


**Anatomy of a Ransomware Attack**

Presented by Matt Hooper  
Session #1



Assess | Improve | Manage  
Information Technology

---

---

---

---


---

---

---

---

**Grand Prize**



Don't forget to fill out your card!



Assess | Improve | Manage  
Information Technology

---

---

---

---

---


---

---

---

**Overview**

Ransomware attacks are unfortunately common.  
Learn what they are, how to avoid an attack and what to do if your city is targeted.



Assess | Improve | Manage  
Information Technology

---

---

---

---

---

---

---

---

### Security Breach Statistics

- The government vertical in the US has become the largest group to suffer loss due to data breaches
- On average, 57 confidential records are lost every second ...that's 4,924,800 records per day
- Almost 1.5 billion were lost in the month of March 2018
- The average cost for organizations reporting data breaches was \$3.62 million dollars per breach
- Security experts believe the majority of data breaches are either undetected or unreported!

4

Assess | Improve | Manage  
Information Technology

---

---

---

---

---

---

---

---

---

---

### What is Ransomware?

Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as Ukash and cryptocurrency are used for the ransoms, making tracing and prosecuting the perpetrators difficult. Ransomware attacks are typically carried out using a Trojan that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the "WannaCry worm", traveled automatically between computers without user interaction.

\*As Defined by Wikipedia

5

Assess | Improve | Manage  
Information Technology

---

---

---

---

---

---

---

---

---

---

### How does Ransomware work? Really?

System is compromised by malware or virus

Malware encrypts your data with a key

Your data is no longer useable

You can opt to pay a ransom to obtain the key

You can then decrypt the data

You can now use your data

6

Assess | Improve | Manage  
Information Technology

---

---

---

---

---

---

---

---


---

---

### Steps of a Ransomware Attack

The concept of file encrypting ransomware was invented and implemented by Young and Yung at Columbia University and was presented at the 1996 IEEE Security & Privacy conference. It is called *cryptoviral extortion* and it was inspired by the fictional facehugger in the movie *Alien*.<sup>[11]</sup> Cryptoviral extortion is the following three-round protocol carried out between the attacker and the victim.

1. [attacker→victim] Attacker generates a key pair. Places public key in the malware. The malware is released to victim's system.
2. [victim→attacker] Malware encrypts the victim's files with a third key. The third key is encrypted with the public key so the attacker can retrieve it later. Victim is shown a message that includes the encrypted third key and how to pay the ransom. The victim sends the encrypted third key and e-money to the attacker.
3. [attacker→victim] Attacker receives the payment, deciphers the third key, and sends the it to the victim. The victim deciphers their encrypted files with the purchased key thereby completing the cryptovirology attack.



Assess | Improve | Manage  
Information Technology

---

---

---

---

---

---


---

---

---


---

### Attacker generates a key pair



ATTACKER

VICTIM



Assess | Improve | Manage  
Information Technology

---

---

---

---

---

---


---

---

---


---

### Public key is placed into the malware/virus. The malware is run on victim's system.



ATTACKER

VICTIM



Assess | Improve | Manage  
Information Technology

---

---

---

---

---

---

---

---

---

---

### Malware locks the victim's files with a user-specific third key

The diagram shows an 'ATTACKER' on the left holding a blue key. A dashed arrow points from the attacker to a 'VICTIM' on the right. The victim is shown with a laptop and a padlock, and a red gear icon indicates a process. A blue box highlights a key being generated or used to lock the files.

10

Assess | Improve | Manage  
Information Technology

---

---

---

---

---

---

---

---

### Victim is shown a message that includes the locked third key and how to pay the ransom.

The diagram shows the 'ATTACKER' on the left. A speech bubble from the attacker to the 'VICTIM' on the right contains the text 'Pay Us \$\$\$!' and 'CODE: [key icon]'. The victim is shown with a padlock and a red gear icon.

11

Assess | Improve | Manage  
Information Technology

---

---

---

---

---

---

---

---

### Victim sends the locked third key and payment to the attacker.

The diagram shows the 'VICTIM' on the right sending a blue key and a Bitcoin icon to the 'ATTACKER' on the left. A dashed arrow points from the victim to the attacker. A speech bubble from the attacker to the victim contains the text 'Pay Us \$\$\$!' and 'CODE: [key icon]'.

12

Assess | Improve | Manage  
Information Technology

---

---

---

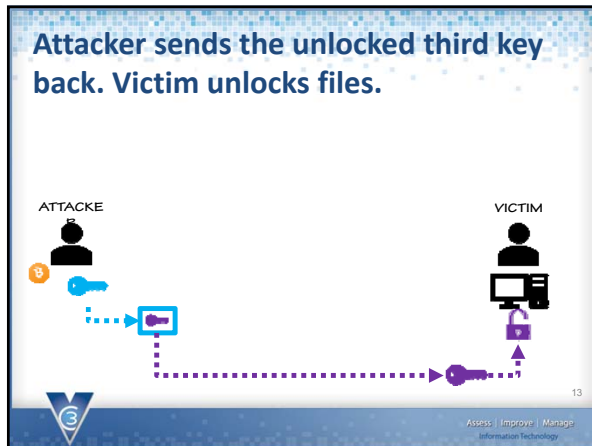
---

---

---

---

---



---

---

---

---

---

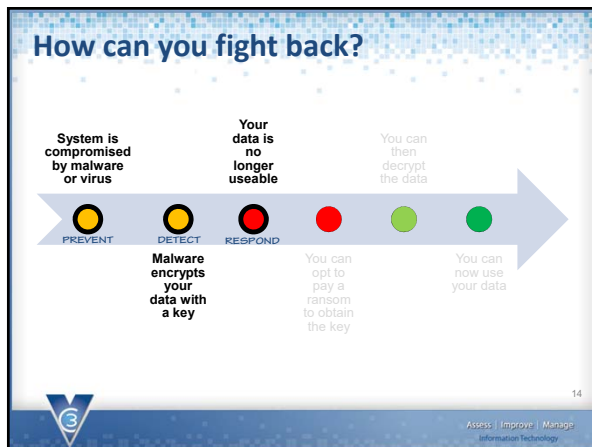
---

---

---

---

---



---

---

---

---

---

---

---

---

---

---

- ### Why are attacks successful?
- Inability to detect rogue systems
  - Anti-Virus Software updates are not automated
  - Anti-Malware lacking or not in place
  - Users running with admin privileges
  - **Lack of Security Awareness Training**
  - Lack of Backup retentions
  - Backups exposed to Production Network
  - Failure to perform periodic audits to ensure all systems are being backed up.
  - Independent validation of security status
- A small '15' is in the bottom right corner of the slide.

---

---

---

---

---

---

---

---

---

---

**Thank You!**  
**For more information contact  
Matt Hooper or Lynn Kenyon.**

[matt.hooper@vc3.com](mailto:matt.hooper@vc3.com)  
[lynn.kenyon@vc3.com](mailto:lynn.kenyon@vc3.com)  
803-753-5441



16  
Assess | Improve | Manage  
Information Technology

---

---

---

---

---

---

---

---

**Don't forget your card!**



Suggestions and feedback?  
Visit [www.vc3.com/masc2018](http://www.vc3.com/masc2018)



17  
Assess | Improve | Manage  
Information Technology

---

---

---

---

---

---

---

---