Duuzer, a data stealer Trojan targets South Korean organizations

October 27, 2015 By Pierluigi Paganini

Researchers at Symantec uncovered bad actors that have been using a backdoor Trojan dubbed Duuzer to target organizations in South Korea and elsewhere.

According to Symantec, threat actors have been using a data stealer Trojan dubbed Duuzer to target organizations mainly located in South Korea. The bad actors conducted targeted attacks against organizations in the manufacturing industry, they served Duuzer backdoor to gain complete control over infected machines.

Duuzer allows attackers to collect system information, access local file system, change the time attributes of files, upload and download files, and of course, execute commands.

According to the experts at Symantec, the Backdoor.Duuzer has been around since at least July 20 2015, the attackers are relying on spear phishing messages and watering hole attacks to spread it.

"Duuzer *is an ongoing threat that is being delivered in targeted attacks. While the exact distribution method is unknown, it's likely that the malware is spreading through spear-phishing emails or watering-hole* attacks." *states a blog post published by Symantec.*

The malware researchers at Symantec collected evidence that bad actors behind the Duuzer campaign are also spreading two other malware, dubbed W32.Brambul and Backdoor.Joanap. The two malware were also used to target organizations in South Korea and serve extra payloads on the compromised machines.

According to Symantec, Duuzer is linked to both malware, every computer infected by Brambul was also infected by Duuzer and shared the same command and control (C&C) servers.

Duuzer is able to infect both 32-bit and 64-bit systems, it implements several methods to avoid detection, for example, it is able to checks for the presence of virtual machines and also rename the malware after an existing legitimate software runs on startup.

"The Duuzer *attackers have been observed trying to disguise their malware on an infected computer. They do this by identifying what software is installed and runs on startup, then renaming their malware to a similar title of an existing, legitimate program." continues the analysis.*

The researchers speculate the threat actors behind the Duuzer campaign have a significant knowledge about malware detection techniques.

"The attackers appear to be manually running commands through the back door *on affected computers. In one case, we observed the attackers creating a camouflaged version of their malware, and in another, we saw them attempting to, but failing to deactivate Symantec Endpoint Protection (SEP)," Symantec said in a blog post.*

The experts provided further information on both Brambul and Joanap threats, Brambul is a worm that spreads from one computer to another by relying on brute-force attacks aimed at the Server Message Block (SMB) protocol, once infected the host it creates a network share to provide the attackers access to the system drive.

"The Brambul worm uses brute-force attacks to propagate. The threat connects to random IP addresses through the Server Message Block (SMB) protocol using a hardcoded list of user names and passwords. The passwords are quite common or easy to guess, such as "123123", "abc123", "computer," "iloveyou," "login", and "password". states the post. "After Brambul compromises a computer, it creates a net share to give attackers access to the system drive (usually the C: drive). It sends a message with the computer's details and login credentials to a hardcoded email address. Brambul's variants may be able to drop additional threats."

Joanap is a classic backdoor to gain control over the infected system.

In order to prevent Duuzer infections Symantec recommends the following best practices:

- Change default credentials
- Use string passwords.
- Keep the operating system and software updated
- Don't open suspicious emails.
- Keep security software up-to-date with the latest definitions

Pierluigi Paganini

(Security Affairs – Duuzer , malware)

Share this...

Duuzer | malware | South Korea | spear phishing | Symantec | Trojan | watering hole

SHARE ON

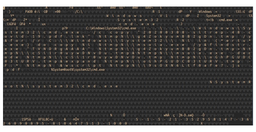
Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 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
The cyber labor market in Israel, the cyber guild

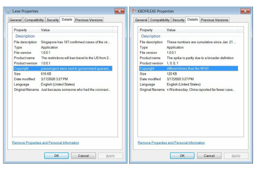
NEXT ARTICLE
15-Year-Old has been identified and arrested for TalkTalk Attack

YOU MIGHT ALSO LIKE



Is APT27 Abusing COVID-19 To Attack People ?!

March 19, 2020 By Pierluigi Paganini



Coronavirus news used by Emotet and Trickbot to evade detection

March 19, 2020 By Pierluigi Paganini

Back to top