Hacker Lexicon: A Guide to Ransomware, the Scary Hack That's on the Rise

Author: Kim Zetter.Kim Zetter Security
WIRED | 2015-09-17

Ransomware is malware that locks your keyboard or computer to prevent you from accessing your data until you pay a ransom, usually demanded in Bitcoin. The digital extortion racket is not new—it's been around since about 2005, but attackers have greatly improved on the scheme with the development of ransom cryptware, which encrypts your files using a private key that only the attacker possesses, instead of simply locking your keyboard or computer.

TL;DR: Ransomware is malware that locks your keyboard or computer to prevent you from accessing your data until you pay a ransom—usually demanded in Bitcoin. A popular and more insidious variation of this is ransom cryptware, which encrypts your files using a private key that only the attacker possesses, instead of simply locking your keyboard or computer.

And these days ransomware doesn't just affect desktop machines or laptops; it also targets mobile phones. Last week news broke of a piece of ransomware in the wild masquerading as a porn app. The so-called Porn Droid app targets Android users and allows attackers to lock the phone and change its PIN number while demanding a $500 ransom from victims to regain access.

Earlier this year, the FBI issued an alert warning that all types of ransomware are on the rise. Individuals, businesses, government agencies, academic institutions, and even law enforcement agents have all been victims. The malware can infect you via a malicious email or website, or attackers can deliver it straight to your computer if they've already infected it with a backdoor through which they can enter.

The Ransom Business Is Booming

Just how lucrative is ransomware? Very. In 2012, Symantec gained access to a command-and-control server used by the CryptoDefense malware and got a glimpse of the hackers' haul based on transactions for two Bitcoin addresses the attackers used to receive ransoms. Out of 5,700 computers infected with the malware in a single day, about three percent of victims appeared to shell out for the ransom. At an average of $200 per victim, Symantec estimated that the attackers hauled in at least $34,000 that day (.pdf). Extrapolating from this, they would have earned more than $394,000 in a month. And this was based on data from just one command server and two Bitcoin addresses; the attackers were likely using multiple servers and Bitcoin addresses for their operation.

Symantec has estimated, conservatively, that at least $5 million is extorted from ransomware victims each year. But forking over funds to pay the ransom doesn't guarantee attackers will be true to their word and victims will be able to access their data again. In many cases, Symantec notes, this doesn't occur.

Ransomware has come a long way since it first showed up in Russia and other parts of Eastern Europe between 2005 and 2009. Many of these early schemes had a big drawback for perpetrators, though: a reliable way to collect money from victims. In the early days, online payment methods weren't popular the way they are today, so some victims in Europe and the US were instructed to pay ransoms via SMS messages or with pre-paid cards. But the growth in digital payment methods, particularly Bitcoin, has greatly contributed to ransomware's proliferation. Bitcoin has become the most popular method for demanding ransom because it helps anonymize the transactions to prevent extortionists from being tracked.

According to Symantec, some of the first versions of ransomware that struck Russia displayed a pornographic image on the victim's machine and demanded payment to remove it. The victim was instructed to make payments either through an SMS text message or by calling a premium rate phone number that would earn the attacker revenue.

The Evolution of Ransomware

It didn't take long for the attacks to spread to Europe and the US, and with new targets came new techniques, including posing as local law enforcement agencies. One ransomware attack known as Reveton that is directed at US victims produces a pop-up message saying your machine has been involved in child porn activity or some other crime and has been locked by the FBI or Justice Department. Unless you pay a fine—in Bitcoin, of course, and sent to an address the attackers control—the government won't restore access to your system. Apparently the fine for committing a federal offense involving child porn is cheap, however, because Reveton ransoms are just $500 or less. Victims are given 72 hours to pay up and an email address, fines@fbi.gov, if they have any questions. In some cases they are threatened with arrest if they don't pay. However improbable the scheme is, victims have paid—probably because the extortionists distributed their malware through advertising networks that operated on pom sites, inducing guilt and fear in victims who had knowingly been perusing pornography, whether it was child porn or not. Symantec determined that some 500,000 people clicked on the malicious ads over a period of 18 days.

In August 2013, the world of ransomware took a big leap with the arrival of CryptoLocker, which used public and private cryptographic keys to lock and unlock a victim's files. Created by a hacker named Slavik, reportedly the same mind behind the prolific Zeus banking trojan, CryptoLocker was initially distributed to victims via the Gameover ZeuS banking trojan botnet. The attackers would first infect a victim with Gameover Zeus in order to steal banking credentials. But if that didn't work, they installed the Zeus backdoor on the victim's machine to simply extort them. Later versions of CryptoLocker spread via an email purporting to come from UPS or FedEx. Victims were warned that if they didn't pay within four days—a digital doomsday clock in the pop-up message from the attackers counted down the hours—the decryption key would be destroyed and no one would be able to help unlock their files.

In just six months, between September 2013 and May 2014, more than half a million victims were infected with CryptoLocker. The attack was highly effective, even though only about 1.3 percent of victims paid the ransom. The FBI estimated last year that the extortionists had swindled some $27 million from users who did pay.

Among CryptoLocker's victims? A police computer in Swansea, Massachusetts. The police department decided to pay the ransom of 2 Bitcoins (about $750 at the time) rather than try to figure out how to break the lock.

"(The virus) is so complicated and successful that you have to buy these Bitcoins, which we had never heard of," Swansea Police Lt. Gregory Ryan told the *Herald News*.

In June 2014, the FBI and partners were able to seize command-and-control servers used for the Gameover Zeus botnet and CryptoLocker. As a result of the seizure, the security firm FireEye was able to develop a tool called DecryptCryptoLocker to unlock victims' machines. Victims could upload locked files to the FireEye web site and obtain a private key to decrypt them. FireEye was only able to develop the tool after obtaining access to a number of the crypto keys that had been stored on the attack servers.

Prior to the crackdown, CryptoLocker had been so successful that it spawned several copycats. Among them was one called CryptoDefense, which used aggressive tactics to strong-arm victims into paying. If they didn't fork over the ransom within four days, it doubled. They also had to pay using the Tor network so the transactions were anonymized

and not as easily traced. The attackers even provided users with a handy how-to guide for downloading and installing the Tor client. But they made one major mistake—they left the decryption key for unlocking victim files stored on the victim's machine. The ransomware generated the key on the victim's machine using the Windows API before sending it to the attackers so they could store it until the victim paid up. But they failed to understand that in using the victim's own operating system to generate the key, a copy of it remained on the victim's machine.

The "malware author's poor implementation of the cryptographic functionality has left their hostages with the key to their own escape," Symantec noted in a blog post.

The business of ransomware has become highly professionalized. In 2012, for example, Symantec identified some 16 different variants of ransomware, which were being used by different criminal gangs. All of the malware programs, however, could be traced back to a single individual who apparently was working full time to program ransomware for customers on request.

The Ransomware to Watch Out for Now

Recently Fox-IT catalogued what they consider to be the top three ransomware families in the wild today, which they identify as CryptoWall, CTB-Locker, and TorrentLocker. CryptoWall is an improved version of CryptoDefense minus its fatal flaw. Now, instead of using the victim's machine to generate the key, the attackers generate it on their server. In one version of CryptoWall they use strong AES symmetric cryptography to encrypt the victim's files and an RSA-2048 key to encrypt the AES key. Recent versions of CryptoWall host their command server on the Tor network to better hide them and also communicate with the malware on victim machines through several proxies.

CryptoWall can not only encrypt files on the victim's computer but also any external or shared drives that connect to the computer. And the shakedown demand can range anywhere from $200 to $5,000. CryptoWall's authors have also established an affiliate program, which gives criminals a cut of the profit if they help spread the word about the ransomware to other criminal buyers.

CTB-Locker's name stands for curve-Tor-Bitcoin because it uses an elliptic curve encryption scheme, the Tor network for hosting its command server, and Bitcoin for ransom payments. It also has an affiliate sales program.

TorrentLocker harvests email addresses from a victim's mail client to spam itself to other victims. Fox-IT calculated at one point that TorrentLocker had amassed some 2.6 million email addresses in this manner.

Protecting against ransomware can be difficult since attackers actively alter their programs to defeat anti-virus detection. However, antivirus is still one of the best methods to protect yourself against known ransomware in the wild. It might not be possible to completely eliminate your risk of becoming a victim of ransomware, but you can lessen the pain of being a victim by doing regular backups of your data and storing it on a device that isn't online.

Go Back to Top. Skip To: Start of Article.

read:https://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/