Hafnium Microsoft Hack– Active Exploitation of Microsoft Exchange and Lateral Movement

attivonetworks.com/hafnium-active-exploitation-of-microsoft-exchange-and-lateral-movement/

March 9, 2021

- **Reading Time: 2 minutes | Published: March 9, 2021 in Active Directory, Blogs, Cloud, Endpoint Protection, Event, ThreatPath**
- **Tags: Active Directory, APT, cloud, lateral movement, Microsoft, MITRE, Privilege Escalation**

Written by the Attivo Research Team – Contributing members: Gorang Joshi, Anil Gupta, Saravanan Mohan – Microsoft and Volexity have confirmed the active exploitation of vulnerabilities published by Microsoft in Exchange Server. Security research has attributed the exploitation to the Advanced Persistent Threat group known as Hafnium operating out of China. After the initial compromise, Hafnium operators accessed email accounts and deployed web shells on the compromised servers, which they then used to steal data and expand the attack. Since enterprises deploy Outlook Web Access (OWA) on public networks, it enabled the group to compromise many organizations across a large set of industries, according to ThreatPost's blog.

Considering the criticality of the vulnerabilities, Microsoft released out-of-band patches on March 2, 2021, to fix the reported vulnerabilities. Unfortunately, many organizations have not patched immediately, and attackers compromised them before the patch was available, resulting in the group using the web shell backdoor to move further inside the network. Volexity confirmed the attackers combined the Exchange exploitation with another vulnerability, CVE-2021-27065, to perform remote code execution (RCE) and conduct lateral movement.

Attivo Networks advises all customers who use vulnerable Exchange Server versions to apply the patch immediately to prevent a compromise. It is also imperative for organizations to know if the Hafnium group has moved laterally inside the network prior to patching Exchange Servers.

Volexity's blog summarizes the threat's criticality for enterprises if the adversary has targeted them.

"In all cases of RCE (remote code execution), Volexity has observed the attacker writing web shells (ASPX files) to disk and conducting further operations to dump credentials, add user accounts, steal copies of the Active Directory database (NTDS.DIT), and move laterally to other systems and environments."

Having robust products and processes to detect lateral movement early before the adversary gains a foothold deep inside the enterprise's network and systems is critical to protect its data and "crown jewels." Fortunately, there are mature tools available to detect lateral movement accurately without incurring significant investment.

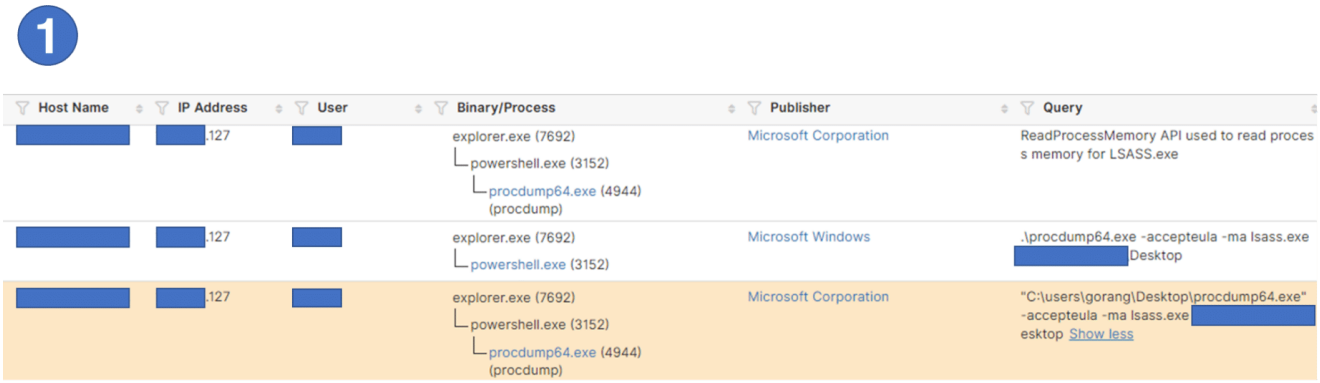
How can Attivo Networks customers detect if they have been exploited and are attempting to move laterally?

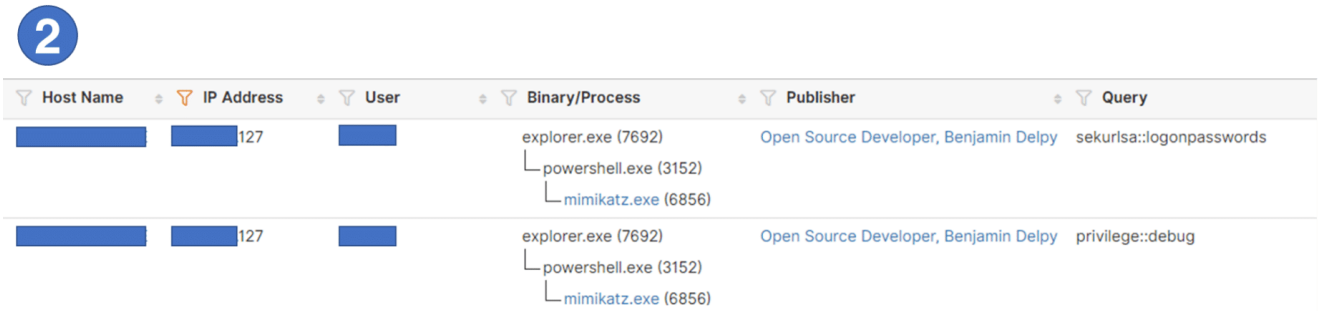
Attivo Networks prevents and detects lateral movement and privilege escalation inside the network by specializing in protecting identities, credentials, and high-value assets across endpoints, Active Directory, and cloud infrastructure.

Below are five examples of Indicators of Compromise captured by Attivo solutions, related to documented adversary activity specific to the group:

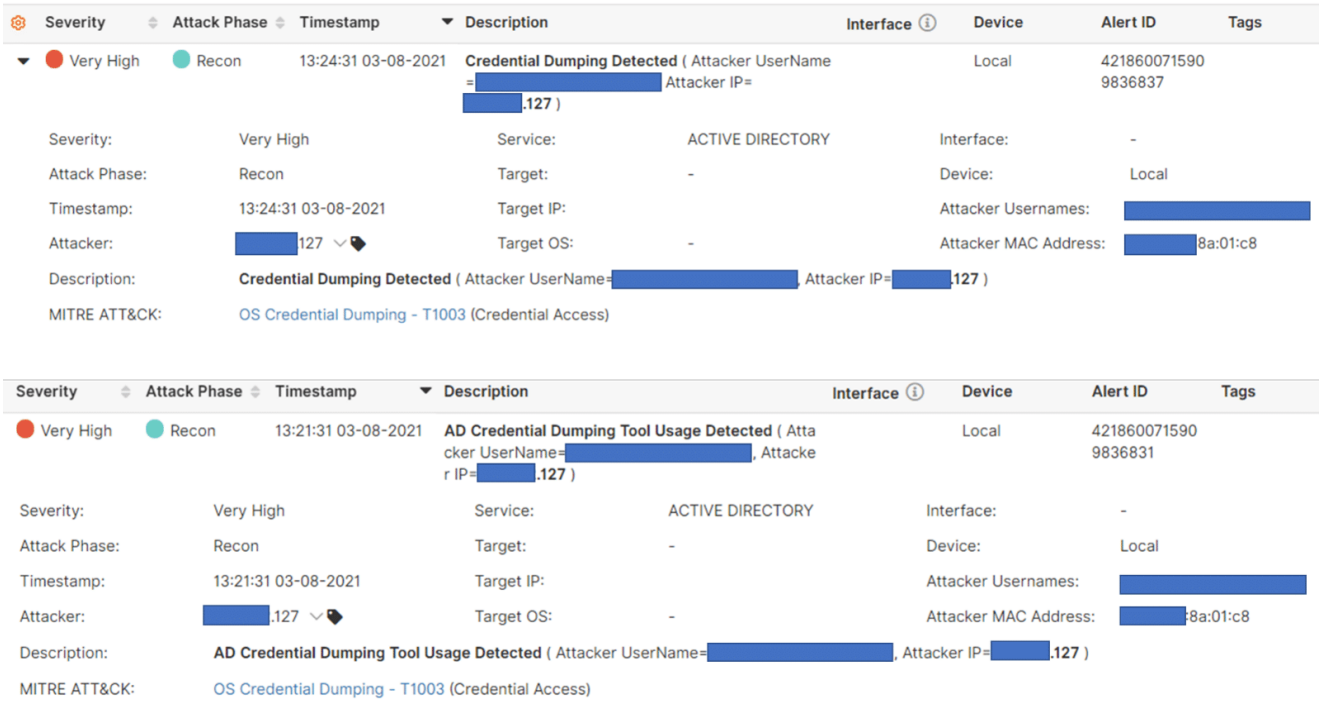
1.The attacker used MITRE ATT&CK Techniques T1003.001, Dumping lsass.exe Process Memory to steal privileged Credentials from Exchange Server using procdump64.exe.

2.Although researchers did not document this specific technique, adversaries widely use MITRE ATT&CK Techniques T1003.001, Dumping lsass.exe Process Memory to Get Credentials using Mimikatz.exe.





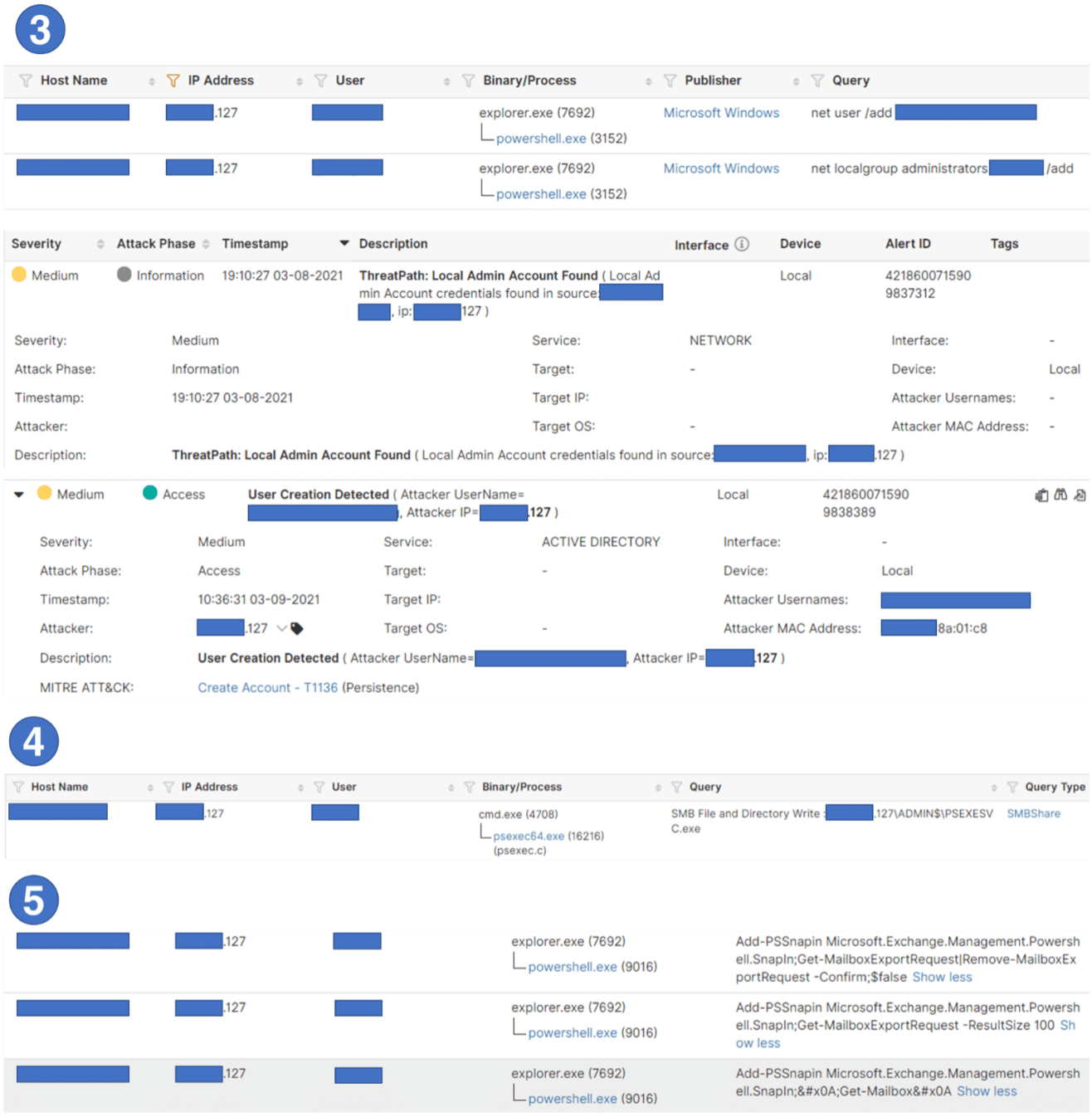
If attackers use these techniques, the Attivo solutions would report the following events.



3.The attackers created Local Admin accounts for persistence. The Attivo EDN ThreatPath module reports when attackers create new Local Admins, Privileged Domain accounts, or Delegated Admin accounts (MITRE ATT&CK Techniques T1136). The EDN ADSecure module prevents adversaries from exploiting domain privileged and local admin accounts by preventing access to them.

4.The group used PSExec against a Remote System (MITRE ATT&CK Techniques T1021).

5.Attackers also added Exchange PowerShell snap-ins to export Mailbox Data (MITRE ATT&CK Techniques T1059).



Conclusion

This incident is another example of how sophisticated attackers can combine multiple attack techniques to exploit and move laterally inside the enterprise. Prevention technologies and patching are critical, but they are not enough, as the attackers have demonstrated. Customers need solutions that will detect adversaries early as they move inside the network to access sensitive or essential data, and Attivo offerings do just that.

Share on:

Free Active Directory Assessment

Get Visibility Into Privilege And Service Account Exposure

For a limited time, Attivo Networks is providing free Active Directory Security Assessments to demonstrate how ADAssessor provides unprecedented and continuous visibility to AD vulnerabilities.

Get Started

Try Our Endpoint Detection Net (EDN) for Free

FAST AND EASY

Free use offer of our Award-winning security solution to prevent attackers from lateral movement, credential theft, and privilege escalation, fast and easy.

Sign up now

Newsletter Signup

-
-
-
- Yes, please opt me in to receive your quarterly newsletter, event invitations, and product updates.

  I understand that I can opt out at any time, and can refer to Attivo Networks Privacy Policy for more information.
-
- This field is for validation purposes and should be left unchanged.

ADSecure 90-Day Free Trial

GET PROTECTION AGAINST UNAUTHORIZED ACCESS TO ACTIVE DIRECTORY

- Hide and deny access to AD objects
- Get alerted on unauthorized queries
- Attack details easily viewable in dashboard

- Your data remains on-premise

Sign me up

RSS

Leave a Comment

Your email address will not be published. Required fields are marked *

three × 2 =

Ready to find out what’s lurking in your network?

Schedule Demo
Contact us

Privacy Overview

This website uses cookies to improve your experience while you navigate through the website. Out of these cookies, the cookies that are categorized as necessary are stored on your browser as they are essential for the working of basic functionalities of the website. We also use third-party cookies that help us analyze and understand how you use this website. These cookies will be stored in your browser only with your consent. You also have the option to opt-out of these cookies. But opting out of some of these cookies may have an effect on your browsing experience.

Necessary cookies are absolutely essential for the website to function properly. This category only includes cookies that ensures basic functionalities and security features of the website. These cookies do not store any personal information.

Any cookies that may not be particularly necessary for the website to function and is used specifically to collect user personal data via analytics, ads, other embedded contents are termed as non-necessary cookies. It is mandatory to procure user consent prior to running these cookies on your website.