THE RISE OF RANSOMWARE

JON STERNSTEIN – STERN SECURITY
JOHN MASER – FBI
PETER NELSON - WAKEMED
INTRODUCTIONS

Jon Sternstein

• Founder & Principal Consultant at Stern Security
• Former Healthcare Data Security Manager
• Co-chair of NCHICA Technology Workgroup
• SANS Institute – Mentor
  – SANS 560: Network Penetration Testing and Ethical Hacking
INTRODUCTIONS

John Maser

• Special Agent FBI – Charlotte Division/Raleigh RA
• Cyber Squad
INTRODUCTIONS

Peter Nelson

• WakeMed Information Security Engineer
• Malware Researcher
AGENDA

• Introducing Ransomware
• Media Coverage
• Ransomware $$
• FBI Insights
• Technical analysis
• Preventative Measures
WHAT IS RANSOMWARE?

Malware

- Encrypts personal files on computers & network shares
- Demands $$ to decrypt
RANSOMWARE IN HEALTHCARE

Methodist Hospital (Kentucky)

- Declared State of Emergency
- Shut down all workstations
- Attackers demanded $1600 (4 bitcoins)
- Back to paper for 5 days
Hollywood Presbyterian Medical Center

- Paid $17,000 (40 bitcoins) to regain access
- Systems were down for 10 days
- Back to paper records
- Some patients redirected to other hospitals
Kansas Heart Hospital

- May 2016
- Paid ransom, but didn’t get decryption keys
- Malware authors demanded second payment
- Hospital refused to pay second ransom
RANSOMWARE IN HEALTHCARE

Encrypts and Steals Data

- June 2016
- Crysis Ransomware
- Reportable Breach
Major News Sites Hit with Malicious Advertisements

- March 2016
- Affected sites: MSN, BBC.com, the New York Times, AOL, Newsweek and more.
- Visitors infected with Cryptowall ransomware
- Ransomware spread through malicious advertisements
- Malware authors acquired ad domains after they expired
Ransomware Variant Infects Macs

- Official “Transmission” BitTorrent client infected
- Signed with valid certificate
- Apple revoked certificate

Ransomware Spreads by Adobe 0-day

- April 2016
- Adobe releases out of band patch
FBI – RANSOMWARE VARIANTS

Report all Crypto Variant complaints to the FBI via www.ic3.gov
FBI FLASH, PINS, PRIVATE SECTOR OUTREACH

• Provide known intelligence on ongoing threat (i.e. indicators, IPs, malware, etc)
TECHNICAL ANALYSIS

Infection start to finish

Delivery ➔ Execution ➔ Ransom ➔ Payment ➔ Decryption

• How does the malware arrive?
• What happens when it runs?
• How is the ransom requested?
• How do I pay the ransom?
• How do I get my data back?
DELIVERY

Most common is email
* Word Document - .doc
* Zip file containing Javascript file - .js
* Windows Script File - .wsf
* Portable Document Format - .pdf

Emerging method is Exploit Kits
* Angler
* Nuclear
Analysis of Word MalDoc

• Typically delivered to the victim under the guise of an invoice.

• When opened the document displays instructions to enable macros.
DELIVERY

What happens next?
Victim complies and enables macros, kicking off the embedded VBA scripts.

- VBA macro creates bat file in %temp%
- Executes %temp%\<filename>.bat
- Bat in turn creates vbs or ps1 in %temp%
- Bat Executes vbs/ps1 using cscript or wscript
- Vbs/ps1 performs a GET request
- The bat file then executes the file saved by the vbs/ps1 script, deletes the vbs/ps1 scripts and deletes itself.
DELIVERY → EXECUTION

Exe is now on the computer and running
• Contacts Command and Control (CnC) Server using either hardcoded IP address or a Domain Generation Algorithm (DGA).
EXECUTION

• Data sent to CnC varies between ransomware families. This data is used to customize the user experience (ransom note), encryption keys and ransom amount.

• Now that the ransomware has communicated with the CnC server and it has what it needs, it begins its malicious behavior.
  – Deletes Volume Shadow copies
  – Add startup registry keys
  – Output instructions .txt/.bmp
  – Encrypt Files
EXECUTION → RANSOM

!!! IMPORTANT INFORMATION !!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers. More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server. To receive your private key follow one of the links:
1. http://twbers4hmi6dx65f.tor2web.org/FED693E7D57FD68E
2. http://twbers4hmi6dx65f.onion.to/FED693E7D57FD68E
3. http://twbers4hmi6dx65f.onion.cab/FED693E7D57FD68E

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: twbers4hmi6dx65f.onion/FED693E7D57FD68E
4. Follow the instructions on the site.

!!! Your personal identification ID: FED693E7D57FD68E !!!
Early ransomware would request a $0.5 – 2 Bitcoin, ~$200-$800.

Newer versions, you must visit the page to get the amount.

I believe they are correlating the data reported back by the executable to determine the victim’s value.

Before you move on to payment you will want to determine the ransomware family.

There is a chance there is a free decryptor already available.

There is always a chance you may not be given the decryptor.
• The site will provide a bitcoin wallet address to send the payment to.

• If you don’t already have Bitcoins, there are services such as Coinbase that provide a way to purchase and send them.
• Once payment is made and verified, the bad actors provide a decryption process (hopefully).
• This could be a key and exe or more recently a pre-packaged point and click exe.
• This decryption process will only work on the computer infected computer. If there are multiple infected machines, ransom will need to be paid for each.
Not all ransomware is created equally.

- Chimera - Threatens to release documents to the internet.
- Ransom32 - Written in Javascript and is sold as Ransomware-as-a-Service (RaaS)
- Samas - Offers bulk decryption prices.
- Cerber - Only targets victims that are not in specified countries. It also talks to you, the ransom text is converted into an audio message and played back.
Implement Security Best Practices

• Nothing new here – same practices apply to ransomware
• SANS 20 Critical Security Controls
  https://www.sans.org/critical-security-controls
SOLUTIONS

⭐ Application Whitelisting ⭐
- Endpoint protection
- Can completely prevent ransomware
- Only allow known good applications

Antivirus
- Endpoint protection
- Won’t prevent, but helps
SOLUTIONS

Backup Important Files

• Help with speedy recovery
• Must test data recovery
• HIPAA requirement
  – Data backup plan (R) § 164.308(a)(7)(ii)(A)
  – Data backup and storage (A) § 164.310(d)(2)(iv)
SOLUTIONS

Email Filtering
• Spam control
• Virus scanning
• Block suspicious attachments: .exe, .jar, .scr, .bat, .aru, .cmd, .vbs, .7z, .ex, .ex_, .ex1, .pif, .application, .gadget, .com, .hta, .cpl, .msc, .vb, .vbe, .js, .jse, .ws, .wsf, .wsc, .wsh, .ps1, .ps1xml, .ps2, .ps2xml, .psc1, .psc2, .scf, .lnk, .inf, .reg, .docm, .dotm, .x1sm, .x1tm, .x1lam, .pptm, .potm, .ppam, .ppsm, .s1dm, .msi, .msp, .mst

Computer Software
• Remove unneeded software
• Patch software
SOLUTIONS

Network Filtering
• Web Filtering
• Egress Filtering

User Profile Protection
Block/Whitelist Office Macros
Network Share Permissions
Intrusion Prevention Systems
Network Segmentation
Vaccines

Details: https://sternsecurity.com/blog/ransomware-prevention-tips
The Ransomware Master List

- Contains a list of known variants
- Lists ways to decrypt files (if available)
- [https://goo.gl/VnAjsn](https://goo.gl/VnAjsn)

<table>
<thead>
<tr>
<th>Name</th>
<th>Extensions</th>
<th>Extension Pattern</th>
<th>Comment</th>
<th>Encryption Algorithm</th>
<th>Also known as</th>
<th>Decryptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>.CryptoHasYou.777</td>
<td>.enc</td>
<td></td>
<td></td>
<td>AES(256)</td>
<td></td>
<td><a href="https://decrypter.ermis">https://decrypter.ermis</a></td>
</tr>
<tr>
<td>7ev3n</td>
<td>.R4A .R5A</td>
<td></td>
<td></td>
<td>XOR</td>
<td>7ev3n-HONE$T</td>
<td><a href="https://github.com/has">https://github.com/has</a></td>
</tr>
<tr>
<td>Block8</td>
<td>.Block8</td>
<td></td>
<td>Based on HiddenTear</td>
<td>AES (256)</td>
<td></td>
<td><a href="http://www.bleepingco">http://www.bleepingco</a></td>
</tr>
<tr>
<td>Alpha Ransomware</td>
<td>.encrypt</td>
<td></td>
<td></td>
<td>AES(256)</td>
<td>AlphaLocker</td>
<td><a href="http://download.bleepi">http://download.bleepi</a></td>
</tr>
<tr>
<td>AutoLocky</td>
<td>.locky</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="https://decrypter.ermis">https://decrypter.ermis</a></td>
</tr>
<tr>
<td>BadBlock</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
REFERENCES

• Methodist Hospital Declares State of Emergency

• Hollywood Presbyterian Medical Center pays ransom
  http://www.theregister.co.uk/2016/02/18/la_hospital_bitcoins/
  http://arstechnica.com/security/2016/02/hospital-pays-17k-for-ransomware-crypto-key/

• Kansas Heart Hospital asked to pay two ransoms

• Malicious Advertisements on major news sites


• Ransomware Master List
  https://docs.google.com/spreadsheets/d/1TWS238xacAtolfKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml#

• Ransomware Prevention Tips
  https://sternsecurity.com/blog/ransomware-prevention-tips

• The Complete Ransomware Guide
  https://blog.varonis.com/the-complete-ransomware-guide