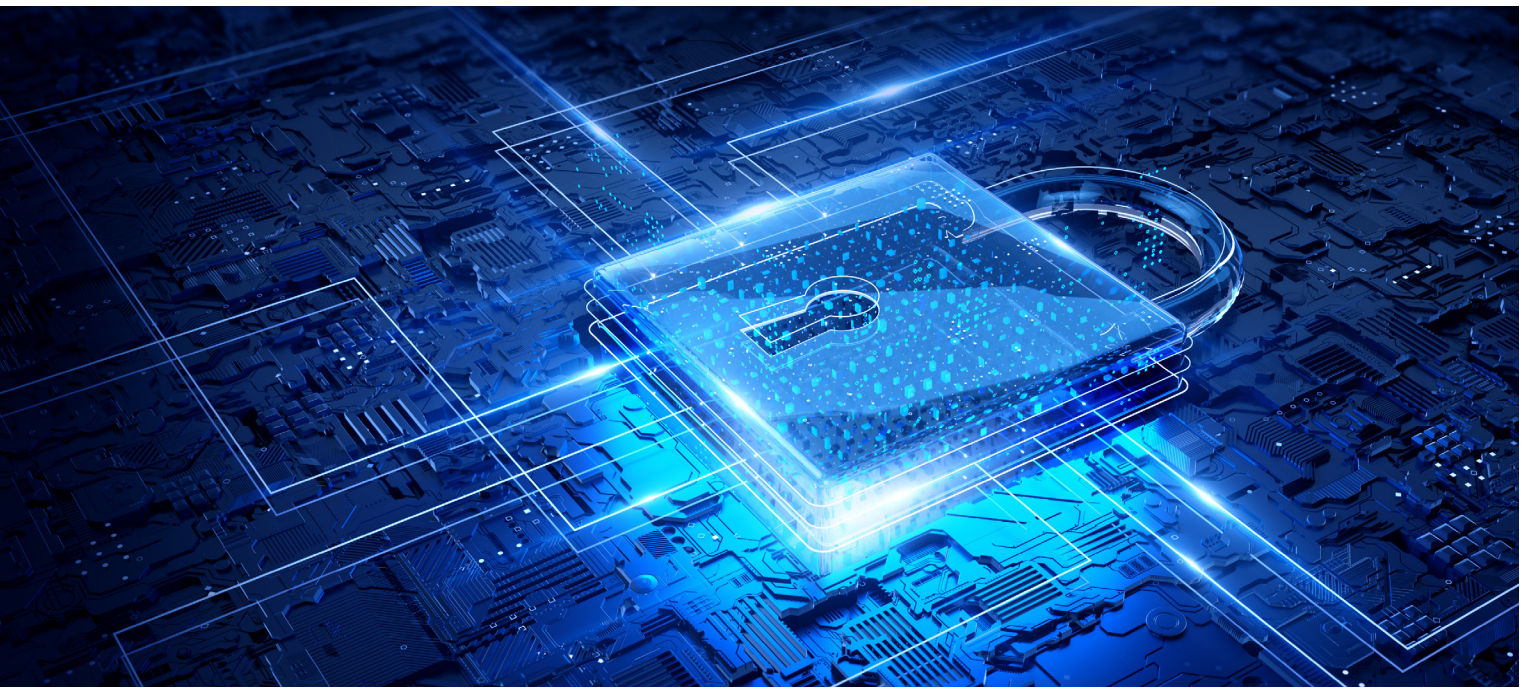
Exchange Server Exploits: How to Spot and Stop Vulnerabilities Resulting from HAFNIUM Attacks

Four cybersecurity experts weigh in on the exploit against on-premises Exchange Servers. Gauge your risk of infection and see how to use Microsoft and Quest® tools to limit damage.

By Paul Robichaux, Microsoft Office Servers and Services MVP; Jeff Guillet, Founder, EXPTA Consulting; Bryan Patton, Stra-tegic Systems Consultant, Quest; Michael Van Horenbeeck, Sr. Solution Architect, The Collective



"How can I tell whether my environment has been compromised? What are the indicators of compromise (IOCs)?"

"Where does the exploit lead? What is happening in infected organizations?"

"How can I protect my environment from future exploits like this?"

Sysadmins like you want the answers to those questions after any major exploit, and the HAFNIUM zero-day attack has been no exception.

This technical brief summarizes the perspectives and advice of four cybersecurity experts. It is designed for any organization with an on-premises Exchange Server, even if that server is there only to help manage hybrid Active Directory or Exchange. The brief explains the measures you should take with tools from Microsoft and the ways in which Quest customers can use Change Auditor to investigate and stop attacks. Because of the quickly evolving nature of this attack, Quest recommends following Practical365.com for the latest details and mitigation techniques.

HOW SERIOUS IS THIS EXCHANGE SERVER ATTACK?

In March 2021, Microsoft reported multiple zero-day exploits against on-premises versions of Exchange Server. It has described the risks and affected versions (2013, 2016 and 2019) of Exchange Server related to security flaws listed in CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065. In April 2021, they reported four more remote code execution flaws: CVE-2021-28480, CVE-2021-28481, CVE-2021-28482 and CVE-2021-28483. (Exchange Online is not affected by the exploit.)

This attack is serious enough to prompt the Federal Bureau of Investigation (FBI) to obtain court authorization to patch some infected servers in the USA. While most companies applied Microsoft's security patches (see below), too many did not.

[1] This technical brief is adapted from the Quest webinar, "HAFNIUM Exchange Server Hack: Why Patching Isn't Enough & Where to Start Hunting," currently available at https://www.quest.com/webcast-ondemand/hafnium-exchange-server-hack-why-patching-isnt-enough-where-to-start-h8147979/

So, the FBI took the unprecedented step of ethically hacking certain U.S. organizations to copy and remove malicious web shells from hundreds of vulnerable computers running on-premises versions of Microsoft Exchange.

That's how serious this attack is.

WHAT'S MY FIRST RESPONSE?

Microsoft has issued a security update for the first set of flaws[2], **which you should install immediately**. To make mitigation as easy as possible, the company has taken the extra step of releasing a script, the Exchange On-premises Mitigation Tool (EOMT). The script runs the Microsoft Safety Scanner (see below), after automatically downloading any needed dependencies. For Exchange deployments with internet access and for admins looking for ways to automate remediation, the script is a smart approach.

Microsoft has issued another security update for the second set of flaws, **which you should also install immediately.**

Note, though, that the flaws are being exploited as part of an attack chain, of which an untrusted connection to Exchange Server is an indicator. That's why, in its recommended response steps, Microsoft has emphasized that patching the four flaws does not remediate already-infected systems. If your Exchange Servers have been compromised (see below), you should expect subsequent exploits, **even if you apply all security patches**.

In other words, plan to **patch, then investigate** whether your system has been compromised, then respond. Like most other attacks, this exploit is an avenue for an attacker to gain access to the rest of your network, so you must investigate beyond Exchange.

Besides the serious hit of having an attacker **put something like a web shell** on your email server, you have to consider that whatever happens next may be even more serious. The threat comes not only from the original attacker's next move, but also from unrelated bad actors who reverse-engineer the patch and exploit the same vulnerabilities. Ransomware and cryptocurrency mining are two of the most likely next moves.

HOW DO I KNOW WHETHER OUR ON-PREMISES EXCHANGE SERVER HAS BEEN COMPROMISED?

Microsoft has released a PowerShell script that scans Exchange Server logs for indicators of compromise related to this attack. That is an important step toward determining your status and what you'll do next.

Is any version of Exchange Server more or less vulnerable than the others?

In short, the versions are equally vulnerable. More important than the version you're running or the country of your premises is whether your server faces the internet; if so, it's vulnerable.

Note that Microsoft has included in the first security updates a patch for Exchange Server 2010, a version it no longer supports but which plays a role in hybrid deployments. That is an indicator of the gravity of the situation and the potential vulnerability.

What about the role of the Exchange Server in hybrid Active Directory? How does that relate to vulnerability?

Many companies have moved their mailboxes to the cloud and now maintain an on-premises Exchange Server only because Microsoft requires it for hybrid Exchange and AD. If that's the only reason for yours **and** you're not publishing from the server to the internet, then your environment is not vulnerable.

Yet.

> If your Exchange Servers have been compromised, you should expect subsequent exploits, even if you apply all security patches.

[2] The first update also covers Exchange Server 2010, for defense-in-depth purposes.

The fact is that a vulnerable Exchange Server, whether exposed to the internet or not, represents a potential threat to your organization. Through lateral movement, an attacker can break into one resource on your network — like Exchange Server — then exploit that access to break into another resource. While a compromised Exchange Server may not broaden your attack surface right now, its wealth of permissions in AD will make your compromised server an appealing target for the next attack.

Note also that your on-premises Exchange Server communicates with Exchange Online over TCP port 443. If your on-premises Exchange Server is only for hybrid AD, then you should close port 443 as a precaution.

Are you maintaining an Exchange Server that just sits there so you can, say, run hybrid PowerShell commandlets? An attacker who can compromise that server may also be able to leapfrog from there into capturing a privileged account or exploiting a vulnerability elsewhere on your network.

What else in our environment do I need to be worried about besides Exchange Server?

The dynamics of the Exchange Server exploit suggest initial penetration followed by a rush of different groups of attackers with different advanced persistent threats (APT). Operating from different countries with different signatures, these large-scale attacks represent a new kind of behavior.

As mentioned above, ransomware such as DearCry is a likely next move, whether by the same attackers or by bad actors taking advantage of this attack. Another likely move is for attackers to persist on the network for now, then launch an exploit later for maximum damage or profit. Imagine a back door placed on the network of a large retailer that introduces a ransomware attack in the run-up to the holiday season.

Besides back doors, a compromised Exchange Server could lead to golden ticket attacks, privilege escalation, AdminSDHolder permissions, delegated permissions and other artifacts of the tight integration between Exchange and AD.

Suppose a domain administrator logs on to the Exchange Server to patch it, and in-memory malware captures those credentials. An attacker could then log on and dump all the credentials from the server. With the hashes of the domain administrator, the attacker can move laterally to, say, a domain controller or any other computer in that tier and do almost anything. It's not easy, but it is possible, and in that state you may have to consider resetting the KRBTGT password to defend against Golden Ticket attacks.

How does this attack work?

The mechanics of this hack are sophisticated.

In essence, it's a new way to exploit a one-line .aspx web shell called China Chopper that has been around since about 2013. It lands through one of the security flaws in Exchange Server. From there it cascades, as this CISA diagram illustrates, by creating a system account, then scheduling a task to fetch a payload that PowerShell executes. That creates a process that connects to another server that eventually ends with mimikatz, a set of tools for harvesting directory accounts and AD passwords.

The main IOCs include an added web shell in the form of .aspx files in the WWWroot\ASP_client folder. There shouldn't be anything there; .aspx files are where you'll find web shells in Windows.

WHAT SHOULD I DO IF OUR EXCHANGE SERVER HAS BEEN COMPROMISED?

The Microsoft Support Emergency Response Tool (MSERT.exe), also called Microsoft Safety Scanner, is designed to thoroughly scan and scrub computers running Windows. It searches for malicious software like the China Chopper web shell and removes it. It's important to **run MSERT repeatedly**, even if it shows no infections and even though it is extremely processor-intensive.

Microsoft updates MSERT one or more times per day and requires that you download a new version every ten days. That way, you're not running an old tool that indicates you're in the clear when you're not.

> More important than the version you're running or the country of your premises is whether your server faces the internet; if so, it's vulnerable.

The dynamics of the Exchange Server exploit suggest initial penetration followed by a rush of different groups of attackers with different advanced persistent threats (APT).

Once you've run MSERT, if you determine that the exploit is running on your Exchange Server, you'll find yourself in incident response mode. You'll be trying to figure out how far the attackers have gotten.

First, it's a matter of the defenses you already had in place. Strong endpoint protection on your Exchange Servers and regular updates to Windows Defender or your antivirus software of choice are your first line. Even if the web shell got past them, they may have identified and eliminated mimikatz before it could gather any credentials.

Next come the security patches mentioned above. If your Exchange Server has not already reminded you to apply them, you can find them here and here. If you run a database availability group (DAG), you should be able to patch each server one at a time without incurring an outage.

Then, work on damage control. If the web shells are present, a conservative assumption is that you've been breached and credential dumping has taken place. A sound response is to reset passwords for all accounts, including local ones. If you have a disaster recovery plan, consider this an opportunity to test it by restoring your Exchange Server to a clean OS — offline — and getting authentication going again.

Finally, start investigating. At this point, you move beyond antivirus software in the protection stage to the endpoint detection and response (EDR) products that will help you identify suspicious activity.

Examine your security groups for accounts that shouldn't be there, such as accounts that didn't exist before and domain admins who haven't been with the company in years. Keep in mind that you're vulnerable in more than just the obvious places. Activity like credential dumping usually triggers high alerts, which have a high probability of detection. To get around that, some attackers will hide their tracks and stick to less-obvious activity that triggers medium, low or no alerts.

Note that you may be tempted to rebuild the entire AD as a precaution. While that seems like an effective, from-the-ground-up measure, it's not practical if you have a single Exchange Server, which is the case in most organizations.

MONITORING THREATS WITH CHANGE AUDITOR

Because the worst threats come from attackers trying to capture and misuse credentials, you have to protect AD as the backbone of your organization. Because AD provides authentication and authorization for access to every resource on your network, the most likely attacks will try to modify AD to grant that access to bad actors.

Change Auditor from Quest performs real-time IT security auditing on changes to AD, Azure AD, Exchange, Office 365, file servers and more. It tracks detailed user activity for logons and authentications to enhance threat detection and security monitoring.

Changes to AD

As you investigate your exposure from the Exchange Server attack, use Change Auditor to run searches on recent changes, like new or changed accounts and privilege escalation. Valuable Active Directory reports and alerts from Change Auditor include changes to Group Policy, changes to the membership of privileged groups, activity of privileged users and new user accounts.

With the search function in Change Auditor you can look for events leading up to user account lockouts and abuse of privileges, then turn them into useful and relevant reports.

Features in Change Auditor allow you to audit and protect the Active Directory database, Ntds.dit, which attackers may attempt to copy and extract. Through the event stream, Change Auditor can protect the database, prevent the extraction and alert you to the attempt.

Authentication risks

The security threat monitoring in Change Auditor can alert you to users trying to capture password hashes in your organization. Its enhanced security auditing is designed to stop attempts to run DCSync, a command associated with mimikatz. DCSync is used to capture the hash for your KRBTGT password, which is one of the elements in creating a Golden Ticket that grants access to the entire domain.

Kerberos tickets are at the heart of authentication and authorization in Windows. By default, they have a time to live (TTL) of 10 hours, so attackers commonly build a ticket with a TTL of 10 years (golden ticket) for persistence. Although you can't look up the ticket lifetime in the Windows event log, with Change Auditor you can set alerts to detect changes in TTL.

HOW DO I PROTECT OUR ENVIRONMENT AGAINST FUTURE EXCHANGE SERVER ATTACKS?

After investigation and response, you'll enter the recovery phase and begin to think about what you can do differently in the future.

Do I really need Exchange Server on premises?

If you're running email yourself, away from the cloud, then obviously you must keep the server on premises.

For hybrid operations with mailboxes moved to the cloud, Microsoft requires that you keep Exchange Server on premises. For now, that is how you manage things like email addresses and distribution groups that are on premises and synchronized with the cloud. It is also how you provide a secure, internal relay for connecting external users to on-premises assets like application servers and printers. The problem is that many organizations have good reasons for keeping Exchange Server on premises, but they don't have the staff, expertise or operational maturity to run it securely.

So, if you must live with Exchange Server on premises, you must also **apply security patches as soon as they are available**. Believe it or not, many sysadmins — maybe some in your company — don't know how to install those patches, usually because they haven't had to do so in a long time. If you're running Exchange Server —or any similar workload —on premises, this is a good time to **ensure that all your sysadmins know how to patch it**. That includes knowing how to download a cumulative update (CU) or patch and install it, and knowing how to perform this task regularly.

As described above, the server is still vulnerable, especially if it faces the internet. Many organizations needed it to face the internet for the hybrid migration, but once migration is finished, that internet connection becomes a vulnerability. Protect your Exchange Server by **blocking it at the firewall from external access**.

Software

It's a good idea to learn from this attack how to build up your software defenses against the next one.

You may be tempted to invest in better antivirus protection. However, an antivirus software scan is not likely to catch zero-day exploits like this one. For that matter, the HAFNIUM attack placed web shells in a web directory where anybody would expect to find them; it's unlikely that antivirus software would find that.

In short, it's no longer enough to install protection and put up fences against this kind of exploit. This is where telemetry EDR comes into play. **Get an endpoint detection and response (EDR) product**, run Sysmon and get the logs in the SIEM, then build your own use cases. It's much more work to piece together what's happening, but it leads to better intelligence. A file landing on the server isn't necessarily malicious, but EDR helps you correlate multiple events, like what that file or shell did next, to detect what's happening.

> It's important to run MSERT repeatedly, even if it shows no infections and even though it is extremely processor-intensive.

While rebuilding AD seems like an effective, from-the-ground-up measure, it's not practical if you have a single Exchange Server, which is the case in most organizations.

Firewall

Installing a web application firewall or gateway in front of the Exchange Server adds protection and detection. It also adds response capabilities, because you can use it to block specific IP addresses, requests, user agents and the like. The crux of the exploit is a web server; therefore, the protection, detection and response from a firewall or gateway would apply here as well.

Placing a **reverse proxy in front of the Exchange Server** would also add a layer of security. Better yet, a smart, reverse-proxy web application firewall can filter incoming requests. While it might not catch every malicious request on the way through to the Exchange Server, it should detect and thwart injection attacks.

Logging/Auditing

Most suspicious events in your environment generate entries in a log, so it makes sense to review your log for bread crumbs during your investigation phase. You're trying to find any evidence of an attack such as credential dumping.

But there's a feast-or-famine aspect to logging and auditing that can trip you up. The feast is that you can easily be so overwhelmed by the volume of events in Windows logs that you can't isolate the most useful bread crumbs. The famine is that too many companies, especially small ones, don't have logging in place or haven't had it in place long enough for it to be useful.

Change Auditor does not rely on Windows event logs or impose the same overhead on servers that Windows auditing policies can impose. It uses an agent to track events so you can identify what has occurred in your environment. Change Auditor pinpoints where the event occurred, who caused it, on which domain controller the change originated and the before- and after- values. The result is a concise view of the event with the details necessary to take the next step.

Privileged Access

To avoid privilege escalation as a result of future attacks, adopt a privileged access strategy if you don't yet have one in place. Bad actors holding privileged access have graduated from perpetrating data thefts to launching ransomware attacks, and tiering is a valuable technique for preserving privileged access.

In brief:

- Tier 0 includes the identity servers, such as domain controllers.
- Tier 1 includes server administrators.
- Tier 2 includes the endpoints.

Accounts with manager privileges in Tier 0 should not have those privileges for Tiers 1 and 2. That way, if an endpoint is compromised, there is no easy path of escalation to Tier 0.

Microsoft has enhanced this AD tier model for the modern enterprise to keep pace with business realities like hybrid environments, multiple clouds and access to both internal and external users.

Backup and Disaster Recovery

The increased danger of ransomware makes it important for you to **back up regularly**.

It's also wise to maintain **an offline copy of your AD database** in a secure area that can't be affected by ransomware, with limited user access. Attackers often extract a copy of the database and hack it offline later, so it's necessary to ensure that only vetted backup tools can copy it. Customers of Quest Recovery Manager for Active Directory Disaster Recovery Edition can accommodate that by creating an allow-list for the AD database, Ntds.dit, in Change Auditor. That authorizes Recovery Manager to back up Active Directory and prevents unauthorized executables from backing it up or copying it.

Beyond the tools, however, is your organization's overall disaster recovery posture. Many admins have tried in vain to make the case to upper management for backup, disaster recovery and the downtime to test them. If you've been sounding the alarm about your company's exposure in case of a disaster, use this attack to **reinforce your case and get the sign-off you need**. If you believe your disaster recovery processes and knowledge are weak, it's a fitting time to talk about the thousands of companies whose lunch money will soon be stolen.

"We don't want that to be us," you'll tell management, "but we need a way to take an offline backup and store it. We need training in incident response. We need retainer agreements with experts so that, if we are attacked, we can turn to somebody for help in cleanup." If you've had trouble in the past getting business approval for those, strike now while the iron is hot. This is not the last time you'll see this class of attack.

CONCLUSION

Finally, our cybersecurity experts reflect on the overarching lessons of the HAFNIUM Exchange Server attack.

- **Support business continuity —** Your tools and approach are rooted in technology, as are threats like zero-days. Your mission, however, goes beyond technology to keeping your business up and running. This is an opportunity to think about how you can sustain business operations in spite of losing portions of your infrastructure.
- **Patch religiously —** Apply the security patches Microsoft has provided to remove your vulnerability, then evict any web shells as soon as possible. Keep in mind that it's easier to explain two hours of downtime to patch Exchange than it is to explain how your organization's credentials ended up on the internet.
- **Stay vigilant —** Why did HAFNIUM attack Exchange? Because Exchange is one of the most widely deployed, on-premises applications in the enterprise. Which other popular, on-premises applications are you running? SAP? Oracle? Plenty of people right now are looking for ways to attack those, so don't think you're in the clear just for having patched Exchange Server.
- **Keep learning —** If you find gaps in your incident response knowledge, your processes, your logging, your auditing or your general security knowledge, plug them. As defenders, we have to be lucky every time, but attackers don't have to be lucky but once to get into your network and then start moving laterally.

Note that Quest recommends following Practical365.com for the latest details on and mitigation techniques for this attack.

NEXT STEP

Change Auditor audits all significant changes to Exchange Server and Exchange Online, including mailbox logins/access, non-owner mailbox activity and permission changes. It simplifies reporting in Exchange with real-time audits that protect your organization's security policies.

Try Change Auditor at no cost for 30 days to see how it can help you prevent compliance violations, system downtime, lateral movement and productivity loss.

ABOUT THE CONTRIBUTORS

Paul Robichaux is a Microsoft Office Servers and Services MVP and senior director of product management at Quest Software.

Jeff Guillet is founder of EXPTA Consulting in the San Francisco Bay Area. He is an Exchange Server Microsoft Certified Master and a Microsoft MVP.

Bryan Patton is a CISSP and principal strategic systems consultant with Quest. He helps Quest's hybrid Active Directory clients secure their infrastructure through AD security assessments. Bryan is an expert on Change Auditor from Quest.

Michael Van Horenbeeck is a Microsoft Certified Solution Master. He is an independent consultant and Microsoft Office Servers and Services MVP.

By default, Kerberos tickets have a time to live (TTL) of 10 hours, so attackers commonly build a ticket with a TTL of 10 years (golden ticket) for persistence.

ABOUT QUEST

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.