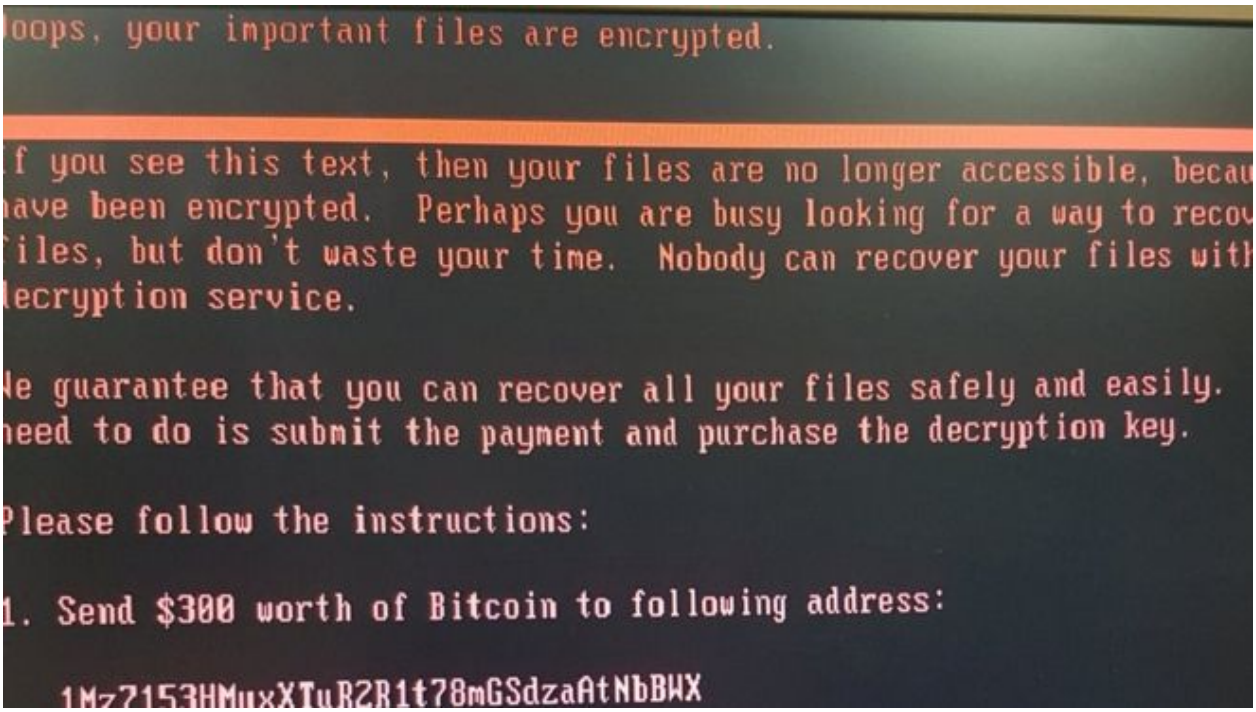
Technology

Ransomware 'here to stay', warns Google study

By Mark Ward
Technology correspondent, BBC News in Las Vegas

27 July 2017 | Technology



Cyber-thieves have made at least $25m (£19m) from ransomware in the last two years, suggests research by Google.

The search giant created thousands of virtual victims of ransomware to expose the payment ecosystem surrounding the malware type.

Most of the money was made in 2016 as gangs realised how lucrative it was, revealed a talk at Black Hat.

Two types of ransomware made most of the money, it said, but other variants are starting to emerge.

Track and trace

"It's become a very, very profitable market and is here to stay," said Elie Bursztein from Google who, along with colleagues Kylie McRoberts and Luca Invernizzi, carried out the research.

Ransomware is malicious software that infects a machine and then encrypts or scrambles files so they can no longer be used or read. The files are only decrypted when a victim pays a ransom. Payments typically have to be made using the Bitcoin virtual currency.

Mr Bursztein said Google used several different methods to work out how much cash was flowing towards ransomware creators.

As well as drawing on reports from people who had paid a ransom, it sought out the files used to infect machines and then ran those on lots of virtual machines to generate "synthetic victims", he said.

Cyber-hacks season:

- **Cyber-security industry 'lacks empathy' claims Facebook**
- **The myth of the 'sophisticated' hacker**
- **Hiding out among the net's criminal class**
- **Cyber-crooks put into rehab camp**

It then monitored the network traffic generated by these victims to work out to where money would be transferred. The data gathered in this stage was also used to find more variants of ransomware and the 300,000 files it found broke down into 34 of them, he said.

The most popular strains were the Locky and Cerber families, added Mr Bursztein.

Payment analysis of the Bitcoin blockchain, which logs all transactions made using the e-currency, revealed that those two strains also made the most money over the last year, he said, with Locky collecting about $7.8m (£5.9m) and Cerber $6.9m (£5.2m).

The research project also revealed where the cash flowed and accumulated in the Bitcoin network and where it was converted back into cash. More than 95% of Bitcoin payments for ransomware were cashed out via Russia's BTC-e exchange, found Google.

On 26 July, one of the founders of BTC-e, Alexander Vinnik, was arrested by Greek police on money laundering charges. The police were acting on a US warrant and his extradition to America is being sought.

The gangs behind the ransomware explosion were not likely to stop soon, said Mr Bursztein, although established strains are facing competition from newer ones.

"Ransomware is a fast-moving market," he said. "There's aggressive competition coming from variants such as SamSam and Spora."

Novel variants were expanding quickly and many were encouraging fast expansion by paying affiliates more if they placed the malware on to large numbers of machines. The ransomware as a service model was already proving popular, he warned.

"It's no longer a game reserved for tech-savvy criminals," he said. "It's for almost anyone."

This week BBC News is taking a close look at all aspects of cyber-security. The coverage is timed to coincide with the two biggest shows in the security calendar - Black Hat and Def Con.

Follow all our coverage via this link

View comments

Related Topics

Google **Cybersecurity**

Share this story About sharing

More on this story

The myth of the 'sophisticated' hacker
27 July 2017

Ransomware spike blamed on easy-to-use malware builders
26 July 2017

Shoddy data-stripping exposes firms to hack attacks
26 July 2017

How easy is it to hack a cash machine?
25 July 2017

Hiding out among the net's criminal class
26 July 2017

Technology

Uber's Travis Kalanick sued for fraud

Dave Lee

North America technology reporter

10 August 2017 | Technology

US stocks fall on North Korea fears

11 August 2017 | Business

Snap shares plunge as losses mount

11 August 2017 | Business

Top Stories

Trump to N Korea: Be very, very nervous
President Trump warns North Korea it should be "very, very nervous" if it does anything to the US.
30 minutes ago

Tonnes of tainted eggs sold in Denmark
5 hours ago

Near miss at Polish rail crossing
3 hours ago

Features

Trump's longstanding nuclear fixation

The Italian highlanders who may have Scottish roots