security affairs

T9000 backdoor, a sophisticated malware that spies on Skype users

February 8, 2016 By Pierluigi Paganini

G+1 14

My Page

The T9000 backdoor discovered by PaloAlto Networks is able to infect victims' machines to steal files, take□ screengrabs, and records Skype conversations.

A new threat is targeting Skype users, it is a backdoor trojan dubbed T9000 that is able to infect a victim's machine to steal files, take□ screengrabs, and record conversations. The T9000 malware dubbed T5000 that was detected in the wild two years ago.

“In addition to the basic functionality all backdoors provide, T9000 allows the attacker to capture encrypted data, take screenshots of specific applications and specifically target Skype users. The malware goes to great lengths to identify a total of 24 potential security products that may be running on a system and customizes its installation mechanism to specifically evade those that are installed.” states a blog post published by PaloAlto Networks.

The T9000 was used by threat actors to targets organizations worldwide, the researchers observed it used in multiple targeted attacks against US organizations.

The backdoor uses a multistage execution flow, which starts when victims opens an RTF file that contained exploits for specific vulnerabilities (i.e. both CVE-2012-1856 and CVE-2015-1641).

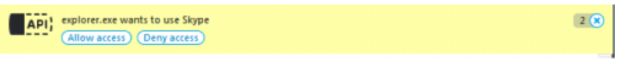
It checks before for the presence of defense solutions and malware analysis tools including Sophos, INCAInternet, DoctorWeb, Baidu, Comodo, TrustPortAntivirus, GData, AVG, BitDefender, VirusChaser, McAfee, Panda, Trend Micro, Kingsoft, Norton, Micropoint, Filseclab, AhnLab, JiangMin, Tencent, Avira, Kaspersky, Rising, and Qihoo 360.

At first stage of the infection the T9000 backdoor collects information on the target system and sends it to the C&C server, then the control infrastructure sends specific command to the bot based on the characteristic of the infected machine.

The researchers at Palo Alto Networks have identified three main plugins in the T9000 backdoor:

- tyeu.dat
- vnkd.dat
- qhnj.dat

tyeu.dat is the component that implemented the features to spy on Skype conversations, when hooking into the Skype API, the victim is presented with the message “explorer.exe wants to use Skype.” Theis Skype module can record both audio and video conversations, spy on text chats and take regular screenshots of video calls.


explorer.exe wants to use Skype

The vnkd.dat component is loaded to steal files on□ the infected computer, meanwhile the third module qhnj.dat implements backdoor functionalities to control the local file system (i.e.□ Create/delete/move, encrypt files and directories,□ and copy the user’s clipboard).

The experts at Palo Alto sustain that the backdoor was developed by skilled professionals due to the evasion technique implemented by the malicious code.

“The author of this backdoor has gone to great lengths to avoid being detected and to evade the scrutiny of the malware analysis community. We hope that sharing the details of how this tool works as well as the indicators in the section below will help others defend themselves against attacks using this tool.”

Pierluigi Paganini

(Security Affairs – Skype, T9000 backdoor)

Share it please ...

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at□ Bit4Id, firm leader in identity□ management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field,□ he is Certified Ethical Hacker at□ EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog□ "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone,□ ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE

Hackers leaked DHS staff records, 200GB of files are in their hands□

NEXT ARTICLE

CVE-2016-0603 - Oracle Issues out-of-box Java emergency patch for Windows

- +Pierluigi Paganini

  Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in□ identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

[redacted]

Back to top ^