ConversationalGeek

5 WAYS *to* MITIGATE RISK

Against *Zero Day Attacks* Targeting Microsoft Exchange

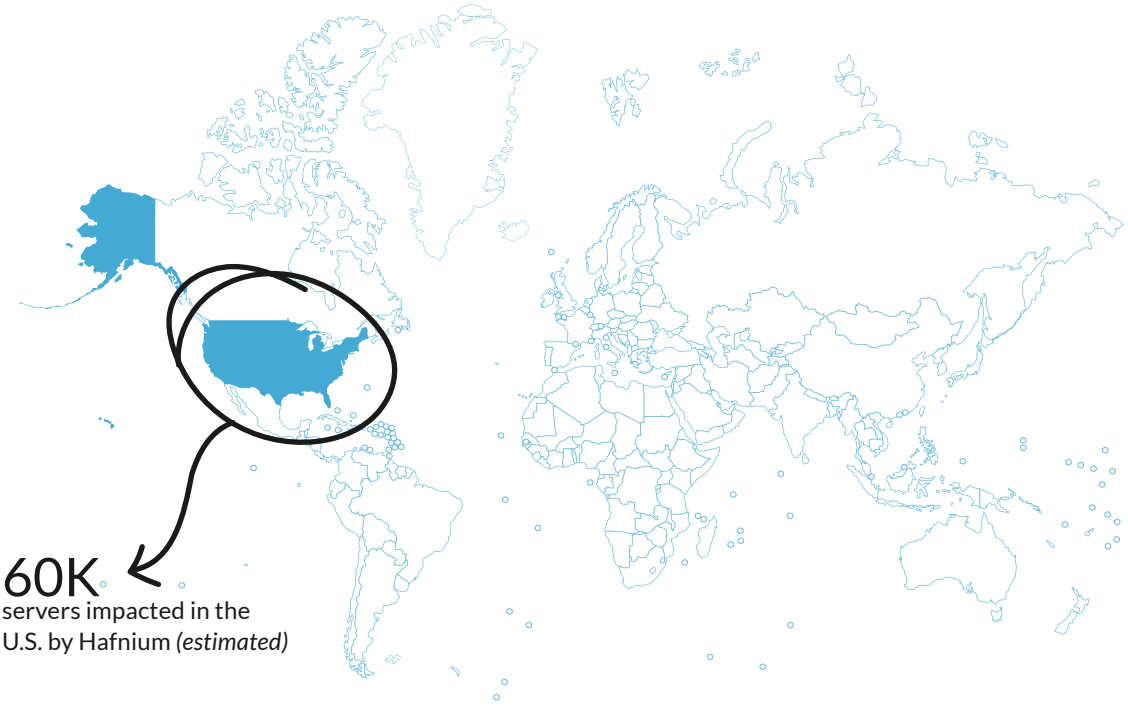
www.conversationalgeek.com

Why Worry About Zero Day Attacks Against Microsoft Exchange?

If you're reading this, your organization likely still utilizes at least one of the estimated 250,000 on-premises Microsoft Exchange servers today. The emails these servers host contain some of your organization's most sensitive information. The servers also represent a critical communication medium that organizations simply can't do without for an extended period of time.

Zero Day Attacks – those attacks that take advantage of a vulnerability found by cybercriminals before a vendor can issue a fix – are one of the cybercriminals greatest advantages. Often providing privileged access, Zero Day Attacks become the means for a single cybercriminal group to potentially gain access to literally tens or hundreds of thousands of organizations in every geography, industry vertical, size, and country.

The most recent Zero Day Attack on Microsoft Exchange originated from a Chinese cyber espionage group, dubbed "Hafnium" and was first spotted by cybersecurity researchers in January of 2021. In total, Hafnium exploited four vulnerabilities to exfiltrate mailbox contents, gain admin control over compromised servers, and install malicious software. In all, it's estimated that as many as 60,000 servers running Microsoft Exchange 2013, 2016, or 2019 in the U.S. alone were affected.



While Microsoft did respond to the attack, initial mitigations and updates were not released until March of 2021. In the time between the attack's discovery and mitigation, organizations that were attack targets were largely helpless to defend themselves.

When zero day attacks like this are announced, it's imperative that organizations work diligently to patch their servers as quickly as possible, following the directions from Microsoft to update affected services and to investigate for indicators of compromise as the basis for any resulting remediation activity.

Should Microsoft Exchange be the target of another zero day attack, what can organizations do proactively to mitigate the risk? The remainder of this eBook will focus on 5 key risk mitigation steps you can take to protect your Microsoft Exchange investment.

#1 Harden your email perimeter

With 94% of all cyberattacks starting with an email, it makes sense that you need to have a layer of protection that resides logically where an email enters your organization. What's needed is a defense-in-depth approach using third-party solutions that augments any built-in security on Microsoft's part. Doing so creates a layered security strategy that is increasingly difficult for cyberattacks to navigate. The result is to stop any zero day attacks that first need to establish a foothold via phishing.

94% of cyberattacks start with email

5 technologies you should use to harden your email perimeter:

- Domain Protection
- Virtual Sandboxing
- URL Protection
- Credential Harvesting Detection
- Shared Threat Intelligence

Domain Protection

Several technologies exist today to ensure the validity and integrity of emails received. The Domain-based Message Authentication, Reporting and Conformance (DMARC) defines a policy around what should be done with an email where the sending domain appears to be impersonated. The Sender Policy Framework (SPF) is used within DNS to identify the hostnames and IP addresses of valid email senders for a given domain. Putting these in place helps eliminate the possibility of successful domain impersonation on the part of the cyber attacker.

Virtual Sandboxing

The opening of an email can be simulated within a virtual environment where attachments can be detonated to see whether they perform a malicious action.

URL Protection

Links can be scanned in real-time and blocked from being clicked if deemed malicious.

Credential Harvesting Detection

Links and redirects can be intelligently followed to see if they take potential victims to spoofed logon pages to Office 365 and other cloud services. Phishing kits used to quickly prop up an entire fake website front-end for harvesting can also be detected.

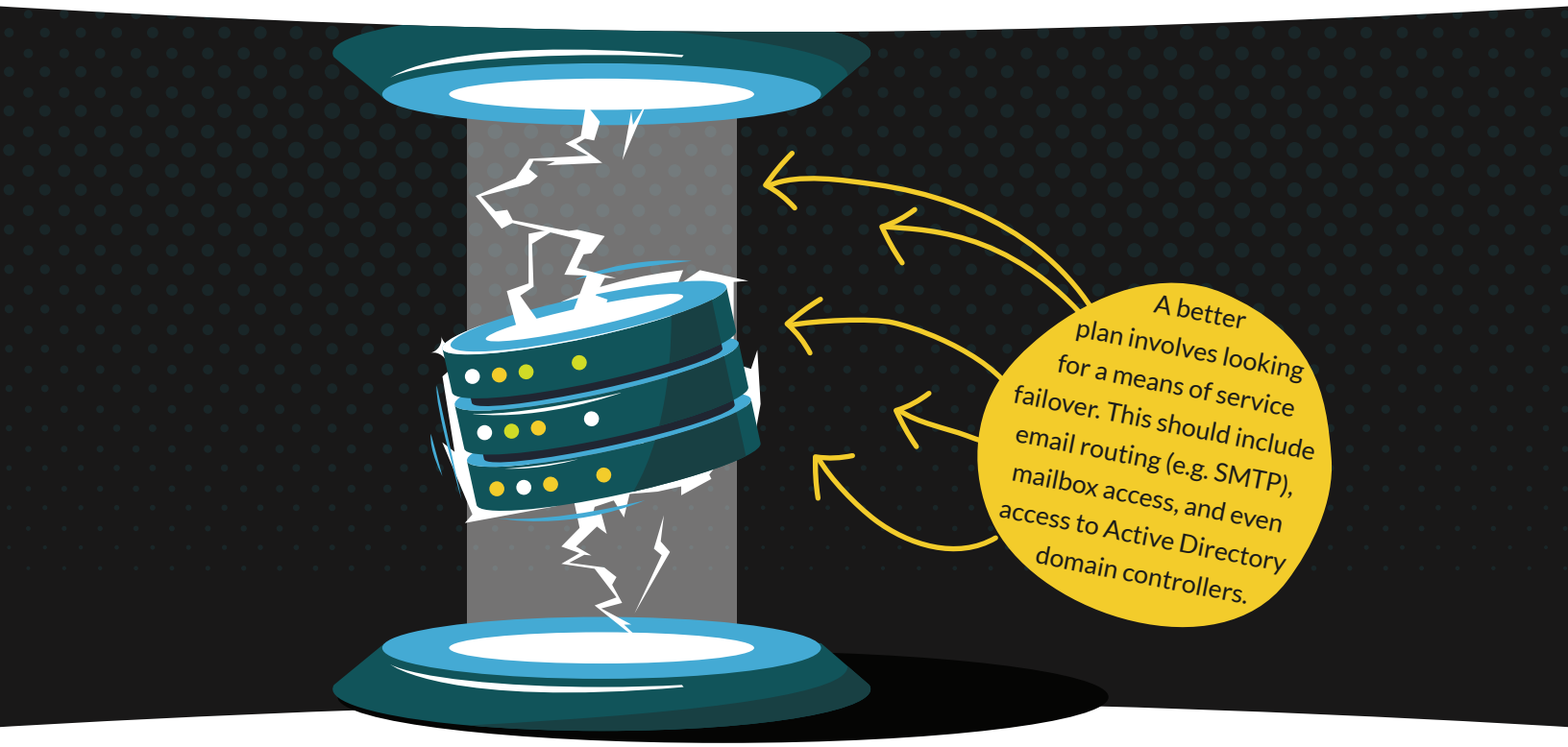
Shared Threat Intelligence

A strong defense rests in it being based on shared threat intelligence to ensure the most up-to-date data to increase detections and reduce risk. In addition, the intel gathered through protecting the email perimeter should be shared back to your SIEM to aid in providing a comprehensive view of what's happening on your network.

#2 Establishing a continuity plan

While there were no reports of Exchange servers rendered completely inaccessible during the Hafnium attack, it's reasonable to assume that impacted servers were taken offline (to eliminate attacker access) while the vulnerabilities were being remediated. Keep in mind remediation may involve the *entire* Exchange environment, taking time to update the affected systems, investigate indicators of compromise, and to perform further remediation to remove access, malware, etc. Additionally, there is no guarantee that the next zero day attack against Microsoft Exchange won't take servers down completely.

So, it's necessary to have a continuity plan – one where email services are available and accessible to some degree. In the simplest of working environments, users of the full Outlook client can continue working offline; while not perfect, it does provide some degree of continuity.



Depending on which servers have been affected (e.g., only an Edge Transport server), it is possible that another server can installed, and the services reconfigured to point to the new server. Additionally, you may have already architected your Exchange environment with some degree of redundancy that, you may be able to isolate affected servers and use secondary servers for some Exchange services.

However, good risk mitigation practices would dictate you don't plan for such a perfect scenario; you need to be thinking what to do if *every* server is down.

Consider third-party solutions that sit externally from your on-premises environment and during normal operations employs SMTP relays to first accept inbound email and then forward it to Exchange. During an outage, email continues to be accepted by the solution and is accessible by special email clients, allowing operations to continue. Once services are restored, any emails that have not yet been forwarded to Exchange, are sent bringing the production Exchange environment current.

This strategy minimizes any downtime caused by either the exploit, updates, or incident response activity. It also specifically mitigates *operational* risk of a zero day attack, keeping the business operational.

#3

Archiving to an independent environment

Along the same vein of thinking as having a continuity plan, those organizations actively relying on an Exchange-based archive, need to be thinking about how long the business can operate without an accessible archive, should the Exchange server hosting your archive be down. There are productivity, legal, and compliance-related ramifications should there be no access to an archive for a prolonged period of time.

Having an archive also can assist with any attacks where attackers modify or delete data within a mailbox, as well as attacks holding Exchange servers for ransom.

The reality is on a daily basis, you don't need to keep everything inside Exchange. In fact, many organizations offload Inbox contents older than just a few months to an archive to minimize the backup data requirements, thereby speeding up recovery operations.

Having a third-party archive that sites outside the Exchange servers mitigates the risk that historical data is inaccessible, inaccurate, or is simple gone.

#4 Ensure Recovery Resilience

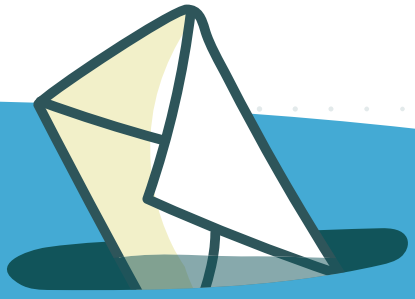
Most victims of the Hafnium zero day attack saw compromised Exchange servers and exfiltrated data. But the potential is there for attackers to continue to exploit the access gained. Actions like data deletion, modification, and encryption (as part of a ransomware attack) are very easy to envision as the next step. While separate archives will help with resilience around older email content, organizations need a way to return the environment back to a working state.

Many victims of a zero day attack may choose to restore servers to an earlier pre-exploit state, but that has implications on productivity, with lost email impacting production. Also, because zero day attacks can begin with a phishing email, simply restoring mailboxes may re-introduce risk.

The idea of resilience in the context of a zero day attack on Exchange includes recovering services and email to a place where operations can quickly continue while simultaneously ensuring no new security risk is introduced.

So, it becomes necessary to not just be able to recover a mailbox and its' data, but to ensure any recovered data is in a known good and known-secure state.

What's needed is to rebuild a mailbox from a compliant, independent source that takes the known good historical mailbox data and updates it with a current (and known-secure) copy of all changes.

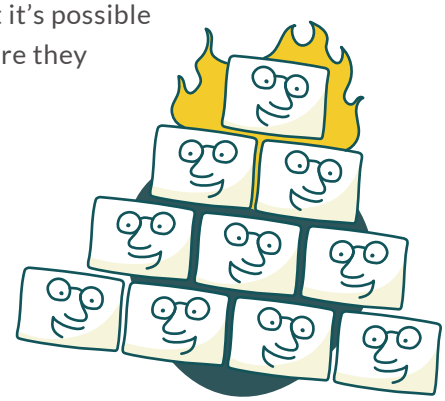


How Do You Solve This?

What's needed is to rebuild a mailbox from a compliant, independent source that takes the known good historical mailbox data and updates it with a current (and known-secure) copy of all changes.

#5 Empower humans and technology to work together to strengthen organizational security

While many zero day attacks focus on servers and services, users play a material role in most cyberattacks, making them a far larger threat surface for the organization. Oftentimes, we look at users as the weakest link in an organization, as they are prone to fall for phishing scams using sophisticated social engineering tactics. But it's possible to turn them into your *"human firewall"*, where they become your last line of defense for your organization.



This is accomplished by combining technology and employees together through continuous *security awareness training*. By using engaging content, users can be taught to have a vigilant mindset, understanding what kinds of attacks are occurring, the tactics used, how to spot them in the middle of doing their job, and to avoid becoming a victim.

But not every employee retains training the same, so organizations need a feedback loop to understand where their greatest human risk exists (that is, which users are most likely to continue to fall for phishing attacks).

By utilizing phishing simulation tests, organizations can gain visibility into which employees are still falling victim to phishing scams, are ignoring obvious signs of impersonation and social engineering, and are clicking links or opening attachments without a scrutinizing eye. These employees represent the greatest risk and can be "patched" through further security awareness training and subsequent phishing testing.

What to do before the next

ZERO DAY ATTACK?

First off, it's important to realize there will be a next time. The harsh reality is the threat actors are becoming more sophisticated and it's necessary to build cyber resilience to be prepared when (not if) attacks occur. Therefore, those organizations currently using an on-premises instance of Microsoft Exchange need to plan ahead. The main question to be answered is "Do you want Exchange to remain on-premises?"

The obvious answer is to migrate to Exchange Online within Microsoft 365. Reportedly, none of Microsoft's Exchange servers within Microsoft 365 were impacted by the Hafnium attack. But a blind lift and shift of your on-premises Exchange data isn't the right answer; should you look to migrate to Microsoft 365, there needs to be a de-risking of the move, including:

Archive Before Migrating

Office 365 only needs to house current business email and content. So, looking to archive before the migration minimizes the amount of data the needs to be pushed into the cloud. Having a solution that can archive your on-premises Exchange pre-migration and then be pointed to Office 365 post-migration is an effective answer.

Plan Licensing

Once you put something in the cloud, there is an immediate monthly cost. Take count of how many employees need licenses, which licenses they need, etc.

Address Support Headcount

Staffing needed to support both the move and the subsequent ongoing management may look different than it does today. Consider headcount needs for administration, backups, licensing, and support.

Take Care of Backups

Microsoft is a firm believer in the shared responsibility model, and backups of all data within Office 365 – including Exchange Online – are the customer's responsibility. Have a solution in place and a backup strategy ready once you begin your migration.

Considering What Else Should be Consolidated

Because the organization will likely take advantage of other services such as Teams, OneDrive for Business, SharePoint Online, and more, there may be a similar opportunity to consolidate which data gets moved to those new platforms.

Assess the risk of "good enough"

Microsoft offers plenty of supporting solutions around Office 365 to address archiving, security, compliance, and more. Assess the risk that may be introduced by relying on a single vendor (something pointed out a few times in this eBook), and consider the need for additional third-party solutions to offset the risk.

mimecast™

Mimecast was born in 2003 with a focus on delivering relentless protection initially for email. Each day, we take on cyber disruption for our tens of thousands of customers around the globe; always putting them first, and never giving up on tackling their biggest security and resilience challenges together. But we haven't stopped there, we are the company that built an intentional and scalable design philosophy that addresses the number one cyberattack vector – email. We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error and technical failure; and to lead the movement toward building a more resilient world.

For more information, visit: www.mimecast.com