



OWASP

Open Web Application
Security Project

Hunt for a Cold War-like Sleeper Malware

Wong Onn Chee

OWASP Singapore Chapter Lead

OWASP : Core Mission

- The Open Web Application Security Project (OWASP) is a 501c3 not-for-profit also registered in Europe as a worldwide charitable organization focused on improving the security of software.
- Our mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks.
- Everyone is welcomed to participate in OWASP and all of our materials are available under free and open software licenses.

Cold War Sleeper Agents

- They lay dormant in enemy countries for decades, leading normal lives. Families were also in the enemy countries. Many a times, their kids did not know their parents were sleeper agents.
- Every morning, sleeper agents would get the daily (newspaper), go to the nearby park and read the classifieds ads for activation code. For instance, a property for rent ads with words such as Sea View, Balcony, Ready to move in, Kids going to college, Price Negotiable"
- Upon activation, their families would go back to their motherland and the agents would kickstart their attacks according to their mission protocol.

Are all "good guys" really good?

BROUGHT TO YOU BY B y w D


SecurityIntelligence NEWS 22 TOPICS INDUSTRIES X-FORCE RESEARCH MEDIA EVENTS & WEBINARS s

Home > News >

NEWS August 22, 2016 @ 5:00 AM

TeamViewer Trojan Makes it Spy on You

By Larry Loeb



Bigstock

victim.

Dr. Web has been following a Trojan that works on TeamViewer, the popular remote control utility, since it first appeared in 2011.

It called the latest iteration of the TeamViewer Trojan "BackDoor.TeamViewerENT.1" to differentiate it from previous instances. Whereas those earlier versions of the Trojan downloaded a malicious library that it installed on the target machine, this version uses the TeamViewer app itself to carry out surveillance on the

TRENDING NEWS

IBM Joins New York Cyber Fellows Program to Address Cyber Skills Shortage
[Read More](#)

Bridging the Security Skills Gap With the First Cyber Careers Show
[Read More](#)

Web Tracking Threat Could Raise the Risk of Cybersecurity Breaches, Researchers Find
[Read More](#)

think 2018 IBM
March 19–22
Las Vegas

Everything IBM Security has to offer in one place, built just for you.



Are all "good guys" really good?



The screenshot shows the SC Media website. At the top left is the SC MEDIA logo. A navigation bar contains links for SC US, SC UK, NEWS, CYBERCRIME, NETWORK SECURITY, PRODUCT REVIEWS, IN DEPTH, EVENTS, WHITEPAPERS, LOG IN, and REGISTER. Below this is the text 'THE CYBERSECURITY SOURCE'. The main header features the SC CYBERCRIME logo and a list of categories: Ransomware, Data Breaches, APTs/Cyberespionage, Malware, Phishing, and Insider Threats. The article title is 'TeamSpy malware exploits TeamViewer in phishing campaign' by Robert Abel, Content Coordinator/Reporter, dated February 21, 2017. The article text states that Heimdal Security researchers spotted a new spam campaign carrying the TeamSpy data-stealing malware. It explains that attackers exploit the TeamViewer remote access tool to grant full access to a compromised device. A small image titled 'Cyberespionage' shows a server rack. A red box on the right side of the page is labeled 'MOST READ ON SC' and contains a list of four articles: 1. Intel advises companies to stop installing Spectre/Meltdown update; 2. Zyklon password stealer exploits Microsoft vulnerabilities via spam campaign; 3. Intel's Spectre/Meltdown patch hold up, what to do while you wait; 4. Malicious Chrome and Firefox extensions block removal to hijack browsers.

SC Media US > Cybercrime > TeamSpy malware exploits TeamViewer in phishing campaign

by Robert Abel, Content Coordinator/Reporter

February 21, 2017

TeamSpy malware exploits TeamViewer in phishing campaign

Heimdal Security researchers spotted a new spam campaign carrying the TeamSpy data-stealing malware.

The attackers exploit the TeamViewer remote access tool to grant an attacker full access to a compromised device. The malware is particularly difficult to stop as it is capable of circumventing two factor authentication and accessing encrypted content, according to a February 20 Heimdal blog post. The blog noted that

Cyberespionage

The attackers exploit the TeamViewer remote access tool to grant an attacker full access to a compromised

MOST READ ON SC

1. Intel advises companies to stop installing Spectre/Meltdown update
2. Zyklon password stealer exploits Microsoft vulnerabilities via spam campaign
3. Intel's Spectre/Meltdown patch hold up, what to do while you wait
4. Malicious Chrome and Firefox extensions block removal to hijack browsers



Who?

- Victim is a medium-sized organisation (<10,000 staff).
- They had invested in sandbox and endpoint protection solutions
- They were (still are) G-Suite for Business customers. G-Suite used strong ciphers. (Hey, they are Google!)
- They were using (still using) MS Office productivity Suites, including MS Outlook for email and collaboration.

When?

- From 2016, victim installed a Outlook "plugin" that allowed their Outlook to sync with G-Suite for Business, primarily with Google Calendar.
- "Plugin" was tested in the sandbox and was subjected to VirusTotal scans, which gave it a clean bill of health.
- "Plugin" was then distributed and installed on all user endpoints.
- Until the D-day in 2017, users had no issues or complaints against the "plugin".

What?

- Sometime in 2017, their helpdesk received an escalation that a user lost all files and folders under his My Documents folder.
- Helpdesk thought it was an user error or hard disk error.
- Until the deluge (aka tsunami) of escalation of lost files and folders were received by their helpdesk.
- From an event which was classified as minor, it got rapidly escalated to a major security incident. Esp when CEO called in to say his My Documents was cleaned out.



What?

- Unlike servers which are backed up daily, users did not (and still don't) back up their endpoints on a daily basis.

How?

- Due to the risk of potential data breach of PII, my team was engaged and came in to investigate 2 days after D-day.
- Representative images of affected endpoints were taken - disk, memory and etc.
- Analysis of the images showed the presence of this unknown (to us) "plugin". However, as users had been using it without issues for a year and VirusTotal again showed clean bill of health, we decided to focus on more critical (or sexy) stuff - registry, boot, ADS, system files, common dlls, event logs and etc.
- However, after 1 week of digging (trenches, not shellscrapes), every sexy stuff panned out to be legit. All hashes matched publicly known good ones.

How?

- No interesting Windows events logs.
- Came back to look at this "plugin". Decided not to RE it until there was further evidence.
- Tried some EDR tools and none of them reported anything of interest.
- Decided to do things old fashioned - run the image in a VM and roll back the date to D-1 day.

How?

- Used the good old Sysinternal tools to monitor.
- D-1 day: nothing happened to our test files in the My Documents in the test VM.
- D day: test files in the My Documents were deleted.
- The deletion was too fast as the test files were too few. Created a python script to generate tons of test files and folders.
- Eureka! Formally confirmed that the "plugin" was deleting the files and folders under My Documents!

How?

- Kickstarted the RE process.

What we found

- "Plugin" had a good side - it did connect to user's Google Calendar for synchronisation with Outlook. Events, Tasks, reminders and etc were all working.
- Hidden among the good codes was a connection to a John Doe Google Calendar. As the traffic to Google Calendar was strongly encrypted (ECDHE/AES/GCM), the connection to the John Doe G-Calendar (also hosted on Google Calendar) could not be detected.
- John Doe G-Calendar was a public G-Calendar. No login is required to view details of all events.
- We had a fun time reading what John Doe did for past year - catch movies, have dinner, lunch, birthday and etc. Just like any John

What we found

- Events on the D-day looked very innocent - such as "Dinner with Micheal Daniels". Lots of hair scratching now.
- Went back to the RE output and found that there were more hidden "Easter Eggs".
- "Dinner with Michael Daniels" or any name with M.D. initials => Delete My Documents
- "Lunch with Adrian Daniels" or any name with A.D. initials => Launch attacks on Active Directory.

What we found

- No privilege escalation.
- No exploitation of CVEs.
- Can bypass all, if not most, network and endpoint security solutions. (I bet it can bypass all EDRs).

Lessons What we found

- Always use software from reputable sources. Not "goodware" recommended in support forums.
- Ensure all software are digitally signed by legitimate and correct sources. For e.g., don't use a Google Calendar plugin signed by Logitech cert. (Huh, Logitech??)
- If source code is available (for e.g. Thunderbird G-Calendar plugins), perform code review. Same applies to plugins, addons, agents and etc.

Trivia

- Has anyone performed an RE on the SilkAir Studio mobile app, which is available within the plane WiFi when you fly SilkAir planes?
- If not, have you installed it without checking for its security, since it is not available from Play Store (not vetted by Google Play Protect)?

Demo Time

Yeah!

Can go back home soon!



OWASP

Open Web Application
Security Project

Hunt for a Cold War-like Sleeper Malware