Global companies attacked, Department of Education hacked, are you armed?

By Damian Michael

6 Jul 2017

Not only did thousands of companies suffer from a severe Petya ransomware attack last week, but closer to home was the hacking of South Africa's Department of Education's system. Is your company prepared for what could still come?

Damian Michael

Ransomware: a brief history

Ransomware and fake-antivirus have been around for many years, relying on social engineering to trick computer users into paying the cybercriminals, so their phoney warnings claim, to avoid fines from police for supposed crimes, or to clean up “viruses” on their computers that don’t actually exist.

But CryptoLocker and CryptoWall – variations of the malware called crypto-ransomware or cryptoware – don’t bother with that sort of trickery. The attackers tell victims upfront that their files have been encrypted by ransomware. Unless you pay for the encryption key held by the attackers, the crooks destroy the private encryption key, making it impossible to recover your files.

Examples of ransomware wreaking havoc around the world

Petya

The initial Petya ransomware was made by Janus Cybercrime Solutions Professionals and they distributed the source code as a ransomware-as-a-service over the darknet.

The recent outbreak dubbed NotPetya is a modified version of the Petya source code acting as a wiper or a phlashdancer. It is meant to destroy data from the victim's computer and professionals believe the cyber-criminals behind this kind of attack created the ransomware not to profit from it but to cause havoc.

WannaCry

This family of ransomware has many names such as Wanna-Wana, Cryptor-Crypt0r, Cryptor-Decryptor, etc. WannaCry propagates using EternalBlue, an exploit of Windows' Server Message Block (SMB) protocol.

Much of the attention and comment around the event was occasioned by the fact that the U.S. National Security Agency (NSA) had already discovered the vulnerability, but used it to create an exploit for its own offensive work, rather than report it to Microsoft. The payload works in the same fashion as most modern ransomware: it finds and encrypts a range of data files, then displays a ransom note informing the user and demanding a payment in bitcoin. It is considered a network worm because it also includes a transport mechanism to automatically spread itself. This transport code scans for vulnerable systems, then uses the EternalBlue exploit to gain access, and the DoublePulsar tool to install and execute a copy of itself.

How it works

A ransomware attack goes through five stages from the time it installs on your computer to the appearance of the ransom warning on your screen.

Crypro-ransomware usually attacks in five stages:

1. **Installation**

   After a victim's computer is infected, the crypto-ransomware installs itself and sets keys in the Windows Registry to start automatically every time your computer boots up.

2. **Contacting headquarters**

   Before crypto-ransomware can attack you, it contacts a server operated by the criminal gang that owns it.

3. **Handshake and keys**

   The ransomware client and server identify each other through a carefully arranged "handshake," and the server generates two cryptographic keys. One key is kept on your computer, the second key is stored securely on the criminals' server.

4. **Encryption**

   With the cryptographic keys established, the ransomware on your computer starts encrypting every file it finds with any of dozens of common file extensions, from Microsoft Office documents to .JPG images and more.

5. **Extortion**

   The ransomware displays a screen giving you a time limit to pay up before the criminals destroy the key to decrypt your files. The typical price, $300 to $500, must be paid in untraceable bitcoins or other electronic payments.

Department of Education website hacked

Andy Walker 29 Jun 2017

How was Department of Education attacked?

These are some of the possible ways the department of education was attacked through ransomware. These could be the vulnerabilities:

- No firewall or misconfigured firewall rules.
- No endpoint protection in place or outdated signatures.
- No anti-spam protection in place for emails and attachments.
- No sandbox or containment technology for emails originating outside the trusted domain.
- Internal policies to regulate the use of technology within the work area.
- Advanced malware protection with updated malware signatures.
- Lack of education or proper training to information handling and technology use.
- No honeypots in place to block network calls of the ransomware to its headquarters.
- Use of unregistered devices on the network – jailbroken, rooted devices etc.
- Use of external hardware such as USB sticks for movies and music downloads etc.

People's susceptibilities to manipulation and influence are the biggest security risks to businesses.

Staying safe from Ransomware attacks

- Restrict write permissions on file servers as much as possible.
- Educate users to contact IT if they encounter suspicious pop-ups.
- Use advanced endpoint protection that can identify new malware variants and detect malicious traffic.
- Make time for regular offline backups; test backups to ensure they can be restored from reliably.
- Use web and email protection to block access to malicious websites and scan all downloads.
- Disconnect from networks immediately if you suspect infection.

Ransomware protection, prevention, and mitigation

- If you suspect you've been compromised by ransomware, you can remove the malware using some free decryption tools available online. Sadly, there's not much you can do to get your files back except to pay the ransom because the encryption is too strong to crack.
- Paying the ransom isn't the best idea because there's no guarantee the criminals won't up the ante, or that they'll actually follow through on their promise to send you the keys to decrypt your files. And paying the ransom also supports a cybercriminal enterprise that will ensnare more victims.
- But it's easy to understand why so many people do pay the ransom, especially if you've lost invaluable corporate or personal data.
- The best defence is a proactive one: always back up all your files, and use anti-malware to protect your devices and anti-spam protections for email.

The reasons why you need a security expert

- Continuous advanced network threats are discovered and analysed rapidly.
- Experts with advanced technology and tools triage the domain to quickly identify the specific damage caused by the attacker and document it.
- Memory is imaged and subject to both static and dynamic analysis to clearly identify threats and the damage they caused.
- Logs are expertly analysed to better document a suspect attack, the staging points it utilised, and the timeline of execution.
- Innove Networks bring important analysis and conclusions to focus quickly and at efficient costs.

ABOUT DAMIAN MICHAEL

Damian Michael is the founder & MD at iNNOVO Networks. Nominated for the second time in this year's Entrepreneur of the Year Awards, Michael holds a wealth of versatile experience in both the public and the private sector. After completing his apprenticeship in the SA Navy as a radio/radar technician, he worked in sales and senior management positions for ICT operators like Vodacom and MTN, and was involved in successfully launching Neotel in South Africa.

- #BizTrends2018: Make sure you're at the heart of disruption - 8 Jan 2018
- Global companies attacked, Department of Education hacked, are you armed? - 6 Jul 2017

View my profile and articles...