TeamViewer Confirms Undisclosed Breach From 2016

 By Sergiu Gatlan
 May 17, 2019
 02:02 PM
 0

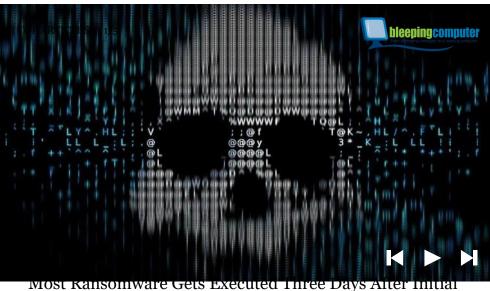


TeamViewer confirmed today that it has been the victim of a cyber attack which was discovered during the autumn of 2016, but was never disclosed. This attack is thought to be of Chinese origins and utilized the Winnti backdoor.

The company behind the highly popular TeamViewer remote desktop software told German publisher Der Spiegel that the attack was discovered before the threat group was capable of doing any damage, with experts and investigators failing to find any evidence of data being stolen during the security incident.

Also, no evidence was found that the hackers were able to compromise or steal source code even though they had access to it, according to TeamViewer.

^



READ MORE >>>

Backdoors which might have been planted during the 2016 attack have also been removed after a data center overhaul and all systems "completely checked, cleaned up and repositioned" at the end of 2016 according to the Der Spiegel report.

When asked by BleepingComputer about when and how the breach was discovered, TeamViewer said they detected the attack before any major damage was done.

"Like many technology leaders, TeamViewer is frequently confronted with attacks by cybercriminals. For this reason, we continuously invest in the advancement of our IT security and cooperate closely with globally renowned experts and institutions in this field.

In autumn 2016, TeamViewer was target of a cyber-attack. Our systems detected the suspicious activities in time to prevent any major damage. An expert team of internal and external cyber security researchers, working together closely with the responsible authorities, successfully fended off the attack."

Seeing that the hackers were not able to steal any data during the attack, TeamViewer decided not to publish a security breach notification to inform the users of the incident.

Regarding the reasons behind the decision to not disclose the breach, a TeamViewer spokesperson further told BleepingComputer that based on consultation with relevant authorities and advisors, it was decided that it was not necessary to disclose the attack.

19-Mar-20, 16:19 2 of 13

Independent experts conducted a thorough investigation using all IT forensic resources available and found no evidence that the security of our users or their IT systems was affected in any way.

Together with the relevant authorities and our security advisors, we came to the joint conclusion that informing our users was not necessary and would have been counterproductive to the effective prosecution of the attackers. Against this backdrop, we decided not to disclose the incident publicly in the interest of the global fight against cybercrime and thus also in the interest of our users.

Attackers have also used the Winnti malware against ThyssenKrupp in 2016 and Bayer in 2018, with ThyssenKrupp CERT investigators monitoring their activity and discovering that the hackers were only interested in stealing technical trade secrets.

In the case of the attack against the largest drugmaker from Germany, investigators from the DCSO cybersecurity group — set up by Bayer with help from Allianz, BASF and Volkswagen — were also able to keep an eye on the group's activity since the initial infiltration in early-2018 until March 2019 and also concluded that the hackers were not able to steal any data.

Service outage due to DoS attack during the summer of 2016

On June 1, 2016, TeamViewer issued a press release acknowledging a service outage caused by a denial-of-service attack (DoS) which targeted the TeamViewer DNS server infrastructure.

This statement followed multiple user reports claiming that attackers took control of their computers using TeamViewer and using their PayPal accounts to either make online purchases or steal money — a list was also created to track all the reported incidents.

Some of the victims also claimed that the attackers successfully compromised their TeamViewer accounts even though they used unique very long passwords or had Two-Factor Authentication enabled, leading them to believe that TeamViewer's computing systems were hacked [1, 2, 3].

However, in their press release, TeamViewer blamed the account hacks reported by its users on "Careless use of account credentials remains to be a key problem for all internet services. This particularly includes the use of the same password across multiple user accounts with various internet services."

TeamViewer also mentioned the possibility of some users having unintentionally downloaded and installed programs infected with malware which could have allowed attackers to "virtually do anything with that particular system – depending on how intricate the malware is, it can capture the entire system, seize or manipulate information, and so forth."

After the user uproar caused by the "careless" word used in the June 1 press release, Teamviewer apologized for using the word through public relation manager, Axel Schmidt.

TeamViewer also stated that the hacks reported by users might have had something to do with the Backdoor. TeamViewer malware besides the initial mention of stolen password credentials.

When asked if there is any connection between the account hacks reported in 2016 and the just disclosed breach, TeamViewer told BleepingComputer that there is no connection.

No. The cyber-attack on TeamViewer is in no way connected to this.

The corresponding reports are presumably related to a theft of large amounts of data from popular internet services (e.g. LinkedIn) in the same year. If affected users had been using identical passwords for

third-party services, such as TeamViewer, it was possible for attackers to abuse them for unauthorized access attempts.

TeamViewer generally recommends using unique passwords for different services and setting up a two-factor authentication to effectively prevent this kind of attack.

The Winnti Umbrella

While there is no attribution for the hacking group behind the 2016 attack TeamViewer just confirmed, multiple hacking groups collectively known by experts as the Winnti Umbrella according to ProtectWise 401 TRG, have been using the Winnti malware during their attacks.

The groups come under various names (i.e., Winnti Group, PassCV, APT17, Axiom, LEAD, BARIUM, Wicked Panda, and GREF) but Winnti Group is the first known to have used the Winnti backdoor during their campaigns.

As Kaspersky's GReAT full report on the Winnti Group from 2013 says, "The main objective of the group is to steal source code of online game projects as well as digital certificates of legitimate software vendors."

BARIUM, another Winnti Umbrella threat group, which mainly targets software and gaming companies [1, 2] and is still active as shown by its involvement in Operation ShadowHammer could be the most probable candidate for this attack.

Kaspersky also found evidence that connected the methods and tools used as part of Operation ShadowHammer with the ones employed in the supply chain attacks against CCleaner and NetSarang from 2017, with the threat actor behind the latter already having been identified as BARIUM by ESET, Microsoft, and other security researchers.

Related Articles:

Chinese Hackers Use New Malware to Backdoor Microsoft SQL Servers

Winnti Group Uses New PortReuse Malware Against Asian Manufacturer

Chinese Cyberspies Appear to be Preparing Supply-Chain Attacks

Virgin Media Data Breach Exposes Info of 900,000 Customers

Carnival Cruise Line Operator Discloses Potential Data Breach

• •

5 of 13 19-Mar-20, 16:19

HACKERS	SECURITY BREACH	TEAMVIEWER	WINNTI

SERGIU GATLAN 🗷 😼

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

✓ PREVIOUS ARTICLE NEXT ARTICLE Post a Comment Community Rules You need to login in order to post a comment Login Not a member yet? Register Now

You may also like:

li

Full	technical
doc	umentation

TeamViewer
Apologizes but still
say they were not
Compromised

Ransomware Recovery Experts

Here's a List of 29 Different Types of USB Attacks

Ad Cloudockit

bleepingcomputer.com

Ad Fast Data Recovery

bleepingcomputer.com

Hardware Security Modules

Chinese Cyberspies Appear to be Preparing Supply-Chain Attacks Finding & Enabling Hidden Features in Windows 10 Using Mach2 Equifax Confi Hackers Used Struts Vulner Breach Its Se

Ad futurex.com

bleepingcomputer.com

bleepingcomputer.com

bleepingcomputer.com

^

POPULAR STORIES



Ransomware Gangs to Stop Attacking Health Orgs During Pandemic



Microsoft Scales Back Office 365 Features to Handle High Loads

NEWSLETTER SIGN UP

To receive periodic updates and news from
BleepingComputer, please use the form below.

Email Address...

Submit

NEWSLETTER SIGN UP

Email Address...

SUBMIT

Follow us:







2

MAIN SECTIONS

News

Downloads

Virus Removal Guides

Tutorials

Startup Database

Uninstall Database

File Database

Glossary

COMMUNITY

Forums

Forum Rules

Chat

USEFUL RESOURCES

Welcome Guide

Sitemap

19-Mar-20, 16:19 12 of 13

COMPANY

About BleepingComputer

Contact Us

Send us a Tip!

Advertising

Write for BleepingComputer

Social & Feeds

Changelog

Terms of Use - Privacy Policy

Copyright @ 2003 - 2020 Bleeping Computer® LLC - All Rights Reserved