IT

Ransomware – The Perfect Crime

Last Edited: July 4, 2016

Last Edited By: Justin Smith

Document Owner: Justin Smith

Where did it come from?

Back in September of 2005, a storm was brewing. The malware landscape included viruses, trojans, and worms, but a new type of threat was beginning to take shape. This new menace was foreboding, a novel implementation of a number of previously separate technologies. Most malware to this point would steal personal data like website logins or credit card numbers, however these methods of criminal gain meant that the possibility existed that eventually the creator could be traced, no doubt a problem if he intended to continue his criminal operation.

That's not to say that tracing a criminal online was easy - if your credit card number was stolen, it may be traded several times on various "carder" internet forums before it was ever used, requiring law enforcement to back track every step in the illicit chain to find the original swindler. If your online banking password was stolen, it was likely that the criminal would use some sort of proxy or other IP masking technique when pretending to be you, preventing the disclosure of their IP address.

These methods were not foolproof though. Sometimes, the credit card number thief would use the card himself and have goods ordered to somewhere near his house; sometimes the banking website password collector forgot to connect to her proxy before logging into the bank to transfer funds out of your account. This would at least give law enforcement a lead to work off of, that may help build a case, and sometimes result in apprehension of the crook.

The problem with this entire process is that the driving economic and psychological principles at play here are that of a theft. A thief initially steals something of value, which in turns forces the victim to exert some tangible amount of effort at recovering the stolen property until it is returned and to finally prosecute the criminal. The victim, and law enforcement working on their behalf are motivated by their desire to regain control over the stolen property and are therefore incentivized to track down the perpetrator continually until she is caught.

Ransomware turned the entire system on its head.

How does it work?

The process of a ransomware infection typically goes something like this:

The initial infection

A user opens an infected attachment or visits an infected webpage which exploits their web browser or some add-on such as Java or Flash

The key creation

Through an algorithm specific to each strain of ransomware, a unique public and private key are generated for each separate infection on a server controlled by the hacker

The key is sent to the infected PC

The infected PC immediately requests its newly formed public key from the server

Encryption starts

The ransomware goes through every file on the PC (usually with the exception of the operating system's installation folder and most times the folders where the applications are stored like Program Files) and encrypts them with the retrieved public key

Ransom note

Once the files have been encrypted, a note is left explaining how and where the ransom can be paid

Key release

If the ransom is paid within a specific period of time, the private key is provided to the victim to begin decryption of their files; if it is not, the private key is permanently deleted from the server, ensuring the files will never be recovered

Is the encryption effective?

The very idea of ransomware starts with public key cryptography. Public key cryptography is a relatively simple encryption method which is used millions or billions of times every day by people connecting to secure websites. The idea is that both sides of a transaction (for example, a webserver and a website user) each have their own public key and each have their own private key which are just extremely large prime numbers. Using some relatively simple math, combining one side's private key (website user) with the other side's public key (webserver) will allow the other side (webserver) to use their private key to read what was encrypted, while at the same time preventing anyone who intercepts this traffic from being able to decipher it.

The crucial point here is that these public and private keys, being made of extremely large prime numbers, prevent any attempt from any adversary from being able to decrypt it. This means that not only other hackers and large service providers but entire governments with nearly unlimited computing power at their disposal are unable to break this encryption.

When protecting your own files, the unbreakable factor is an important quality to have; the knowledge and implicit trust that your data is secure from any prying eyes is the very essence of the concept. Unfortunately, because the underlying math takes no sides and just simply exists, there is no way to assert true ownership of any particular piece of encrypted data. The closest you can come is to assert that the holder or controller of the encryption key is likely the owner. In this case, the ransomware author holds the key; he controls your files.

Game changer

As recently as 2013, ransomware was still traceable. Similar to the theft of credit card numbers and banking logins, tracing where the data was being exfiltrated to, or in the case of ransomware where the public key was being retrieved from, was still rather straightforward. Not only were the servers relatively out in the open but ransoms would typically be paid in MoneyPak cards (global

loadable payment cards) or other gift cards which could theoretically be traced by law enforcement.

In late 2013[1] a crushing but inevitable breakthrough was made by developers of the infamous CryptoLocker[2] ransomware: the combination of using the TOR network for the storage and disbursement of keys, and the use of bitcoin as the method of payment.

TOR[3], or The Onion Router, is a public mesh network of servers and PCs with the ultimate goal of providing anonymous communication. It accomplishes this goal by routing every request in a series of nested, encrypted layers (where the term "onion" comes from) and intentionally routing the request through multiple nodes before reaching its destination. TOR uses public key cryptography in every link in the chain making the decryption of traffic essentially impossible, and the routing method used prevents any one node from knowing the full details of a request; a node may know where a request is coming from, or where it's going, but never both. These factors combine to provide near-perfect anonymity for its users.

Bitcoin[4] is a peer-to-peer virtual currency, or cryptocurrency, that uses a distributed ledger called a blockchain to record transactions. Bitcoins are held in wallets that are designed to be anonymous and are transacted directly between members without any intermediaries; a wallet is essentially just a long string of letters and numbers that is cryptographically secure and unique, and is protected by either a password or other form of security. No identifying data is necessary to send bitcoin from one user to another anywhere in the world. Finally, the blockchain itself is cryptographically secured which provides its users with relative certainty that once a transaction takes place, it cannot been tampered with retroactively.

By combining TOR, an anonymous communication tool, with bitcoin, an anonymous currency, the developers of CryptoLocker had built the perfect criminal tool, one that would be difficult, if not impossible, to trace and one that was mathematically proven to be secure.

Often imitated, regularly duplicated

When the first version of CryptoLocker was released on September 5, 2013[5], the world took notice. With 250,000 infected computers in the first 3 months demanding payment for the decryption key necessary to get their data back, and at a price of $300USD per infection, the authors had taken in approximately $27 million in ransom[6]. In 3 months.

Malware authors around the globe took notice. They realized that the entire paradigm of malware had changed. Unlike in a thief and victim scenario, where the victim is incentivized to track down

[1] http://www.bbc.com/news/technology-25506020
[2] https://en.wikipedia.org/wiki/CryptoLocker
[3] https://en.wikipedia.org/wiki/Tor_(anonymity_network)
[4] https://en.wikipedia.org/wiki/Bitcoin
[5] http://www.bbc.com/news/technology-25506020
[6] http://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/

the thief because he holds something considered valuable to the victim, the use of anonymizing technologies and strong encryption meant that there was no need to track down the criminal – they were standing right there in front of the victim, almost advertising themselves, but doing so without the previous fear of being tracked.

The psychology of this new ransomware also meant that unlike in a robbery scenario, the victim always had control of his data; his data has never *left*, it was simply in an unusable state. While the thief may have encrypted the data and made it functionally useless for the owner, it was never *physically* removed like it would have been in a proper theft. This shift in physical location, while seemingly small at first, now puts the victim in a strange position mentally: she can reasonably assume that the thief will provide the decryption key assuming she pays the ransom, but that there are no good alternatives to not paying if restoring her files from backup is not an option.

Knowing that people were paying ransoms by the truckload – it is estimated by the FBI that the CryptoWall (not to be confused with "CryptoLocker") strain netted its authors $18 million USD by June 2015 – malware authors around the world immediately jumped on the bandwagon and began putting together their own versions of ransomware. Setting up the infrastructure was relatively easy, the money being paid per infection was relatively high, and the likelihood of being caught due to the encryption and technologies involved was relatively low.

In April 2016, there were even "ransomware-as-a-service" offerings popping up[7] where even the most novice "hacker" could pay a developer some amount of money or bitcoin to have a ransomware strain created specifically for them, and then they would also pay a percentage of each infection. This budding cottage industry of malware was the sign that the pendulum had swung decisively in the malware authors' direction.

Summary

Ransomware and the ransomware industry is here to stay. As long as strong cryptography remains provably secure, ransomware authors will continue to remain fully anonymous while reaping in the benefits of a very attractive work-to-reward ratio. The incentives greatly outweigh the risks and with almost no chance of prosecution due to the anonymity afforded to them by the TOR network and bitcoins, the authors will almost certainly continue to collect their ransoms for months and years to come.

Unfortunately there is no magic solution that will completely prevent your networks from being affected, but taking a defense-in-depth strategy toward your network will give you the best chance at surviving an infection incident. By limiting the attack surfaces that an infection can infect your users, by limiting what your users have access to, and by limiting the methods in which an infection can communicate with its criminal controllers, you can limit the damage that any one infection can cause.

[7] http://www.techrepublic.com/article/ransomware-as-a-service-is-exploding-be-ready-to-pay/

Appendix A – Protection methods

There are a number of ways that an administrator can limit the destruction a particular ransomware infection can cause but they are all far from perfect. Implementing multiple prevention methods can positively impact your chances of successful recovery of your data but there are no one-size-fits-all solution.

Backups

Having current and working offline backups is the most important thing an administrator can do to protect her network. Most new ransomware will attempt to delete or corrupt Microsoft Shadow Copies on Windows-based file servers so these are not considered backups. Having physically detached backup media is the only way to be certain your backups will not be infected.

Least Privilege Security Assignment

Giving your users only the absolute minimum access necessary to complete their assigned tasks is crucial to protecting your network. New ransomware variants are attempting to scan for and infect any and all network shares (both mapped and un-mapped) that the user has access to. Ensuring that any one user only has access to files they need for their specific job requirements can help limit the damage a single infection can inflict.

Attachment Filtering

One of the most common ways to get infected with ransomware is still by infected email attachments. The most common infection vectors are Microsoft Office and PDF documents, and .ZIP files with JavaScript containing the infection logic, so putting an extra emphasis on scanning attachments should be a priority.

Browser Runtime Environments (Java and Flash); Banner Ads

Another common way for a user to get infected is by drive-by exploits that are embedded in banner ads that exploit unpatched versions of Java and Flash. Ensuring that these are kept as up-to-date as possible is very important. Deploying some form of ad blocking technology (for example, browser extensions like uBlock Origin or Adblock Plus) can also prevent these infected ads from running.

Application Whitelisting

Providing an authorized list of applications which can be run in your environment will drastically cut down on the number of infections you see. Very few ransomware strains use novel infection methods; the encryption application is almost always a standard PE executable that can be prevented from running on a computer simply by not being whitelisted.

File Server Resource Manager

Microsoft Windows Server 2008 introduced a role called File Server Resource Manager. When installed, this role can prevent the infection of writing the encrypted versions of each file on a

Windows File Server by utilizing "file screens", basic filename filters that can be manually created or downloaded automatically from the internet[8].

Up to date antivirus/IDS/IPS

Ensuring that your edge gateways to the internet have the most recent definitions available can help prevent ransomware from ever making it to your user's desktops. As this collective method relies on a vendor's having seen a particular sample of ransomware, it is advisable to diversify between multiple vendors for each point (for example, using both Symantec antivirus and Symantec IDS is not advisable as they likely share the same source of definitions) to ensure the widest possible coverage of protection.

DNS block lists

There are various providers[9] that offer continually updated DNS zones with known malware-related hostnames. These usually work by updating your internal DNS infrastructure to resolve through this provider rather than directly through root hints or your ISP's resolvers and provide another level of protection. While they cannot prevent against a TOR-based infection, they can prevent the various exploit kits which are sometimes used as the initial infection vector from downloading the ransomware payload in the first place.

Last Edited By	Version	Changes Made
Justin Smith	1.0	Original document creation

Contents

[8] https://fsrm.experiant.ca/

[9] http://opendns.com