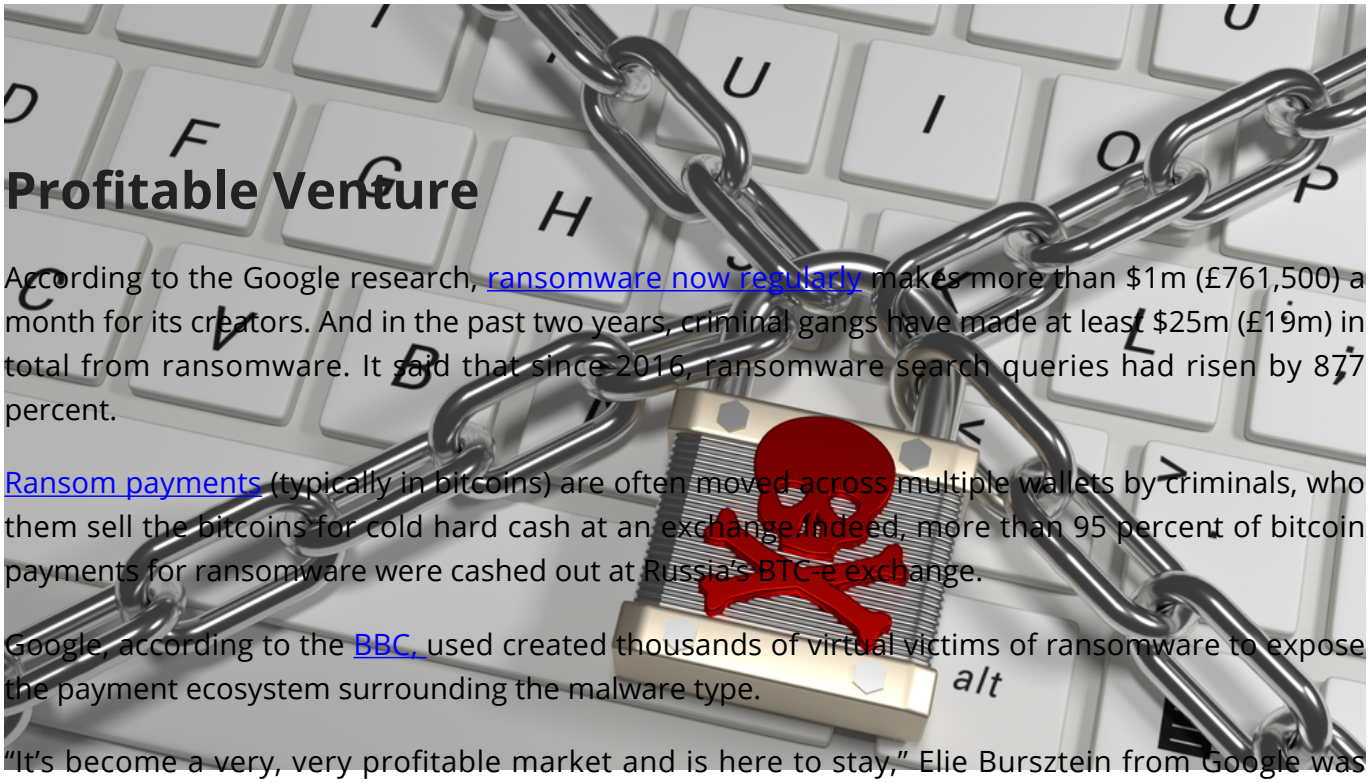
Google: Ransomware Will Remain A Very Real Threat

The scourge of ransomware is here to stay, Google has warned in new research presented at the Black Hat 2017 security conference in Las Vegas.

The study, produced by Google, with input from the University of California San Diego, New York University and blockchain analysis firm Chainalysis, found that ransomware has also become a profitable venture for criminal gangs in the past year and a half.

It comes as ransomware continues to plague computer systems worldwide, shutting down factories, the NHS, and even traffic camera systems around the world.



Profitable Venture

According to the Google research, ransomware now regularly makes more than $1m (£761,500) a month for its creators. And in the past two years, criminal gangs have made at least $25m (£19m) in total from ransomware. It said that since 2016, ransomware search queries had risen by 877 percent.

Ransom payments (typically in bitcoins) are often moved across multiple wallets by criminals, who then sell the bitcoins for cold hard cash at an exchange. Indeed, more than 95 percent of bitcoin payments for ransomware were cashed out at Russia's BTC-e exchange.

Google, according to the BBC, used created thousands of virtual victims of ransomware to expose the payment ecosystem surrounding the malware type.

"It's become a very, very profitable market and is here to stay," Elie Bursztein from Google was quoted as saying.

Bursztein alongside colleagues Kylie McRoberts and Luca Invernizzi, carried out the research.

Bursztein said that the most most popular ransomware strains were the Locky and Cerber families. He said that a payment analysis had shown that Locky collected about $7.8m (£5.9m) and Cerber $6.9m (£5.2m).

Bursztein also reportedly warned that the gangs behind the ransomware explosion were not likely to stop soon, although established strains are facing competition from newer ones.

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

And he said that a new trend saw criminal affiliates being paid more more if they placed the malware on to large numbers of machines. The ransomware as a service model was already proving popular, Bursztein warned.

“It’s no longer a game reserved for tech-savvy criminals,” he said. “It’s for almost anyone.”

Expert Take

“Malware is bad,” said Mark James, a security specialist at ESET. “Some infections are worse than others, but generally time, knowledge and an understanding of how the infection has taken root will enable you to remove most malware. Ransomware however, is a whole new level.

“It comes in two parts, the infection side of things will do all it possibly can to get on your machine, exploits, vulnerabilities, phishing, spam or email. Once infected the Ransomware can then take hold. More often than not the encryption used is the same strength as would be recommended by professional companies to keep your data safe from prying eyes.

“Once your files are encrypted and your ‘scary screen of sorrow’ is on display you only have a few choices; paying the ransom should not be a choice, all you are doing is helping them fund their next venture or paying the criminals for their hard work. Decrypting the data could be an option – all you need is a public decryptor tool or a lot of GPUS (Graphics processing unit) and a time machine. Of course you could just restore from your backup…. You did backup right?”

***Quiz:** What do you know about cyber security in 2017?*