New Westminster Police Department

RansomWare Incident

Table of Contents

- Background information – What happened
- The Magnitude of the Situation
- How it happened
- The Solution
- Main Take-a-Ways
- Other Examples
- Some Statistics

BACKGROUND INFORMATION

NWPD uses a multi-tiered backup strategy. They are:

- 4-times-a-day NAS snapshots (at 8 AM, noon, 4 PM, and midnight) onto the NAS itself.
- NAS snap-mirror replication every 4 hours (6 snap-mirrors per day) to an off-site NAS appliance.
- Daily backups of changed data to the on-site backup server.
- Weekly backups of all data to the on-site backup server.

BACKGROUND INFORMATION

- Weekly backup of all data to tape.
- Windows drives replicate in real-time to off-site Windows servers.

NWPD was using standard, signature-based anti-virus software which checks all programs against its database of known viruses (so unknown ones can be an issue)

What Happened?

- 2 staff members came to IT complaining of not being able to access their files
- IT immediately disconnected the 2 users from the network
- An examination of the file system was begun to determine the scope of the damage
- A message was found that said we would need to pay $500 to decrypt the files

The Magnitude of the Situation

- Infected files were not restricted to the unit's folder but also all other folders they had access to
- The RansomWare attack began at 9:30 am and by 11:30 over 5 TB of data had been encrypted
- In total, 3 million files in 6 separate top level folders were encrypted
- A text file was found in each folder which contained instructions to pay the ransom


We Have Your
Data Pay!

Typical Ransomware Message

#What happened to your files?

All of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm
For more information you can use Wikipedia
*attention: Don't rename or edit encrypted files
because it will be impossible to decrypt your files

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need two key

1-Public key: you need it for encryption
2-Private Key: you need it for decryption

So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can receive your Private Key in 3 easy steps:

Step1: You must send us One Bitocin for each affected PC to receive Private Key.

Step2: After you send us one Bitcoin, Leave a comment on our blog with these detail: Your Bitcoin transaction reference + Your Computer name

*Your Computer name is: COMPUTERNAME VARIABLE

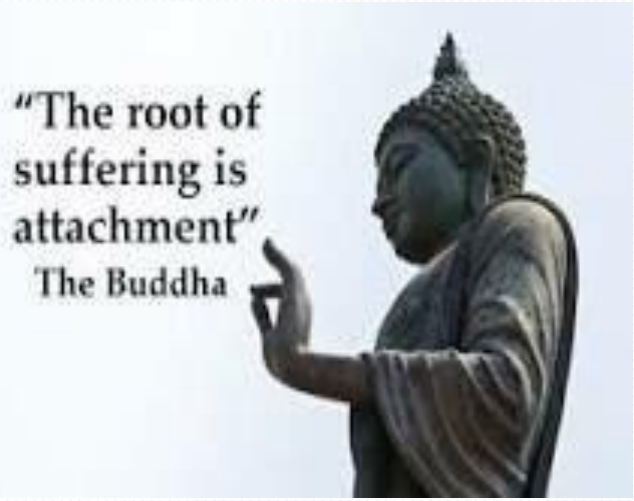
Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

*Our blog address:

How did it happen?

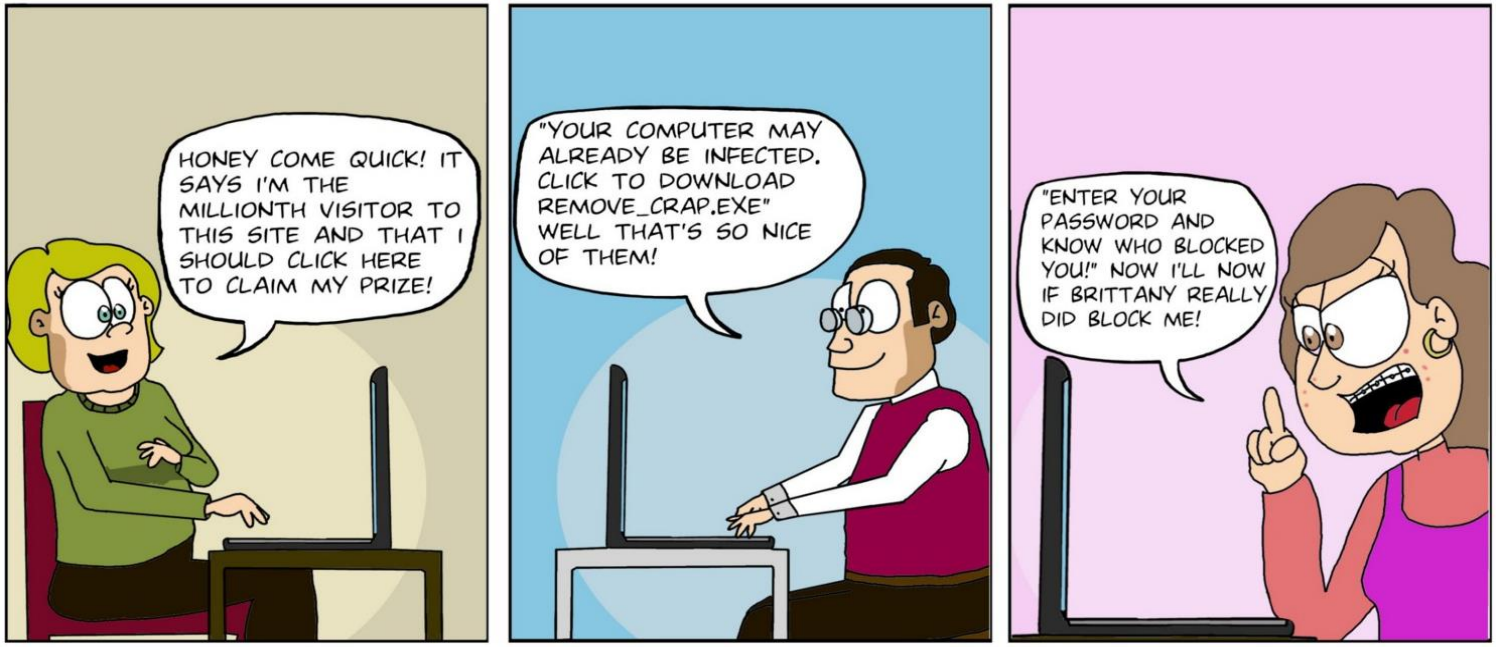
An attack commonly begins when a person opens a piece of malware disguised as a recognizable, sometime personalized e-mail attachment. Once opened, it freezes data block by block until everything is locked. It can also can be spread through drive-by downloading which occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge.

Buddha knew exactly the reason for cyberattacks, hackings and ransomware.



How did it happen?

- In our case, it was likely a person visiting an infected website
- We don't know what they clicked on but it could have been something like:



The Solution!

- IT ran the infected computer against 2 different anti-virus programs but neither found a virus
- The infected computer was reimaged, thus removing any trace of the virus, and restoring the encrypted files on the local hard drive.
- The fastest recovery was to use the snapshot of the day (at 8 am) before the virus hit, as the recovery point for the files
- This meant that updates made on any file after 8 am would be lost

The Solution!

- IT manually navigated to each affected folder, and overwrote the encrypted files with the 8 am version of those same files.
- The recovery took over 4 hours to complete. All folders were recovered by the end of the same work day.
- Almost all files were recovered but edits to files after 8 am were lost, and had to be re-edited.
- Fortunately, minimal work was lost.

" WELL SIR, I THINK WE'VE FINALLY GOTTEN THE VIRUS OUT OF THE OFFICE COMPUTERS. "

Take-A-Ways

- Employ a multi-tiered backup strategy and recovery plan for all critical information.
- Keep your operating system and software up-to-date with the latest patches.
- Maintain up-to-date Next-Gen (Behavior Based) anti-virus software, and scan all software downloaded from the internet prior to executing.
- Restrict users' ability (permissions) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services.
- Avoid enabling macros from email attachments.
- Provide security awareness training for all users

Who is been targeted?

An NBC New report states:

Cyber criminals who have forced hospitals, schools and cities to pay hundreds of millions in blackmail or see their computer files destroyed are now targeting the unlikeliest group of victims — local police departments.

The perps try to maximize panic with the elements of a real-life hostage crisis, including ransom notes and countdown clocks.

If the victim won't pay, the hackers threaten to delete the files, which they did last year to departments in Alabama and New Hampshire.

Mekinac, Que

- Last September (2018), staff in the regional municipality of Mekinac, Que. got a threatening message on their computers notifying them they were locked out of all their files. The attackers had used ransomware to demand money in return for keys to unlock the data. After about two weeks, Mekinac's IT department eventually negotiated the cyber extortionists down and paid $30,000 in Bitcoin to regain access.

The City of Atlanta

In March 2018, the alleged creators of the SamSam ransomware launched an attack on the infrastructure of the City of Atlanta GA. The attack affected many of the city's essential municipal functions. Among those affected were citizens' ability to pay water bills or parking tickets. The ransomware demand was $51,000 (unpaid) while the recovery costs were estimated at $17 million

Dickson County Sheriff's Office

Someone in the Dickson County Sheriff's Office did something many of us have done, clicked on a link to malicious software likely hidden inside an email link. The malware locked up the office's case files. All of them. You can see how difficult it might be to operate a law enforcement office without access to evidence or records.

Though the program didn't tamper with the files, it fully blocked all access and demanded the sheriff's office pay a ransom for the files' access. The FBI were brought in, and eventually it was determined that the best way to deal with the problem was to pay the ransom.

The asking price was $500, payable in the online crypto-currency Bitcoin.

The Moral Dilemma

The attacks are increasingly forcing police chiefs into frustrated deliberations over whether or not — against all their training and instincts — to reward extortionists whose identity they may never know.

“My initial reaction was ‘No way!” said Sheriff Todd Brackett of Lincoln County, Maine, whose system was frozen last spring. After “48 long hours,” Brackett reluctantly paid.

“We are cops,” he said with a sigh. “We generally don’t pay ransoms.”

What makes the ransoms so maddeningly tempting for cops to pay is that most attacks that have disabled police department computers have sought just a few hundred dollars.

Some Stats

- Ransomware costs businesses more than $75 billion per year. (Source: Datto)
- The average cost of a ransomware attack on businesses was $133,000. (Source: Sophos)
- 75% of companies infected with ransomware were running up-to-date endpoint protection. (Source: Sophos)
- A new organization will fall victim to ransomware every 14 seconds in 2019. (Source: Cyber Security Ventures)
- 1.5 million new phishing sites are created every month. (Source: webroot.com)
- The NotPetya ransomware attack cost FedEx $300 million in 2017. (Source: Reuters)

Some Stats

- 34% of businesses hit with malware took a week or more to regain access to their data. (Source: Kaspersky)
- Ransomware generates over $25 million in revenue for hackers each year. (Source: Business Insider)
- 75% of infected Canadian companies paid the ransom, 58% in the UK, and 22% in Germany. Only 3 % of US companies paid. (Source: Security Week)
- For 2019, McAfee analysts suggest that individuals with a large number of connected devices and a high net worth are some of the most attractive targets. (Good news, that leaves out most government finance officers)


S.KELLY
CREATORS SYNDICATE
©2017
SO, WHERE'S A CRIPPLING RANSOMWARE ATTACK WHEN YOU REALLY NEED ONE?
CHIPS

Questions?

Comments?