Microsoft Exchange attacks cause panic as criminals go shell collecting

blog.malwarebytes.com/malwarebytes-news/2021/03/microsoft-exchange-attacks-cause-panic-as-criminals-go-shell-collecting/

Pieter Arntz March 9, 2021

Only last week we posted a blog about multiple zero-day exploits being used to attack on-premises versions of Microsoft Exchange Server in limited and targeted attacks. Seeing how this disclosure came with a patch being available, under normal circumstances you would see some companies update quickly and others would dally until it bubbled up to the top of their to-do list.

This attack method, called ProxyLogon and attributed to a group called Hafnium, was different. It went from “limited and targeted attacks” to a full-size panic in no time. Attackers are using the Exchange bugs to access vulnerable servers before establishing web shells to gain persistence and steal information.

How did this situation evolve? A timeline

To demonstrate how this situation came about we want to show you this timeline of developments:

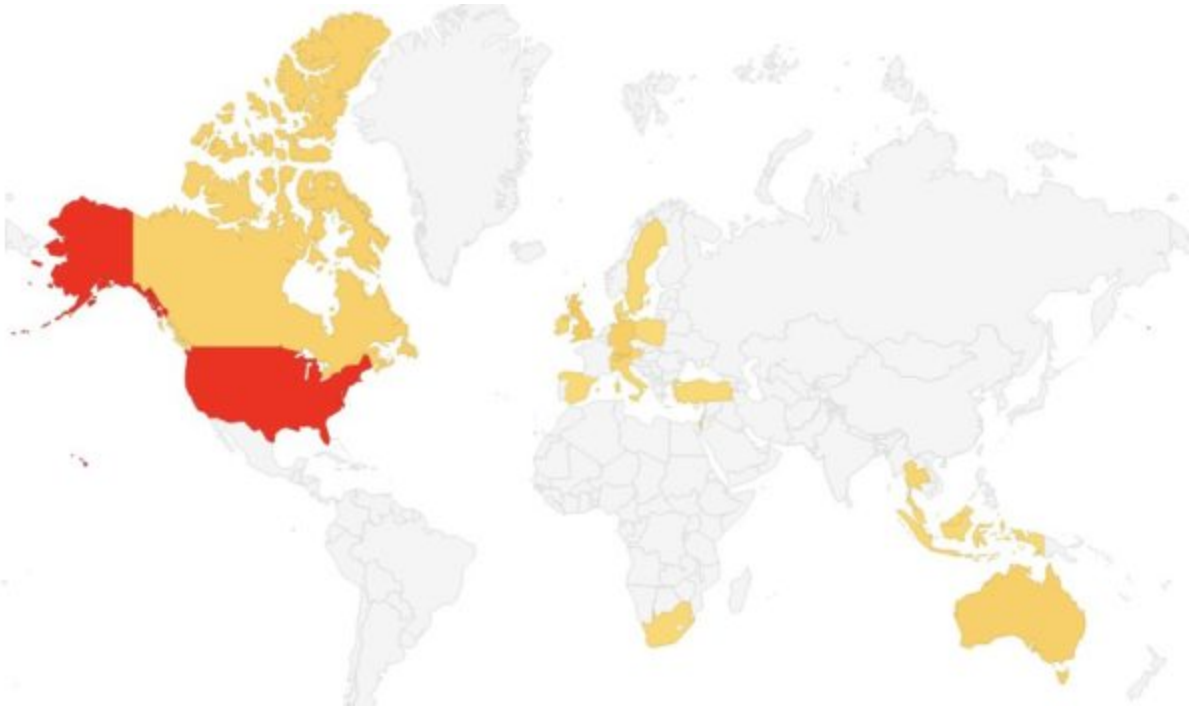
- December 2020, CVE-2021-26855 is discovered by DEVCORE, who named the vulnerability ProxyLogon.
- January 2021, DEVCORE send an advisory and exploit to Microsoft through the MSRC portal.
- January 2021, Volexity and Dubex start to see exploitation of Exchange vulnerabilities.
- January 27, 2021, Dubex shares its findings with Microsoft.
- February 2, 2021, Volexity informs Microsoft of its findings.
- March 2, 2021, Microsoft publishes a patch and advisory, which has been updated a few times since then.
- March 4, 2021, The Cybersecurity and Infrastructure Security Agency issues an emergency directive after CISA partners observe active exploitation of vulnerabilities in Microsoft Exchange on-premises products.
- March 5, 2021, Microsoft and many security vendors see increased use of these vulnerabilities in attacks targeting unpatched systems, by multiple malicious actors, not just Hafnium.
- March 8, 2021, CISA issues a warning that it is aware of widespread domestic and international exploitation of these vulnerabilities.

The attacks went from a limited Advanced Persistent Threat (APT) used against targeted victims to cryptomining operations run by “common” cybercriminals in no time flat.

What often happens after vulnerabilities get disclosed and patched is that criminals reverse engineer the fix to create their own copycat exploits, so they can attack while systems are unpatched. Sometimes it takes a lot of skills and perseverance to get a vulnerability to work for you, but looking at the rapid introduction of these Exchange exploits into the threat landscape, this one looks like a piece of cake.

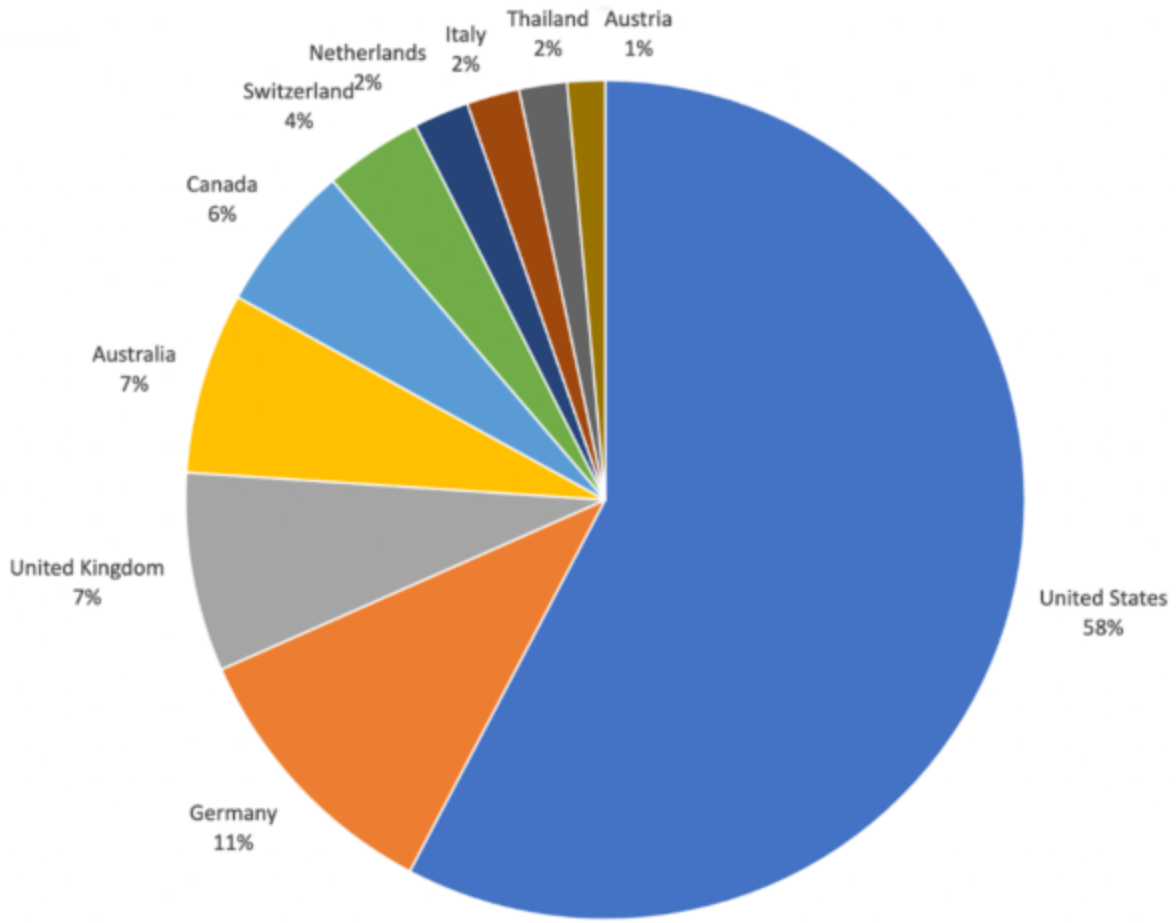
Victims

As of 8 March, Malwarebytes had detected malicious web shells on close to 1,000 unique machines already. Although most of the recorded attacks have occurred in the United States, organizations in other countries are under attack as well.



Instances found of Backdoor.Hafnium

Chris Krebs, the former director of CISA, reckons government agencies and small businesses will be more affected by these attacks than large enterprises. Enterprises tend to use different software than on-premises Exchange Servers.



Distribution of Backdoor.Hafnium detections by country by 8 March, 2021
But Brian Krebs, in a post on his site, states that the Hafnium hackers have accelerated attacks on vulnerable Exchange servers since Microsoft released the patches. His sources told him that 30,000 organizations in the US have been hacked as part of this campaign.

Web shells

A web shell is as a malicious script used by an attacker that allows them to escalate and maintain persistent access on an already compromised web application. (Not every web shell is malicious, but the non-malicious ones are not interesting to us in this context.)

Web shells don't attack or exploit a remote vulnerability, they are always the second step of an attack. Even if it opens the door to further exploitation, a web shell itself is always dropped after an initial exploitation.

Web shell scripts can be written in any of the programming languages designed for use on the web. You will find PHP, ASP, Perl, and many others. Attackers who successfully use web shells take advantage of the fact that many organizations do not have complete visibility into the HTTP sessions on their servers. And most web shells are basically non-executable files, which can make it hard for traditional antivirus software to detect them. The tiniest web shell in PHP on record is only this big:

```
<?=`$_GET[1]`?>
```

A shell like this will simply execute whatever command an attacker sends to the compromised server. They run it by calling the script in their browser, or from a command line HTTP client. For example, the following url would cause a tiny web shell running on example.com to execute whatever we put replaced `{command}` with:

```
www.example.com/index.html?1={command}
```

As you can see the use of this type of backdoor is easy. Once you have planted the web shell, you can use it to create additional web shells or steal information from the server.

What can we do?

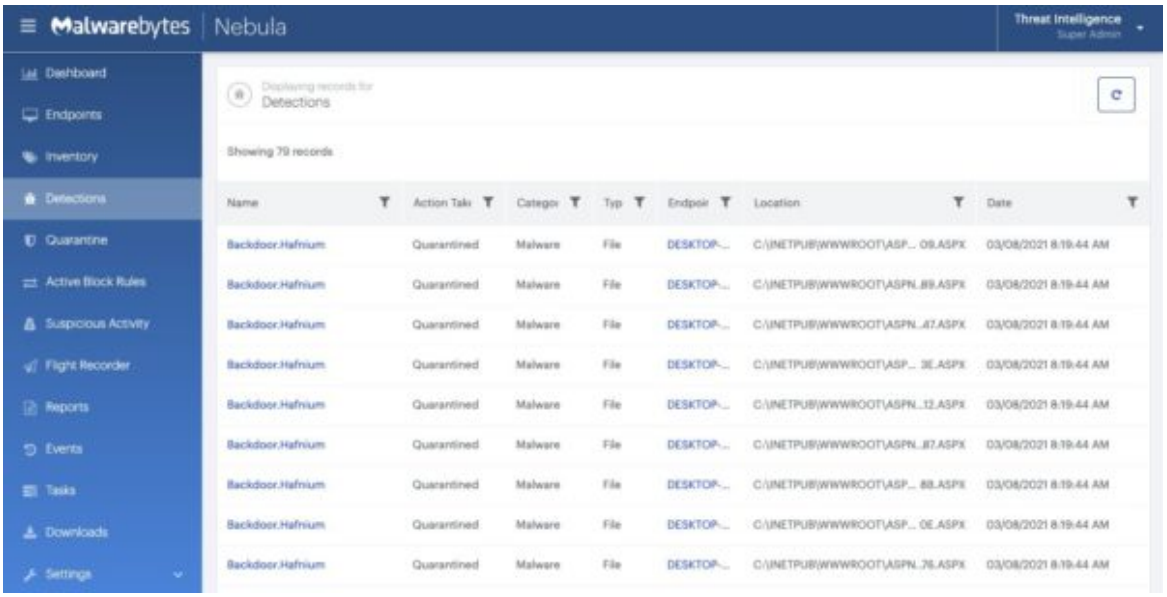
Patch as soon as you can.

Microsoft's team has published a script on GitHub that can check the security status of Exchange servers. The script has been updated to include indicators of compromise (IOCs) linked to the four zero-day vulnerabilities found in Microsoft Exchange Server.

It was important to patch last week, when it was just targeted attacks, but it's all the more urgent now that it's wild west out there. If you can't patch your Exchange server, block internet access to it, or restrict access to it by blocking untrusted connections, or putting the server behind your VPN.

Scan your server for the presence of malicious web shells. Security vendors have added detection for the publicly posted IOCs and some will detect other malicious web shells as well.

Malwarebytes' generic detection name for malicious web shells is Backdoor.WebShell and the detection name for the web shells that are tied directly to the Hafnium group is Backdoor.Hafnium.



Malwarebytes detecting Backdoor.Hafnium

We'll update the timeline in our first article on this topic as more developments and fresh information comes to light.

Stay safe, everyone!