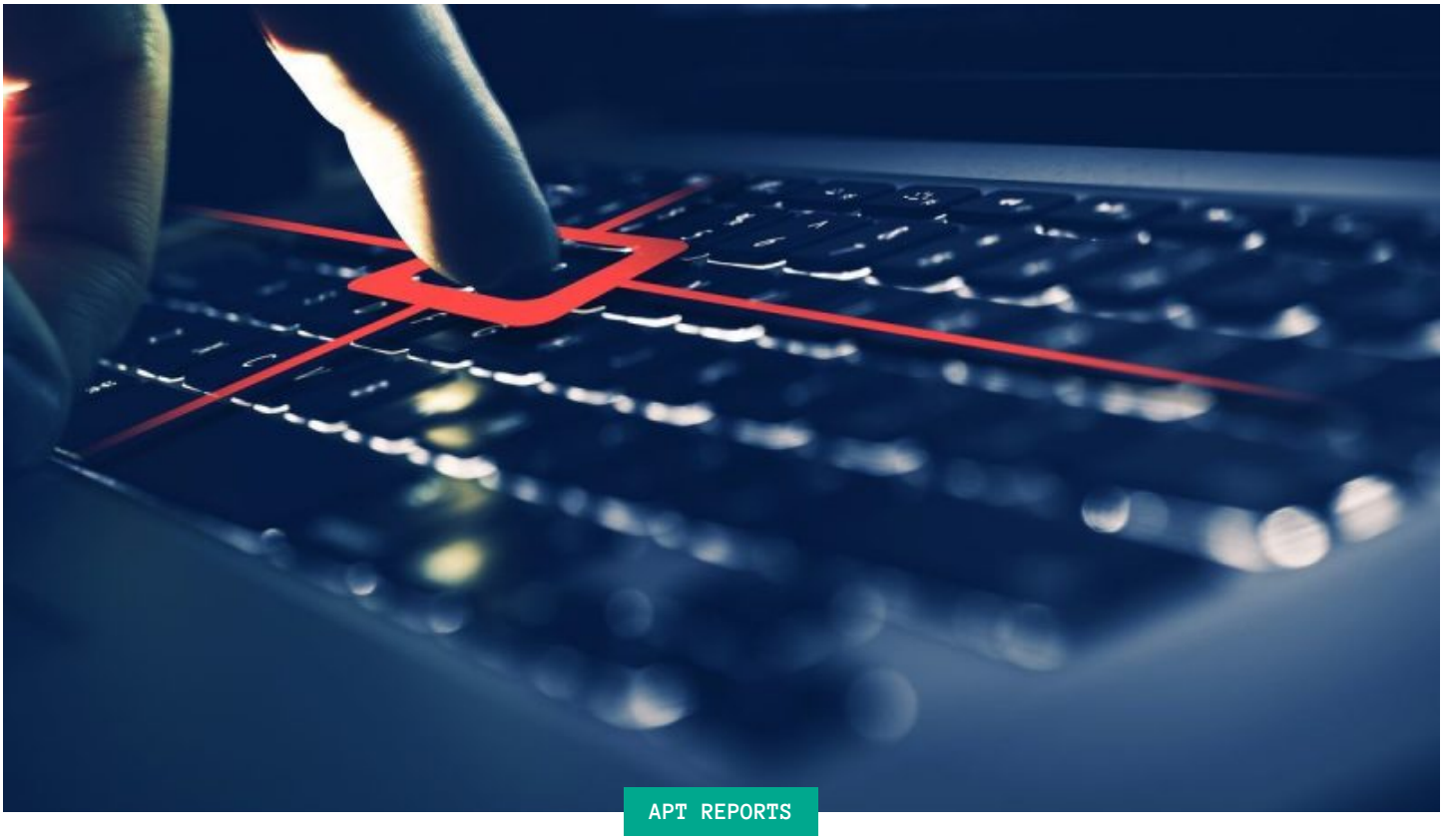
SECURELIST



APT REPORTS

Operation ShadowHammer

25 MAR 2019 minute read

Earlier today, Motherboard published a story by Kim Zetter on Operation ShadowHammer, a newly discovered supply chain attack that leveraged ASUS Live Update software.

While the investigation is still in progress and full results and technical paper will be published during SAS 2019 conference in Singapore, we would like to share some important details about the attack.

In January 2019, we discovered **a sophisticated supply chain attack involving the ASUS Live Update Utility**. The attack took place between June and November 2018 and according to our telemetry, it affected a large number of users.

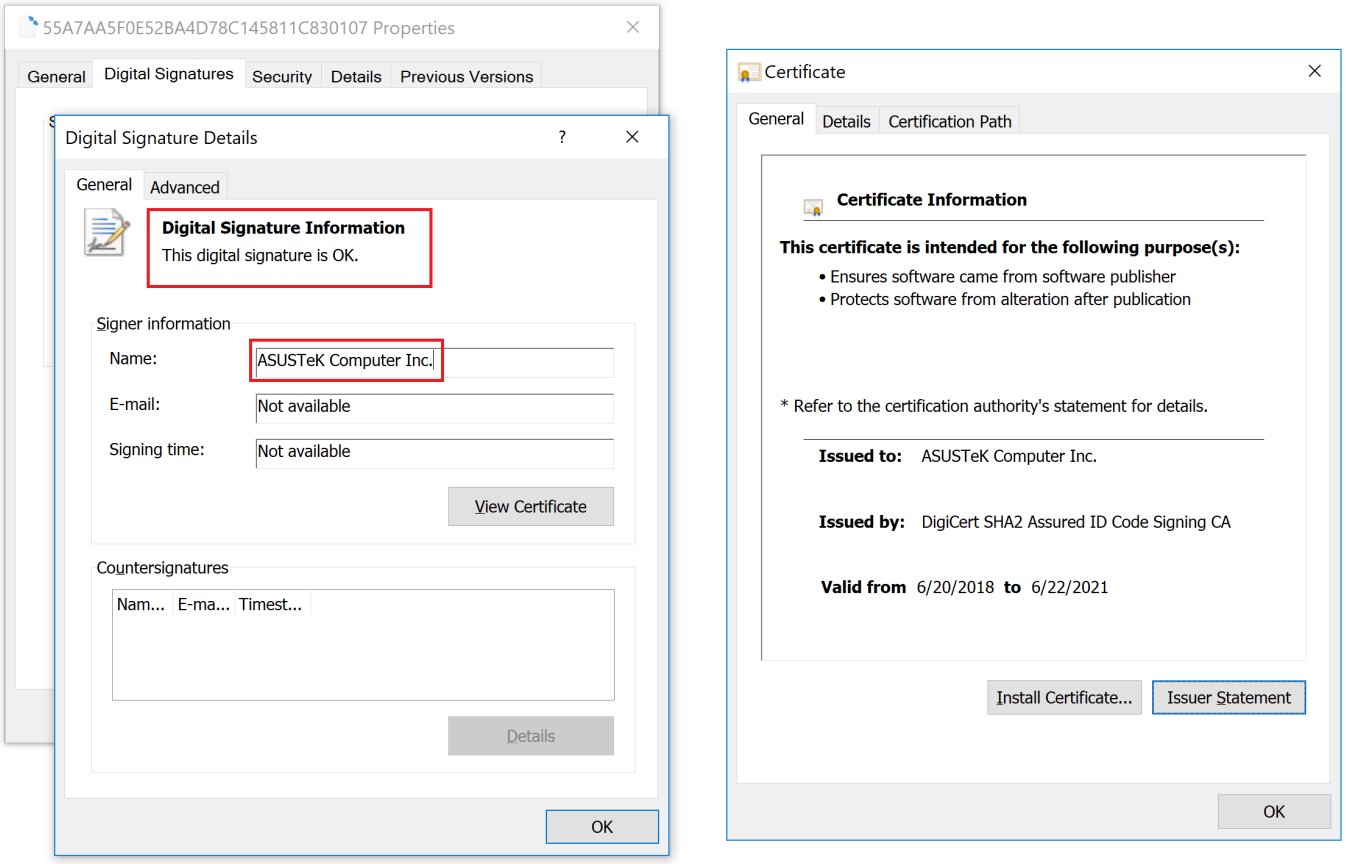
ASUS Live Update is an utility that is pre-installed on most ASUS computers and is used to automatically update certain components such as BIOS, UEFI, drivers and applications. According to Gartner, ASUS is the world's 5th-largest PC vendor by 2017 unit sales. This makes it an extremely attractive target for APT groups that might want to take advantage of their userbase.

Based on our statistics, **over 57,000 Kaspersky users have downloaded and installed the backdoored version of ASUS Live Update** at some point in time. We are not able to calculate the

total count of affected users based only on our data; however, we estimate that the real scale of the problem is much bigger and is possibly affecting over a million users worldwide.

The **goal of the attack was to surgically target an unknown pool of users, which were identified by their network adapters' MAC addresses**. To achieve this, the attackers had hardcoded a list of MAC addresses in the trojanized samples and this list was used to identify the actual intended targets of this massive operation. We were able to extract more than 600 unique MAC addresses from over 200 samples used in this attack. Of course, there might be other samples out there with different MAC addresses in their list.

We believe this to be a very sophisticated supply chain attack, which matches or even surpasses the Shadowpad and the CCleaner incidents in complexity and techniques. The reason that it stayed undetected for so long is partly due to the fact that the trojanized updaters were signed with legitimate certificates (eg: "ASUSTeK Computer Inc."). The malicious updaters were hosted on the official liveupdate01s.asus[.]com and liveupdate01.asus[.]com ASUS update servers.



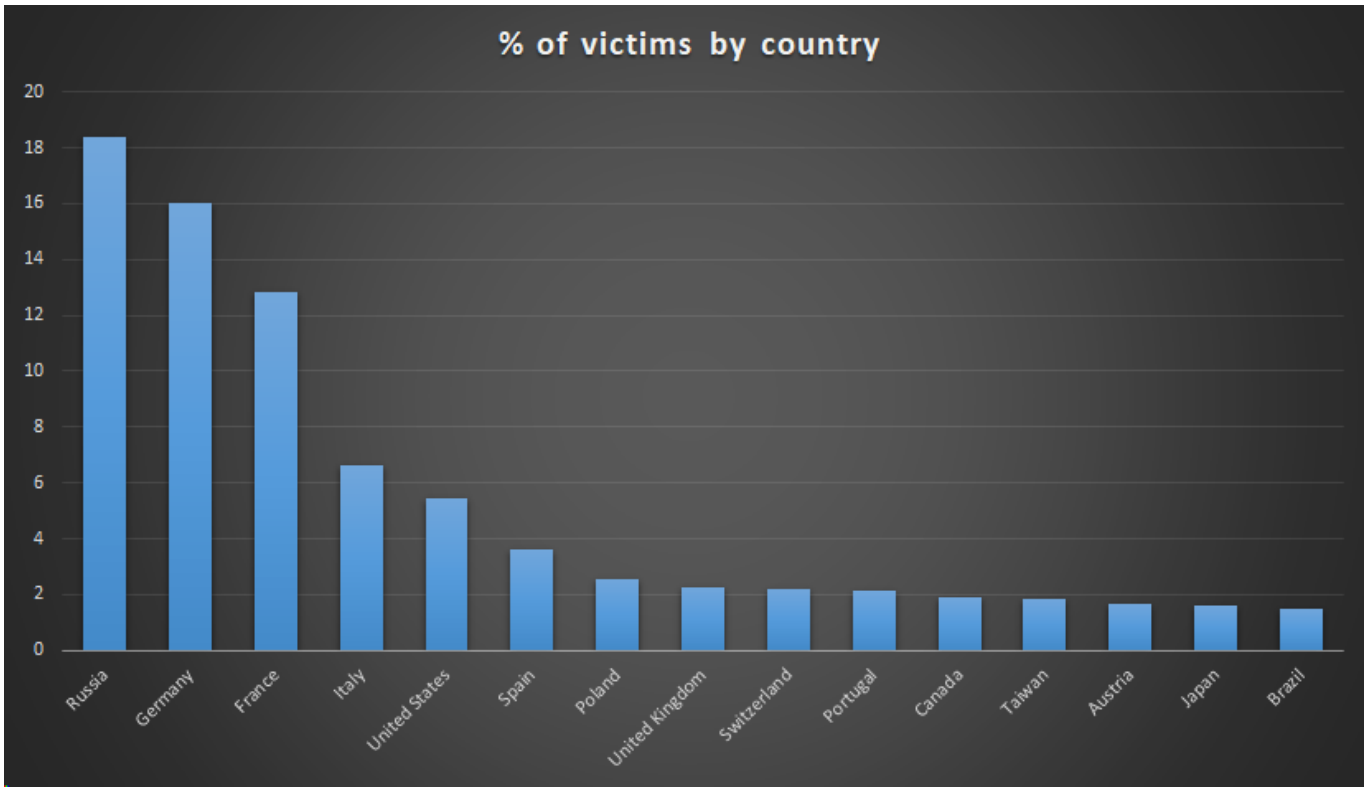
Digital signature on a trojanized ASUS Live Update setup installer
Certificate serial number: 05e6a0be5ac359c7ff11f4b467ab20fc

We have contacted ASUS and informed them about the attack on Jan 31, 2019, supporting their

investigation with IOCs and descriptions of the malware.

Although precise attribution is not available at the moment, certain evidence we have collected allows us to link this attack to the ShadowPad incident from 2017. The actor behind the ShadowPad incident has been publicly identified by Microsoft in court documents as BARIUM. BARIUM is an APT actor known to be using the Winnti backdoor. Recently, our colleagues from ESET wrote about another supply chain attack in which BARIUM was also involved, that we believe is connected to this case as well.

A victim distribution by country for the compromised ASUS Live Updater looks as follows:



It should be noted that the numbers are also highly influenced by the distribution of Kaspersky users around the world. In principle, the distribution of victims should match the distribution of ASUS users around the world.

We've also created a tool which can be run to determine if your computer has been one of the surgically selected targets of this attack. To check this, it compares MAC addresses of all adapters to a list of predefined values hardcoded in the malware and alerts if a match was found.

Download an archive with the tool (.exe)

Also, you may check MAC addresses online. If you discover that you have been targeted by this operation, please e-mail us at: shadowhammer@kaspersky.com

IOCs

Kaspersky Lab verdicts for the malware used in this and related attacks:

- HEUR:Trojan.Win32.ShadowHammer.gen

Domains and IPs:

- asushotfix[.]com
- 141.105.71[.]116

Some of the URLs used to distribute the compromised packages:

- hxxp://liveupdate01.asus[.]com/pub/ASUS/nb/Apps_for_Win8/LiveUpdate/Liveupdate_Test_VER365.zip
- hxxps://liveupdate01s.asus[.]com/pub/ASUS/nb/Apps_for_Win8/LiveUpdate/Liveupdate_Test_VER362.zip
- hxxps://liveupdate01s.asus[.]com/pub/ASUS/nb/Apps_for_Win8/LiveUpdate/Liveupdate_Test_VER360.zip
- hxxps://liveupdate01s.asus[.]com/pub/ASUS/nb/Apps_for_Win8/LiveUpdate/Liveupdate_Test_VER359.zip

Hashes (Liveupdate_Test_VER365.zip):

- aa15eb28292321b586c27d8401703494
- bebb16193e4b80f4bc053e4fa818aa4e2832885392469cd5b8ace5cec7e4ca19

A full set of IOCs and Yara rules is available to customers of Kaspersky Intelligence Reporting service – contact intelreports@kaspersky.com

VULNERABILITIES AND EXPLOITS | TARGETED ATTACKS | DIGITAL CERTIFICATES | BACKDOOR | SUPPLY-CHAIN ATTACK | UEFI | BIOS | DRIVERS | ASUS | SHADOWHAMMER

Authors

Expert GREAT Expert AMR

Operation ShadowHammer

Your email address will not be published. Required fields are marked *

Type your comment here

Name *

Email *

Comment

YE MAN AUNG
Posted on March 25, 2019. 2:44 pm

support and fix

Reply

MAURICE
Posted on March 25, 2019. 5:59 pm

Yes next steps support an fix please....

Reply

SALAM MALANCHU
Posted on March 25, 2019. 8:40 pm

Any idea if ASUS wireless routers were affected by this as well? I noticed in that same time frame that several of these that I manage required multiple reboots to resolve wireless connectivity issues (wireless signal dropping unexpectedly, unexplained slow internet speeds, etc) when previously these were behaving perfectly.

Reply

GO2112
Posted on March 26, 2019. 10:52 pm

I have experienced the same issue with my router Asus and the Almesh routers i have. and it seems some clients are not yet connected.
I was expecting my local Wifi to not be "controlled" by Asus servers .... not sure if i'm now confident with Asus anymore.

Reply

JORDAN
Posted on March 27, 2019. 1:43 pm

Im wondering the same thing. Luckily ALL 5 of my ASUS motherboard PCs arent infected, as well as my ASUS laptop. But ironically I had bought a brand new ASUS router last year (RT-N66u) and it happened to be one of the very few routers that were one of the models to get their Firmware infected with malware (possibly even having the malware on the router when I bought it brand new from newegg.com) Definitely not neweggs fault , but kinda scary knowing that other people and possibly mine as well were shipped brand new with the infected firmware that could be dormant for an indefinite amount of time and then enabled remotely one day to start relaying data to Russia etc. AKa using peoples bandwidth to turn their network into a botnet to give them access to a very large amount of routers to use at their disposal for DDoS attacks etc.

Reply

LITHOR
Posted on April 1, 2019. 3:06 pm

This was an exploit to the Asus Live Update software for their Laptops. If this program was uninstalled or not updated after the hack occurred you wouldn't be affected.

Reply

SRI HARSHA SATISH
Posted on March 26, 2019. 10:21 am

Well Done Kaspersky.

Reply

PLAUSIBLE DENIABILITY
Posted on March 27, 2019. 4:28 am

So the DOC grabs their fall guy from ShadowPad 2017 and points the finger at BARIUM to support Russian collusion! Amazing how much Russia comes up these days.

Reply

PETER
Posted on March 31, 2019. 9:00 pm

Huh?

Reply

CURIOSITY
Posted on March 28, 2019. 1:48 am

Have 600 Mac addresses been released?

Reply

LORRY MC'DOGGEL
Posted on March 29, 2019. 10:22 am

You can find them here:

https://skylightcyber.com/2019/03/28/unleash-the-hash-shadowhammer-mac-list/

Reply

PRADEEP KUMAR
Posted on March 31, 2019. 5:03 pm

My friend's laptop was affected by this virus in January and after that, his laptop was unable to boot properly. Neither he was able to install a fresh copy of Linux. Is there any solution to it, if anyone knows any then please tell me.

Reply

X0DX0A
Posted on April 2, 2019. 3:58 pm

Is the second HASH recorded actually 2 hashes? Should it read:
aa15eb28292321b586c27d8401703494
bebb16193e4b80f4bc053e4fa818aa4e
2832885392469cd5b8ace5cec7e4ca19

Reply

E K
Posted on April 3, 2019. 8:57 am

No, there are MD5 and SHA256 hashes of the archive.

Reply

GEBSTER
Posted on April 29, 2019. 3:43 am

Is it possible that the certificate was left on a server, and then used to sign the malware making it look legitimate? so perhaps ASUS should have secured their certificates better?

Reply

GARY MACKNER
Posted on May 20, 2019. 6:02 pm

I have been fighting this virus for over 10 years. Everyone i contacted all told me that a BIOS could not get malware. I built a system using an Asus MB that keep losing its MBR. I reflashed the BIOS and reload Win 7 and it would run as long as you didn't reboot then I would lose the MBR again. I could see sector 0 was corrupted and copied into hundreds of other sectors. Had to wipe and zero out the entire HD and try again. New HD did no better. I figured it had to coming from the BIOS and contacted Asus. They had me send my MB to them upon they swapped a new BIOS chip on it. Upon reinstalling it, it ran fine for a short time and then just did the same thing again. I contacted Asus and they sent me a brand new MB which also ran fine for a a short time. I still have the 2 MBs and the Asus BIOS flash software. this malware also writes to any write-able software.

Reply

// LATEST POSTS

Outlaw cybergang attacking targets worldwide

CRISTIAN SOUZA, ASHLEY MUÑOZ, EDUARDO OVALLE

Triada strikes back

DMITRY KALININ

Operation SyncHole: Lazarus APT goes back to the well

SOJUN RYU, VASILY BERDNIKOV

Russian organizations targeted by backdoor masquerading as secure networking software updates

IGOR KUZNETSOV, GEORGY KUCHERIN, ALEXANDER DEMIDOV

// LATEST WEBINARS

CYBERTHREAT TALKS

CYBERTHREAT TALKS

11 MAR 2025, 5:00PM 60 MIN

In-depth analysis of cyberattacks: key findings from Kaspersky's Incident Response report

AYMAN SHAABAN

18 FEB 2025, 5:00PM 60 MIN

Silent shields & digital dragons: MDR's proactive protection

SERGEY SOLDATOV

TRAININGS AND WORKSHOPS

23 DEC 2024, 5:00PM 60 MIN

From chaos to control: streamlining detection engineering in Security Operation Centers

SARIM RAFIQ UDDIN

CYBERTHREAT TALKS

17 DEC 2024, 5:00PM 60 MIN

Crimeware and financial cyberthreats in 2025

FABIO ASSOLINI, MARC RIVERO, TATYANA SHISHKOVA

// REPORTS

Operation SyncHole: Lazarus APT goes back to the well

Kaspersky GReAT experts uncovered a new campaign by Lazarus APT that exploits vulnerabilities in South Korean software products and uses a watering hole approach.

IronHusky updates the forgotten MysterySnail RAT to target Russia and Mongolia

GOFFEE continues to attack organizations in Russia

Operation ForumTroll: APT attack with Google Chrome zero-day exploit chain

Threats

Categories

Archive
Webinars
Statistics
Threats descriptions

All tags
APT Logbook
Encyclopedia
KSB 2024

kaspersky