Tech

Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers

By **Kim Zetter** March 25, 2019, 9:00am

Researchers at cybersecurity firm Kaspersky Lab say that ASUS, one of the

world's largest computer makers, was used to unwittingly install a malicious backdoor on thousands of its customers' computers last year after attackers compromised a server for the company's live software update tool. The malicious file was signed with legitimate ASUS digital certificates to make it appear to be an authentic software update from the company, Kaspersky Lab says.

ASUS, a **multi-billion dollar computer hardware company** based in Taiwan that manufactures desktop computers, laptops, mobile phones, smart home systems, and other electronics, was pushing the backdoor to customers for at least five months last year before it was discovered, according to new research from the Moscow-based security firm.

The researchers estimate half a million Windows machines received the malicious backdoor through the ASUS update server, although the attackers appear to have been targeting only about 600 of those systems. The malware searched for targeted systems through their unique MAC addresses. Once on

a system, if it found one of these targeted addresses, the malware reached out to a command-and-control server the attackers operated, which then installed additional malware on those machines.

Kaspersky Lab said it uncovered the attack in January after adding a new supply-chain detection technology to its scanning tool to catch anomalous code fragments hidden in legitimate code or catch code that is hijacking normal operations on a machine. The company plans to release a full technical paper and presentation about the ASUS attack, which it has dubbed ShadowHammer, next month at its **Security Analyst Summit** in Singapore. In the meantime, Kaspersky has published some of the technical details on **its website**.

“We saw the updates come down from the Live Update ASUS server. They were trojanized, or malicious updates, and they were signed by ASUS.”

The issue highlights the growing threat from so-called supply-chain attacks, where malicious software or components get installed on systems as they’re manufactured or assembled, or afterward via trusted vendor channels. Last year the US launched a **supply chain task force** to examine the issue after a number of supply-chain attacks were uncovered in recent years. Although most attention on supply-chain attacks focuses on the potential for malicious implants to be added to hardware or software during manufacturing, vendor software updates are an ideal way for attackers to deliver malware to systems after they’re sold, because customers trust vendor updates, especially if they’re signed with a vendor’s legitimate digital certificate.

“This attack shows that the trust model we are using based on known vendor names and validation of digital signatures cannot guarantee that you are safe from malware,” said Vitaly Kamluk, Asia-Pacific director of Kaspersky Lab’s Global Research and Analysis Team who led the research. He noted that ASUS

denied to Kaspersky that its server was compromised and that the malware came from its network when the researchers contacted the company in January. But the download path for the malware samples Kaspersky collected leads directly back to the ASUS server, Kamluk said.

Motherboard sent ASUS a list of the claims made by Kaspersky in three separate emails on Thursday but has not heard back from the company.

Read more: What Is a 'Supply Chain Attack?'

But the US-based security firm Symantec confirmed the Kaspersky findings on Friday after being asked by Motherboard to see if any of its customers also received the malicious download. The company is still investigating the matter but said in a phone call that at least 13,000 computers belonging to Symantec customers were infected with the malicious software update from ASUS last year.

"We saw the updates come down from the Live Update ASUS server. They were trojanized, or malicious updates, and they were signed by ASUS," said Liam O'Murchu, director of development for the Security Technology and Response group at Symantec.

This is not the first time attackers have used trusted software updates to infect systems. The infamous **Flame spy tool**, developed by some of the same attackers behind **Stuxnet**, was the first known attack to trick users in this way by hijacking the Microsoft Windows updating tool on machines to infect computers. Flame, discovered in 2012, was signed with an unauthorized Microsoft certificate that attackers tricked Microsoft's system into issuing to them. The attackers in that case did not actually compromise Microsoft's update server to deliver Flame. Instead, they were able to redirect the software update tool on the machines of targeted customers so that they contacted a

malicious server the attackers controlled instead of the legitimate Microsoft update server.

Two different attacks discovered in 2017 also compromised trusted software updates. One involved the computer security cleanup tool known as CCleaner that was **delivering malware to customers** via a software update. More than 2 million customers received that malicious update before it was discovered. The other incident involved the infamous notPetya attack that began in Ukraine and infected machines via a **malicious update** to an accounting software package.

Costin Raiu, company-wide director of Kaspersky's Global Research and Analysis Team, said the ASUS attack is different from these others. "I'd say this attack stands out from previous ones while being one level up in complexity and stealthiness. The filtering of targets in a surgical manner by their MAC addresses is one of the reasons it stayed undetected for so long. If you are not a target, the malware is virtually silent," he told Motherboard.

But even if silent on non-targeted systems, the malware still gave the attackers a backdoor into every infected ASUS system.

Tony Sager, senior vice president at the Center for Internet Security who did defensive vulnerability analysis for the NSA for years, said the method the attackers chose to target specific computers is odd.

"Supply chain attacks are in the 'big deal' category and are a sign of someone who is careful about this and has done some planning," he told Motherboard in a phone call. "But putting something out that hits tens of thousands of targets when you're really going only after a few is really going after something with a hammer."

Kaspersky researchers first detected the malware on a customer's machine on

January 29. After they created a signature to find the malicious update file on other customer systems, they discovered that more than 57,000 Kaspersky customers had been infected with it. That victim toll only accounts for Kaspersky customers, however. Kamluk said the real number is likely in the hundreds of thousands.

Most of the infected machines belonging to Kaspersky customers (about 18 percent) were in Russia, followed by fewer numbers in Germany and France. Only about 5 percent of infected Kaspersky customers were in the United States. Symantec's O'Murchu said that about 15 percent of the 13,000 machines belonging to his company's infected customers were in the U.S.

Kamluk said Kaspersky notified ASUS of the problem on January 31, and a Kaspersky employee met with ASUS in person on February 14. But he said the company has been largely unresponsive since then and has not notified ASUS customers about the issue.

The attackers used two different ASUS digital certificates to sign their malware. The first expired in mid-2018, so the attackers then switched to a second legitimate ASUS certificate to sign their malware after this.

Kamluk said ASUS continued to use one of the compromised certificates to sign its own files for at least a month after Kaspersky notified the company of the problem, though it has since stopped. But Kamluk said ASUS has still not invalidated the two compromised certificates, which means the attackers or anyone else with access to the un-expired certificate could still sign malicious files with it, and machines would view those files as legitimate ASUS files.

This wouldn't be the first time ASUS was accused of compromising the security of its customers. In 2016, the company was **charged by the Federal Trade Commission** with misrepresentation and unfair security practices over

multiple vulnerabilities in its routers, cloud back-up storage and firmware update tool that would have allowed attackers to gain access to customer files and router log-in credentials, among other things. The FTC claimed ASUS knew about those vulnerabilities for at least a year before fixing them and notifying customers, putting nearly a million US router owners at risk of attack. ASUS settled the case by agreeing to **establish and maintain a comprehensive security program** that would be subject to independent audit for 20 years.

The ASUS live update tool that delivered malware to customers last year is installed at the factory on ASUS laptops and other devices. When users enable it, the tool contacts the ASUS update server periodically to see if any firmware or other software updates are available.

“They wanted to get into very specific targets and they already knew in advance their network card MAC address, which is quite interesting.”

The malicious file pushed to customer machines through the tool was called setup.exe, and purported to be an update to the update tool itself. It was actually a three-year-old ASUS update file from 2015 that the attackers injected with malicious code before signing it with a legitimate ASUS certificate. The attackers appear to have pushed it out to users between June and November 2018, according to Kaspersky Lab. Kamluk said the use of an old binary with a current certificate suggests the attackers had access to the server where ASUS signs its files but not the actual build server where it compiles new ones. Because the attackers used the same ASUS binary each time, it suggests they didn’t have access to the whole ASUS infrastructure, just part of the signing infrastructure, Kamluk notes. Legitimate ASUS software updates still got pushed to customers during the period the malware was being pushed out, but these legitimate updates were signed with a different certificate that used enhanced validation protection, Kamluk said, making it

more difficult to spoof.

The Kaspersky researchers collected more than 200 samples of the malicious file from customer machines, which is how they discovered the attack was multi-staged and targeted.

Buried in those malicious samples were hard-coded MD5 hash values that turned out to be unique MAC addresses for network adapter cards. MD5 is an algorithm that creates a cryptographic representation or value for data that is run through the algorithm. Every network card has a unique ID or address assigned by the manufacturer of the card, and the attackers created a hash of each MAC address it was seeking before hard-coding those hashes into their malicious file, to make it more difficult to see what the malware was doing. The malware had 600 unique MAC addresses it was seeking, though the actual number of targeted customers may be larger than this. Kaspersky can only see the MAC addresses that were hard-coded into the particular malware samples found on its customers' machines.

IMAGE: SHUTTERSTOCK

The Kaspersky researchers were able to crack most of the hashes they found to determine the MAC addresses, which helped them identify what network cards the victims had installed on their machines, but not the victims themselves. Any time the malware infected a machine, it collected the MAC address from that machine's network card, hashed it, and compared that hash against the ones hard-coded in the malware. If it found a match to any of the 600 targeted addresses, the malware reached out to **asushotfix.com**, a site masquerading as a legitimate ASUS site, to fetch a second-stage backdoor that it downloaded to that system. Because only a small number of machines contacted the command-and-control server, this helped the malware stay under the radar.

"They were not trying to target as many users as possible," said Kamluk. "They wanted to get into very specific targets and they already knew in advance their network card MAC address, which is quite interesting."

Symantec's O'Murchu said he's not sure yet if any of his company's customers were among those whose MAC addresses were on the target list and received the second-stage backdoor.

The command-and-control server that delivered the second-stage backdoor was registered May 3 last year but was shut down in November before Kaspersky discovered the attack. Because of this, the researchers were unable to obtain a copy of the second-stage backdoor pushed out to victims or identify victim machines that had contacted that server. Kaspersky believes at least one of its customers in Russia got infected with the second-stage backdoor when his machine contacted the command-and-control server on October 29 last year, but Raiu says the company doesn't know the identity of

the machine's owner in order to contact him and investigate further.

There were early hints that a signed and malicious ASUS update was being pushed to users in June 2018, when a number of people posted comments in a **Reddit forum** about a suspicious ASUS alert that popped up on their machines for a "critical" update. "ASUS strongly recommends that you install these updates now," the alert warned.

In a post titled "ASUSFourceUpdater.exe is trying to do some mystery update, but it won't say what," a user named GreyWolfx wrote, "I got an update popup from a .exe that I had never seen before today….I'm just curious if anyone knows what this update would possibly be for?"

When he and other users clicked on their ASUS updater tool to get information about the update, the tool showed no recent updates had been issued from ASUS. But because the file was digitally signed with an ASUS certificate and because scans of the file on the VirusTotal web site indicated it was not malicious, many accepted the update as legitimate and downloaded it to their machines. **VirusTotal** is a site that aggregates dozens of antivirus programs; users can upload suspicious files to the site to see if any of the tools detect it as malicious.

"I uploaded the executable [to VirusTotal] and it comes back as a validly signed file without issue," one user wrote. "The spelling of 'force' and the empty details window are indeed odd, but I noticed odd grammar errors in other ASUS software installed on this system, so it's not a smoking gun by itself," he noted.

Kamluk and Raiu said this may not be the first time the ShadowHammer attackers have struck. They said they found similarities between the ASUS attack and ones previously conducted by a group dubbed ShadowPad by

Kaspersky. ShadowPad targeted a Korean company that makes enterprise software for administering servers; the same group was also linked to the CCleaner attack. Although millions of machines were infected with the malicious CCleaner software update, only a subset of these got targeted with a second stage backdoor, similar to the ASUS victims. Notably, ASUS systems themselves were on the **targeted CCleaner list**.

The Kaspersky researchers believe the ShadowHammer attackers were behind the ShadowPad and CCleaner attacks and obtained access to the ASUS servers through the latter attack.

“ASUS was one of the primary targets of the CCleaner attack,” Raiu said. “One of the possibilities we are taking into account is that’s how they intially got into the ASUS network and then later through persistence they managed to leverage the access … to launch the ASUS attack.”

Listen to CYBER, Motherboard’s new weekly podcast about hacking and cybersecurity.

Tagged:

ASUS BACKDOOR HACKING KASPERSKY LAB MOTHERBOARD SECURITY SUPPLY CHAIN TECH

Share:

MORE LIKE THIS

VTuber, Want to Yap and Game on Stream? Here's What To Keep in Mind

BY ANA VALENS 11 HOURS AGO

Comfort and Style Make the FlexiSpot C7 Pro Max Ergonomic Chair a Front Runner To Replace Your Current Seat (Review)

BY SHAUN CICHACKI 12 HOURS AGO

Is Soundgarden About to Drop an Unreleased Album Featuring Chris Cornell?

BY STEPHEN ANDREW GALIHER 13 HOURS AGO

Dyson's Excellent Humidifier/Air Purifier Combo Is $200 Off—And Worth It

13 HOURS AGO

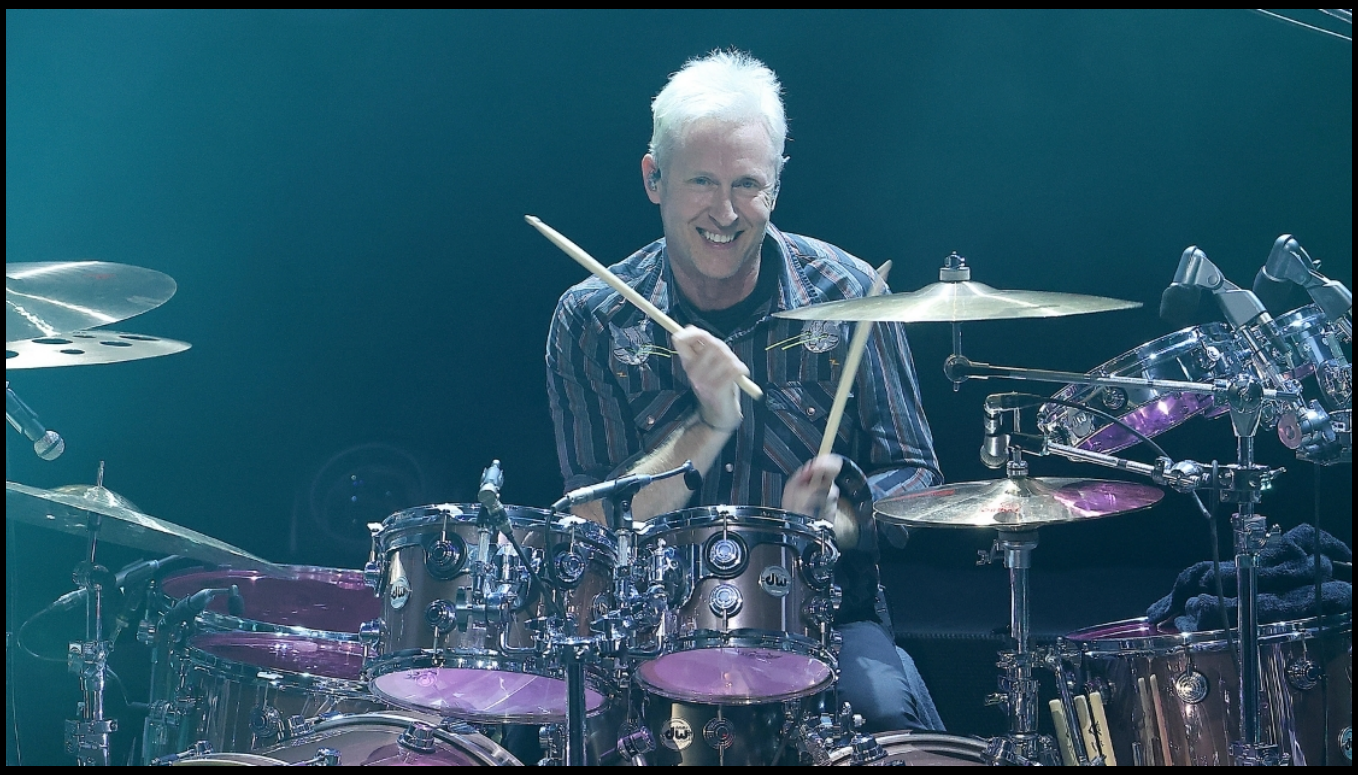
Mark Hoppus Talks Blink 182 and Green Day 2000s Tour Rivalry

13 HOURS AGO

X Is Selling Check Marks to US-Sanctioned Groups, Says Report

BY MATT JANCER 13 HOURS AGO

MORE FROM VICE



Ex-Foo Fighters Drummer Josh Freese Has a Hilarious List of Reasons for His Firing

13 HOURS AGO BY STEPHEN ANDREW GALIHER

14 HOURS AGO BY SHAUN CICHACKI

‘MISERY’ May Have One of the Best Gameplay Reveal Trailers Ever, and I Need This Game in My Life Now

14 HOURS AGO BY ANTHONY FRANKLIN II

Former Sony Boss Shuhei Yoshida Doesn’t Think Gamers Should Be Complaining About the Price of Games, and I Think He’s Missing the Point

14 HOURS AGO BY BRENT KOEPP

Horrifying ‘Baldur’s Gate 3’ Figurines Give Ugly ‘Witcher 3’ Geralt Statue A Run for Its Money – Why’d They Do Shadowheart Like That?