MASTERMIND BEHIND EUR 1 BILLION CYBER BANK ROBBERY ARRESTED IN SPAIN

26Mar2018

Press Release

Cybercrime syndicate infiltrated over 100 financial institutions in 40 countries

The leader of the crime gang behind the Carbanak and Cobalt malware attacks targeting over a 100 financial institutions worldwide has been arrested in Alicante, Spain, after a complex investigation conducted by the Spanish National Police, with the support of Europol, the US FBI, the Romanian, Moldovan, Belarussian and Taiwanese authorities and private cyber security companies.

Since 2013, the cybercrime gang have attempted to attack banks, e-payment systems and financial institutions using pieces of malware they designed, known as Carbanak and Cobalt. The criminal operation has struck banks in more than 40 countries and has resulted in cumulative losses of over EUR 1 billion for the financial industry. The magnitude of the losses is significant: the Cobalt malware alone allowed criminals to steal up to EUR 10 million per heist.

Modus operandi

The organised crime group started its high-tech criminal activities in late 2013 by launching the Anunak malware campaign that targeted financial transfers and ATM networks of financial institutions around the world. By the following year, the same coders improved the Anunak malware into a more sophisticated version, known as Carbanak, which was used in until 2016. From then onwards, the crime syndicate focused their efforts into developing an even more sophisticated wave of attacks by using tailor-made malware based on the Cobalt Strike penetration testing software.

In all these attacks, a similar modus operandi was used. The criminals would send out to bank employees spear phishing emails with a malicious attachment impersonating legitimate companies. Once downloaded, the malicious software allowed the criminals to remotely control the victims' infected machines, giving them access to the internal banking network and infecting the servers controlling the ATMs. This provided them with the knowledge they needed to cash out the money.

EUROPOL

Carbanak / Cobalt

How it works

1 **DEVELOPMENT**

The cybercriminal is the brains of the operation and develops the malware

Spear-phishing emails are sent to bank employees to infect their machines

2 **INFILTRATION AND INFECTION**

The cybercriminal deploys the malware through the bank's internal network, infecting the servers and controlling ATMs

Bank employee

Infected infrastructure

3 **HOW THE MONEY IS STOLEN**

MONEY TRANSFER

The criminal transfers the money into their account or foreign bank accounts

INFLATING ACCOUNT BALANCES

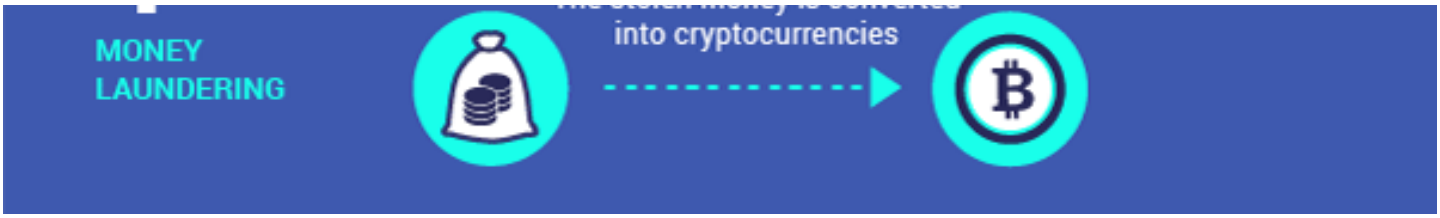
The criminal raises the balance of bank accounts and money mules withdraw the money at ATMs

CONTROLLING ATMs

The criminal sends a command to specific ATMs to spit out cash and money mules collect the money

4

The stolen money is converted



Cashing out

The money was then cashed out by one of the following means:

- ATMs were instructed remotely to dispense cash at a pre-determined time, with the money being collected by organised crime groups supporting the main crime syndicate: when the payment was due, one of the gang members was waiting beside the machine to collect the money being 'voluntarily' spit out by the ATM;
- The e-payment network was used to transfer money out of the organisation and into criminal accounts;
- Databases with account information were modified so bank accounts balance would be inflated, with money mules then being used to collect the money.

The criminal profits were also laundered via cryptocurrencies, by means of prepaid cards linked to the cryptocurrency wallets which were used to buy goods such as luxury cars and houses.

International police cooperation

International police cooperation coordinated by Europol and the Joint Cybercrime Action Taskforce was central in bringing the perpetrators to justice, with the mastermind, coders, mule networks, money launderers and victims all located in different geographical locations around the world.

Europol's European Cybercrime Centre (EC3) facilitated the exchange of information, hosted operational meetings, provided digital forensic and malware analysis support and deployed experts on-the-spot in Spain during the action day.

The close private-public partnership with the European Banking Federation (EBF), the banking industry as a whole and the private security companies was also paramount in the success of this complex investigation.

Wim Mijs, Chief Executive Office of the European Banking Federation, said: "This is the first time that the EBF has actively cooperated with Europol on a specific investigation. It clearly goes beyond raising awareness on cybersecurity and demonstrates the value of our partnership with the cybercrime specialists at Europol. Public-private cooperation is essential when it comes to effectively fighting digital cross border crimes like the one that we are seeing here with the Carbanak gang."

Steven Wilson, Head of Europol's European Cybercrime Centre (EC3), said: "This global operation is a significant success for international police cooperation against a top level cybercriminal organisation.

The arrest of the key figure in this crime group illustrates that cybercriminals can no longer hide behind perceived international anonymity. This is another example where the close cooperation between law enforcement agencies on a worldwide scale and trusted private sector partners is having a major impact on top level cybercriminality."

VIEW FULL INFOGRAPHIC

EN Carbanak/Cobalt infographic [1.43 MB]

CRIME AREAS	Cybercrime • High-Tech crimes • Forgery of money and means of payment • Payment Fraud • Money Mulling
TARGET GROUPS	General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
COUNTRIES	Spain
ENTITIES	European Cybercrime Center (EC3) • Joint Cybercrime Action Taskforce (J-CAT)
SUPPORT & SERVICES	Operational coordination • Information exchange • Forensics • Analysis • Strategic • Operational

Source URL: https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain