What WannaCry can cause in ICS infrastructure?

Vyacheslav Kopeytsev
Security Researcher, Kaspersky Lab
The beginning of the story

Client says that:

1. Above 150 computers are affected
2. Corporate and ICS network affected
3. ICS operators stations are unavailable due to frequent BSODs and reboots

Client asked us:

1. What’s happened? What threat or attack was exposed in our equipment?
2. What attack vector was used?
3. What systems were affected?
4. What the damage was done?
Creating an incident response plan

All available evidences like:
1. Hard drives
2. Network traffic
3. Any logs
Any evidences can be important!

Find suspicious data in collected evidences
Understand reasons of BSODs and reboots

1. Find all machines that contain suspicious data
2. Create a timeline of incident
3. Find first infected machine

Collect data → Stop malware propagation → Identify and analyze threat → Find all affected machines → Forensics at first affected system → Mitigation, Reporting

If malware exists in this case
Understand attack vector of first machine

Malware analysis
Forensics
Incident response

Any evidences can be important!
What we should do first?

• Evidences acquisition is a very important stage of an incident response.
• Of course, a customer usually says that his first priority is to stop the active phase of infection.
• But if you cure the systems usually you will destroy the evidences.
• Use tools with logging and backups.
• Log all actions.
Malware files deep analysis

Initial dropper

SMB exploit

Servers

Workstations

Other networks

Encryption

Ransom GUI

Keys

Text of demand

Tor config

Other stuff
DoS by WannaCry
How we can make an incident timeline?

1. Network equipment logs
2. AV product logs
3. Evidences from hard drives (filesystem, registry, etc)

1. No logging on network equipment
2. AV with very old bases
3. Evidences from hard drives (filesystem, registry, etc)
4. Files timestamps are not valid
Another possible ways of infection
Silent infection

Somebody can bring infected device to organization

Infect company network
## Mail dump from Exchange Server

<table>
<thead>
<tr>
<th>FTP Explorer</th>
<th>Epic</th>
<th>Bitcoin Armory</th>
</tr>
</thead>
<tbody>
<tr>
<td>FireFTP</td>
<td>Staff FTP</td>
<td>Bitcoind (Browser)</td>
</tr>
<tr>
<td>FAR Manager</td>
<td>FTPGetter</td>
<td>Pocomail</td>
</tr>
<tr>
<td>Total Commander</td>
<td>ALFTP</td>
<td>IncrediMail</td>
</tr>
<tr>
<td>WS_FTP</td>
<td>Internet Explorer</td>
<td>The Bat!</td>
</tr>
<tr>
<td>CuteFTP</td>
<td>Dreamweaver</td>
<td>Outlook</td>
</tr>
<tr>
<td>FlashFXP</td>
<td>DeluxeFTP</td>
<td>Thunderbird</td>
</tr>
<tr>
<td>FileZilla</td>
<td>Google Chrome</td>
<td>FastTrackFTP</td>
</tr>
<tr>
<td>FTP Commander</td>
<td>Chromium / SRWare Iron</td>
<td>Bitcoin</td>
</tr>
<tr>
<td>BulletProof FTP</td>
<td>ChromePlus</td>
<td>Electrum</td>
</tr>
<tr>
<td>SmartFTP</td>
<td>Bromium (Yandex Chrome)</td>
<td>MultiBit</td>
</tr>
<tr>
<td>TurboFTP</td>
<td>Nichrome</td>
<td>FTP Disk</td>
</tr>
<tr>
<td>FFFTP</td>
<td>Comodo Dragon</td>
<td>Litecoin</td>
</tr>
<tr>
<td>CoffeeCup FTP / Sitemap</td>
<td>RockMelt</td>
<td>Namecoin</td>
</tr>
<tr>
<td>CoreFTP</td>
<td>K-Meleon</td>
<td>Terracoin</td>
</tr>
<tr>
<td>32bit FTP</td>
<td>Putty</td>
<td>BBQcoin</td>
</tr>
</tbody>
</table>
Work on mistakes and mitigation

1. Cure machines
2. Install modern AV products with centralized control and updates to all workstations
3. Install specialized security solutions for ICS (for example KICS)
4. Change network configuration
5. Change software policy
6. Enable logging for all servers, PLC, network devices, security products (if possible)
7. Work with employees
8. Trainings, audits etc.
LET’S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com