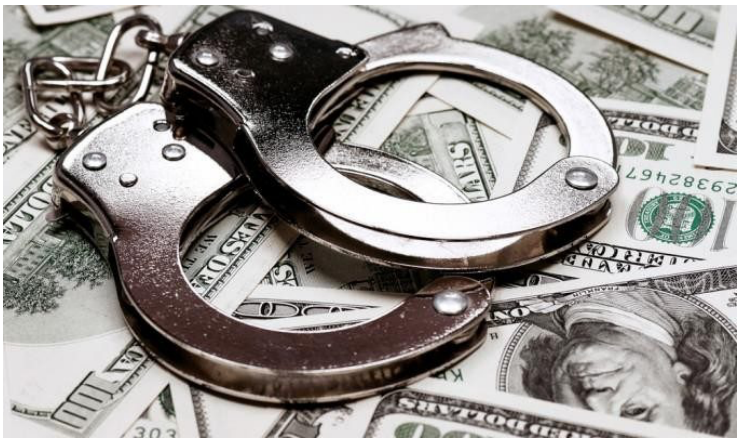
Alleged Mastermind Behind Carbanak Crime Gang Arrested

Author:
Lindsey O'Donnell

March 27, 2018 / 5:28 pm

3 minute read

Share this article:



The suspected leader behind the cyber crime group that targeted banks to rack up more than one billion Euros in damage over the past few years has been apprehended, according to the Spanish National Police.

The suspected mastermind behind the Carbanak criminal gang, which is notorious for stealing as much as $1 billion from more than 100 financial institutions in a string of attacks, has been apprehended, according to the Spanish National Police.

According to the European Union Agency for Law Enforcement Cooperation (aka Europol), the cyber crime syndicate designed sophisticated malware to attack banks, e-payment systems and financial institutions. The Carbanak group is best known for its malware – Carbanak and Cobalt – and a 2015 string of hacks that pilfered as much as $1 billion from financial institutions.

"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," according to Europol's statement. "The magnitude of the losses is significant: the Cobalt malware alone allowed criminals to steal up to EUR 10 million per heist."

The crime group would send out bank employees spear phishing emails, impersonating legitimate companies, which harbored a malicious attachment. If the attachments were executed, the criminals would use their malware to remotely control the victims' machines, giving them access to the internal banking network and allowing them to infect servers controlling the ATMs.

The malicious actor then remotely instructed ATMs to dispense cash at a pre-determined time, with one of the gang members waiting nearby. The hacking group also use the e-payment networks to transfer money from financial companies into criminal accounts.

"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," according to Europol.

The group first launched a campaign in 2013 using malware known as Anunak to target financial transfers and ATM networks of financial institutions, but by the following year that malware had been improved into a more sophisticated version known as Carbanak.

"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," according to Europol.

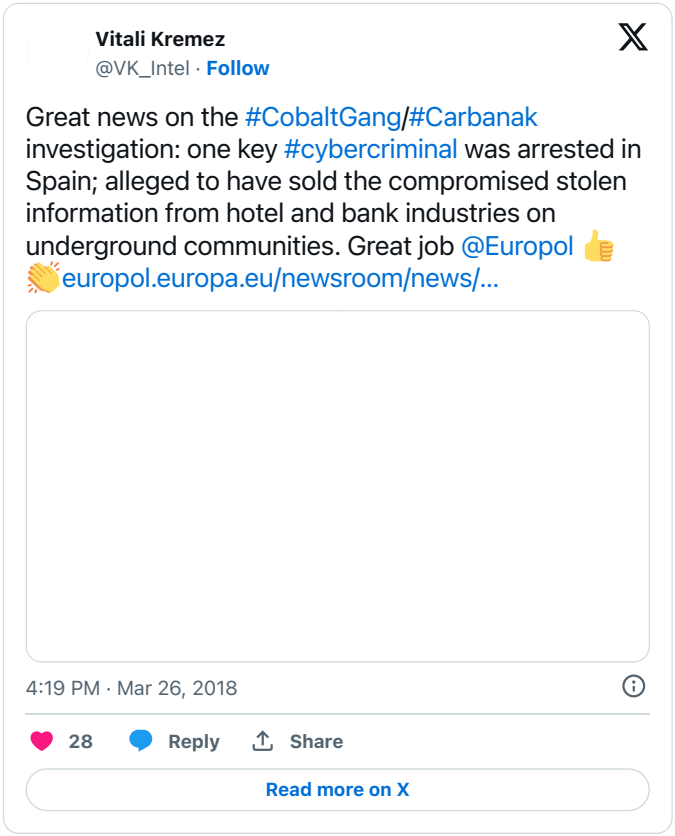
The organized crime group has been business since 2013 but its malware has been continually evolving and growing more sophisticated over the years.

As recently as January 2017, Carbanak ramped up its activity to include a new host of targets – including hitting a number of organizations in the hospitality, restaurant and retail markets, as well as a new command and control strategy involving Google's cloud-based services like Google Forms and Google Sheets.

In May 2017, reports emerged of the cyber gang devising a new way to gain persistence on targeted systems, involving a bogus instance of a Microsoft Windows app compatibility feature to more effectively pull off financially motivated crimes.

Europol, who supported the Spanish National Police in the investigation and subsequent arrest, said the gang leader, whom it didn't identify by name, was arrested in Alicante, Spain. Reports state Spain's Interior Ministry named the suspect as Denis K, a Ukrainian national.

Vitali Kremez, senior intelligence analyst at Flashpoint, said the arrest was "great news" in a tweet.



"The arrest of the key figure in this crime group illustrates that cybercriminals can no longer hide behind perceived international anonymity," said Steven Wilson, Head of Europol's European Cybercrime Centre in a statement. "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."

The Carbanak criminal gang has been a thorn in the side of the security community for years. It's tactics and targets were ever changing. In Jan. 2017, Carbanak moved from an almost exclusive focus on financial services and switched targets to those within the hospitality, restaurant and retail markets.

"They are very stubborn and very good," remarked Trustwave last year. "They've been doing it for years; it's their profession. Their malware and capabilities are cutting edge. They don't make dumb mistakes. They're stealthy how they infiltrate victims, they're good at lateral movement and leaving backdoors so that it's easy to re-engage. It's their professionalism really."

The gang's influence on other cybercriminals was also noted by cybersecurity professionals. In November, Kaspersky Lab observed a group called Silence, which bares a sharp resemblance to Carbanak.

The spear-phishing emails contain attachments that eventually download and execute a dropper that reaches out to the attacker's infrastructure. The backdoor is used to send system information and execute malicious code that uploads data, steals credentials and initiates tasks such as screen recording, which was a hallmark of Carbanak.