KASPERSKY lab

RANSOMWARE OVERVIEW

Global B2B Product Marketing Team

- What is ransomware
- Why it’s bad
- Can an AV detect it?
- Why it’s even worse
- What to do
  - Preventive
  - Reactive
- More info

WHAT IS RANSOMWARE?

- Malware
- Keeps your data hostage
- Wants you money
- May kill the hostage even if money is paid

CRYPTOLOCKER

- Installed by an (unaware) user
- Silently encrypts your data
  - You will never notice that
- Data can only be decrypted with a key stored on attacker's server
  - Key is unique for each case
- Victim is asked to pay
- There's a countdown (about 3 days) after that the key will be destroyed
- It's considered to be impossible to decrypt without the key
- It's impossible to recover data even with special tools

Cryptolocker Wants Your Money! (by Costin Raiu)
http://www.securelist.com/en/blog/208214109/Cryptolocker_Wants_Your_Money

HOW WE DETECT - VERDICTS

The most widespread variants of the Cryptolocker malware are detected by Kaspersky products with the following verdicts:

Trojan-Ransom.Win32.Blocker.cfkz, Trojan-Ransom.Win32.Blocker.cmkv, Trojan-Ransom.Win32.Blocker.cggx, Trojan-Ransom.Win32.Blocker.cfow, Trojan-Ransom.Win32.Blocker.cjzj, Trojan-Ransom.Win32.Blocker.cgmz, Trojan-Ransom.Win32.Blocker.cguo, Trojan-Ransom.Win32.Blocker.cfwh, Trojan-Ransom.Win32.Blocker.cllo, Trojan-Ransom.Win32.Blocker.coew

HOW WE DETECT - VERDICTS

The most widespread variants of the Cryptolocker malware are detected by Kaspersky products with the following verdicts:

Trojan-Ransom.Win32.Blocker.cfkz, Trojan-Ransom.Win32.Blocker.cmkv, Trojan-Ransom.Win32.Blocker.cggx, Trojan-Ransom.Win32.Blocker.cfow, Trojan-Ransom.Win32.Blocker.cjzj, Trojan-Ransom.Win32.Blocker.cgmz, Trojan-Ransom.Win32.Blocker.cguo, Trojan-Ransom.Win32.Blocker.cfwh, Trojan-Ransom.Win32.Blocker.cllo, Trojan-Ransom.Win32.Blocker.coew

HOW EASY IS TO CREATE A NEW, UNKNOWN “VARIANT” OF MALWARE?

- If you have a source code – piece of cake

```
#include <stdio.h>

int main()
{
   char Mutation[] = "I'm a bad malware";
   printf(Mutation);
   getchar();
}
```

HASH:
6bdc01ed0316d778ad54955e52f10bf5

```
#include <stdio.h>

int main()
{
   char Mutation[] = "I'm an even worse malware";
   printf(Mutation);
   getchar();
}
```

HASH:
b3e722a971727b244a120e1c2dcde061

WHY IT'S EVEN WORSE?

- Because this type of malware exploits absolutely legitimate behavior!
  - By observing just the encryption process you can not tell the difference between encryption intentionally launched by user and encryption launched by a deceived user
- Users do launch attachments received from unknown sources
- Users do ignore or override security warnings
- Users do set heuristic settings to minimum
- Users do believe signature protection is all they need
- People do pay money to the attackers

HOW TO COUNTER: BEFORE

- Set you security solution settings to maximum (this will allow technologies like heuristic analysis and automatic exploit prevention do their job)
  - Use KSN
- Educate your users:
  - not to open attachments unless they know exactly what the attachment is
  - Read OS and security solution warnings
  - Be (at least a little bit) paranoid
- No network shares! (no mapped/attached drives!)
- Back up religiously – COLD backups only!

HOW TO COUNTER: AFTER

- Do not feed the beast (do not pay)
- Attempt to recover data with help of specialists (key words: shadow copies, back ups)
- Clean the system(s) (*only if you decided to follow the right path - not paying the ransom!*) – the data is gone
- Move on (learn the lesson though)

MORE LINKS FOR SELF-EDUCATION (BECAUSE YOU DO WANT TO KNOW – YOU HAVE A PC AT HOME!)

http://www.securelist.com/en/blog/208214109/Cryptolocker_Wants_Your_Money

http://blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransomware-what-you-need-to-know/

http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

THANK YOU

KASPERSKY lab