Vxer is offering Cobian RAT in the underground, but it is backdoored

securityaffairs.co/wordpress/62573/malware/cobian-rat-backdoor.html

September 1, 2017

September 1, 2017 By Pierluigi Paganini

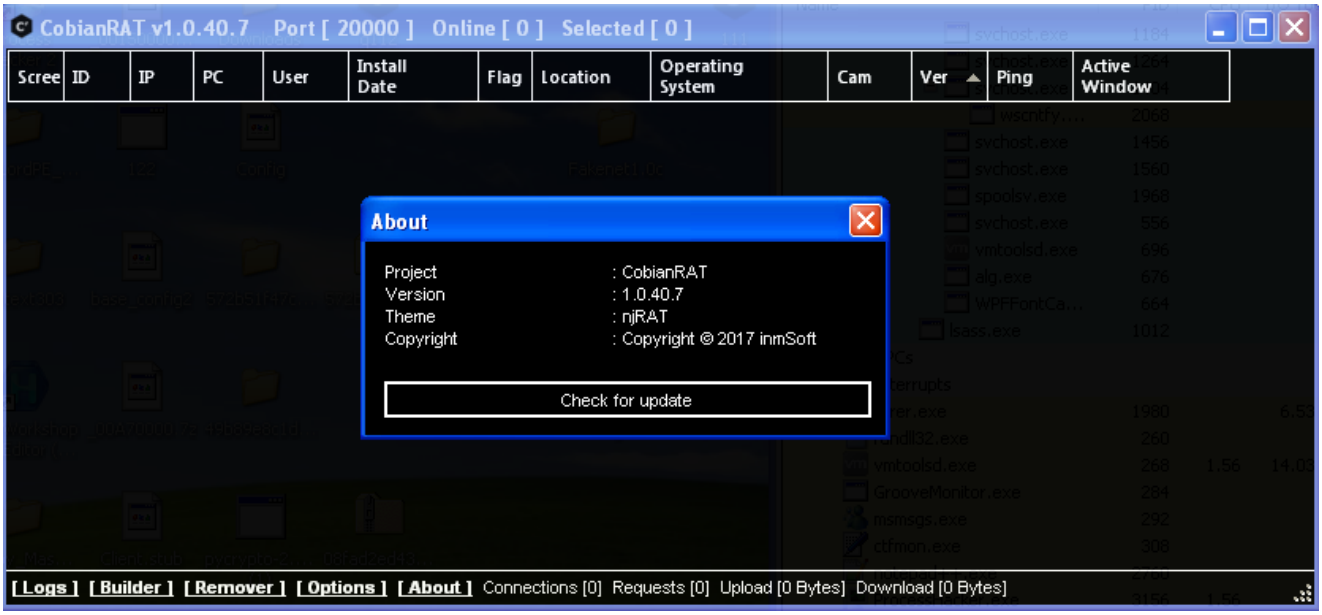
Malware writer is offering for free a malware dubbed Cobian RAT in the underground, but the malicious code hides an ugly surprise.

In the dark web, it is quite easy to find alone vxers and hacking forums that offer malware and customize them according to buyers' needs.

Recently researchers from Zscaler have spotted a remote access trojan dubbed Cobian remote RAT that was offered for free in the underground. It is fairly elemental malicious code based on an old RAT known as njRAT, it implements common spying features such as keylogger, webcam hijacker, screen capturing and of course the ability to execute attackers' code on the victim's system.

"The Zscaler ThreatLabZ research team has been monitoring a new remote access Trojan (RAT) family called Cobian RAT since February 2017. The RAT builder for this family was first advertised on multiple underground forums where cybercriminals *often buy and sell exploit and malware kits." reads the analysis from Zscaler. "This RAT builder caught our attention as it was being offered for free and had* lot *of similarities to the njRAT/H-Worm family, which we analyzed in this report."*

Unfortunately, the Cobain RAT hides a malicious feature in an encrypted library, the code allows the author of the malware to take full control of machines infected with the RAT.



The code could be used by the author also to completely cut off the crooks who initially infected the machine with the Cobain RAT.

The malware researchers noticed that the backdoor module hidden in the Cobian builder kit communicates with a preset page on Pastebin that was managed by the original author. In this way, the malware gets the current address of the command and control servers run by the original writer, but it first checks for the presence of the second level operator online to avoid being detected.

The experts speculate the original author's purpose is to build a massive botnet exploiting the effort of second operators in spreading the Cobian RAT.

"It is ironic to see that the second level operators, who are using this kit to spread malware and steal from the end user, are getting duped themselves by the original author. The original author is essentially using a crowdsourced model for building a mega Botnet that leverages the second level operators Botnet." concluded. "The original author is essentially using a crowdsourced model for building a mega Botnet that leverages the second level operators' Botnet."

Pierluigi Paganini

(Security Affairs – Cobian RAT, malware)

Share On

You might also like

There you can buy or download for free private and compromising data of your competitors. We public schemes, drawings, technologies, political and military secrets, accounting reports and clients databases. All this things were gathered from the largest worldwide companies, conglomerates and concerns with every activity. We gather data using vunlerability in their IT infrastructure. in their IT infrastructure.

Industrial spy team processes huge massives every day to devide you results. You can fid it in their portal:

http://[redacted]

(Tor browser required)

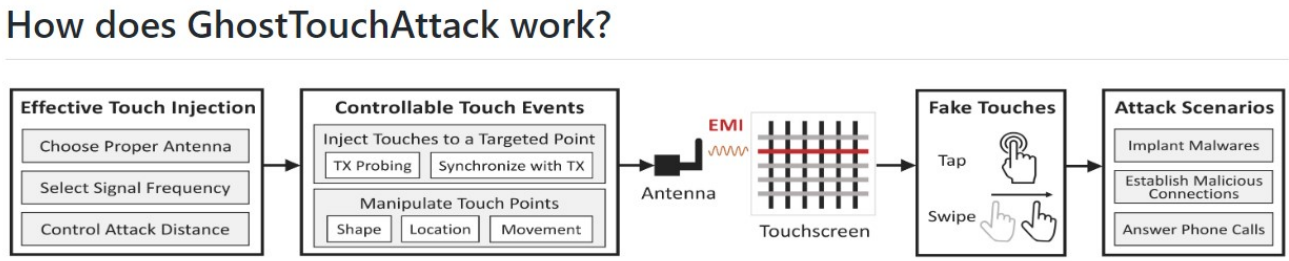
We can save your time gaining your own goals or goals of your company.With our information you could refuse partnership with unscrupulous partner, reveal dirty secrets of your competitors and enemies and earn millions dollars using insider information.

"He who owns the information, owns the world"

Nathan Mayer Rothschild

The strange link between Industrial Spy and the Cuba ransomware operation

May 28, 2022 By Pierluigi Paganini



GhostTouch: how to remotely control touchscreens with EMI

May 27, 2022 By Pierluigi Paganini

Back to top

- Home
- Cyber Crime
- Cyber warfare

- APT
- Data Breach
- Deep Web
- Digital ID
- Hacking
- Hacktivism
- Intelligence
- Internet of Things
- Laws and regulations
- Malware
- Mobile
- Reports
- Security
- Social Networks
- Terrorism
- ICS-SCADA
- EXTENDED COOKIE POLICY
- Contact me