Presenters

• Majed Oweis: CISCIP Analyst, US-CERT
• Srujan Kotikela: Senior Threat Scientist, Armor
• Ed Cabrera: V.P. Cybersecurity Strategy, Trend Micro
• Luis Mendieta: Sr. Threat Researcher, ThreatStream
• Dennis Palmer: Senior Security Analyst, HITRUST
NCCIC/US-CERT
TLP: GREEN – Locky Ransomware

Highlight of an advisory on the Locky Ransomware received from one (1) US-CERT coordinating partner:

Observations made in the report on Locky:

- First identified around 16 FEB 2106 by Palo Alto Networks, who reported over 400,000 cases of ransomware delivered to multiple sectors. Capable of spreading via network shares.
- Ransom observed to be charged is 1 BTC (approximately 415 USD).
- Delivered by spam email.
- Ransomware contains weaponized MS Office documents. Tactic associated with Dridex, Dyre, and Pony trojans.
- Identified as a macro belonging to the W97M.dropper family.
- Designed to delete the Volume Shadow Copy Service (VSS).
- Able to encrypt multiple systems, including unmapped shares.
- Sign of infection is that the victim system's desktop background turns black, with a message in red saying their files have been encrypted.
- Creates C2 domains on specific times and dates using a domain generation algorithm (DGA). The DGA has reportedly been reversed engineered, and been made available in open source. The expectation is that the DGA will be undergoing a recode.
- The advisory includes further analysis and a mitigation strategy. CISCP is arranging to make the advisory available in the CISCP compartment of the US-CERT portal.
TLP: GREEN – Locky Ransomware

Answers to Questions from the Call:

• Question one (1): Is there any evidence that the Locky ransomware is designed to not run on systems with Russian keyboard support, as has been seen in other recent ransomware?
  – Answer: The question has been submitted to our POCs in US-CERT, follow-up pending. Avast, in their blog post, "A Closer Look at the Locky Ransomware", 10MAR2016 (https://blog.malwarebytes.org/intelligence/2016/03/look-into-locky/) included the section "Exclusion of Russian PCs": "The newer version of the malware contains a new hard-coded config value to disable Locky’s encryption on PCs whose locale is set to Russia or whose language is set to Russian (0x19). The hard-coded config value also determines how long Locky should remain dormant after its execution to avoid sandbox detections."

• Question two (2): Is there evidence of a delayed ransom request to allow time for encryption of full-cycle backups?
  – Answer: We’ve not seen any indication that Locky delays its ransom request to wait for the completion of a backup process on a victim system.

US-CERT Resources:

• TLP: AMBER FOOU - IB-16-20079 – Indicators of Compromise Associated with Locky Ransomware

• TLP: GREEN – Malware Initial Findings Report (MIFR) – 10054561 - Cryptolocker ‘Locky’ Downloader
  – https://portal.us-cert.gov/documents/70338/108826/MIFR-10054561/59d0c6a7-bae1-4499-9ebc-2704c4bf87f2
Questions? Comments?

Contact US-CERT at:
• Email: soc@us-cert.gov
• Phone: 1-888-282-0870
• Website: www.us-cert.gov

Contact CISCP at: CISCP@us-cert.gov
ARMOR: TOP THREAT ACTORS AND COMMAND AND CONTROL ACTIVITY
## Top Vulnerability Exploits for the last 30 days

<table>
<thead>
<tr>
<th>NAME</th>
<th>HITS</th>
<th>RELATED TECHS/MALWARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2016-0800 (DROWN)</td>
<td>225</td>
<td>OpenSSL, SSL, TLS, Home Depot, ZTE Corp.</td>
</tr>
<tr>
<td>CVE-2016-1010</td>
<td>146</td>
<td>Adobe, Kaspersky Lab, Adobe Flash Player, Linux, Microsoft</td>
</tr>
<tr>
<td>APSB16-08</td>
<td>53</td>
<td>Adobe, Adobe Flash Player, Kaspersky Lab, Security Bulletin, Microsoft Windows</td>
</tr>
<tr>
<td>CVE-2014-0160 (Heartbleed)</td>
<td>37</td>
<td>OpenSSL, Yahoo, Google, Encryption, SSL</td>
</tr>
<tr>
<td>CVE-2013-5838</td>
<td>35</td>
<td>Oracle Corp, Security Explorations, CPUs, Linux, Security Fix</td>
</tr>
<tr>
<td>MS16-036</td>
<td>20</td>
<td>Adobe, Adobe Flash Player, Microsoft Windows, Microsoft, MSB</td>
</tr>
<tr>
<td>CVE-2014-6271 (Shellshock)</td>
<td>19</td>
<td>Bash, Yahoo, Linux, Mac OS X, Apple</td>
</tr>
<tr>
<td>CVE-2016-1562</td>
<td>19</td>
<td>@DTE_Energy, Android, CWE</td>
</tr>
<tr>
<td>Stagefright Vulnerability</td>
<td>13</td>
<td>Android, Google, Smartphone, Zimperium, T-Mobile</td>
</tr>
<tr>
<td>CVE-2016-0996</td>
<td>12</td>
<td>Adobe, Adobe Flash Player, código arbitrario</td>
</tr>
<tr>
<td>CVE-2015-7547 (glibc)</td>
<td>12</td>
<td>glibc, Domain Name System, Linux, Google, RCE</td>
</tr>
<tr>
<td>CVE-2016-1001</td>
<td>11</td>
<td>Adobe, Adobe Flash Player, código arbitrario</td>
</tr>
<tr>
<td>CVE-2016-0995</td>
<td>11</td>
<td>Adobe, Adobe Flash Player, código arbitrario</td>
</tr>
<tr>
<td>CVE-2016-0994</td>
<td>11</td>
<td>Adobe, Adobe Flash Player, código arbitrario</td>
</tr>
<tr>
<td>CVE-2016-1000</td>
<td>11</td>
<td>Adobe, Adobe Flash Player, código arbitrario</td>
</tr>
<tr>
<td>MS16-027</td>
<td>11</td>
<td>Microsoft Windows, Windows Media Player, Windows 8, Windows 7</td>
</tr>
<tr>
<td>MS16-035</td>
<td>11</td>
<td>Microsoft, Microsoft Windows, Windows 8, Windows 10, XML</td>
</tr>
<tr>
<td>CVE-2016-0992</td>
<td>11</td>
<td>Adobe, Adobe Flash Player, código arbitrario</td>
</tr>
</tbody>
</table>

**Action Item:**

- Ensure your environments are scanned for vulnerabilities
- Evaluate the risk factors of your devices on a regular basis
## Top Emerging Malware Entities

<table>
<thead>
<tr>
<th>NAME</th>
<th>HITS</th>
<th>RELATED TECHS/MALWARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>KeRanger</td>
<td>6043</td>
<td>Mac OS X, Apple, Linux.Encoder.1, Bitcoin, Transmission</td>
</tr>
<tr>
<td>PowerSniff</td>
<td>69</td>
<td>OTX, Palo Alto Networks</td>
</tr>
<tr>
<td>BadMirror</td>
<td>25</td>
<td>Android</td>
</tr>
<tr>
<td>Aadhar</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Gorpro</td>
<td>10</td>
<td>Rootnik, Ztorg</td>
</tr>
<tr>
<td>Credential Stuffing</td>
<td>9</td>
<td>Sentry MBA</td>
</tr>
<tr>
<td>Lunacy</td>
<td>6</td>
<td>BMW AG</td>
</tr>
<tr>
<td>Swabfex</td>
<td>4</td>
<td>Microsoft Windows, Computers</td>
</tr>
<tr>
<td>UltraMon</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Nebula</td>
<td>3</td>
<td>Netflix</td>
</tr>
<tr>
<td>Banloader</td>
<td>3</td>
<td>Microsoft Windows, Mac OS X, Linux, Kaspersky Lab, Mobile Devices</td>
</tr>
<tr>
<td>Cruzbot</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>android[.]ndk</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>android[.]buildTypes</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Log Spoofing</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

**Action Item:**

- Ensure your devices are not susceptible to commonly used malware
- Have your security teams increase awareness of your employees on high hit malware
# Top Corporate Targets

<table>
<thead>
<tr>
<th>NAME</th>
<th>HITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Bank of Bangladesh</td>
<td>493</td>
</tr>
<tr>
<td>New York Fed</td>
<td>253</td>
</tr>
<tr>
<td>Ku Klux Klan</td>
<td>177</td>
</tr>
<tr>
<td>Islamic State in Iraq and the Levant</td>
<td>148</td>
</tr>
<tr>
<td>Ofcom</td>
<td>135</td>
</tr>
<tr>
<td>Staminus Communications</td>
<td>42</td>
</tr>
<tr>
<td>Starwood Hotels &amp; Resorts Worldwide, Inc.</td>
<td>35</td>
</tr>
<tr>
<td>Hollywood Presbyterian Medical Center</td>
<td>32</td>
</tr>
<tr>
<td>Apple</td>
<td>30</td>
</tr>
<tr>
<td>U.S. Federal Reserve System</td>
<td>30</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAME</th>
<th>HITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twitter</td>
<td>14</td>
</tr>
<tr>
<td>AOL Ad-Network</td>
<td>13</td>
</tr>
<tr>
<td>Bank of Uganda</td>
<td>13</td>
</tr>
<tr>
<td>Thales SA</td>
<td>12</td>
</tr>
<tr>
<td>Clark County Water Reclamation District</td>
<td>12</td>
</tr>
<tr>
<td>Sony Corp</td>
<td>12</td>
</tr>
<tr>
<td>Seniat</td>
<td>10</td>
</tr>
<tr>
<td>Federal Bureau of Investigation</td>
<td>9</td>
</tr>
<tr>
<td>Spotify</td>
<td>8</td>
</tr>
<tr>
<td>Anthem</td>
<td>6</td>
</tr>
</tbody>
</table>

**Action Item:**

- Have your threat intel teams monitor your companies, partners and customers risk to ensure your systems are tuned for the latest threats
# Top Suspicious IP Addresses

<table>
<thead>
<tr>
<th>NAME</th>
<th>HITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>188.[118].[2].[26]</td>
<td>25</td>
</tr>
<tr>
<td>118.[170].[130].[207]</td>
<td>23</td>
</tr>
<tr>
<td>46.[109].[168].[179]</td>
<td>22</td>
</tr>
<tr>
<td>81.[183].[56].[217]</td>
<td>22</td>
</tr>
<tr>
<td>183.[60].[48].[25]</td>
<td>8</td>
</tr>
<tr>
<td>114.[44].[192].[128]</td>
<td>8</td>
</tr>
<tr>
<td>184.[154].[89].[128/29]</td>
<td>6</td>
</tr>
<tr>
<td>108.[170].[20].[114]</td>
<td>5</td>
</tr>
<tr>
<td>186.[215].[94].[180]</td>
<td>5</td>
</tr>
<tr>
<td>89.[45].[67].[30/24]</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAME</th>
<th>HITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>212.[83].[136].[137]</td>
<td>5</td>
</tr>
<tr>
<td>185.[117].[73].[30/24]</td>
<td>4</td>
</tr>
<tr>
<td>92.[222].[171].[216]</td>
<td>4</td>
</tr>
<tr>
<td>184.[154].[135].[120/29]</td>
<td>4</td>
</tr>
<tr>
<td>218.[61].[13].[38]</td>
<td>4</td>
</tr>
<tr>
<td>212.[129].[26].[221]</td>
<td>4</td>
</tr>
<tr>
<td>91.[236].[75].[4]</td>
<td>4</td>
</tr>
<tr>
<td>42.[236].[75].[85]</td>
<td>4</td>
</tr>
<tr>
<td>183.[3].[202].[105]</td>
<td>4</td>
</tr>
<tr>
<td>183.[3].[202].[108]</td>
<td>4</td>
</tr>
</tbody>
</table>

**Action Item:**

- Have your defense mechanisms tuned to block out known bad IP’s
Adobe Releases Flash Security Update to Patch Exploited Vulnerability

Adobe has released another update, this time to address 23 reported vulnerabilities in Flash.

- (APSB16-08) Adobe notes that patch addresses critical vulnerabilities which could allow an attack to gain control of an affected system.
- It is noted one of the vulnerabilities (CVE-2016-1010) “is being used in limited, targeted attacks.”
- Users of Adobe Flash Player Desktop Runtime are advised to update to the latest version (21.0.0.182 for Windows and Mac; 11.2.202.577 for Linux).
- Use this link https://www.adobe.com/software/flash/about/?PID=6157437 to check if their software version.
- Flash Player installed in Google Chrome, Microsoft Internet Explorer, and Microsoft Edge, will be updated automatically.

Action Item:
- Verify the version of software running on your systems
- Keep up with vulnerability updates
IBM Flash System cross site request forgery

**Affected:** IBM Flash System V9000 up to 7.4.1.3/7.5.1.2/7.6.0.3

**Published:** 03/12/2016

**Risk:** Problematic

A vulnerability was found in IBM Flash System V9000 up to 7.4.1.3/7.5.1.2/7.6.0.3 and classified as problematic. This issue affects an unknown function. The manipulation with an unknown input leads to a cross site request forgery vulnerability. Impacted is integrity. The summary by CVE is:

Cross-site request forgery (CSRF) vulnerability in IBM Flash System V9000 7.4 before 7.4.1.4, 7.5 before 7.5.1.3, and 7.6 before 7.6.0.4 allows remote attackers to hijack the authentication of arbitrary users for requests that insert XSS sequences.

The identification of this vulnerability is CVE-2015-7446. The exploitation is known to be easy. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation. The technical details are unknown and an exploit is not publicly available. Upgrading to version 7.4.1.4, 7.5.1.3 or 7.6.0.4 eliminates this vulnerability.

**Action Item:**

- Ensure you keep up with software in your environment and upgrade promptly
First OS X ransomware actually a Linux file scrambler

• The world's first fully functional OS X ransomware, KeRanger, is really a Mac version of the Linux Encoder Trojan..

• The infected OS X torrent update carrying KeRanger looks virtually identical to version 4 of the Linux Encoder Trojan that has already infected thousands of Linux servers this year.

• KeRanger spread via an infected version of an otherwise legitimate open source BitTorrent application, Transmission. The tainted version (2.90) was available for download between March 4 and March 5, 2016 and came signed with a legitimate developer certificate.

• Apple's OS X ships with a security feature called Gatekeeper, allowing users to restrict which sources they can install applications from in order to minimize the likelihood of deploying a malicious app. The default setting allows users to install applications from the Mac App Store or applications that are digitally signed by a developer. By using a developer certificate to sign their wares, the crooks behind KeRanger were able to circumvent Apple's GateKeeper control. Apple has since revoked the misused certificate, which was issued to a Turkish firm, so the immediate panic is over.

• Once the infected installer is executed, the Trojan connects to the command and control centers via TOR and retrieves an encryption key. After encryption finishes, the KeRanger ransomware creates a file called README_FOR_DECRYPT.txt, which holds the information on how the victim should pay the ransom. The encryption functions are identical to those deployed by the Linux.
Phishing

Google Security AccountRecovery@google.com

This email is to notify you that your Google account has been disabled due to a possible compromise of your account.

In order to unlock your account, you must initiate a password reset.

To initiate the password reset process to re-activate your Google Account, click the link below: https://www.google.com/settings/recovery

Sincerely,
Goog1e Apps Security
Note: This email address cannot accept replies.

Action Item:
• Ensure your spamming tools are tuned to detect malicious mail
• Educate your employees on cross-verifying mails
TREND MICRO: CERBER: CRYPTO-RANSOMWARE THAT SPEAKS – SOLD IN RUSSIAN UNDERGROUND
CERBER Crypto-Ransomware

“Attention! Attention! Attention!”

“Your documents, photos, databases and other important files have been encrypted!”
CERBER: Sample Ransom Note

Your documents, photos, databases and other important files have been encrypted!

To decrypt your files follow the instructions:

1. Download and install the "Tor Browser" from https://www.torproject.org/
2. Run it
3. In the "Tor Browser" open website:
   http://decrypttoxybarc.onion/BFA2-30EC-FB00-003F-302B
4. Follow the instructions at this website

«...Quod me non necat me fortiorum facit.»
CERBER: Landing Page Asking for Language Preference
CERBER: CERBER config file code primed for customization
CERBER: CERBER config file code primed for customization
Malware Detections
Malicious URLs

- hxxp://d21s1xi1bwlv6y.cloudfront.net/hgstatic/img/favicon2.ico
- hxxp://service.bandoobe.com/ext_login_stats.php
- hxxp://www.adnetworkperformance.com/favicon.ico
- hxxp://ad.directrev.com/favicon.ico
- hxxp://disorderstatus.ru/order.php
- hxxp://differentia.ru/diff.php
- hxxp://dy109hmwzquzs.cloudfront.net/web/css/u_cdn.css?v=1.64
THREATSTREAM: FILE-LESS POWERSHELL MALWARE ALIVE N WELL...
Overview

- **Powershell Malware**: Malicious programs that leverage powershell in order to infect systems. The beauty of this method is the ability to leave little or no trace on the system.

- Recent campaigns are loading payloads into memory, therefore they might be immune to traditional forensic techniques.
Methods of Infection

• Malware delivery is via phishing campaigns. The attackers craft a very believable email that uses full name of target “in this specific campaign C-level execs were being targeted”, phone number and sometimes address were also observed on the lures.

• Subject:
  • {Employee First Name}, Ignoring this account hurts you. Deal with it today {Company}
  • {Employee First Name}, We can help you with your outstanding balance {Company}
  • {Employee First Name}, Let’s work together on this {Company}
  • {Employee First Name}, Disregarding this account hurts you. Deal with it today{Company}
  • From: <various_senders>
  • Attachment name: Collection_Profile_{Employee First Name}_{13 digits}.doc
Sample lure email:

Andrew Warnett
To: [email protected]

Please close this unpaid obligation Ref.0297292

Hi Mr [redacted]

This is a reminder that the [redacted] account with us is listed as unpaid. Our records show that you have a current outstanding balance of $1,964.00. We would greatly appreciate if you could clear this payment this week, kindly see instructions attached.

Regards,

---

Two Men and A Truck | Finance Compliance Department
7739 County Highway 112, Upper Sandusky, OH, 43351
Tel.: 956-781-2401

Communication Ref:03190661357
Payload

• The malware typically comes embedded in a word document in the form of a macro. The macro then executes a hidden powershell call that allows the second stage to be downloaded.

• The second stage is usually downloaded from a compromised site or a rogue github account.
Macro analysis.

tools used to extract the macro: officemalscanner
Second Stage Analysis.

- Initial shellcode is served for win32 and win64 flavors of windows. The check is located on the initial powershell call in an if statement.
- The shellcode decrypts and executes an embedded payload. Once decoded it checks for VM presence by checking the following strings: TEQUILABOOMBOOM, SANDBOX, VIRUS, MALWARE.
Second Stage Analysis

It also checks for certain dll’s related with vm activity.

- sbiedll.dll = Sanboxie
- dbghelp.dll = Vmware
- api_log.dll = Sunbelt
- dir_watch.dll = Sunbelt
- pstorec.dll = Sunbelt
Second Stage Analysis

The malware gathers info such as IP addresses, hostname and checks for artifacts that are related with the following strings:

• Type 1 strings:
  – school, hospital, college, health, nurse

• Type 2 strings:
  – POS, STORE, SHOP, SALE

• Type 3 strings:
  – TEACHER, STUDENT, SCHOOLBOARD, PEDIATRICS, ORTHOPED.

If strings of interests are found a type of “666” is used, else a type of “555” is used. the malware is mainly interested in type 3 strings.
Network Communication

Above is the initial c2 callout some of the parameters are self explanatory like user, id, os, host and type. However the parameter k is used as a decryption seed in the c2 response. It is suspected that the strings are encrypted using x-tea.
Network Communication continued

• When the c2 is available it would return an encrypted dll which in turn it would get executed using rundll32.exe
Powershell Malware Mitigation

- Disable macro execution on Office.
- User education on spearphishing attacks.
- Updated IDS NID signatures.
- Upgrade to powershell 5.0 in order to enable better logging capabilities
Macro Virus Detection.

Yara Rule:

```yara
rule malicious_macro
{
    meta:
        author: "Luis Mendieta Anomali Labs"
    strings:
        $sig = { D0 CF 11 E0 A1 B1 1A E1 }
        $string = "Win32_ProcessStartup" nocase
        $string2 = "ThisDocument"
        $string3 = "winmgmts:\\"
        $string4 = "Download" nocase
        $string5 = "String" nocase
        $string7 = "\root\cimv2:Win32_Process"
    condition:
        $sig at 0 and all of ($string*) and new_file
}
```
Detection

snort Rule:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"powershell macro C2 Callout"; flow:from_client,established; content:"POST"; nocase; fast_pattern; uricontent:"/yuppi/?user="; classtype:trojan-activity;)
```
Thank you!!!! any questions?
CSF Controls Related to Threats

CSF Control for Phishing

• Control Reference: 01.f Password Use
  – Control Text: Users shall be made aware of their responsibilities for maintaining effective access controls and shall be required to follow good security practices in the selection and use of passwords and security of equipment
  – Implementation Requirement: Users are made aware of the organization’s password policies and requirements to keep passwords confidential, select quality passwords, use unique passwords, not provide their password to any one for any reason, and change passwords when there is suspected compromise.
CSF Controls Related to Threats

CSF Control for Suspicious IP Addresses

• Control Reference: 01.i Policy on the Use of Network Services
  - Control Text: Users shall only be provided access to internal and external network services that they have been specifically authorized to use. Authentication and authorization mechanisms shall be applied to users and equipment.
  - Implementation Requirement: The organization shall specify the networks and network services to which users are authorized access.
CSF Controls Related to Threats

CSF Control for malicious code

• Control Reference: 09.j Controls Against Malicious Code
  – **Control Text:** Detection, prevention, and recovery controls shall be implemented to protect against malicious code, and appropriate user awareness procedures on malicious code shall be provided.
  – **Implementation Requirement:** Protection against malicious code shall be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls.
CSF Controls Related to Threats

CSF Control for CERBER (or other) Crypto-Ransomware

• Control Reference: 09.1 Backup
  – Control Text: Back-up copies of information and software shall be taken and tested regularly.
  – Implementation Requirement: Back-up copies of information and software shall be made, and tested at appropriate intervals. Complete restoration procedures shall be defined and documented for each system.
CSF Controls Related to Threats

CSF Control for Cross Site Scripting

• Control Reference: *10.b Input Data Validation

  – Control Text: Data input to applications and databases shall be validated to ensure that this data is correct and appropriate

  – Implementation Requirement: The organization shall develop applications based on secure coding guidelines to prevent common coding vulnerabilities in software development processes including injection flaws (SQL injection), buffer overflow, insecure cryptographic storage, insecure communications, improper error handling, broken authentication, cross-site scripting (XSS), and cross-site request forgery (CSRF).
CSF Controls Related to Threats

CSF Control for Ransomware (unauthorized software)

• Control Reference: *10.h Control of operational software
  – Control Text: There shall be procedures in place to control the installation of software on operational systems
  – Implementation Requirement: The organization shall maintain information systems according to a current baseline configuration and configure system security parameters to prevent misuse.
CSF Controls Related to Threats

CSF Control for Vulnerability Patching

• Control Reference: *10.m Control of technical vulnerabilities
  – **Control Text:** Timely information about technical vulnerabilities of systems being used shall be obtained; the organization's exposure to such vulnerabilities evaluated; and appropriate measures taken to address the associated risk
  – **Implementation Requirement:** Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within Appropriate, timely action shall be taken in response to the identification of potential technical vulnerabilities. Once a potential technical vulnerability has been identified, the organization shall identify the associated risks and the actions to be taken. Such action shall involve patching of vulnerable systems and/or applying other controls.
Visit [www.HITRUSTAlliance.net](http://www.HITRUSTAlliance.net) for more information

To view our latest documents, visit the [Content Spotlight](http://www.HITRUSTAlliance.net)