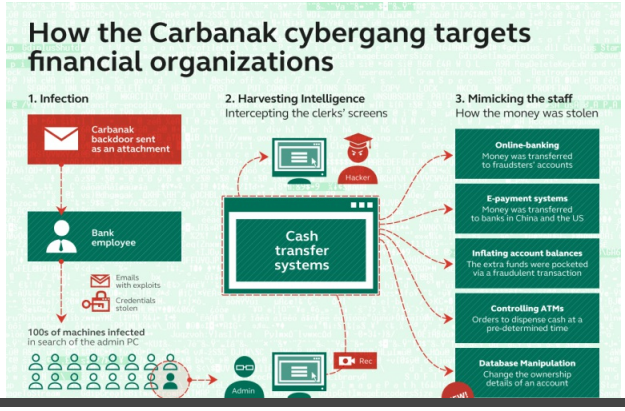
Carbanak cybergang is back and it is not alone

February 9, 2016 By Pierluigi Paganini

Experts at Kaspersky Lab discovered that Carbanak cybergang is back and other groups are adopting similar APT-style techniques to steal money.

Security researchers at the 2016 edition of SAS in Tenerife revealed that the infamous Carbanak gang is back, and it is not the unique group that is adopting APT-style techniques to steal money from banks.



Last year, Kaspersky investigated a number of cyber attacks on 29 Russian organizations, the researchers believe that these attacks launched by Carbanak and two other groups dubbed “Metel” and “GCMAN,” that adopted similar hacking techniques in their operations.

In September 2015, security experts at CSIS discovered that the Carbanak malware was still being used in spear phishing attacks against major organizations in UE and Europe.

“Just recently, CSIS carried out a forensic analysis involving a Microsoft Windows client that was compromised in an attempt to conduct fraudulent online banking transactions. As part of the forensic task, we managed to isolate a signed binary, which we later identified as a new Carbanak sample. *” wrote the CSIS in a blog post published by the CSIS.*

“We speculate that the main purpose of this company is to receive money from fraudulent transactions. As stated in the Kaspersky report, Carbanak*-related transfers are rather huge. Possibly, they have registered a company and opened bank accounts in order to receive their stolen money while having full control of the transferring process,”*

The CSIS experts noticed that new binaries used by the Carbanak gang were similar to the previous versions, apart in a number of improvements. The new binaries were mutexes and random files, meanwhile, the communication with the C&C server relies on a proprietary protocol.

“We have observed at least four different new variants of Carbanak *targeting key financial personnel in large international corporations.”*

The new Carbanak trojan was relying on predefined IP addresses instead of domains and in order to improve the evasion capability its code was signed with a digital certificate issued by Comodo to a Russia-based wholesale company.

Kaspersky confirmed that the Carbanak gang (also

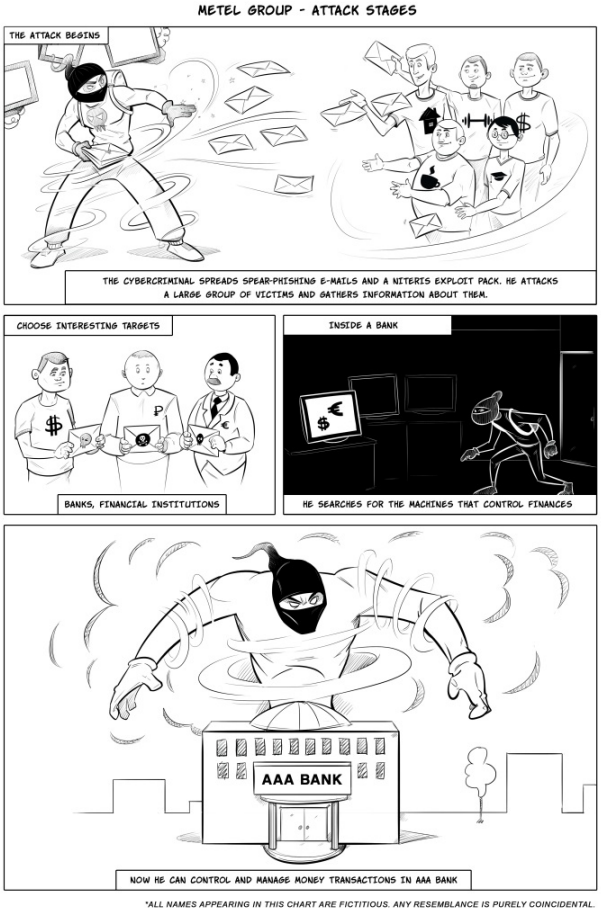
called Carbanak 2.0 by Kaspersky) was behind the attacks spotted by CSIS and revealed that the group is now targeting also the budgeting and accounting departments of various types of organizations, a including financial institution, and a telecoms company.

The group that targeted a Russian bank used a strain of malware known as Metel (aka Corkow) to compromise banks' networks via spear-phishing emails.

The financial institution hit by the group discovered that hackers stole millions of rubles in just one night from the ATMs of other financial institutions. The hackers used ATM balance rollbacks to steal money while balances remained untouched.

"In summer 2015, a bank in Russia discovered it had lost millions of rubles in a single night through a series of strange financial transactions. The bank's clients were making withdrawals from ATMs belonging to other banks and were able to cash out huge sums of money while their balances remained untouched. The victim bank didn't realize this until it tried to recoup the money withdrawn from the other banks' ATMs." states a blog post published by Kaspersky.

"The malware, used exclusively by the Metel *group, infected the bank's corporate network via e-mail and moved laterally to gain access to the computers within the bank's IT systems. Having gained access to the bank operator's money-processing system, the gang pulled off a clever trick by automating the rollback of ATM transactions. This meant that money could be stolen from ATM machines via debit cards while the balance on the cards remained the same, allowing for multiple transactions at different ATM machines."*



According to Kaspersky, the Metel group is still active and targeted at least 30 Russian financial organizations.

The experts followed also the operations of a third group dubbed GCMAN.

Also in this case, the hackers are using APT tactics and techniques, the hackers compromised systems of its targets with malware disguised as a Word document.

Once compromised one of the systems inside the target network they used tools like Putty, VNC and Meterpreter to move laterally and compromise other machines. In one case the GCMAN used a script designed to send $200 every minute.

“Our investigation revealed an attack where the group then planted a cron *script into bank’s server, sending financial transactions at the rate of $200 per minute.” states the post.*

Give a look to the report … it is full of interesting data and demonstrates the rapid evolution of criminal organizations and the efficiency of their techniques.

Pierluigi Paganini

(Security Affairs – Carbanak, hacking)

Share it please ...

ATM | bank | Carbanak cybergang | Cybercrime | GCMAN | Hacking | Kaspersky | malware | Metel | RAT | Remote Access Tool

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
Global and Modern Terrorism/Cyber Terrorism

NEXT ARTICLE
Rent the infamous AlienSpy backdoor is now quite easy

YOU MIGHT ALSO LIKE

Man charged of Laundering $19.6 Million earned with PBX system hacking

February 14, 2016 By Pierluigi Paganini

The IPT ruled that GCHQ spies can legally hack any electronic devices

February 13, 2016 By Pierluigi Paganini

- +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]

1. Banking Tutorial For Beginners

2. Bank Internetowy

3. Best European Banks

4. Banking Information

5. Bank Profits

6. SME Banking

7. Equitable Bank

8. Transaction Banking

Back to top