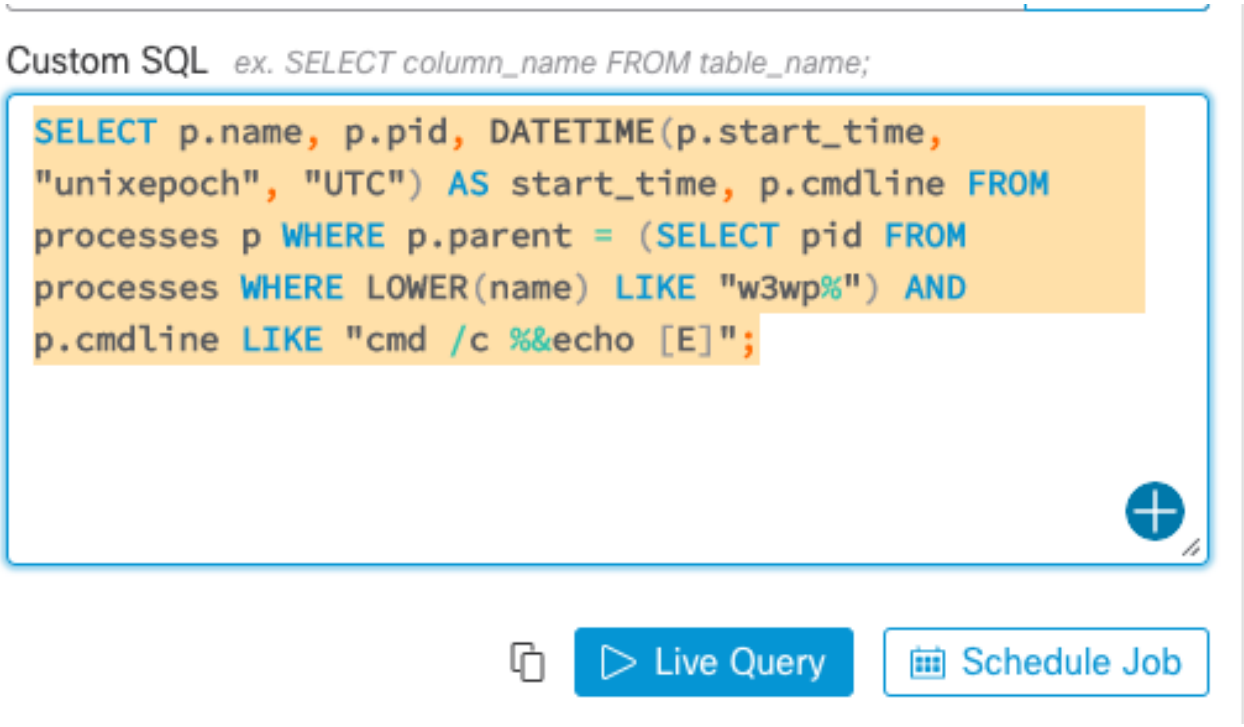
Hafnium Update: Continued Microsoft Exchange Server Exploitation

blog.talosintelligence.com/2021/03/hafnium-update.html

Update 3/11: The following OSQuery detects active commands being run through webshells observed used by actors on compromised Exchange servers. While systems may have been patched to defend against Hafnium and others, threat actors may have leveraged these vulnerabilities to establish additional persistence in victim networks. A thorough forensic investigation will be required to determine additional compromises.



It's been a week since Microsoft first disclosed several zero-day vulnerabilities in Exchange Server — and the scope has only grown since then. In its disclosure, Microsoft stated that a new threat actor known as Hafnium was exploiting these vulnerabilities to steal emails.

Since Microsoft's initial disclosure, Cisco Talos has seen shifts in the tactics, techniques, and procedures (TTPs) associated with this activity. The majority of the activity continues to follow the guidance that was previously provided. We are, however, starting to see other groups' activity in active incidents Cisco Talos Incident Response (CTIR) is responding to. These actors appear to be separate from the initial "HAFNIUM" actor and include groups that are leveraging infrastructure previously attributed to cryptocurrency mining campaigns, groups creating or accessing web shells using notepad.exe or notepad++.exe and large amounts of scanning activity without successful exploitation.

We have also identified organizations that may be involved in post-exploitation activity. The victimology shows that financial services have been disproportionately affected by exploitation, with a few other notable verticals following including health care, education and local/state governments. This shows that, although the initial activity may have followed closely with the guidance provided by Microsoft, as time passes, the amount of groups exploiting these vulnerabilities is only going to increase. This compounds the importance of patching these vulnerabilities as soon as possible.

Talos also has some new additions to the IOCs to look out for and other forms of coverage in Cisco Secure products.

As the days have passed the amount of victims and scope of the compromise has grown significantly. As more actors move into the space, it's likely going to get worse. We encourage everyone to patch as soon as possible. However, it may be too late for any users who had a Microsoft Exchange server exposed. In those cases, it's important to hunt for potential exploitation and any consequences. First, we'll walk through Cisco Secure Orbital queries and how they can help users who fear they could be targets.

Hunting Hafnium using OSQuery and Orbital

Cisco Secure Endpoint customers have access to Orbital queries. These leverage osquery to allow customers to query their endpoints directly. There are several ways a customer can leverage this to identify potential Hafnium incidents.

Let's start by looking for the backdoors that may be present on servers. We'll begin by executing a query looking for them. These payloads can include things like web shells and potentially other utilities like powercat. After the user has logged into the Orbital portal, they can select the endpoints they want to run the queries against, which in this case, may be the applicable Exchange servers. Then, you provide a custom SQL looking for the web shells, which has been provided below.

```
SELECT script_path, script_text, DATETIME(time, "unixepoch", "UTC") AS creation_time FROM orbital_powershell_events WHERE regex_match(script_text, "New-Object\s+System\.Net\.Sockets\.TCPClient.+.GetStream\s*\(\s*\).*\[\s*byte\s*\[\s*\]\s*\].*0\.\.65535\|:ASCII\)\.GetBytes.+.Write\s*\(.+.Flush\s*\(\s*\)\s*\}.+.Close\s*\(\s*\)",0);
```

One thing of note here is that the orbital_powershell_events table is being used. Those familiar with osquery may have been expecting powershell_events, but the Orbital team has built their own version and that is what the query is based on. If you are attempting more general osquery requests outside of orbital, please use powershell_events instead. This particular regex will match on the web shells that have been attributed to these campaigns. Any results should be triaged and responded to accordingly.

The example above is an example of how to search for the webshells. Now, let's focus on some of the other payloads like powercat. Here is a second query that is specifically looking for powercat, one of the other non-webshell based payloads, which is provided below:

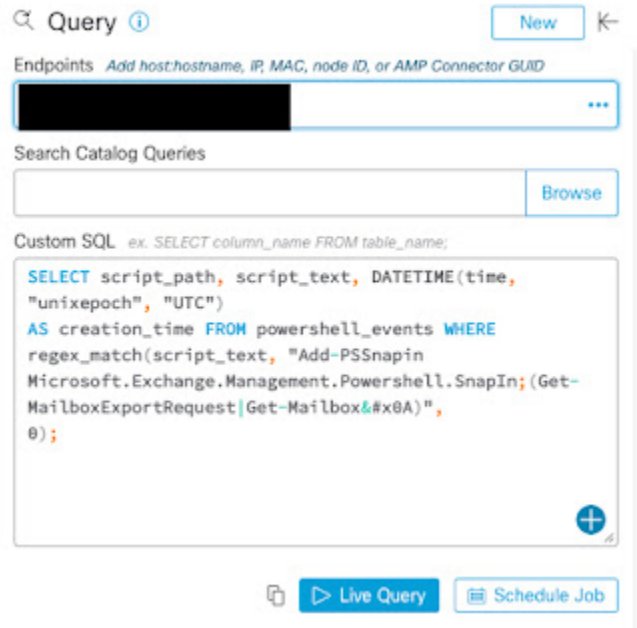
> SELECT script_path, script_text, DATETIME(time, "unixepoch", "UTC") AS creation_time FROM orbital_powershell_events WHERE script_path LIKE "%raw.githubusercontent.com/besimorhino/powercat%" OR script_path LIKE "%powercat.ps1%"

Again, this query makes use of orbital_powershell_events and should be modified if applying it to non-orbital-based systems. This query, once executed, should also provide customers with the systems where this activity is likely to be found.

Let's move past the initial compromise and start looking for some of the post-exploitation activity. One of the most common post-exploitation activities was for the adversaries to export mailboxes. This can also be found using the same Orbital interface with another query, provided below.

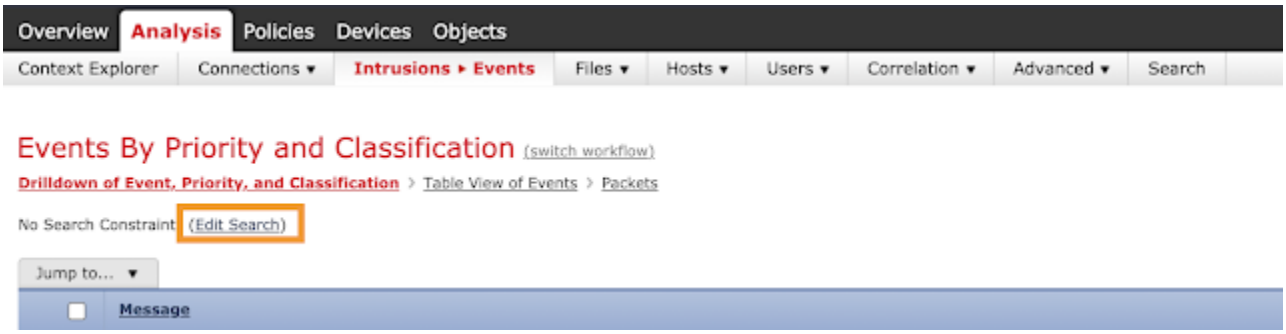
> SELECT script_path, script_text, DATETIME(time, "unixepoch", "UTC") AS creation_time FROM orbital_powershell_events WHERE regex_match(script_text, "Add-PSSnapin Microsoft.Exchange.Management.Powershell.SnapIn;(Get-MailboxExportRequest|Get-Mailbox&#x0A)", 0);

This query will identify the mailbox export requests that are part of the TTPs associated with these campaigns. Again, if executed properly, it should show the customer what systems have potentially been affected and whether or not a mailbox export has already occurred. These types of queries can be invaluable to a security organization trying to identify, not only if they were a victim, but how severe the effects may be. These queries are an excellent resource for security organizations, but it isn't the only way you can identify the activity in your environment.

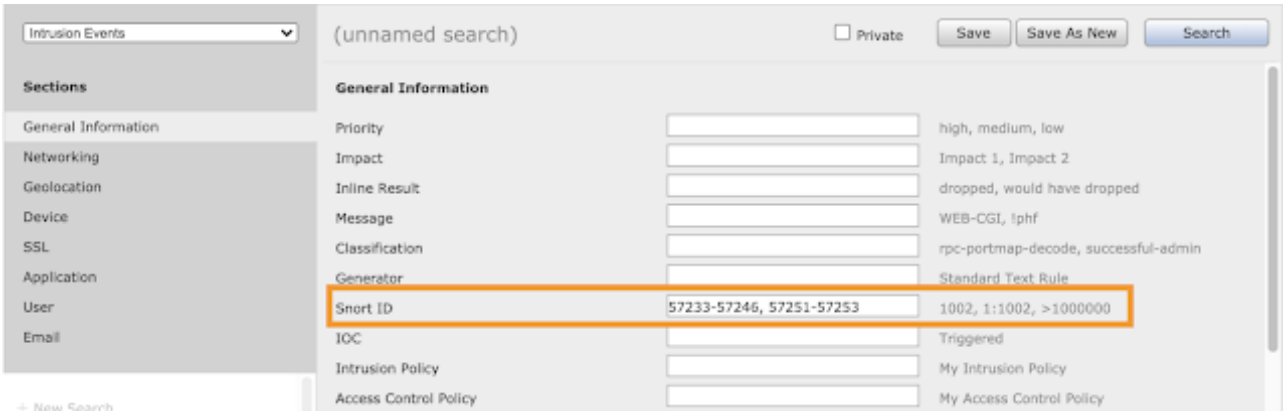


Hunting Hafnium using Cisco Secure IPS

Part of our coverage includes NGIPS signatures that can identify the scanning and exploitation activity, as well as the post exploitation activity of web shells. As such, it can be leveraged to see if and how your enterprise may have been affected. Start by logging into your console and then browsing to intrusion events and editing a search (shown below).



Now you can focus the search for just the applicable signatures associated with Hafnium (57233-57246, 57251-57253). This will allow only the events associated with Hafnium and applicable webshells to be shown, this can be achieved by searching by Snort ID (shown below). Please note that some of these signatures do require TLS decryption to be in place with Exchange servers similar to how it was required for Blue Keep detection.



After adjusting the search to cover the applicable time frame, there will be a list of the signatures that fired in the environment during that period. If you click through, you can get details about the systems that are affected and review any packet capture data obtained.

Shown below are the details provided for the events that triggered the signature, including source and destination information and country of origin.

At this point, defenders can use the IOCs derived from these events to potentially focus any additional investigations or as potential support of investigations already underway.

One of the most important takeaways for defenders is around the web shell signatures. Just because you found a web shell does not mean you were a Hafnium target Web shells are a common payload and may be the result of other actors leveraging other vulnerabilities. Regardless of their origins, they should be thoroughly investigated and remediated.

These are just a few examples of ways that Cisco Secure products can be leveraged to identify if your enterprise was potentially affected and what payloads may have been dropped by the adversary. Customers could also search for other relevant IOCs such as domains and IPs in other Cisco Secure solutions like Umbrella and Cisco Secure Network Analytics.

If you find yourself a victim to this campaign or others that have dropped webshells and think you may need incident response help. CTIR has already been dealing with multiple incidents and stands ready to help remediate any issues that may have been uncovered.

Conclusion

As the days have passed, the effect of Hafnium has only grown. Patching is the first order of business for any organization, but shortly thereafter, or concurrently, investigation into if and

how you were compromised is going to be paramount. Talos' intelligence provides many avenues for defenders to not only prevent compromise from occurring as the amount of actors leveraging these vulnerabilities increases, but also hunt for any activity that may have already occurred. As we learn more about the nature of these attacks and the end goals, we will continue to provide updates on what we are seeing in the field from the perspective of our threat intelligence researchers and incident responders.

Coverage

Snort SIDs:

- CVE-2021-26857 — 57233-57234
- CVE-2021-26855 — 57241-57244
- CVE-2021-26858 & CVE-2021-27065 — 57245-57246
- CVE-2021-24085 — 57251
- CVE-2021-27065 — 57252-57253
- Html.Webshell.Hafnium — 57235-57240

Please note that TLS Decryption is required for detection of the Exchange related SIDs. This is similar to what was required for blue keep. ClamAV coverage:

- Win.Trojan.MSExchangeExploit-9838898-0
- Win.Trojan.MSExchangeExploit-9838899-0
- Win.Trojan.MSExchangeExploit-9838900-0
- Asp.Trojan.Webshell0321-9839392-0
- Asp.Trojan.Webshelljs0321-9839431-0
- Asp.Trojan.Webshell0321-9839771-0

Additional AMP Cloud IOCs for tools and malware related to these attacks:
Powercat:

- Signature name: 20200719101800-3: PowerShell Download String
- Signature name: 20190301175656-4: Raw GitHub Argument

Lsass dumping:

Signature name: 20201124100140-2: RunDLL32 Suspicious Process

Product	Protection
Cisco Secure Endpoint (AMP for Endpoints)	✓
Cloudlock	N/A
Cloud Web Security	N/A
Cisco Secure Email	N/A
Cisco Secure Firewall/Secure IPS (Network Security)	✓
Cisco Secure Network Analytics (Stealthwatch)	N/A
Cisco Secure Cloud Analytics (Stealthwatch Cloud)	N/A
Cisco Secure Malware Analytics (Threat Grid)	✓
Umbrella	✓
Cisco Secure Web Appliance (Web Security Appliance)	N/A

Cisco Secure Endpoint (AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try AMP for free here.

Cloud Web Security (CWS) web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email Email Security can block malicious emails sent by threat actors as part of their campaign.

Cisco Secure Firewall/Secure IPS (Network Security) appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), Cisco ISR, and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Network/Cloud Analytics (Stealthwatch / Stealthwatch Cloud)

Cisco Secure Malware Analytics (Threat Grid) helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Cisco Secure Web Appliance (Web Security Appliance)

Additional protections with context to your specific environment and threat data are available from the Firepower Management Center.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Indicators of Compromise (IOCs)

Domains (Previously associated with Powerghost):
owa[.]conf1g[.]com
box[.]conf1g[.]com Suspicious Powershell download activity:
hxxp://cdn.chatcdn[.]net/p?hig190509
hxxp://cdn.chatcdn[.]net/p?hig190521
hxxp://cdn.chatcdn[.]net/p?hig200720
hxxp://cdn.chatcdn[.]net/p?hig210304
hxxp://cdn.chatcdn[.]net/p?hig210305
hxxp://cdn.chatcdn[.]net/p?low190617
hxxp://p.estonine[.]com/low?ipc
hxxp://p.estonine[.]com/p?e
hxxp://p.estonine[.]com/p?smb