Russian Metel group manipulated ruble-dollar exchange rate with malware

February 10, 2016 By Pierluigi Paganini

A Russian group of cyber criminals known as METEL has hacked the systems at the Kazan-based Energobank and manipulate Ruble-Dollar Exchange Rate infecting them with a malware.

A Russian cyber gang has hacked the systems at the Kazan-based Energobank and manipulate Ruble-Dollar Exchange Rate infecting them with a malware.

The event occurred exactly one year ago, in Feb 2015, when the hacking group dubbed **METEL** breached into the Russian Regional Bank for just 14 minutes resulting in the fluctuation of the exchange between 55 and 66 rubles per dollar.

The Moscow Exchange denied that its

the currency market manipulation. The Moscow Exchange explained that fluctuations observed by the users could have been caused by traders' mistakes.

The security firm Group-IB that was involved in the investigation on the case discovered that the Metel Hacking group infected Kazan-based Energobank, the hackers used the Corkow Trojan and placed more than $500 million in orders at non-market rates.

Corkow is a backdoor that breached 250,000 computers worldwide in more than 100 financial institutions.

> *"This is the first doc attack using this vir has potential to do more damage," Dmitr Volkov, the head of IB's cyber intelige department, told Bloomberg.*
>
> *"Once the malware h penetrated a local ne is sophisticated eno infect computers tha even not connected t Internet."" Dmitry Vo head of Group-IB's c intelligence departm Bloomberg*

The threat actors used spear phishing messages containing malicious links to hack the victim's accounts. The economic impact of the attack has been estimated in 244 Million Rubles, nearly $3.2 million.

The Metel group is the same referred in the report recently published by the Kaspersky Lab on the Carbanak 2.0.

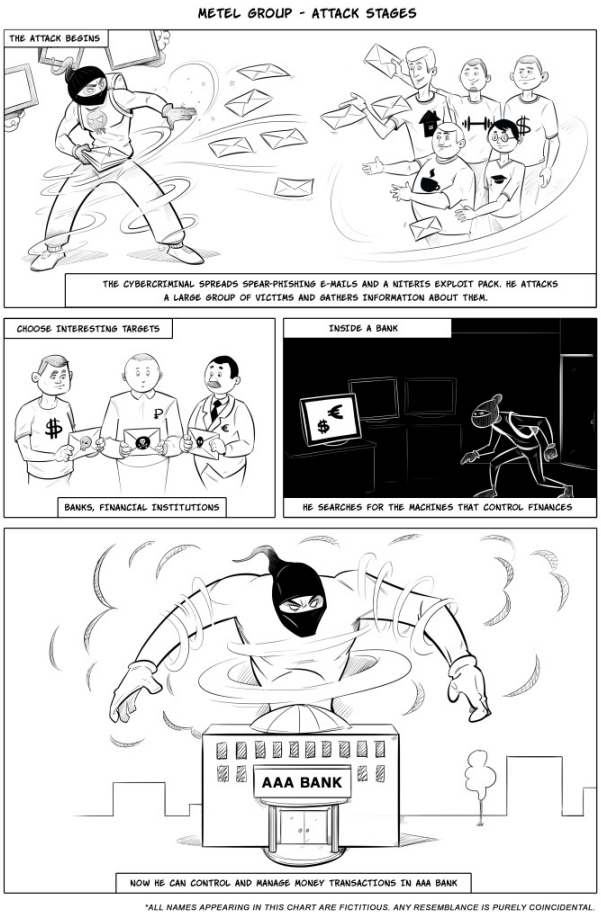
According to Kaspersky, the group targeted a Russian bank with the malware known as Metel

(aka Corkow) and compromise banks' networks via spear-phishing emails.

The financial institution targeted 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."*



Carbanak 2 0 Report issued by Kaspersky – METEL

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

Group-IB confirmed it, and added that the group is only known to be active in Russia where affected 73% Russian Banks.

Pierluigi Paganini

(Security Affairs – Carbanak, Metel)

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

Are you searching for a Facebook Hacking Tool? Be careful!

NEXT ARTICLE

February 2016 Patch Tuesday - All Windows are affected by a critical flaw

- +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. Bank Internetowy

2. Best European Banks

3. Banking Information

4. Bank Profits

5. SME Banking

6. Transaction Banking

7. Banking Institution

8. Lebanese Banks

Back to top