No, I Did Not Hack Your MS Exchange Server

krebsonsecurity.com/2021/03/no-i-did-not-hack-your-ms-exchange-server/

New data suggests someone has compromised more than 21,000 **Microsoft Exchange Server** email systems worldwide and infected them with malware that invokes both KrebsOnSecurity and Yours Truly by name.

Let's just get this out of the way right now: It wasn't me.

The Shadowserver Foundation, a nonprofit that helps network owners identify and fix security threats, says it has found 21,248 different Exchange servers which appear to be compromised by a backdoor and communicating with **brian[.]krebsonsecurity[.]top** (NOT a safe domain, hence the hobbling).

Shadowserver has been tracking wave after wave of attacks targeting flaws in Exchange that Microsoft addressed earlier this month in an emergency patch release. The group looks for attacks on Exchange systems using a combination of active Internet scans and "honeypots" — systems left vulnerable to attack so that defenders can study what attackers are doing to the devices and how.

David Watson, a longtime member and director of the Shadowserver Foundation Europe, says his group has been keeping a close eye on hundreds of unique variants of backdoors (a.k.a. "web shells") that various cybercrime groups worldwide have been using to commandeer any unpatched Exchange servers. These backdoors give an attacker complete, remote control over the Exchange server (including any of the server's emails).

On Mar. 26, Shadowserver saw an attempt to install a new type of backdoor in compromised Exchange Servers, and with each hacked host it installed the backdoor in the same place: "**/owa/auth/babydraco.aspx.**"

“The web shell path that was dropped was new to us,” said Watson said. “We have been testing 367 known web shell paths via scanning of Exchange servers.”

OWA refers to **Outlook Web Access**, the Web-facing portion of on-premises Exchange servers. Shadowserver’s honeypots saw multiple hosts with the Babydraco backdoor doing the same thing: Running a Microsoft Powershell script that fetches the file “krebsonsecurity.exe” from the Internet address **159.65.136[.]128**. Oddly, none of the several dozen antivirus tools available to scan the file at **Virustotal.com** currently detect it as malicious.

The Krebsonsecurity file also installs a root certificate, modifies the system registry, and tells Windows Defender not to scan the file. Watson said the Krebsonsecurity file will attempt to open up an encrypted connection between the Exchange server and the above-mentioned IP address, and send a small amount of traffic to it each minute.

Shadowserver found more than 21,000 Exchange Server systems that had the Babydraco backdoor installed. But Watson said they don’t know how many of those systems also ran the secondary download from the rogue Krebsonsecurity domain.

“Despite the abuse, this is potentially a good opportunity to highlight how vulnerable/compromised MS Exchange servers are being exploited in the wild right now, and hopefully help get the message out to victims that they need to sign up our free daily network reports,” Watson said.

There are hundreds of thousands of Exchange Server systems worldwide that were vulnerable to attack (Microsoft suggests the number is about 400,000), and most of those have been patched over the last few weeks. However, there are still tens of thousands of vulnerable Exchange servers exposed online. On Mar. 25, Shadowserver tweeted that it was tracking 73,927 unique active webshell paths across 13,803 IP addresses.

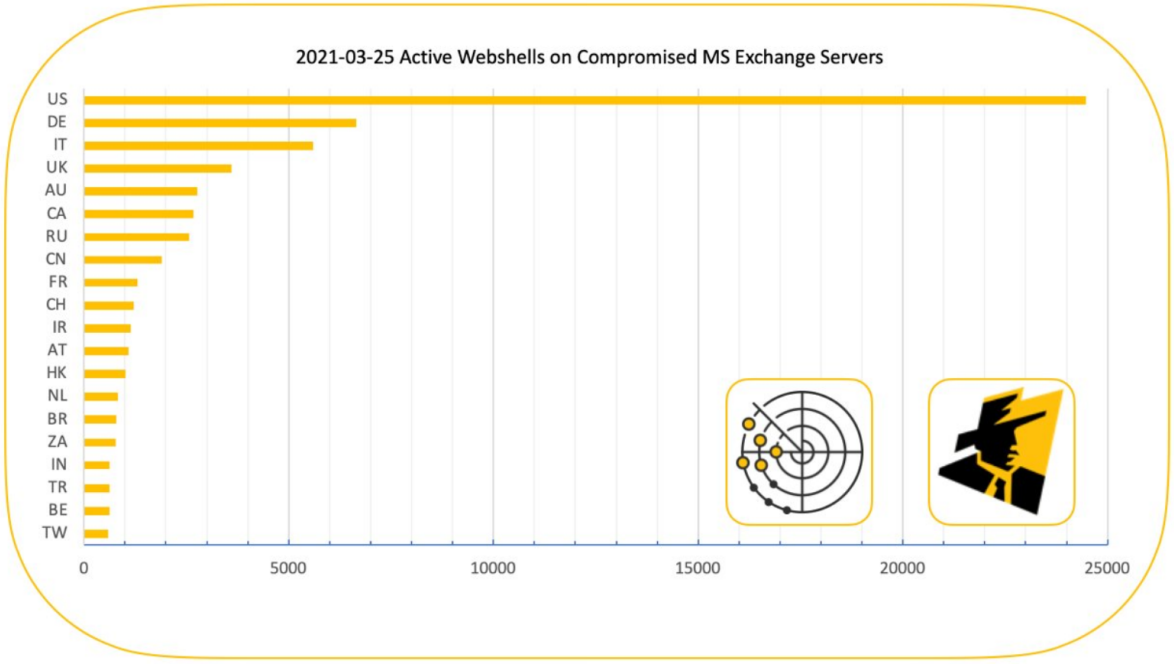

Image: Shadowserver.org

Exchange Server users that haven't yet patched against the four flaws Microsoft fixed earlier this month can get immediate protection by deploying Microsoft's "One-Click On-Premises Mitigation Tool."

The motivations of the cybercriminals behind the Krebonsecurity dot top domain are unclear, but the domain itself has a recent association with other cybercrime activity — and with harassing this author. I first heard about the domain in December 2020, when a reader told me how his entire network had been hijacked by a cryptocurrency mining botnet that called home to it.

"This morning, I noticed a fan making excessive noise on a server in my homelab," the reader said. "I didn't think much of it at the time, but after a thorough cleaning and test, it still was noisy. After I was done with some work-related things, I checked up on it – and found that a cryptominer had been dropped on my box, pointing to XXX-XX-XXX.krebsonsecurity.top'. In all, this has infected all three linux boxes on my network."

What was the subdomain I X'd out of his message? Just my Social Security number. I'd been doxed via DNS.

This is hardly the first time malware or malcontents have abused my name, likeness and website trademarks as a cybercrime meme, for harassment, or just to besmirch my reputation. Here are a few of the more notable examples, although all of those events are almost a decade old. That same list today would be pages long.

Further reading:

A Basic Timeline of the Exchange Mass-Hack

Warning the World of a Ticking Timebomb

At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software

Microsoft: Chinese Cyberspies Used 4 Exchange Server Flaws to Plunder Emails