
ITU

Ransomware: Incident response best practices

Fyodor Skvortsov, BI.ZONE LLC.

Ransomware landscape

- Popularity and amount of ransomware constantly fluctuate
- In 2018, there are fewer ransomware families, but more variants
- Still popular and profitable for the attackers
- Average cost of ransomware attack is rising!

Attack types

- Mass attacks (indiscriminate mass phishing/malspam)
- More deliberate attacks – brute forcing RDP access or attacking vulnerable routers/network gear (SHODAN scans etc.)
- Targeted (?) attacks – Dridex/Mamba/Carbanak activities

Mass attacks

- Indiscriminate malspam campaigns
- Most common way to spread ransomware
  - Locky, Shade, etc.
- Attachments with MS Office macros/ JavaScript/PowerShell, you name it
- It works!

Targeted attacks

- Targeted ransomware attacks are recent appearance (2016+)
- Dridex (FriedEx), Mamba, PetrWrap
- Deliberately target financial organizations (Mamba) and hospitals (Dridex)
- Cases of attacks on banks by Cobalt/Carbanak where after stealing money attackers deployed PeterWrap ransomware

RDP brute forcing

- Most common way to gain access inside the company's network
- Many small companies outsource their IT infrastructure (Windows Server w/Hyper-V)
- Support staff doesn't care enough about strong passwords

RDP brute forcing (continued)

- Attackers scan the internet for open RDP ports (3389) and attempt to brute force passwords
- GlobeImposter ransomware is the most notorious example
- Ransom amount – usually from 0.2 to 0.5 BTC (~1000 to ~3000 EUR)

RDP brute forcing (continued)

- After getting inside, the attackers scan company's network for critical systems and launch ransomware (usually manually)
- Wiping RDP and other logs in process to make response/investigation more difficult
- After encryption, ransomware usually deletes itself

Special case: Ransomware worms

- And of course there's WannaCry (still lurking on some systems) and NotPetya cases
- Self-spreading ransomware/wipers using unpatched vulnerabilities/credential harvesting
- Worst that can happen to any organization

What can we do?

- Stages of Incident Response:
  - **Preparation** (must have a team/procedures/checklist ready)
  - **Detection and analysis** (is this really an incident? when WannaCry happens, you usually know it right away)
  - **Containment** (prevent further damage/stop malware from spreading)
  - **Eradication** (cleanup malware, roll out backups, restore network connectivity)

The main question

- Can the data be decrypted?
  - Requires detailed malware analysis/reverse engineering
  - In most of the real-world cases, the answer is NO :(
  - Public key cryptography usually makes decryption impossible
  - But you can try as the last resort (if you have a memory dump)

Response, part 1

- Prevention! The most important part.
  - Use antivirus software. Really.
  - In almost all of our cases, victims of ransomware didn't have an AV installed
  - HIPS (Behavioral Detection)
  - Use mail AV if you use your own mail server
  - Use VPN. Do not allow RDP access without VPN
  - Strong passwords are great, so is updating software

Response, part 2: Ransomware is running

- Hibernation/sleep
- Suspending processes/threads
- Prevent processes from exiting
- Dump malware executable to search for the keys
- Dump system RAM as the last resort
- Do not reboot infected system! Disconnect it from the network instead

Response, part 3: Company network

- Isolate infected systems
- Monitor PowerShell/remote service creation
- Do not access users' systems with the domain admin accounts!
- Change privileged users' passwords. Quickly.
- Malware analysis – determine Indicators of Compromise (in-house team or malware analysis services)
- Block running of certain executables based on gathered IoCs

The last resort

- Got encrypted, but have memory dump?
- Could try to extract keys. It could work (Microsoft CryptoAPI likes to cache the encryption keys)
- Pay the ransom? You decide.

Questions?