DAILY

Article by

Bad Rabbit: A new ransomware epidemic is on the rise

Share

Preliminary results of the internal investigation into alleged incidents reported by US media

Are dating apps safe?

October 25, 2017

THREATS

In October 2017, Kaspersky Lab initiated a thorough review of our telemetry logs in relation to alleged 2015 incidents described in the media. We were aware only of one single incident that happened in 2014 during an APT investigation when our detection subsystems caught what appeared to be Equation malware source code files and decided to check if there were any similar incidents. Additionally, we decided to investigate if there were any third party intrusions in our systems besides Duqu 2.0 at the time of this alleged 2015 incident.

We have performed a deep investigation associated with the case from 2014 and preliminary results of this investigation revealed the following:

- During the investigation of the Equation APT (Advanced Persistent Threat), we have observed infections from all around the world, in more than 40 countries.
- Some of these infections have been observed in the USA.
- As a routine procedure, Kaspersky Lab has been informing the relevant U.S. Government institutions about active APT infections in the USA.
- One of the infections in the USA consisted in what appeared to be new, unknown and debug variants of malware used by the Equation group.
- The incident where the new Equation samples were detected used our line of products for home users, with KSN enabled and automatic sample submission of new and unknown malware turned on.
- The first detection of Equation malware in this incident was on September 11 2014. The following sample was detected:
  - 44006165AABF2C39063A419BC73D790D
  - mpdkg32.dll

  Verdict: HEUR:Trojan.Win32.GrayFish.gen
- Following these detections, the user appears to have downloaded and installed pirated software on his machines, as indicated by an illegal Microsoft Office activation key generator (aka "keygen") (md5: a82c0575f214bdc7c8ef5a06116cd2a4 — for detection coverage, see this VirusTotal link) which turned out to be infected with malware. Kaspersky Lab products detected the malware with the verdict Win32.Mokes.hvl.
- The malware was detected inside a folder named "Office-2013-PPVL-x64-en-US-Oct2013.iso". This suggests an ISO image mounted in the system as a virtual drive/folder.

Article by

Share

- Detection for the Backdoor.Win32.Mokes.hvl (the fake keygen) has been available in Kaspersky Lab products since 2013.
- The first detection of the malicious (fake) keygen on this machine was on October 4 2014.
- To install and run this keygen, the user appears to have disabled the Kaspersky products on his machine. Our telemetry does not allow us to say when the antivirus was disabled, however, the fact that the keygen malware was later detected as running in the system suggests the antivirus had been disabled or was not running when the keygen was run. Executing the keygen would not have been possible with the antivirus enabled.
- The user was infected with this malware for an unspecified period, while the product was inactive. The malware dropped from the trojanized keygen was a full blown backdoor which may have allowed third parties access to the user's machine.
- At a later time, the user re-enabled the antivirus and the product properly detected (verdict: "Win32.Mokes.hvl") and blocked this malware from running further.
- After being infected with the Win32.Mokes.hvl malware, the user scanned the computer multiple times which resulted in detections of new and unknown variants of Equation APT malware.
- The last detection from this machine was on November 17 2014.
- One of the files detected by the product as new variants of Equation APT malware was a 7zip archive.
- The archive itself was detected as malicious and submitted to Kaspersky Lab for analysis, where it was processed by one of the analysts. Upon processing, the archive was found to contain multiple malware samples and source code for what appeared to be Equation malware.
- After discovering the suspected Equation malware source code, the analyst reported the incident to the CEO. Following a request from the CEO, the archive was deleted from all our systems. The archive was not shared with any third parties.
- No further detections have been received from this user in 2015.
- Following our Equation announcement from Feb 2015, several other users with KSN enabled have appeared in the same IP range as the original detection. These seem to have been configured as "honeypots", each computer being loaded with various Equation-related samples. No unusual (non-executable) samples have been detected and submitted from these "honeypots" and detections have not been processed in any special way.
- The investigation has not revealed any other related incidents in 2015, 2016 or 2017.
- No other third party intrusion, besides Duqu 2.0, were detected in Kaspersky Lab's networks.
- The investigation confirmed that Kaspersky Lab has never created any detection of non-weaponized (non-malicious) documents in its products based on keywords like "top secret" and "classified".

We believe the above is an accurate analysis of this incident from 2014. The investigation is still ongoing, and the company will provide additional technical information as it becomes available. We are planning to share full information about this incident, including all technical details with a trusted third party as part of our Global Transparency Initiative for cross-verification.

Post was updated to include timestamps.

Article by

Equation APT backdoors detect duqu duqu 2.0 keygens

Share

Read Next

SPECIAL PROJECTS

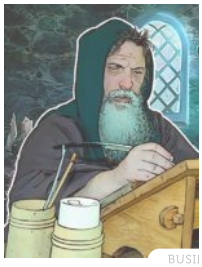
What just hit the fan: FAQs

BUSINESS

Trends in targeted attacks

BUSINESS

Lazarus: Modus operandi and countermeasures



BUSI

Moonlight Ma: from history