Blocking Ransomware: Real World Example with a Locky Domain

ISSA – SLC Chapter, Fall Seminar

Jordan Gackowski
Consulting Systems Engineer
September 22nd 2016
What is OpenDNS?

DNS Services Built for World’s Largest Security Platform

GLOBAL NETWORK

• 80B+ DNS requests/day
• 65M+ biz & home users
• 25 Data Centers
• 100% uptime
• Any port, protocol, app

UNIQUE ANALYTICS

• security research team
• automated classification
• BGP peer relationships
• 3D visualization engine

= 80M+
malicious requests blocked/day
DNS is Used by Every Device on Your Network

ANY OWNER
network’s DHCP tells every connected device where to point DNS

ANY TOPOLOGY
no matter how your LAN or WAN is set up, it simply works

ANY OPERATING SYSTEM
Win, Mac, iOS, Android, Linux, custom app servers, and even IoT
Leveraging a Single Global Recursive DNS Service

**BENEFITS**
- Global Internet Activity Visibility
- Network Security w/o Adding Latency
- Consistent Policy Enforcement
- Internet-Wide Cloud App Visibility

Who Resolves Your DNS Requests?
- Authoritative DNS for Intranet Domains
- Recursive DNS for Internet Domains

Leveraging a Single Global Recursive DNS Service

- Home Users
- Mobile Devices
- Roaming Laptops
- Remote Sites
- Enterprise Location A
  - Internal InfoBlox Appliance
- Enterprise Location B
  - Internal Windows DNS Server
- Enterprise Location C
  - Internal BIND Server

ISP 1
ISP 2
ISP 3

ISP ?
ISP ?
ISP ?

mobile carrier
Predictive Detectors Used by OpenDNS

- SecureRank
- Co-Occurrences
- NLPRank
- DGA Detectors
- Traffic Spike Detectors
- IP Space Monitoring
Typical Ransomware Infection

- Infection Vector
- C2 Comms & Asymmetric Key Exchange
- Encryption of Files
- Request of Ransom
Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently encrypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.
# Most Ransomware Relies on C2 Callbacks

<table>
<thead>
<tr>
<th>NAME</th>
<th>DNS</th>
<th>IP</th>
<th>NO C2</th>
<th>TOR</th>
<th>PAYMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locky</td>
<td>✤</td>
<td>✤</td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>SamSam</td>
<td></td>
<td></td>
<td></td>
<td>✤</td>
<td>DNS (TOR)</td>
</tr>
<tr>
<td>TeslaCrypt</td>
<td>✤</td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>CryptoWall</td>
<td>✤</td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>TorrentLocker</td>
<td>✤</td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>PadCrypt</td>
<td>✤</td>
<td></td>
<td></td>
<td></td>
<td>DNS (TOR)</td>
</tr>
<tr>
<td>CTB-Locker</td>
<td>✤</td>
<td></td>
<td></td>
<td>✤</td>
<td>DNS</td>
</tr>
<tr>
<td>FAKBEN</td>
<td>✤</td>
<td></td>
<td></td>
<td></td>
<td>DNS (TOR)</td>
</tr>
<tr>
<td>PayCrypt</td>
<td>✤</td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>KeyRanger</td>
<td>✤</td>
<td></td>
<td></td>
<td>✤</td>
<td>DNS</td>
</tr>
</tbody>
</table>
Feeling Locky?

- Encrypts & renames the infected device’s important files with .locky extension
- Appx 90,000 victims per day [1]
- Ransom ranges from 0.5 – 1.0 BTC (1 BTC ~ 799 USD)

[1] Forbes Ransomware Crisis
Blocking Ransomware: Real World Example with a Locky Domain
dqtfhkgskushlum[.]org (detection date: March 15th 2016)

DETAILS FOR DQTFHKGSKUSHLUM.ORG

This domain is currently in the OpenDNS Security Labs block list.

This domain is associated with the following attack: Locky Ransomware

DOMAIN TAGGING

<table>
<thead>
<tr>
<th>Period</th>
<th>Category</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 27, 2016 - Current</td>
<td>Malware</td>
<td></td>
</tr>
<tr>
<td>May 15, 2016 - Current</td>
<td>Malware</td>
<td></td>
</tr>
</tbody>
</table>
What do we know about this domain?

dqtfhkgskushlum.org

CO-OCCURRENCES

dwytrqgblrynsgtew.org (51.61) 6dtxgqam4crv6rr6.onion.cab (13.43) 25z5g623wpqpdwis.onion.to (11.47) cwprfpjtmjb.biz (9.56) 32kl2rswjvcjeui7.onion.to (7.73) i3ezlvkoj7fwood.onion.to (6.79)

CO-OCCURRENCES

6dtxgqam4crv6rr6.onion.cab (26.55) 25z5g623wpqpdwis.onion.to (24.64) cwprfpjtmjb.biz (18.81) 32kl2rswjvcjeui7.onion.to (15.25) i3ezlvkoj7fwood.onion.to (14.74)
Locky – Blocking a Ransomware Domain

Original Domain and malware URL.

Known Malware Hashes hosted on that domain.

Shared IP Address Space.

TOR Hosted Domains

Co-Occuring Domains
Locky – Blocking a Ransomware Domain

Initial Domain and Related Infrastructure Points – one TOR and one Unleaded.

Domains with high rate of Co-occurrence.

TOR Based Domain Hosting Separate Cluster of Malware Hashes. Multiple sites to direct the victim to the malware.
As you may see from the tags, the protection is enforced across all Cisco products.
Discover the Threats Before They Happen

VT Link: https://www.virustotal.com/en/file/4f7bbe0037f4faf2eaa5b08821c7bb22da0b0634f1cc82594b88a5a96fc05f96/analysis/
(first analysis: 5-28-2016, 10 days after first sample hit ThreatGrid, see previous slide)
#DemoTime!