Dyre crackdown, the biggest effort to date by Russian authorities against cybercrime

February 7, 2016 By Pierluigi Paganini

Russian authorities raided offices of a Russian film distribution and production company as part of an operation against the Dyre gang.

Russian law enforcement and intelligence agencies in November raided offices of a Russian film distribution and production company as part of an operation against one of the world's most notorious cybercrime ring.

The authorities were supported by the experts at Kaspersky Lab who confirmed the involvement and announced it would reveal details about the operation at its annual conference.

This is the biggest effort to date of Russian authorities against the cybercrime.

caused overall losses for more than tens of millions of dollars.

The list of victims includes names like Bank of America Corp and JPMorgan Chase & Co.

According to the Reuters that published the news in exclusive, authorities haven't commented the operations, meanwhile the CEO of the film company refused to provide further information.

"A spokesman for the Russian Interior Ministry's cybercrime unit said his department was not involved in the case. The FSB, Russia's main intelligence service, said it had no immediate comment.

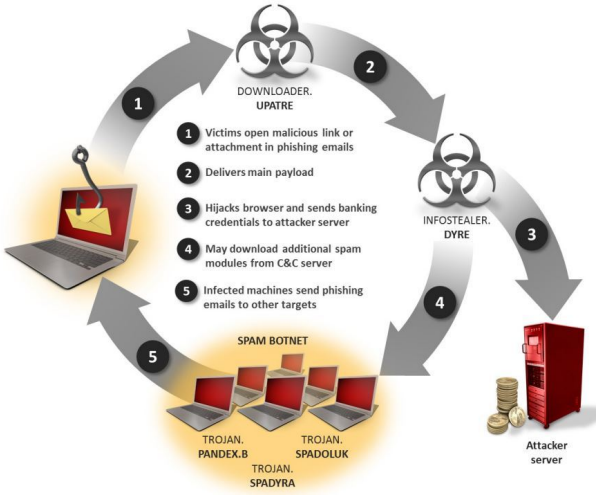
Nikolay Volchkov, the chief executive of the film company named 25th Floor, said he could not answer questions about the raid." wrote the Reuters.

Reuters clarified that it has no evidence that Volchkov or the film company is directly involved the criminal organization.

The unique certainly is that rarely criminal rings operating in from Russian are persecuted by the government if they don't target Russian organizations.

According to the Heimdal Security, in November 2015 more than 80.000 machines were already infected with Dyre Trojan across the world. The experts at Dell SecureWorks estimated that more than 400 financial institutions have fallen victim of the infamous trojan.

Dyre is usually downloaded by the malicious trojan Upatre, it is a powerful malware capable to perform man-in-the-middle attacks through browser injections and harvest the victim's credential.



The experts believe that the operation of the Russian authorities has successfully beheaded the organization behind the Dyre Trojan.

“We have seen a disruption over the last few months that is definitely consistent with successful law enforcement action,” explained security expert John Miller from iSight Partners.

There is another mystery in the story, the film company was working on a production called Botnet. a film on cybercrime ring with a story that has many similarities with the Dyre gang.

The company also hired the firm Group-IB to advise the Botnet director and writers on the finer points of cybercrime.

Group-IB CEO, Ilya Sachkov, said he met Volchkov at a security conference.

“He asked if we would be interested in consulting with a scriptwriter they would hire in the United States,” Sachkov said.

In November, Sachkov received a strange and an urgent call from Volchkov, saying he needed to meet.

“He was afraid. His colour *was totally white,” said Sachkov. “He knows there is an ongoing investigation about cybercrime.”*

Pierluigi Paganini

(Security Affairs – Dyre crackdown, hacking)

botnet | Cybercrime | Dyre | Hacking | malware | Russia

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
Security Affairs newsletter Round 46 – News of the week

NEXT ARTICLE
Reuse of login credentials put more than 20M Alibaba accounts at risk

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. Best Antivirus Software 

2. Remove Antivirus Scan 

3. Cheap Laptops Online 

4. Cell Phone Reviews 

5. Top 10 Cell Phones 

6. Password Management Software 

7. Computer Repair Services 

8. Protect Your Privacy 

Back to top