Monthly Cyber Threat Briefing
February 2016
Presenters

• Majed Oweis: CISCP Analyst, US-CERT
• Srujan Kotikela: Senior Threat Scientist, Armor
• Jon Clay: Sr. Mgr – Global Threat Communications, Trend Micro
• Luis Mendieta: Sr. Threat Researcher, ThreatStream
• Dennis Palmer: Senior Assurance Associate, HITRUST
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-2015-0160</td>
<td>5</td>
<td>Bluetooth, Alphabet Inc., Android, Telephony</td>
</tr>
<tr>
<td>CVE-2014-3566</td>
<td>5</td>
<td>SSL, Google, Encryption, OpenSSL, IBM Corporation</td>
</tr>
<tr>
<td>CVE-2015-067</td>
<td>5</td>
<td>Conficker, Honey pot, Microsoft, DCE/RPC, Connection</td>
</tr>
<tr>
<td>CVE-2015-0311</td>
<td>5</td>
<td>Schneider Electric, IMT25, CVSS v2</td>
</tr>
<tr>
<td>CVE-2015-5655</td>
<td>4</td>
<td>Adobe, Adobe Flash Player, Firefox, Microsoft Word, Microsoft Windows</td>
</tr>
<tr>
<td>CVE-2013-0634</td>
<td>4</td>
<td>Adobe Flash Player, Adobe, Angler Exploit Kit, Nuclear Pack Exploit Kit, Trend Micro</td>
</tr>
<tr>
<td>CVE-2015-7645</td>
<td>4</td>
<td>Adobe Flash Player, Adobe, Flash 15.0.0.242, Microsoft IE, Forbes</td>
</tr>
</tbody>
</table>

## Action Item:

1. Follow-up related vulnerabilities (attack tree)
2. Identify the patch status of your systems
3. Prioritize your remediating efforts
## Top Emerging Malware Entities

<table>
<thead>
<tr>
<th>NAME</th>
<th>HITS</th>
<th>RELATED TECHS/MALWARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cherry Picker</td>
<td>499</td>
<td>Abaddon, Point of Sale, Trustwave, Encryption, Radar</td>
</tr>
<tr>
<td>Bookworm</td>
<td>207</td>
<td>Microsoft, Kaspersky Lab, Palo Alto Networks, Deluxe Corp, PlugX - Korplug - Sogu</td>
</tr>
<tr>
<td>b374k web shell</td>
<td>85</td>
<td>Unix shell, PDO, Perl, Injection, Java</td>
</tr>
<tr>
<td>KillerRat</td>
<td>9</td>
<td>njRAT - Bladabindi</td>
</tr>
<tr>
<td>Candle Jar</td>
<td>9</td>
<td>Positive Energy, ClearBox, Results Hub, Sun Washed Linen, Diluents</td>
</tr>
<tr>
<td>Fastoplayer</td>
<td>5</td>
<td>Microsoft Windows</td>
</tr>
<tr>
<td>BadBarcode</td>
<td>5</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>TinyLoader</td>
<td>4</td>
<td>VAWTRAK, Abaddon, Proofpoint, Fareit, Microsoft Word</td>
</tr>
<tr>
<td>Karrot</td>
<td>4</td>
<td>Mobile Phone, TalkTalk Telecom Group</td>
</tr>
<tr>
<td>GoMovix</td>
<td>4</td>
<td>Microsoft IE, Firefox, Mozilla, Google</td>
</tr>
</tbody>
</table>

**Action Item:**

1. Identify malware entities related to your environment and block
2. Ensure your network sensors are always up-to-date and tuned to detected indicators
## Hacker Activity

<table>
<thead>
<tr>
<th>NAME</th>
<th>HITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous</td>
<td>2794</td>
</tr>
<tr>
<td>CtrlSec</td>
<td>378</td>
</tr>
<tr>
<td>Cyber Caliphate</td>
<td>257</td>
</tr>
<tr>
<td>Lizard Squad</td>
<td>75</td>
</tr>
<tr>
<td>GhostSec</td>
<td>18</td>
</tr>
<tr>
<td>Anonymous Legion</td>
<td>16</td>
</tr>
<tr>
<td>Anonymous Argentina</td>
<td>14</td>
</tr>
<tr>
<td>Mujahidin Cyber Army</td>
<td>11</td>
</tr>
<tr>
<td>Armada Collective</td>
<td>6</td>
</tr>
<tr>
<td>Anonymous Ireland</td>
<td>6</td>
</tr>
<tr>
<td>Cracka With Attitude</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAME</th>
<th>HITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous Palestine</td>
<td>2</td>
</tr>
<tr>
<td>APT17 Deputy Dog</td>
<td>2</td>
</tr>
<tr>
<td>Anonymous Mexico</td>
<td>2</td>
</tr>
<tr>
<td>Kelvin Security Team</td>
<td>1</td>
</tr>
<tr>
<td>AnonGh0st</td>
<td>1</td>
</tr>
<tr>
<td>Hunter Gujjar</td>
<td>1</td>
</tr>
<tr>
<td>Anonymous Operation Philippines</td>
<td>1</td>
</tr>
<tr>
<td>Guardians of Peace</td>
<td>1</td>
</tr>
<tr>
<td>Al Qassam Cyber Fighters</td>
<td>1</td>
</tr>
<tr>
<td>Anonymous Canada</td>
<td>1</td>
</tr>
</tbody>
</table>

### Action Item:

1. Follow hacker activity that are a threat to your brand
2. Subscribe to threat intelligences feeds for constant updates
## Top Suspicious IP Addresses

<table>
<thead>
<tr>
<th>NAME</th>
<th>HITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>46[.]109[.]168[.]179</td>
<td>30</td>
</tr>
<tr>
<td>188[.]118[.]2[.]26</td>
<td>24</td>
</tr>
<tr>
<td>118[.]170[.]130[.]207</td>
<td>18</td>
</tr>
<tr>
<td>81[.]183[.]56[.]217</td>
<td>11</td>
</tr>
<tr>
<td>114[.]44[.]192[.]128</td>
<td>10</td>
</tr>
<tr>
<td>87[.]222[.]67[.]194</td>
<td>6</td>
</tr>
<tr>
<td>23[.]239[.]65[.]180</td>
<td>4</td>
</tr>
<tr>
<td>216[.]243[.]31[.]2</td>
<td>4</td>
</tr>
<tr>
<td>93[.]174[.]95[.]77</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAME</th>
<th>HITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>89[.]248[.]167[.]155</td>
<td>4</td>
</tr>
<tr>
<td>84[.]200[.]65[.]2</td>
<td>4</td>
</tr>
<tr>
<td>41[.]33[.]194[.]107</td>
<td>4</td>
</tr>
<tr>
<td>208[.]100[.]26[.]230</td>
<td>4</td>
</tr>
<tr>
<td>176[.]98[.]26[.]188</td>
<td>4</td>
</tr>
<tr>
<td>113[.]207[.]36[.]253</td>
<td>3</td>
</tr>
<tr>
<td>123[.]151[.]149[.]222</td>
<td>3</td>
</tr>
<tr>
<td>112[.]82[.]223[.]47</td>
<td>3</td>
</tr>
</tbody>
</table>

**Action Item:**

1. Ensure your security monitor list is updated with the latest threat IPs
Ransomware Criminals Infect Thousands with Weird WordPress Hack

An unexpectedly large number of WordPress websites have been mysteriously compromised and are delivering the TeslaCrypt ransomware to unwitting end-users. Antivirus is not catching this yet.

Malware researchers from Malwarebytes and other security firms have reported that a massive number of legit WordPress sites have been compromised and are silently redirecting visitors to sites with the Nuclear Exploit Kit.

Currently it's not yet clear how the WordPress sites are getting infected, but it is highly likely that there is a new vulnerability that is being exploited in either WP or a very popular WP plugin.

The WordPress sites are injected with huge blurbs of rogue code that perform a silent redirection to domains appearing to be hosting ads.

The compromised WordPress sites were hacked and included encrypted code at the end of all legitimate JavaScript files. The malware tries to infect all accessible .js files.

The attack tries to conceal itself and the code redirects end-users through a series of sites before dropping the ransomware payload. Once a WP Server is infected, the malware also installs a variety of backdoors on the machine.

**Action Item:**
1. Patch Server Operating Systems
2. Patch WordPress
3. Get rid of unused WP plugins as soon as possible and patch the current ones
4. Update all your WP instances at the same time to prevent cross-infections
5. Lock down all WP instances with a very strong password and the WP 2-factor authentication
7. Regularly pentest your websites
Healthcare Supply Chain List Posted on Deepweb

Threat Actor: Thanos
TTP: Supply Chain Attacks

On January 19th, 2016, an actor known as 'Thanos' shared some contact information for supply chain providers to Healthcare Organizations.

While all of the information is generally public, the packaging of the information in this format could indicate future supply chain attacks against US and EU based healthcare organizations.

Organizations are advised to pay close attention to interconnections and communication (including email) to and from the listed organizations.

Action Item:  
1. Patch Server Operating Systems
Critical Fixes for IE Vulnerabilities and updates for Flash Player

Microsoft released 13 security bulletins addressing vulnerabilities in Internet Explorer, Microsoft Windows, and Microsoft. Out of these bulletins 6 are tagged as Critical while 7 are marked as Important.

One of the critical bulletins (MS16-009) resolves issues affecting older versions of Internet Explorer (IE 9, 10) as well as IE 11. When exploited successfully, it could lead to remote code execution thus compromising the security of the system. Microsoft announced that it will have limited support for older versions of IE, and encouraged users to upgrade to the latest version, which is currently IE 11.

Microsoft Edge also has critical vulnerabilities which can also result to remote code execution once successfully exploited. Another notable security bulletin for this month’s cycle is MS16-015, which fixes flaws in Microsoft Office. Attackers can execute arbitrary code when they leverage these vulnerabilities.

Adobe also rolled out several patches for Adobe Connect, Adobe Experience Manager, Adobe Flash Player, and Adobe Photoshop CC and Bridge CC. Several of the bugs found in Flash Player are considered as critical vulnerabilities that may lead to attackers compromising the system or taking full control of the affected systems.

**Action Item:**
Ensure only the updated version of software are running in your environment.
Suspicious Domain Registrations: hitrust (January 2016)

hitrustnow.com (Pattern: hitrust): administrativecontact_city: Panama City
administrativecontact_country: PANAMA administrativecontact_email: admin@whoisfoundation.com
administrativecontact_name: DOMAIN MAY BE FOR SALE, CHECK AFTERNIC.COM Domain Admin administrativecontact_organization: Whois Foundation administrativecontact_postalcode: 0823 administrativecontact_street: Ramon Arias Avenue, Ropardi Building, Office 3-C PO Box 0823-03015 administrativecontact_telephone: 5078365679 auditAuditupdateddate: 2016-01-17 00:00:00 UTC contactemail: admin@whoisfoundation.com createddate: 17-Jan-2016 domainname: hittrustnow.com expiresdate: 17-Jan-2017 nameservers: NS27.ROOKDNS.COM|NS28.ROOKDNS.COM| registrant_city: Panama City registrant_country: PANAMA registrant_email: admin@whoisfoundation.com registrant_name: DOMAIN MAY BE FOR SALE, CHECK AFTERNIC.COM Domain Admin registrant_organization: Whois Foundation registrant_postalcode: 0823 registrant_state: Ramon Arias Avenue, Ropardi Building, Office 3-C PO Box 0823-03015 registrant_telephone: 5078365679 registrarianaid: 303 registrarnname: PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM standardregcreateddate: 2016-01-17 00:00:00 UTC standardregexpiresdate: 2017-01-17 00:00:00 UTC standardregupdateddate: 2016-01-17 00:00:00 UTC status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited technicalcontact_city: Panama City technicalcontact_country: PANAMA technicalcontact_email: admin@whoisfoundation.com technicalcontact_name: DOMAIN MAY BE FOR SALE, CHECK AFTERNIC.COM Domain Admin technicalcontact_organization: Whois Foundation technicalcontact_postalcode: 0823 technicalcontact_state: Ramon Arias Avenue, Ropardi Building, Office 3-C PO Box 0823-03015 technicalcontact_telephone: 5078365679 updateddate: 17-Jan-2016 whoisserver: whois.PublicDomainRegistry.com

hitrustexperts.info (Pattern: hitrust): administrativecontact_city: Yorba Linda administrativecontact_country: UNITED STATES administrativecontact_email: timronevich@hotmail.com administrativecontact_name: Tim Roncevich administrativecontact_postalcode: 92887 administrativecontact_state: California administrativecontact_street: 28135 Shady Meadow Lane auditAuditupdateddate: 2016-01-26 00:00:00 UTC billingcontact_city: Yorba Linda billingcontact_country: UNITED STATES billingcontact_email: timronevich@hotmail.com billingcontact_name: Tim Roncevich billingcontact_postalcode: 92887 billingcontact_state: California billingcontact_street: 28135 Shady Meadow Lane billingcontact_telephone: 7143182458 contactemail: timronevich@hotmail.com createddate: 2016-01-26T00:44:59Z domainname: hitrustexperts.info expiresdate: 2017-01-26T00:44:59Z nameservers: NS53.DOMAINCONTROL.COM|NS54.DOMAINCONTROL.COM| registrant_city: Yorba Linda registrant_country: UNITED STATES registrant_email: timronevich@hotmail.com registrant_name: Tim Roncevich registrant_postalcode: 92887 registrant_state: California registrant_telephone: 7143182458 registrarianaid: 146 registrarnname: GoDaddy.com, LLC standardregcreateddate: 2016-01-26 00:44:59 UTC standardregexpiresdate: 2017-01-26 00:44:59 UTC status: serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited technicalcontact_city: Panama City technicalcontact_country: PANAMA technicalcontact_email: admin@whoisfoundation.com technicalcontact_name: DOMAIN MAY BE FOR SALE, CHECK AFTERNIC.COM Domain Admin technicalcontact_organization: Whois Foundation technicalcontact_postalcode: 0823 technicalcontact_state: Ramon Arias Avenue, Ropardi Building, Office 3-C PO Box 0823-03015 technicalcontact_telephone: 5078365679

Action Item:
1. Educated your employees to look into certificate information
TREND MICRO: RANSOMWARE
Motivation: Return per Malware Infection

- Spam bot
- Banking Trojan
- Ransomware
2015 Comparison

- Ransomware: 17%
- Crypto-Ransomware: 83%
## Jan 2016 Regional Ransomware Outbreaks

<table>
<thead>
<tr>
<th>Sat</th>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
</tr>
<tr>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
</tr>
<tr>
<td>30</td>
<td>31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cryptowall: Number of clicks on malicious URLs per hour on day of outbreak - June 2015
Cryptowall: Number of clicks on malicious URLs per hour on day of outbreak - July 2015
Typical Spam Outbreak

Spam Bot → Spam → Malware
Cryptowall 4.0 Outbreaks

ISP  Spam  Malicious Webservers  Malware
TorrentLocker Outbreaks

Hosted Spam Landing Page (Captcha) Malware

[Diagram showing the flow of how infections spread through TorrentLocker outbreaks]
Conclusion

• Campaigns with excellent operational execution
  – A lot of effort on Evasion
  – Using $ to make some of this evasion happen
• Moving from a consumer threat towards business
• Starting to use encryption for system hostage
• No Silver Bullets
  – Defense in Depth
Best Practices (IT Managers)

• Turn on Web & Email Reputation
• Turn off macros if not needed
• Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task
• Disable AutoPlay to avoid automatic execution of executable files in removable/network drives
• Turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access.
• Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared
• Standard Stuff
  – Do end-user education
  – Enforce a strong password policy
  – Apply security patches for all programs and the Operating Systems
  – Backups!!
Best Practices (when compromised)

• When a computer is compromised, isolate it immediately from the network
• During system infection, temporarily restrict write accesses to shared folders
• Contact Law Enforcement
THREATSTREAM: NJRAT TROJAN ALIVE AND KICKING....
Overview:

• njRAT - remote access trojan. designed to capture keystrokes, steal saved browser data and upload/download files.
• Tool of choice due to is ease to use and it wide community support e.g “tutorials”.
Who uses njRAT

• used in cyberespionage ops in the middle east. also by hacktivist and Sirian electronic army.

• Lately as of few months ago there has been a spike of its usage in the Brazilian region.

• Also used by script kiddies
njRAT and the Healthcare industry

• 36% of infections related with the healthcare vertical were related with njrat according with fireeye report. [1]

Geographic distribution of jRAT c2’s
njRAT Distribution Methods

Figure 1 — Phishing email

Picture credit to Phishme Labs.
njRAT Capabilities

• Complete remote system administration capabilities
• Scrapes saved credentials from browser
• Uploads/downloads files
• Command execution
• Key logging
• Webcam control
njRAT weekly build count
njRAT Mitigation

• Have antivirus software with the latest definitions
  – May not help if packed
• Application whitelisting
• User education on spearphishing attacks
• Up-to-date Network IDS
njRAT Detection

rule njRat
{
    strings:
        $s1 = {7C 00 27 00 7C 00 27 00 7C} // |'|
        $s2 = "netsh firewall add allowedprogram" wide
        $s3 = "Software\Microsoft\Windows\CurrentVersion\Run" wide
        $s4 = "yyyy-MM-dd" wide
        $s5 = "abcdefghijklmnopqrstuvwxyz" wide

        $v1 = "cmd.exe /k ping 0 & del" wide
        $v2 = "cmd.exe /c ping 127.0.0.1 & del" wide
        $v3 = "cmd.exe /c ping 0 -n 2 & del" wide

    condition:
        all of ($s*) and any of ($v*) and new_file
}

rule courtesy of: https://malwareconfig.com/yara/
njRAT Detection

snort Rule:

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"njRAT C2 Callout"; flow:from_client,established; content:"|00|lv|7C 27 7C 27 7C 27 7C|"; fast_pattern; classtype:trojan-activity;);
Thank you!!!! Any questions?
CSF Controls Related to Threats

• CSF Control for njRAT distribution, Suspicious IP addresses, Ransomeware (WordPress Ransomware)
  – 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 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.
CSF Controls Related to Threats

• CSF Control for Top Emerging Malware Entities
  – 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 Ransomware (autorun functions)
  – Control Reference: *09.o Management of Removable Media
    • Control Text: Formal procedures shall be documented and implemented for the management of removable media.
    • Implementation requirement: The organization shall formally establish and enforce controls for the management of removable media and laptops including restrictions on the type of media and usage, and registration of certain types of media including laptops. (disable autorun, sanitize media before connecting)
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.
QUESTIONS?
Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight