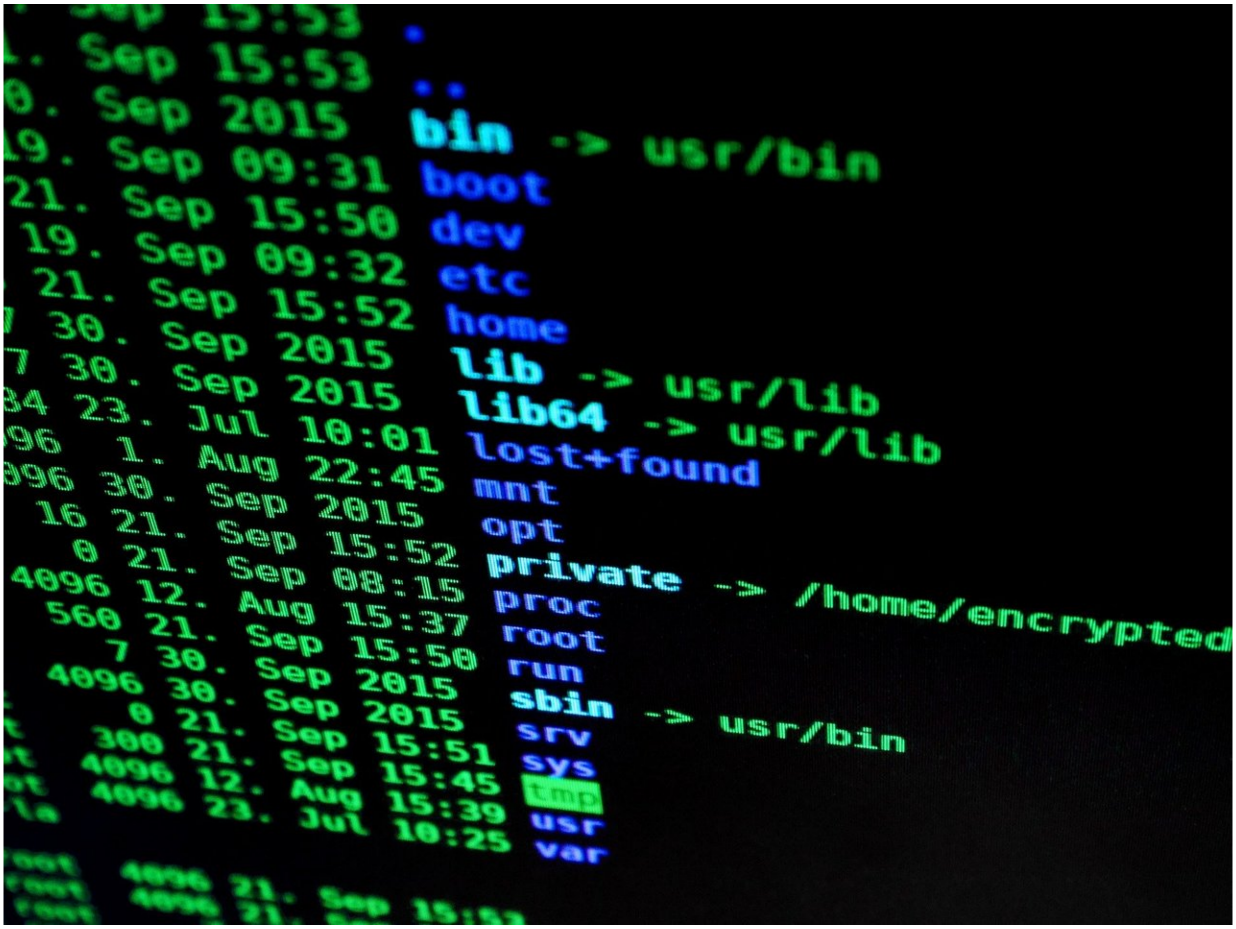
Hackers rushed in as Microsoft raced to avert mass cyber-attack

March 15 2021, by Kartikay Mehrotra and Alyza Sebenius, Bloomberg News



```
   Sep 15:53 .
1. Sep 15:53 ..
0. Sep 2015 bin -> usr/bin
19. Sep 09:31 boot
21. Sep 15:50 dev
19. Sep 09:32 etc
21. Sep 15:52 home
7 30. Sep 2015 lib -> usr/lib
7 30. Sep 2015 lib64 -> usr/lib
84 23. Jul 10:01 lost+found
96 1. Aug 22:45 mnt
096 30. Sep 2015 opt
16 21. Sep 15:52 private -> /home/encrypted
0 21. Sep 08:15 proc
4096 12. Aug 15:37 root
560 21. Sep 15:50 run
7 30. Sep 2015 sbin -> usr/bin
4096 30. Sep 2015 srv
0 21. Sep 15:51 sys
300 21. Sep 15:45 tmp
4096 12. Aug 15:39 usr
4096 23. Jul 10:25 var
4096 21. Sep 15:53
4096 21.
```

Credit: CC0 Public Domain

It was late February, and Microsoft Corp. engineers had been working for weeks on a handful of alarming weaknesses in the company's popular Exchange email service. They were rushing to send out a fix, targeting the second Tuesday of March—part of a monthly ritual known in cybersecurity circles as "patch Tuesday."

The hackers got a head start. Following weeks of discreet attacks, Chinese hackers shifted into high gear. The result was a sprawling campaign that engulfed thousands of organizations in a matter of days.

Something had gone wrong. What is normally a relatively smooth process—the one Microsoft uses regularly for identifying and fixing weaknesses in its popular software—has morphed into a global cybersecurity crisis now consuming the attention of the White House.

In all, researchers had identified four vulnerabilities and classified them as critical, meaning hackers can use them unseen to steal emails and other data.

But on Feb. 26, before the software giant released its patches, attackers began infiltrating those email systems en masse—almost as though they knew their window of opportunity was about to close, said Ryan Kalember, executive vice president of cybersecurity strategy at the email security firm, Proofpoint Inc.

Microsoft is now investigating the possibility of a leak that may have triggered these mass Exchange compromises ahead of its patch release, according to two sources with knowledge of the company's response to the attack. The sources, who weren't authorized to speak on the matter, said a leak, if indeed there was one, may have come from one of the company's security or government partners, or from independent researchers. A leak may have been malicious, or it could have been part of a separate security breach, they said.

A Microsoft spokesperson declined to comment on the investigation.

When Microsoft released its patches, a week ahead of schedule on March 2, it protected some clients, but also served as an accelerant for attacks, as more hackers piled on. In their race to break into networks before victims could lock their doors, the hackers breached banks and governments globally, as well as schools, hospitals, manufacturers and regional hotel chains.

The number of cyber-espionage gangs attacking Exchange servers has now reached at least 10, cyber-security firm ESET said in a recent blog post, and there were at least 60,000 global victims of the hack by the end of last week, said a former U.S. official with knowledge of the investigation. The number of attackers is likely dramatically higher now that the vulnerability has been widely distributed in criminal hacking circles, according to security researchers."The president has been briefed and is tracking the issue closely," a spokesperson for the U.S. National Security Council said Wednesday in an email. "The White House is working around the clock with our public and private partners, keeping Congress updated, assessing the impact and defining the next steps we need to take."

Importance of Zero-Days

Hackers are constantly looking for critical flaws in software, known as zero-days, because they can be used to steal data from users. The more widely used the software, the more valuable knowledge of a flaw. Although many governments and large companies had already migrated to more modern systems, Microsoft Exchange is still in use by tens of thousands of customers around the world.The company appears to have learned of the flaws in its Exchange email software sometime from early January to early February. A Taiwan-based cyber-research firm called DEVCORE first alerted Microsoft on Jan. 5, DEVCORE said. A

Virginia-based cybersecurity firm, Volexity, and a researcher known for finding such flaws—who goes by the intentionally cryptic name Orange Tsai—said they alerted the company to the zero-days between January and early February.It often takes several weeks for Microsoft to create a safer version of popular software, and the company works to keep wider knowledge of any flaws secret during that time.

A few agencies in the U.S. government typically get advance notice, including the U.S. National Security Agency and the U.S. Department of Homeland Security, according to a former U.S. official familiar with the process. So do 82 cybersecurity firms in different parts of the world, which are provided advanced notice through the Microsoft Active Protections Program, or MAPP.The reason is simple. Once Microsoft issues the patch, hackers around the world race to find the underlying weaknesses being fixed, then try to hack companies that are slow to update their equipment.MAPP members include Chinese companies like Alibaba Group Holding Ltd. and Baidu Inc., although not every member gets advanced noticed regarding every zero-day. "It's very much per vendor and per incident," said Joe Slowik, senior security researcher at DomainTools, a cybersecurity company.

Attacks Escalate

About 10 days before Microsoft had planned to release fixes for its flawed email software, the number of Exchange customers being hacked suddenly jumped dramatically, according to several companies that tracked the activity said. Beginning Feb. 28, ESET observed five new cyber-espionage groups using the Exchange zero-days—groups that security researchers have nicknamed "Tick," "Lucky Mouse," "Calypso," "Websiic" and "Winnti." That was in addition to an advanced Chinese hacking group identified by Microsoft as Hafnium, which had been using the flaws for months.

Beijing on March 3 described Microsoft's allegation of Chinese culpability as a "groundless accusation" and called for evidence to support it.

While ESET hasn't done its own analysis of the groups' origins, various security researchers have published reports suggesting that the five additional groups also have connections to China—for example, assessing that the hackers in the groups speak Chinese languages or operate from IP addresses based in China.

Lucky Mouse used the flaw to breach a government organization in the Middle East, while Calypso took advantage of Microsoft Exchange to break into government targets in the Middle East and South America. Websiic targeted a government organization in Eastern Europe in addition to private companies in Asia, ESET said.The hackers hit private sector companies as well. Tick compromised the server of an information technology company in East Asia, according to ESET. And Winnti used the flaw to hack emails at an oil-and-gas company and a construction equipment company in East Asia, hitting both targets within hours of the patch release.

The hacks come just three months after the discovery of a sprawling Russian attack in which malware was downloaded onto the computers of as many as 18,000 customers of Texas-based software company, SolarWinds Corp.

Cybersecurity experts and former government officials fear the incidents signal that once more discerning government hackers are moving to mass intrusion campaigns, wreaking havoc as they go.

Unlike the SolarWinds hack, which ultimately targeted high-value government and technology networks, the Microsoft Exchange victims include many small- and medium-sized businesses, along with local government networks. Between the two hacks, attackers have made victims out of a large swath of the networks connected on the internet, said Jim Jaeger, a former U.S. Air Force brigadier general who is now president and chief cyberstrategist at Arete Advisors.

Victims come forward

The identity of most of the victims of China's attack are still unknown. The Norwegian Parliament announced it was hacked as part of the Microsoft Exchange campaign, and said that significant data had been lost. The European Banking Authority said it was a victim as well, but has yet to find evidence that the hackers stole secrets.Meanwhile, many Microsoft customers remain at risk. BitSight Technologies, a Boston-based cybersecurity firm, said internet-wide scans this week show that nearly one-third of vulnerable Microsoft Exchange customers have yet to patch their systems, despite urgent entreaties to do so from the FBI and Homeland Security Department.Proofpoint's Kalember, whose company specializes in email security, said the last couple of weeks have shown how serious the consequences from a breakdown in Microsoft's patching process can be."There were many bad bugs that were supposed to still be a secret and internal to Microsoft," he said. "Clearly they weren't.

©2021 Bloomberg L.P.
Distributed by Tribune Content Agency, LLC

Citation: Hackers rushed in as Microsoft raced to avert mass cyber-attack (2021, March 15) retrieved 20 April 2024 from https://techxplore.com/news/2021-03-hackers-microsoft-avert-mass-cyber-attack.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.