Crooks $2 Million A Month

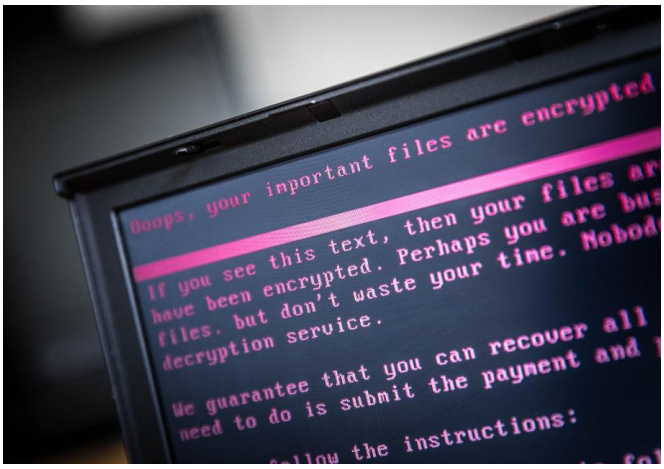
Security / #CyberSecurity

JUL 25, 2017 @ 10:00 AM 4,425

Google Warns Ransomv Crooks $2 Million A Mc

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms. **FULL BIO**



Ransomware has been disastrous for some businesses, but the biggest-earning variants, Cerber and Locky, haven't made as much news as the WannaCry and NotPetya strains. (Photo crec ROB ENGELAAR/AFP/Getty Images)

As the ransomware scourge calms down for the summer holidays, Google has taken a retrospective at that particular pesky form o cybercrime, finding it only become massivel profitable in the last year and a half.

That was largely thanks to two forms of ransomware, Locky and Cerber. They're the illicit market's kingpins that really came to

making in excess of $2.5 million every mont
according to the research, produced alongsi
researchers at University of California San Diego, New York University and blockchain analyst firm Chainalysis.

Compared to the $140,000 made by WannaCry and $10,000 by NotPetya, both o which have been deemed destructive in nature and possibly the produce of nation state hackers, the figures are astronomical. “They [WannaCry and NotPetya] were clear not interested in cashing out the money,” noted Luca Invernizzi, research scientist in Google's anti-abuse team.

The data also showed a significant jump in overall ransomware profits from the first quarter of 2016 the the next, rising from jus $100,000 to $2.5 million in a short timeframe. In recent months, revenues have actually dipped, though. "Maybe they’ve gor on holiday," suggested Elie Bursztein, Google's anti-abuse lead.

Cerber is the current number one menace, making $6.9 million to date, according to th research, released ahead of the Black Hat conference in Las Vegas this week. It’s been consistently earning more than $200,000 a month. Locky, meanwhile, remains a nasty strain and the overall biggest earner at $7.8 million. It was the first to earn above $1 million a month.

Riding atop botnets

Their success, and the sudden jump in revenue, is down to their distribution via botnets, in particular one known as Necurs,

According to data from IBM from April, Necurs was in control of 6 million victim PC and is also responsible for delivering one of the world's most pernicious banking malwa types, Dridex. A sudden surge in Locky attacks, delivered via spam, was witnessed b Cisco's Talos division in April this year too, thanks to resurgent Necurs activity. All are believed to be the work of Russian cybercriminals.

To dive into the ransomware market, Googl and its university colleagues were able to tal advantage of the tech giant's vast collection malware, including 301,588 ransomware fil across just 34 families. From there, they we able to look across Bitcoin transactions from the Blockchain. They determined that since 2014, ransomware crooks have made more than $25 million. It's likely the figures aren' representing the true cost of ransomware, a the researchers only added to the total wher they had high confidence it was a true ranso payment.

As for where the criminals are cashing out, per cent of ransom funds were cashed out at the Russian exchange BTC-E. That chimes with the indication that the biggest ransomware types are the produce of the biggest organized criminal gangs working ou of Russia.

In 2017, expect more innovation from the criminals, including more "ransomware-as- service" models with fancier customer support, said Invernizzi. The increasing professionalization of the digital underworld shows little sign of abating.

Forbes

tbthomasbrewster@gmail.com for PGP ma
Get me on Signal on +447837496820 or use
SecureDrop to tip anyone at Forbes.

Comment on this story

Website Feedback News Tip Report Corrections Reprints & Permissi