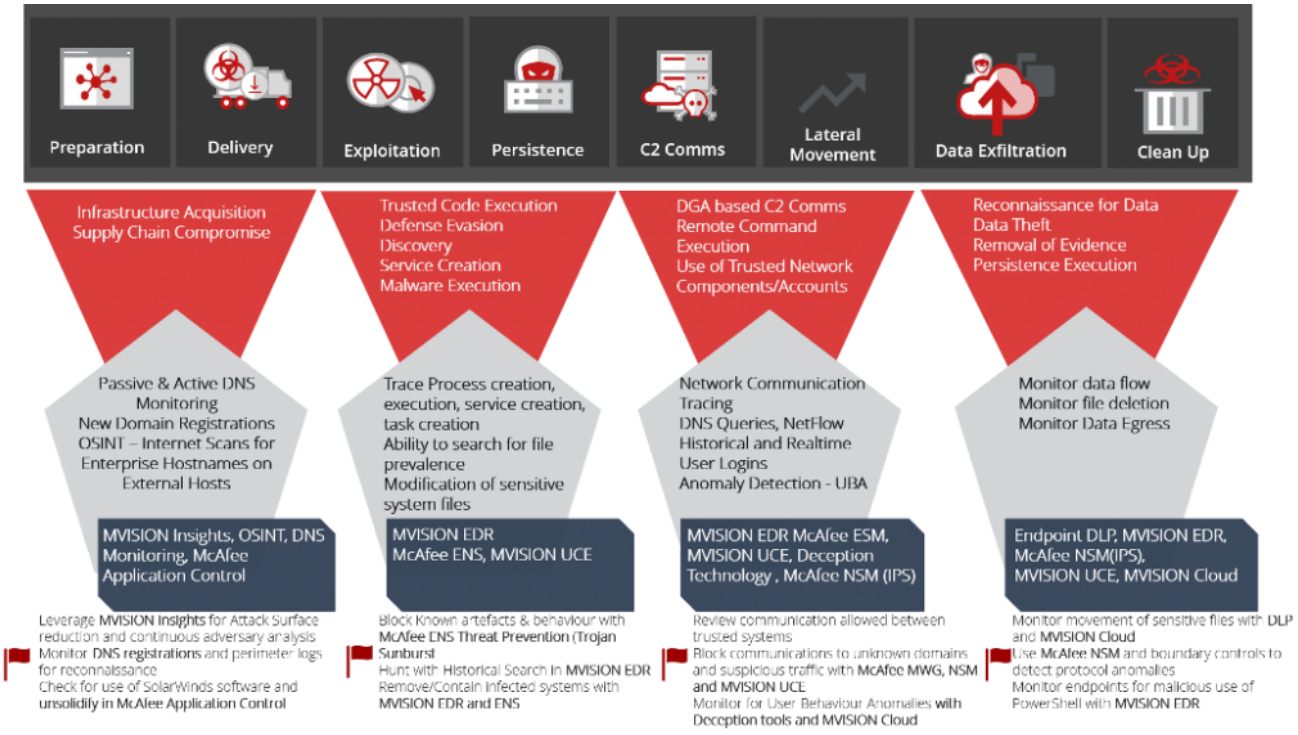


Figure 5: Device to Cloud Security Architecture

While the attacker is no doubt sophisticated and stealthy, the multi-stage aspect of the attack presents opportunities to detect or stop at multiple points and perhaps even before the attack gains a foothold. We cover more about how to use McAfee EDR to search for or detect some of the techniques used in SUNBURST in next section. However, there are some other key cyber defense capabilities that may be overlooked in your organizations but are critical to having a chance at detection and mitigation. We highlight those in this section below.

Getting inside the attacker's preparation

Normally this is beyond what most organizations have time to do. However, in this case, you need to gain any advantage. We discussed MVISION Insights above so here we will cover additional guidance. During the preparation phase of this attack, the attacker obtains infrastructure within the target geo to host their command and control server. During this phase, they also set the hostnames of their C2 servers to mimic target organization hostnames. A scan for your domain names on external IP blocks can reveal the attack formation. Open source tools such as Spiderfoot offer a number of plugins to gather and analyze such types of data. Passive DNS with combination of hosts communicating with unusual domain names also represent a window of detection whereby Advanced DNS Protection solutions such as from our SIA partner Infoblox can detect behavior-based DGA usage by malware and automatically block such DNS resolution requests.

Visibility on DNS

DNS queries often provide the first layers of insights into any type of C2 communication and data exfiltration. You should enable logging ideally at an upstream resolver(s) where you can see traffic from your entire infrastructure. More information can be found here for Windows DNS Servers and Linux Bind DNS Servers. This could be forwarded to McAfee ESM/other SIEMs for analysis and correlation for detection of DGA-type activities.

NetFlow Logging

Being able to detect unusual flows should also be a priority for incident responders. Along with DNS queries, NetFlow data when combined with UBA provides a great source of detection, as the attackers' use of VPS providers can be combined with user login data to detect an "impossible rate of travel event."

Hunting for Indicators with MVISION EDR

As described in the defensive architecture, MVISION EDR plays a vital role in hunting for prevalence of indicators related to the SUNBURST backdoor and ensuing post compromise activity. The role of MVISION EDR becomes even more important due to the usage of manual OPSEC by the threat actor where what follows the initial breach is driven by how the threat actor is targeting the organisation.

Hunting for Presence of Malicious Files

You can use MVISION EDR or MAR to search endpoints for SUNBURST indicators as provided by Microsoft and FireEye. If you are licensed for MVISION Insights, you can pivot directly to MVISION EDR to search for indicators. MVISION EDR supports real-time searches to hunt for presence of files on the endpoints and allows for sweeps across the estate. The following query can be used with the pre-populated malicious file hash list. The

presence of the file on the system is itself does not mean it was successful and further hunting to check for execution of the actual malicious code on the system.is needed. See the search syntax below.

Begin MVEDR Query Syntax…

Files name, full_name, md5, sha256, created_at, create_user_name, create_user_domain and HostInfo hostname, ip_address, os and LoggedInUsers username, userdomain where Files sha256 equals “ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c” or Files sha256 equals “c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77” or Files sha256 equals “eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed” or Files sha256 equals “dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b” or Files sha256 equals “32519685c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77” or Files sha256 equals “d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600” or Files sha256 equals “53f8dfc65169ccda021b72a62e0c22a4db7c4077f002fa742717d41b3c40f2c7” or Files sha256 equals “019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134” or Files sha256 equals “ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6” or Files sha256 equals “32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77” or Files sha256 equals “292327e5c94afa352cc5a02ca273df543f2020d0e76368ff96c84f4e90778712” or Files sha256 equals “c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71”

…End MVEDR Query Syntax

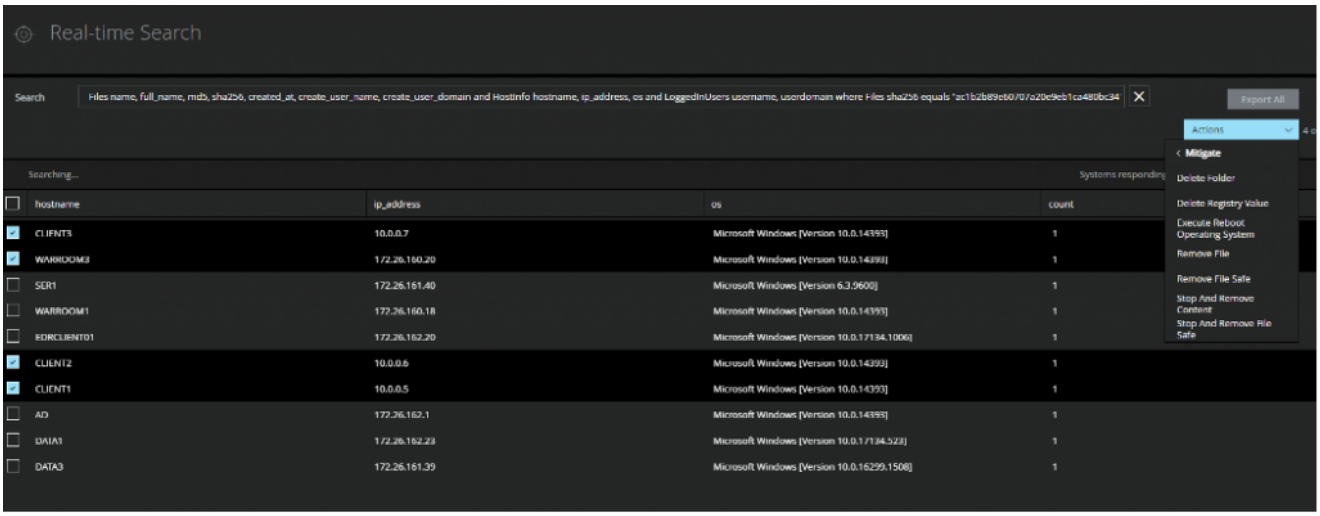


Figure 6: Real Time Search for indicators

Additionally, you can do a historical search creation and deletion of files going back up to 90 days in cloud storage.

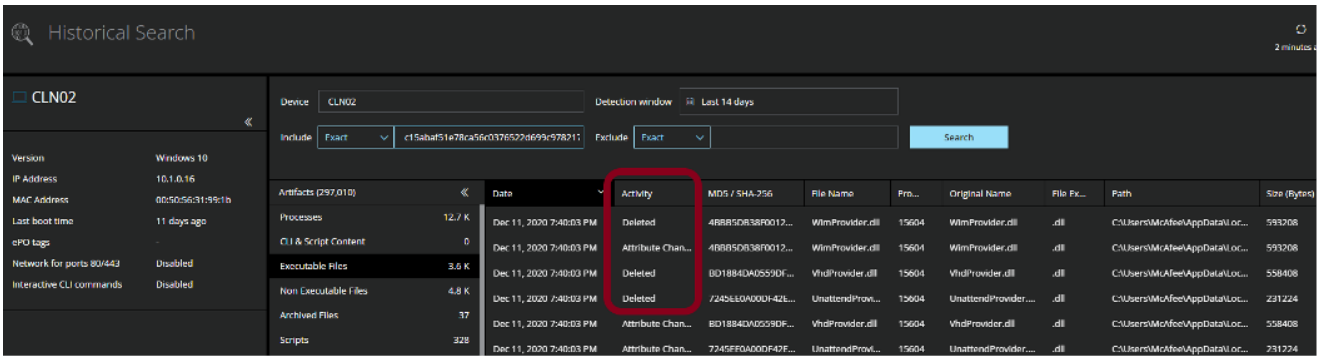


Figure 7: Historical Search and Modification of Files

The threat actor is known to rename system utilities/files and clean up their tracks. MVISION EDR can review historical changes to the file system, this is crucial in determining if an endpoint was a victim of this attack. The flexible search interface can be used to filter down and track the progress of the completion of the attacker's objectives for e.g. look at changes triggered from the infected dll's such as netsetupsvc.dll.

Hunting for Malicious Network Connections

MVISION EDR allows for tracing of active network connections leveraging the real time search functionalities

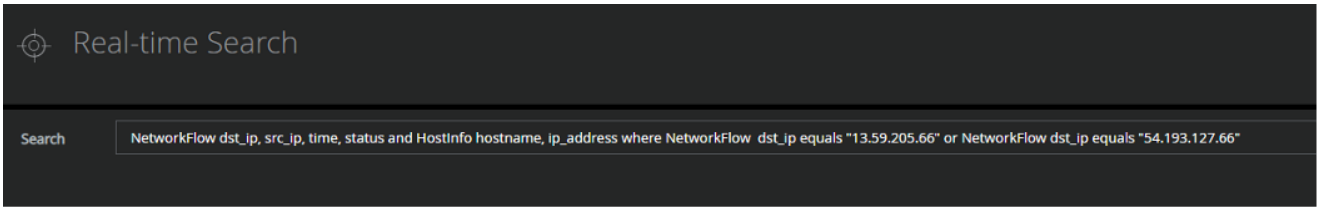


Figure 8: Realtime Network Connections

```
NetworkFlow dst_ip, src_ip, time, status and HostInfo hostname,
ip_address where NetworkFlow  dst_ip equals "13.59.205.66" or
NetworkFlow dst_ip equals "54.193.127.66" or NetworkFlow dst_ip equals
"54.215.192.52" or NetworkFlow dst_ip equals "34.203.203.23" or
NetworkFlow dst_ip equals "51.89.125.18" or NetworkFlow dst_ip equals
"167.114.213.199" or NetworkFlow dst_ip equals "139.99.115.204" or
NetworkFlow dst_ip equals "5.252.177.25" or NetworkFlow dst_ip equals
"5.252.177.21" or NetworkFlow dst_ip equals "204.188.205.176"
```

You can also leverage the historical search function to look for historical connections related to the command and control activity for this threat actor. The filtering by process ID and source/destination IP allows analysts to track down the malicious communications.

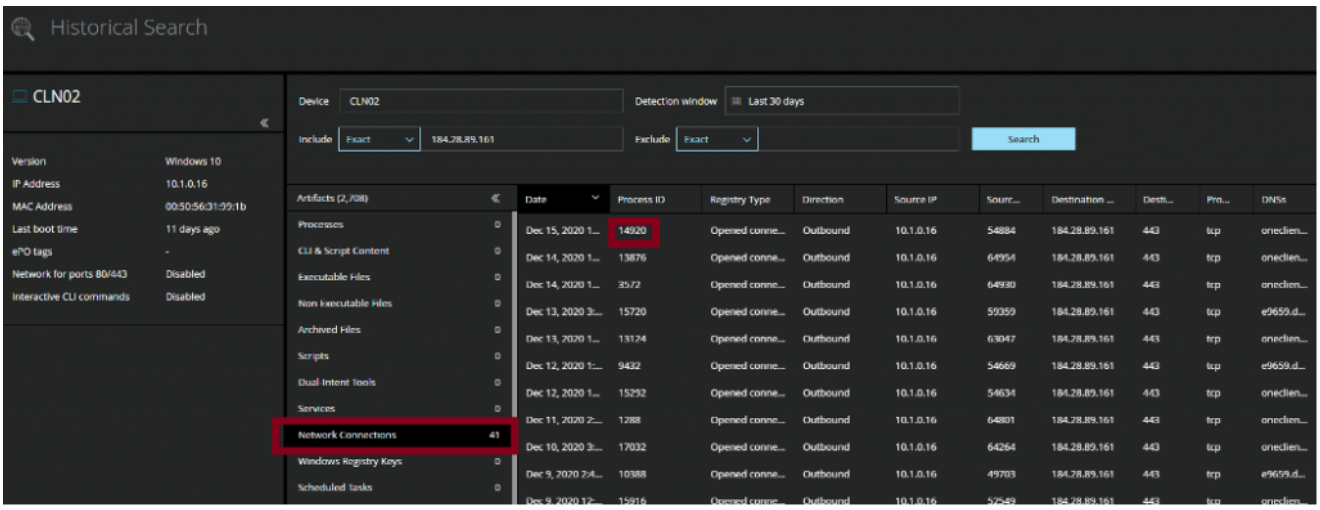


Figure 9: Historical Network Connections

MVISION EDR also allows analysts to review historical DNS lookups thus allowing for the ability to hunt for malicious DNS lookups. This is a very important capability in the product as many organizations do not log DNS or have a DNS hierarchy that makes it harder to log the end device making the actual request.

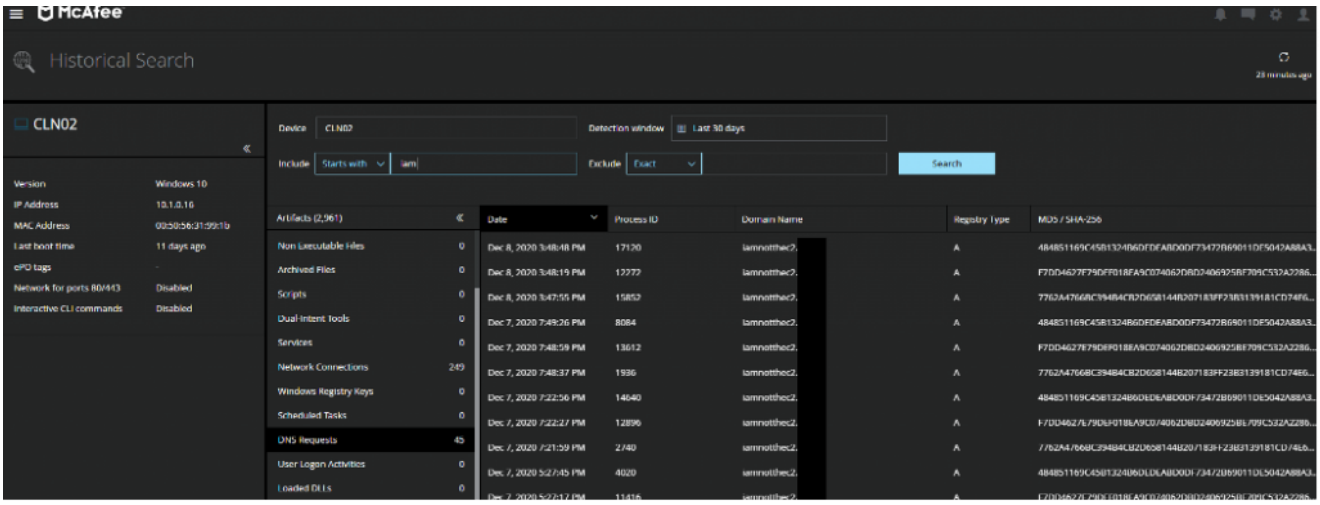


Figure 10: Historical DNS Searches

Hunting for Malicious Named Pipes Across the Estate

MVISION EDR includes custom collector creation ability that allows for execution of custom commands across the estate. In this case, it's possible to look for the existence of the Named Pipes by executing the following Powershell command:

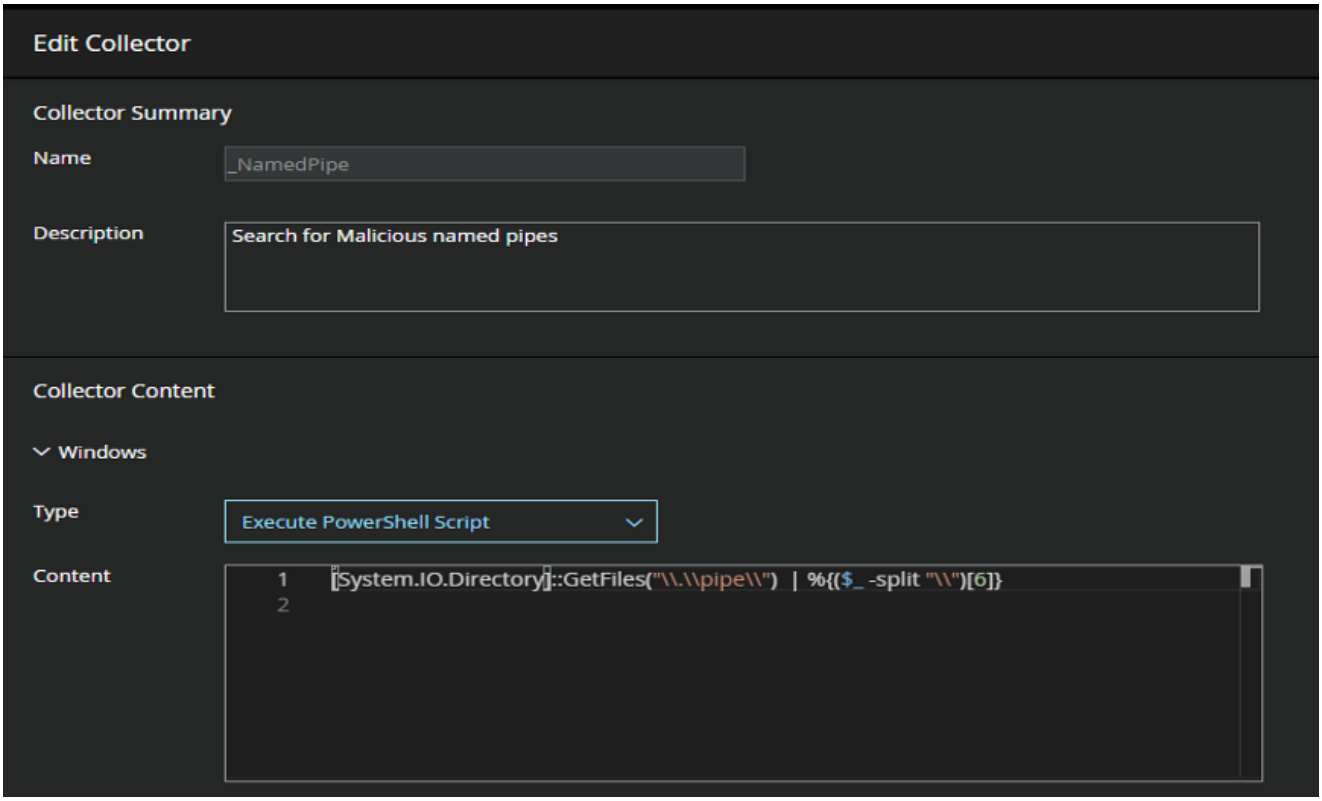


Figure 11: EDR Named Pipe Collector
Powershell Command for Pipe detection [System.IO.Directory]::GetFiles("\\.\\pipe\\") | %{($_ -split "\\")[6]}

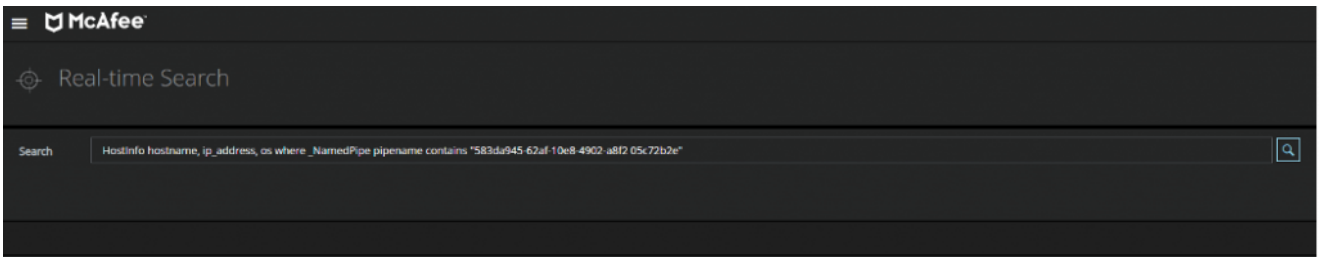


Figure 12: Realtime Search for Named Pipe
HostInfo hostname, ip_address, os where _NamedPipe pipename contains "583da945-62af-10e8-4902-a8f2 05c72b2e"

Hunting for Malicious Processes

It is known the attacker in its final stages leverages legitimate SolarWinds processes to complete their objectives:

\Windows\SysWOW64\WerFault.exe

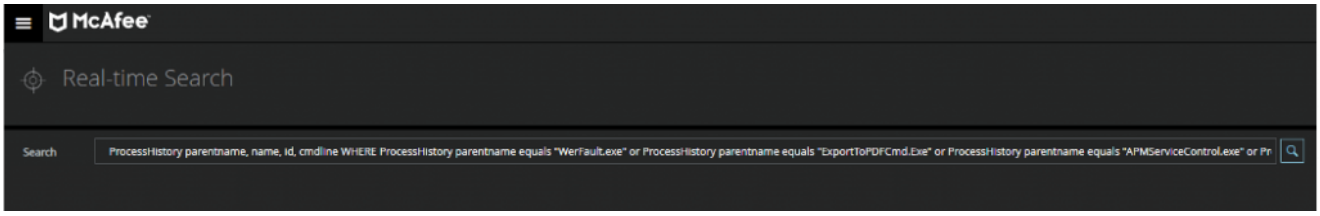
\SolarWinds\Orion\ExportToPDFCmd.Exe

\SolarWinds\Orion\APM\APMServiceControl.exe

\SolarWinds.Credentials\SolarWinds.Credentials.Orion.WebApi.exe

\SolarWinds\Orion\Topology\SolarWinds.Orion.Topology.Calculator.exe

\SolarWinds\Orion\Database-Maint.exe



ProcessHistory parentname, name, id, cmdline WHERE ProcessHistory parentname equals “WerFault.exe” or ProcessHistory parentname equals “ExportToPDFCmd.Exe” or ProcessHistory parentname equals “APMServiceControl.exe” or ProcessHistory parentname equals “SolarWinds.Credentials.Orion.WebApi.exe” or ProcessHistory parentname equals “SolarWinds.Orion.Topology.Calculator.exe” or ProcessHistory parentname equals “\SolarWinds\Orion\Database-Maint.exe”

Hunting back longer than 90 days with EDR Trace Data

MVISION EDR’s architecture leverages the Data Exchange Layer to stream trace data to our cloud service where we apply analytics to identify or investigate a threat. Trace data are artifacts from the endpoint, such as file hashes, processes, communications, typically needed for endpoint detection and searches. The DXL architecture allows that data to be streamed to the cloud as well to a local data store such as a SIEM or other log storage like Elastic simultaneously.

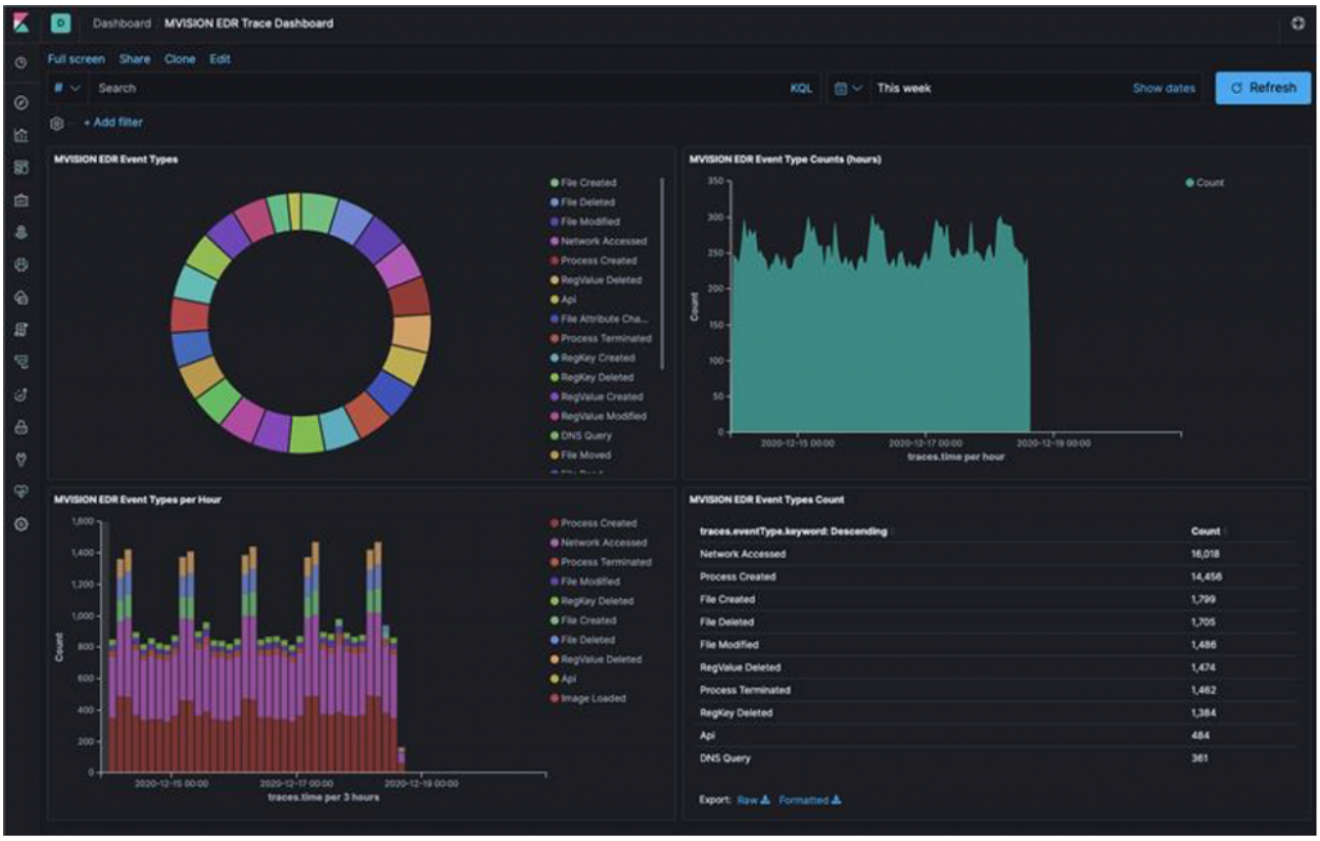


Figure 14: Long term search of EDR trace data in a Kibana dashboard

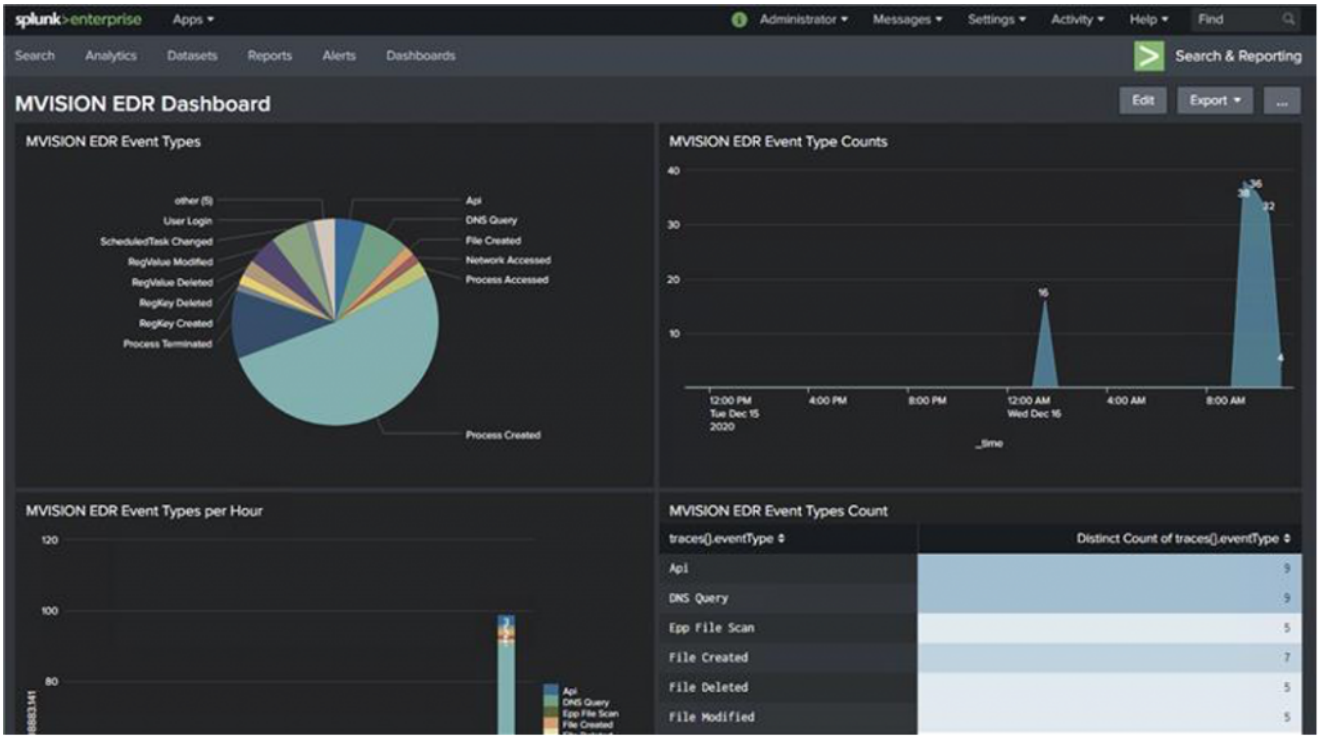


Figure 15: Long term search of EDR trace data in a Sp dashboard

You can store the data longer than the 90-day maximum McAfee stores in our cloud. Why is this important? Recent analysis of SUNBURST suggests that the attack goes as far back as March 2020, and perhaps earlier. This local storage would provide capability to hunt for indicators further back as needed, if so configured.

Assessing Visibility

How do you know what data sources are needed to detect Mitre Att&ck tactics and techniques? Carlos Diaz from MVISION EDR engineering wrote a great tool called Mitre-Assistant to simplify that process. You can download that tool here.

Detecting Actions on Objective

Post Initial Exploit Threat Detection and Analysis in EDR

One of the key challenges threat hunters and security analysts face is where the attack progresses through to the second phase of the attack, where it is understood the attacker has dropped malware to execute and complete their objectives. This usage of sophisticated execution of malware from a trusted process is detected by MVISION EDR and automatically mapped to the MITRE ATT&CK Framework. As part of the detection and process tracing, EDR also captures the command executed on the endpoint. This becomes invaluable in case of tracking the manual OPSEC aspect of the second phase of the attack.

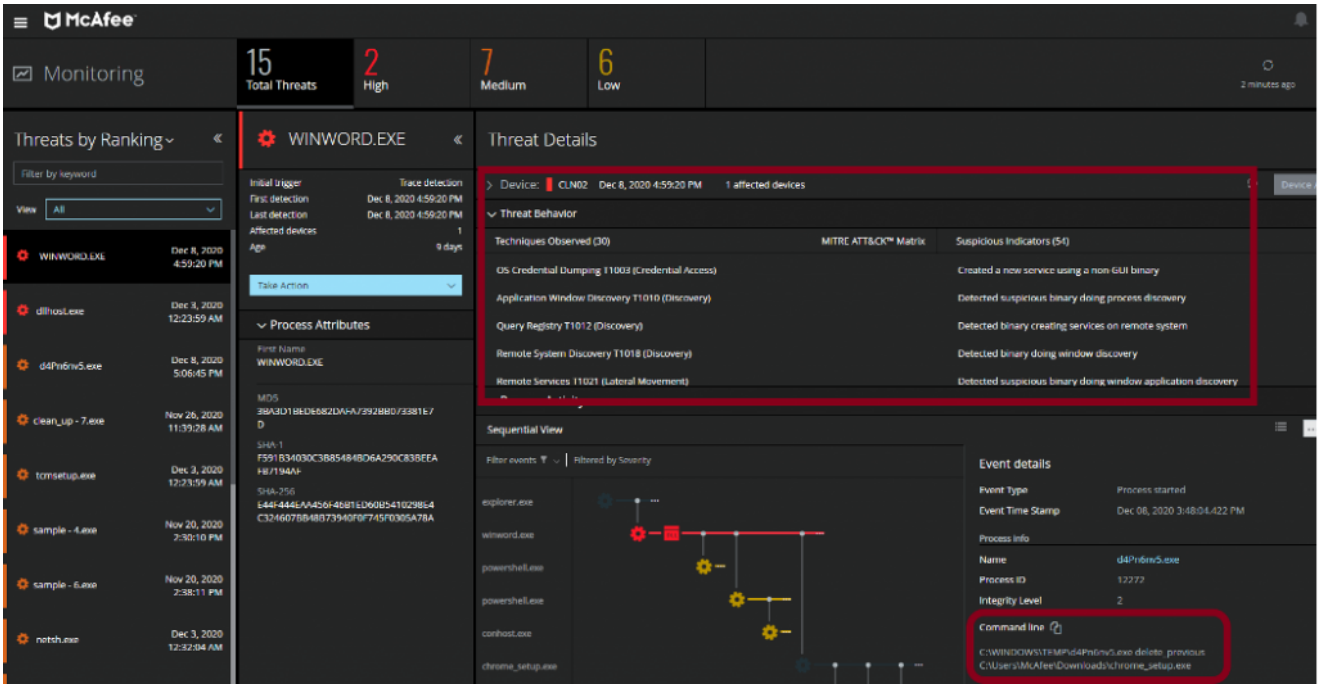


Figure 16: Mitre analysis and threat detection for post exploit execution

MVISION EDR provides extensive capabilities to respond to threats once they have been assessed, e.g. real-time searches once executed allows analysts to scope the affected endpoints rapidly at which point the solution offers multiple options as a method for containment and remediation of the threat across the estate through bulk operations.

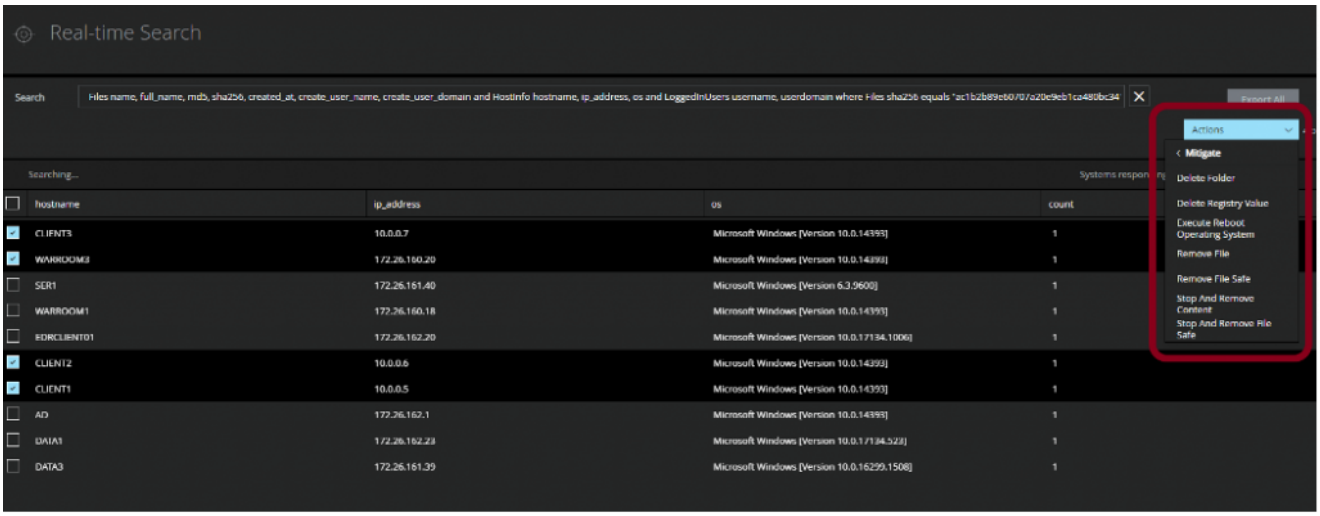


Figure 17: EDR Bulk Threat Mitigation

Detecting Data Exfiltration, Lateral Movement and Prevention

MVISION EDR provides a way to easily visualize data egress by looking at topology view of the endpoints where malicious activity has been detected, by observing the network-flow map the outlier connections can be easily identified and then correlated with WHOIS, IP reputation and Passive DNS data from providers like McAfee GTI and Virustotal. Once established, the external connections can be blocked and the endpoint can be quarantined from the EDR console. EDR also shows common processes spawning across multiple endpoints to showcase lateral movement and is also tagged as part of the MITRE techniques being identified and detected.

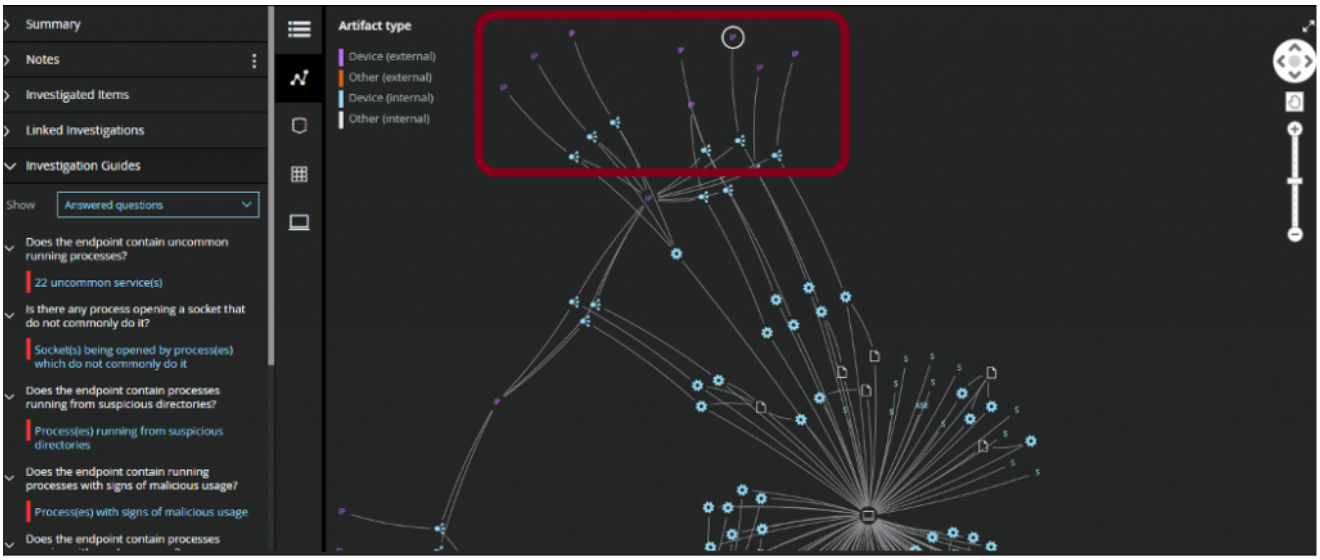


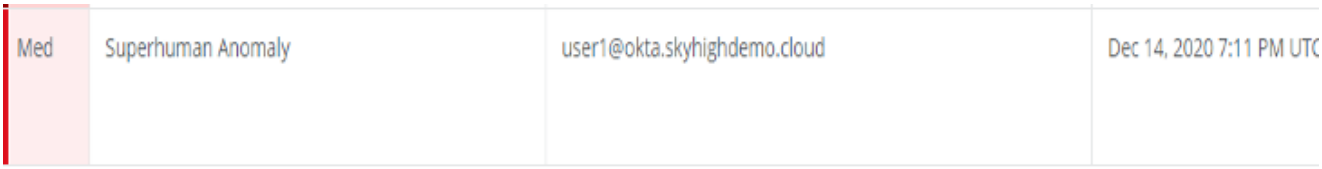
Figure 18: EDR Lateral Movement and Exfiltration

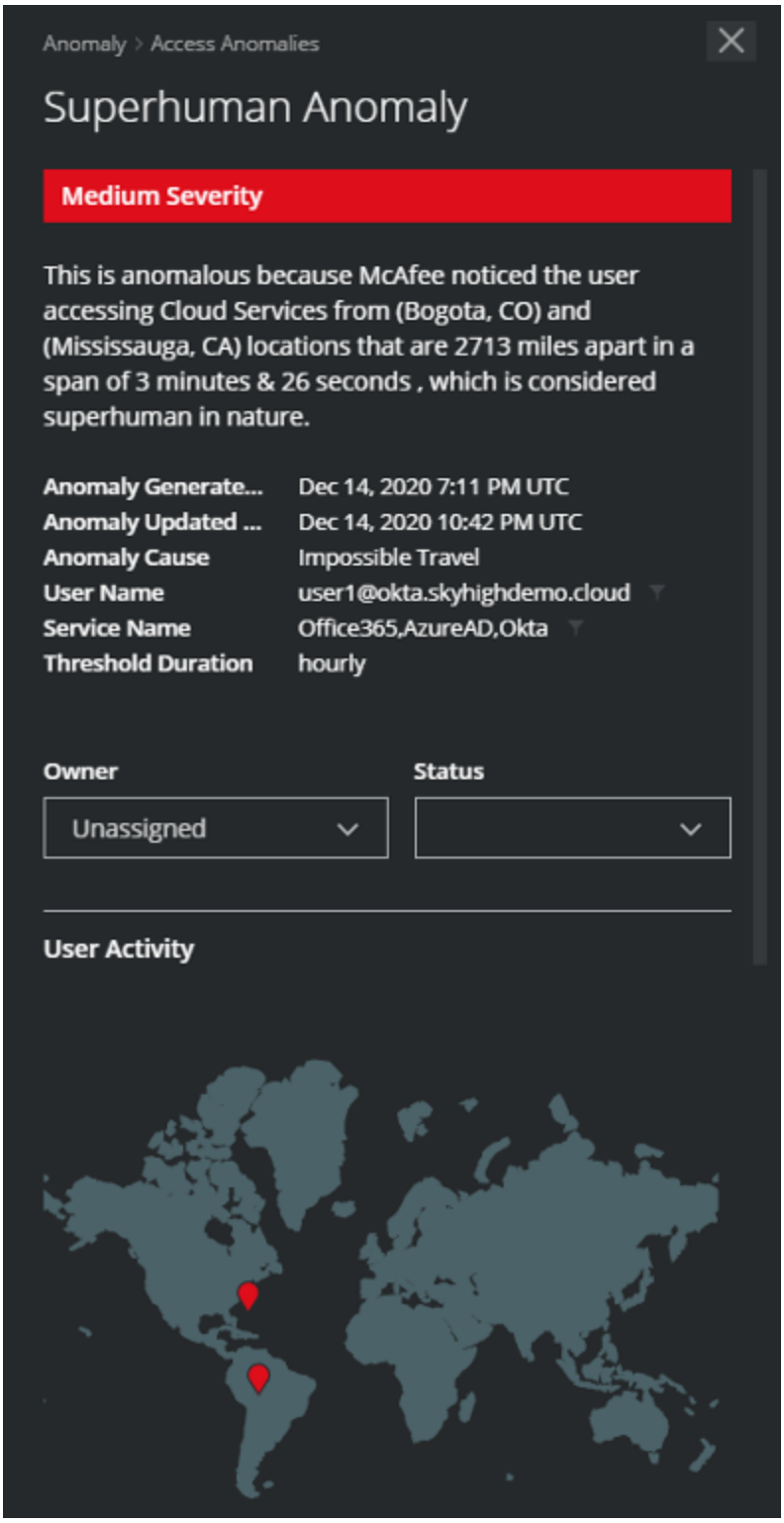
Combining EDR with Deception technology such as that from Attivo Networks brings together a combination of offensive detection where the attacker can be effectively trapped as result of not getting hold of the real credentials required to make the lateral movement/ privilege escalation a success thus failing in their objective completion.

An integrated approach to DLP can also provide effective protection against the completion of the objectives for e.g. unified DLP policy across the endpoint and web-gateway looking for exfiltration of sensitive organizational data can also provide valuable defenses. McAfee's UCE platform provides such unified data protection capabilities.

Cloud account compromise detection

Our latest research indicates attacker is actively looking to establish additional footholds into customer cloud environments such as Azure AD or bypass multi-factor authentication by hijacking SAML sessions, McAfee's MVISION Cloud Access Control and User Anomaly Detection can identify suspicious access attempts to cloud services and infrastructure.





It is recommended to increase monitoring and investigations into such activity especially with privileged accounts on sensitive infrastructure

Supply Chain and Intellectual Property Protection

In addition to architecture review and continuous hunting for indicators, it is recommended that customers work with their suppliers – IT, Cloud Services, Infrastructure, Hardware, etc. – to validate integrity. Secondly, review controls, detection use cases in the SOC and logs, specifically related to your intellectual property. A tabletop exercise to rehearse crisis management and breach notification procedures is also recommended.

Summary and Next Steps

It's important to note that analysis of this attack is ongoing across the globe and events are still unfolding. The presence/detection of the backdoor and affected software is just the beginning for many customers. MVISION EDR or other tool detections of malicious named-pipe presence and domains help indicate to a customer if the backdoor was running, but with the gathered system information, the adversary may have valid accounts and access to AD or Cloud systems in some cases. The adversary has been wiping information/log files to erase traces. Incident Response is a critical piece of your overall business resilience and if you are affected, you will no doubt be asking yourself these types of questions.

- When did we install the vulnerable software?
- Did they compromise user-accounts and have AD access?
- Did they install additional backdoors?
- How many systems and accounts are affected?
- Were cloud or enterprise resources accessed?
- Was information stolen? If so, do we have notification procedures?
- Are there other supply chain compromises yet undiscovered?

McAfee will continue to post analysis results and defensive guidance as we learn more about the attack. Customers should follow McAfee Labs posts, check the Insights Preview Dashboard for latest threat intelligence, and continually check the Knowledge Center for latest product guidance.

Mo Cashman Director of the Enterprise Architecture team at Intel Security.
Mo Cashman is one of the company's passionate leaders in cyber security. As an Enterprise Security Architect and Principal Engineer at McAfee, Mo advises our largest global customers and partners...