Exploits on Organizations Worldwide Grow Tenfold after Microsoft's Revelation of Four Zero-days

blog.checkpoint.com/2021/03/11/exploits-on-organizations-worldwide/

March 11, 2021

Following the revelation of four zero-day vulnerabilities currently affecting Microsoft Exchange Server, Check Point Research (CPR) discloses its latest observations on exploitation attempts against organizations that it tracks worldwide.

****Updated March 15th 2021 5:30 ET***

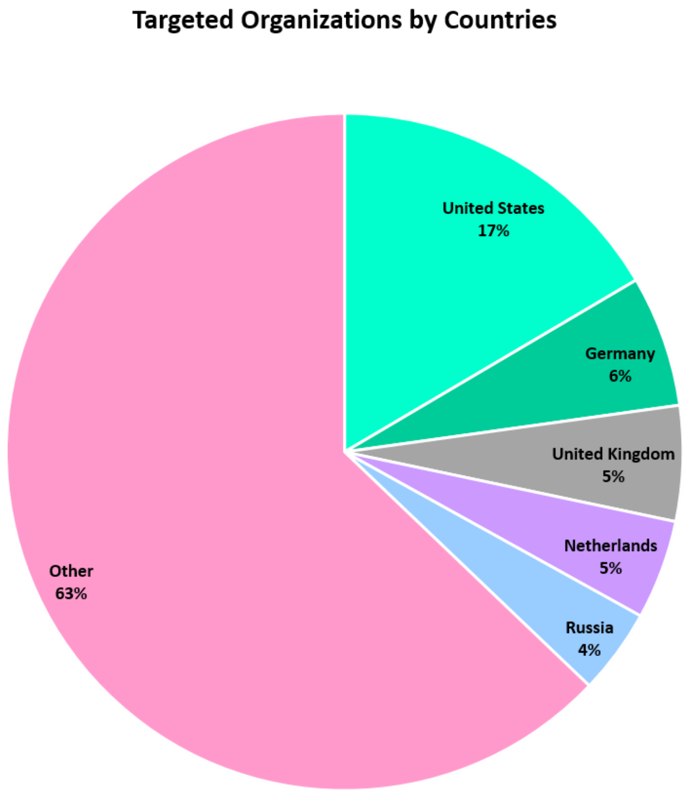
By, Yaniv Balmas, Head of Cyber Research; Lotem Finkelsteen, Threat Intelligence Group Manager; Adi Ikan, Head of Network Research and Protection; Sagi Tzadik, Security Researcher

- **CPR has seen thousands of exploit attempts against organizations worldwide**
- **CPR has observed that the number of attempted attacks have increased tenfold from 700 on March 11 to over 7,200 on March 15.**
- **The country most attacked has been The United States (17% of all exploit attempts), followed by Germany (6%), the United Kingdom (5%), The Netherlands (5%) and Russia (4%).**
- **Most targeted industry sector has been Government/Military (23% of all exploit attempts), followed by Manufacturing (15%), Banking & Financial Services (14%), Software vendors (7%) and Healthcare (6%).**

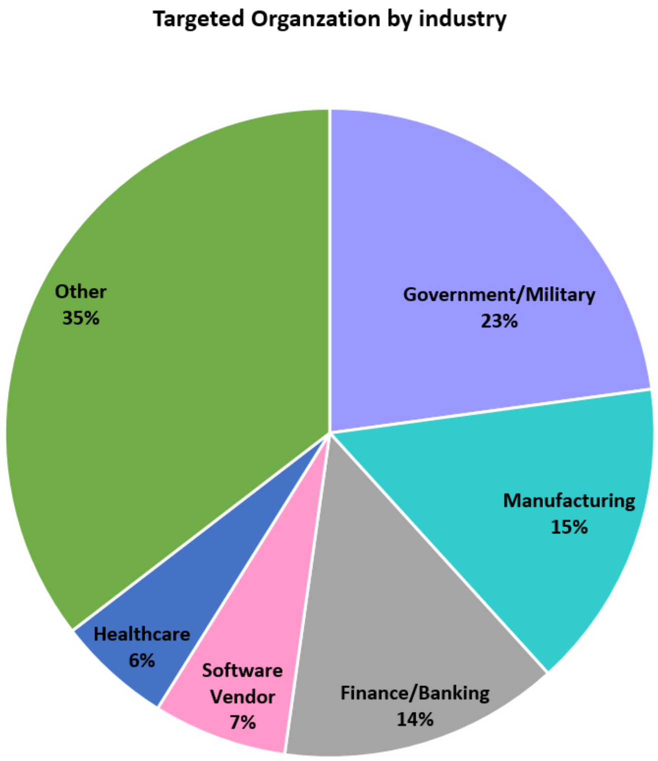
Since the recently disclosed vulnerabilities on Microsoft Exchange Servers, a full race has started amongst hackers and security professionals. Global experts are using massive preventative efforts to combat hackers who are working day-in and day-out to produce an exploit that can successfully leverage the remote code execution vulnerabilities in Microsoft Exchange.

CPR has outlined the disclosed vulnerabilities, the targeted organizations by country and industry, and then recommendations to prevent the attacks, which are yet to come.

Current attack attempts in numbers


Targeted Organizations by Countries

The country most attacked has been The United States (17% of all exploit attempts), followed by Germany (6%), the United Kingdom (5%), The Netherlands (5%) and Russia (4%).


Targeted Organzation by industry

Most targeted industry sector has been Government/Military (23% of all exploit attempts), followed by Manufacturing (15%), Banking & Financial Services (14%), Software vendors (7%) and Healthcare (6%).

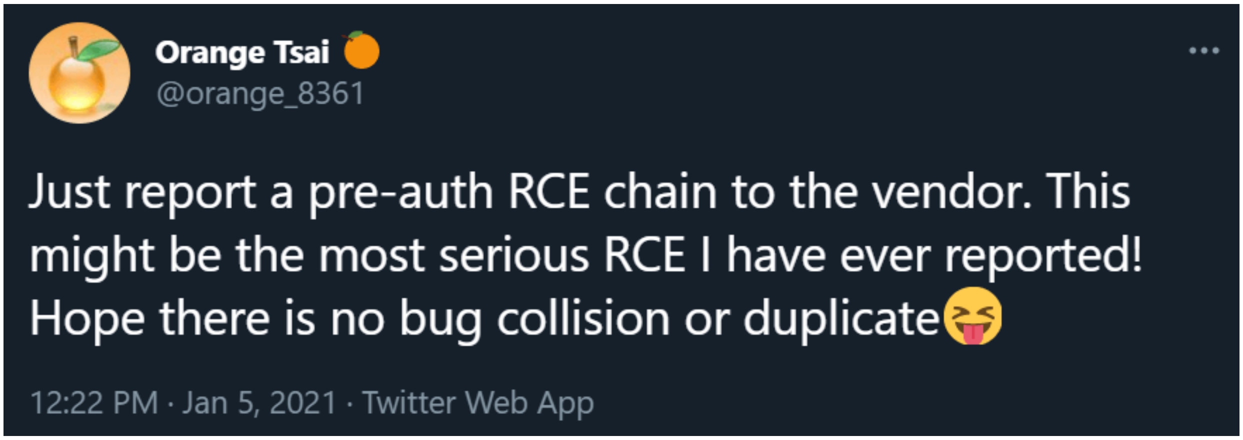
Behind-the-scenes of the Zero Days

On March 3, 2021 Microsoft released an emergency patch for its Exchange Server product, the most popular mail server worldwide. All incoming and outgoing emails, calendar invitations and virtually anything accessed within Outlook goes through the Exchange server.

Orange Tsai (Cheng-Da Tsai) from DEVCORE, a security firm based in Taiwan, reported two vulnerabilities in January. Unware of the full magnitude of these findings, Microsoft was prompted to further investigate their Exchange server. The investigation uncovered five more critical vulnerabilities.

The vulnerabilities allow an attacker to read emails from an Exchange server without authentication or accessing an individual's email account. Further vulnerability chaining enables attackers to completely take over the mail server itself.

Once an attacker takes over the Exchange server, they can open the network to the internet and access it remotely. As many Exchange servers have internet exposer (specifically Outlook Web Access feature) and are integrated within the broader network, this poses a critical security risk for millions of organizations.



Orange Tsai 🍊
@orange_8361

Just report a pre-auth RCE chain to the vendor. This might be the most serious RCE I have ever reported! Hope there is no bug collision or duplicate😝

12:22 PM · Jan 5, 2021 · Twitter Web App

Orange Tsai (Cheng-Da Tsai) teaser for pre-authentication remote code execution chain on Twitter, Jan 05,2021

What organizations are at risk?

If your organization's Microsoft Exchange server is exposed to the internet, and has not been updated with the latest patches nor protected by a third party software such as Check Point, then you should assume the server is completely compromised. Compromised servers could enable an unauthorized attacker to extract your corporate emails and execute malicious code inside your organization with high privileges.

Technical Explanation

- CVE-2021-26855 – is a server-side request forgery (SSRF) vulnerability in Exchange which allows the attacker to send arbitrary HTTP requests and authenticate as the Exchange server.
- CVE-2021-26857 – is an insecure deserialization vulnerability in the Unified Messaging service. Insecure deserialization is where untrusted user-controllable data is desterilized by a program. Exploiting this vulnerability gives HAFNIUM the ability to run code as SYSTEM on the Exchange server. This requires administrator permission or another vulnerability to exploit.
- CVE-2021-26858 – is a post-authentication arbitrary file write vulnerability in Exchange. If HAFNIUM could authenticate with the Exchange server then they could use this vulnerability to write a file to any path on the server. They could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin's credentials.
- CVE-2021-27065 – is a post-authentication arbitrary file write vulnerability in Exchange. If HAFNIUM could authenticate with the Exchange server then they could use this vulnerability to write a file to any path on the server. They could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin's credentials.

Since the disclosure, CPR has received questions regarding the identity of the attackers, their motivation and the wide context of recent major hacks.

In this attack, as in Sunburst, a particularly common platform was used as a front door for covert entry and prolonged stay within the network. The good news is that only highly skilled and well-financed threat actors are capable of using the front door to potentially enter tens of thousands of organizations worldwide. While hacking the exchange server with zero days is quite impressive, the purpose of the attack and what cybercriminals wanted within the network is still unknown. Organizations who are at risk should not only take preventive actions on their Exchange, but also scan their networks for live threats and assess all assets.

Prevent Future Attacks and Remain Protected

Here are Check Point's recommendations to prevent future attacks and remain protected:

- **Patch** – immediately update all Microsoft Exchange Servers to the latest patched versions available by Microsoft. This *update is not automatic* and you are expected to perform it manually.
- **Threat Prevention protections** – Check Point provides comprehensive security coverage to the vulnerabilities reported by Microsoft with the following Threat Prevention protections:

IPS

- CVE-2021-26855 – CPAI-2021-0099
- CVE-2021-26857 – CPAI-2021-0107
- CVE-2021-26858 – CPAI-2021-0107
- CVE-2021-27065 – CPAI-2021-0099

Threat Emulation

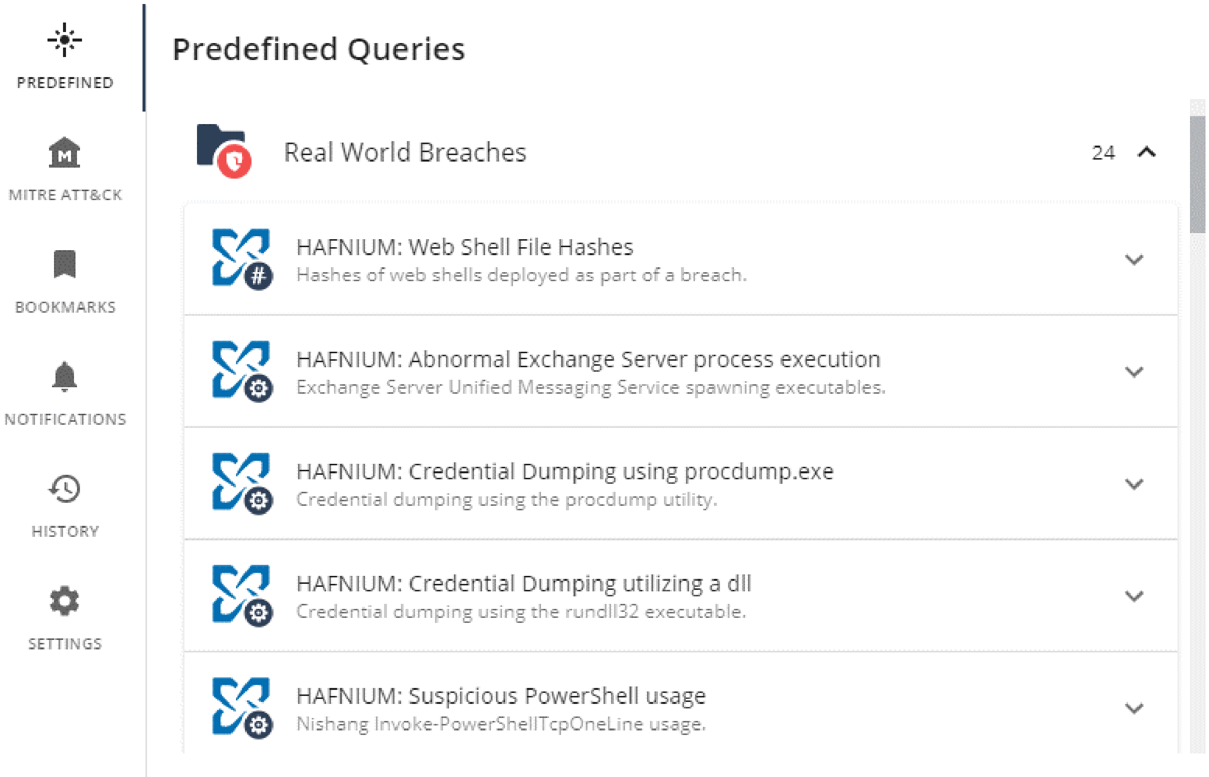
WinsCVE-2021-27065.A

Anti-Virus

- TC. XXX
- Win32.Hafnium.TC.XXX

Check Point **Harmony Endpoint (formally known as SandBlast Agent)**

- Win.SuspExchange.A
- Win.SuspExchange.B
- Win.SuspExchange.C
- Win.SuspExchange.D



Predefined Queries

Real World Breaches 24

HAFNIUM: Web Shell File Hashes
Hashes of web shells deployed as part of a breach.

HAFNIUM: Abnormal Exchange Server process execution
Exchange Server Unified Messaging Service spawning executables.

HAFNIUM: Credential Dumping using procdump.exe
Credential dumping using the procdump utility.

HAFNIUM: Credential Dumping utilizing a dll
Credential dumping using the rundll32 executable.

HAFNIUM: Suspicious PowerShell usage
Nishang Invoke-PowerShellTcpOneLine usage.

Harmony Endpoint: predefined queries for threat hunting

Behavior Guard Updates

“Behavioral Guard” – Harmony Endpoint’s behavior protection engine – has also been promptly updated with the relevant signatures which includes post exploitation detection of data collections attempts and credential dumping. These signatures are being automatically updated with all Harmony Endpoint installations to ensure protection for Harmony Endpoint customers.