Google ransomware tracking finds vicious infection cycle

Elizabeth Weise, USATODAY Published 2:34 p.m. ET July 25, 2017 | **Updated 4:14 p.m. ET July 25, 2017**

(Photo: Getty Images/iStockphoto)

SAN FRANCISCO — Ransomware surged last year, becoming a multi-million dollar business that's so profitable it's creating a "vicious cycle" of ever-increasing attacks, say researchers at New York University and Google who tracked the criminals' payment networks.

“It’s here to stay,” said Elie Bursztein, anti-abuse research lead at Google.

The findings suggest that — even though the last two large ransomware attacks, WannaCry (/story/news/2017/05/13/european-cyber-police-battle-unprecedented-global-hacking/101633374/) and Petya (/story/tech/news/2017/06/27/petya-ransomware-attack-windows-wannacry-protect/103241420/), did not seem to raise that much money — the criminal cyber industry in general has much to gain by exploiting users with these attacks.

The research team was able to track ransomware payment addresses and information via public sales of the digital currency bitcoin, watching more than $25 million in payments over the past two years. They plan to present their research on Wednesday in Las Vegas at Black Hat (https://www.blackhat.com/us-17/speakers/Elie-Bursztein.html), one of the country's largest computer security conferences.

Ransomware is malicious software that criminals use to first infect a victim's computer and then encrypt the files on it. To regain access to their files, victims must pay a ransom, typically in anonymous digital currency such as bitcoin.

It is increasingly one of the biggest money-makers for cyber criminals, who have been diligently creating new forms of it to boost their earnings. A recent variant, Cerber, is able to fully encrypt a newly-infected computer in under a minute and has consistently made $200,000 per month over the last year, the researchers found.

“It’s a vicious cycle, the more money they make, the more aggressively they spread the malware,” said Bursztein.

Related:

How to protect yourself against ransomware (https://www.usatoday.com/story/tech/2015/06/24/protect-against-ransomware-fbi/29216917/)

One popular method is "ransomware-as-a-service, (/story/tech/news/2016/12/18/ransomware---service-yes-s-thing/95397468/)" where criminal organizations rent out ransomware programs and the support system necessary to get paid to other criminals, charging a cut of the profits for the service, according to a 2017 Verizon report on data breach investigations (http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/).

Other innovations include time limits after which the criminals delete encrypted files, ransoms that increase the longer the victim takes to pay, ransom prices that vary based on the estimated sensitivity of filenames and a new option that allows victims to decrypt their files for free if they help infect others.

Ransomware programs aren't typically “owned” by any one group of criminals. In fact, the researchers tracked 34 different families of ransomware that are being distributed by criminals.

However, some of those criminals are better at making money off their crimes than others and have developed real expertise in how to push their programs out to more victims and make it easy for victims to pay them, said Damon McCoy, a New York University computer science and engineering professor who researches ransomware.

Criminal innovations: help desks

This can include amenities such as multi-lingual help desks to assist the victims in buying digital currency to pay the ransom.

With these new features, infection numbers began to shoot up in the second quarter of 2016 and have stayed high ever since — and it doesn't seem likely they're going to come down any time soon because it's such a profitable crime, said McCoy.

It’s also difficult to stop because it’s hard to track where the money’s going and thus find the criminals who are receiving it. The research team found that 95% of the ransoms they observed being paid went through BTC-E, a bitcoin exchange platform.

“It’s hard for law enforcement to put pressure on BTC-E because it’s a Russian-operated bitcoin exchange," said McCoy.

Google has seen concern about ransomware among the public ratchet up significantly in the past year and a half. Searches about ransomware have increased more then ten times, said Berzstein.

While the researchers couldn't offer a fix for the overall problem of ransomware, they did have one piece of advice – back data up regularly. A Google survey found that just 37% of people do so, putting them at risk for losing irreplacable photos and documents forever.

"We really really want to encourage people to back up their files," said McCoy.

Read or Share this story: https://usat.ly/2v5DzBk