Modern Malware Threats

Josh McCune
Network Security Analyst
mccunej@ksu.edu
History of APT

- “Advanced Persistent Threat”
- Term first used by Air Force in 2006, more in reference to who was attacking, not the nature of the attack (“how”); now it seems to be more focused on how
- Was used early in 2010 by Google in relation to Operation Aurora where they claimed the Chinese govt. infiltrated their corporation and ~30 others (Yahoo, Symantec, Juniper, Morgan Stanley, Northrop Grumman, Dow Chemical, etc.)
- Went viral after that due to media and marketing
Definition of APT

- **Advanced** = sophisticated, new (some argue otherwise), professional form of attack; use multiple attack vectors; not your average script kiddie, but may use commodity malware

- **Persistent** = determined, prolonged attack at a specific target rather than a widespread opportunistic attack (Symantec claims that 75% of malware on 50 computers or less); involves continuous monitoring and interaction to achieve goal

- **Threat** = skilled, motivated, organized and well-funded attack by humans with a specific objective rather than automated, mindless widespread blast

- “low and slow deliberate attack at a specific target”
Stuxnet

Advanced
- Used four 0-day exploits (unprecedented)
- 7 methods of replication, including USB flash drives
- Used a programmable logic controller (PLC) rootkit
- Digitally signed code with two private keys from stolen digital certificates (from two companies in Taiwan)
- Symantec estimates that the group developing Stuxnet would have consisted of anywhere between 5 and 30 people, and would have taken six months to develop

Persistent
- Targeted specific Siemens SCADA system manufactured in China... at a facility that was raided by Chinese govt. authorities and equipment/plans confiscated.
- Spread indiscriminately, but only activated when encountered specific SCADA controllers
- Caused physical damage – centrifuges spun fast, then slow, creating vibration that would supposedly destroy themselves while the malware made operation appear normal on the gauges/meters. A cyber attack with kinetic effects

Threat
- Targeted specific system in Iranian uranium processing facility that destroyed 1/5th of their nuclear capability, setting them back several years.
- Many have implicated Israel, others U.S., Russia, or China
Stuxnet

Dropper (on Windows PCs) → Payload (Siemens controllers) → Target: Natanz FEP

Mission Goal: No Nukes For Iran
Percentage of Hits from W32.Stuxnet by Country

Data from Symantec
Wikileaks fallout

❖ Oct. 2010 – 400,000 military documents about the war in Iraq
❖ Nov. 2010 - 250,000 U.S. State Department diplomatic docs/correspondence
❖ Interesting social, political, ethical, historical, commercial, military, technical, and security implications
  Friend or foe of a democratic state and an administration that based its successful campaign on increased transparency?
  Julian Assange a hero or villain (irrespective of the allegations of sexual misconduct in Sweden)?
  How did a PFC in the U.S. Army access those documents? (DoD FAIL!)
  Launched all kinds of censorship/anti-censorship debates
Wikileaks fallout

““The first serous infowar is now engaged. The field of battle is WikiLeaks. You are the troops.” John Perry Barlow, EFF

Resulting “cyber war” fascinating

Wikileaks hit by massive DDoS an hour before publishing diplomatic cables
Companies started dropping support of WikiLeaks because of comparable attacks (EveryDNS, Amazon.com, PayPal, Bank of America)
Then those companies were attacked because they stopped doing business with WikiLeaks!
In many cases, were grass roots DDoS on both sides of the debate, a form of cyber activism (individuals downloaded DoS tools and launched them at a particular target, loosely coordinated in various online forums)
Wikileaks fallout

- Hacker group “Anonymous” got in the game, attacking Swedish govt. sites, MasterCard, and Visa. They attacked the govt. of Zimbabwe and Tunisia for censoring WikiLeaks; had implications in the 2011 Tunisian protests
- US federal court subpoenaed Twitter accts of Bradley Manning, Julian Assange, WikiLeaks, and others, with gag order not to notify anyone (USA PATRIOT Act)
- HBGary Federal CEO, Aaron Barr, bragged that they had infiltrated Anonymous and was going to name/shame them, belittle them
  Anonymous response swift and humiliating…
HBGary vs. Anonymous

- Broke into HBGary Federal servers (SQL injection), grabbed emails and published them, destroyed data, defaced their website, usurped Aaron Barr’s Twitter account
- This is a company that provides contract security services to the U.S. government!
- US Chamber of Commerce contracted them to discredit unions and progressive groups
- Sold rootkits to the govt – clear indication US govt. involved in cyber-espionage
- Work on behalf of Bank of America to discredit supporters of WikiLeaks with falsified documents, disinformation, sabotage
HBGary Secrets Exposed

- **Task B (stealth delivery method)**
  slip a piece of stealth software onto a target laptop without the owner's knowledge

- **12 Monkeys**
  Super-rootkit for Windows XP

- **Psyops**
  “…political cartoons that leverage current events to seize the target audience's attention and propagate the desired messages and themes”

- **Persona Management Software**
  Enabling agents to manipulate multiple social network personas to infiltrate jihadist websites, influence public opinion, etc..
Other disconcerting incidents

☒ Hack of RSA SecurID token-based authentication system
☒ Hack of reseller (Registration Authority/RA) of Comodo (the Certificate Authority/CA) SSL certs
  RA hacked, got username/pw of privileged account
  Used that account to submit command to Comodo to issue valid SSL certs for:
  ✌️ mail.google.com, www.google.com
  ✌️ login.yahoo.com (actually used in the wild)
  ✌️ login.skype.com, login.live.com
  ✌️ addons.mozilla.org
  Firefox, Chrome quietly issued browser updates to revoke the bogus certs
  Undermines SSL-based trust mechanism for “secure” web sites
What is ISC doing for you?

(a behind the scenes look at recent initiatives)

- URL filtering (mostly phishing scams)
- Dynamic firewalling
- Intrusion Detection
  ...and Prevention?
- Analyzing binaries collected on the wire
URL Filtering

This Page Has Been Blocked

Why?
The IT Security team has blocked the site you are trying to visit because it is capable of harming you or your computer. There are two types of sites that may be blocked in this way.

1. Information Harvesters: These are sites that are linked from Phishing Scam emails. They attempt to gather your personal information for use by malicious users who could use that information to do anything from accessing your K-State accounts to taking out credit cards in your name.

2. Drive-by Websites: These sites attempt to infect your computer with malicious software, and there is no user interaction required, to become infected all you have to do is visit the website.

More information?
You can find more information about Phishing Scams on the IT Security Phishing Scam page.

You can find more information on how your computer can be infected on the IT Security Malware page.
URL Filtering

KSU Phishing URLs:

- http://perifernozrenie.info/*  Proxy  Eternal
- http://topoffters4.me/*  Proxy  Eternal
- http://*.vistahosting.cn/*  Proxy  Eternal
- http://*.9hz.com/*  Proxy  Eternal
- http://updatingsystem.zxq.net/upgrad/  Proxy  Added: 2011-02-15T09:46:02-06:00
- http://zmail-login.4-all.org/  Proxy  Added: 2011-02-21T08:18:54-06:00
- http://etechwebonline.net/update/login.php  Proxy  Added: 2011-02-22T09:00:08-06:00
## Procera Packtlogic

### Redirect Phishing URLs

<table>
<thead>
<tr>
<th>Redirect Phishing URLs</th>
<th>129.88.33.786</th>
<th>129.130.168.85</th>
<th>74.55.180.59</th>
<th>80</th>
<th>6</th>
<th>HTTP</th>
<th>ads01.9hz.com</th>
</tr>
</thead>
</table>

### Block RI Malicious Hosts

<table>
<thead>
<tr>
<th>Block RI Malicious Hosts</th>
<th>129.88.33.795</th>
<th>129.130.168.85</th>
<th>121.254.205.5</th>
<th>80</th>
<th>6</th>
<th>Being analyzed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block RI Malicious Hosts</td>
<td>129.88.33.796</td>
<td>129.130.168.85</td>
<td>121.254.205.5</td>
<td>80</td>
<td>6</td>
<td>Being analyzed</td>
</tr>
<tr>
<td>Block RI Malicious Hosts</td>
<td>129.88.33.796</td>
<td>129.130.168.85</td>
<td>121.254.205.5</td>
<td>80</td>
<td>6</td>
<td>Being analyzed</td>
</tr>
<tr>
<td>Block RI Malicious Hosts</td>
<td>129.88.33.797</td>
<td>129.130.168.85</td>
<td>121.254.205.5</td>
<td>80</td>
<td>6</td>
<td>Being analyzed</td>
</tr>
<tr>
<td>Block RI Malicious Hosts</td>
<td>129.88.33.797</td>
<td>129.130.168.85</td>
<td>121.254.205.5</td>
<td>80</td>
<td>6</td>
<td>Being analyzed</td>
</tr>
<tr>
<td>Block RI Malicious Hosts</td>
<td>129.88.33.797</td>
<td>129.130.168.85</td>
<td>121.254.205.5</td>
<td>80</td>
<td>6</td>
<td>Being analyzed</td>
</tr>
<tr>
<td>Block RI Malicious Hosts</td>
<td>129.88.33.798</td>
<td>129.130.168.85</td>
<td>121.254.205.5</td>
<td>80</td>
<td>6</td>
<td>Being analyzed</td>
</tr>
<tr>
<td>Block RI Malicious Hosts</td>
<td>129.88.33.798</td>
<td>129.130.168.85</td>
<td>121.254.205.5</td>
<td>80</td>
<td>6</td>
<td>Being analyzed</td>
</tr>
<tr>
<td>Block RI Malicious Hosts</td>
<td>129.88.33.849</td>
<td>129.130.168.85</td>
<td>91.212.104.104</td>
<td>80</td>
<td>6</td>
<td>Being analyzed</td>
</tr>
<tr>
<td>Block RI Malicious Hosts</td>
<td>129.88.33.855</td>
<td>129.130.168.85</td>
<td>91.212.104.104</td>
<td>80</td>
<td>6</td>
<td>Being analyzed</td>
</tr>
<tr>
<td>Block RI Malicious Hosts</td>
<td>129.88.33.855</td>
<td>129.130.168.85</td>
<td>91.212.104.104</td>
<td>80</td>
<td>6</td>
<td>Being analyzed</td>
</tr>
<tr>
<td>Block RI Malicious Hosts</td>
<td>129.88.33.856</td>
<td>129.130.168.85</td>
<td>91.212.104.104</td>
<td>80</td>
<td>6</td>
<td>Being analyzed</td>
</tr>
<tr>
<td>Block RI Malicious Hosts</td>
<td>129.88.33.856</td>
<td>129.130.168.85</td>
<td>91.212.104.104</td>
<td>80</td>
<td>6</td>
<td>Being analyzed</td>
</tr>
<tr>
<td>Block RI Malicious Hosts</td>
<td>129.88.33.954</td>
<td>129.130.168.85</td>
<td>121.254.205.5</td>
<td>80</td>
<td>6</td>
<td>Being analyzed</td>
</tr>
<tr>
<td>Block RI Malicious Hosts</td>
<td>129.88.33.955</td>
<td>129.130.168.85</td>
<td>121.254.205.5</td>
<td>80</td>
<td>6</td>
<td>Being analyzed</td>
</tr>
</tbody>
</table>

### Filtering known malicious infrastructure
Snort: New Hardware!
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin"; flow:established,to_server; content:"GET";
 http_method;
 content:" HTTP/1.1|0d 0a|Accept-Language|3a| ";
 content:"|0d 0a|User-Agent|3a| Mozilla/4.0 |28|compatible|3b| MSIE";
 http_header; content:" [\d\s\w\-]+\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\; ";
 http_header; content:" [\d\s\w\-]+\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\|\s\d\; HTTP/1.1";
 classtype:trojan-activity;
 sid:218265;
 rev:1;)

04/09 09:02:12.797788 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.012766 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.081222 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.248977 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.292312 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.347491 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.394189 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.401619 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.401760 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.401819 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.401869 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.426332 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.434930 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.439089 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.499641 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.503718 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
04/09 09:02:13.581259 [**]  ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin [**] [classification: A Network Trojan was Detected] [Priority: 1] [TCP] 129.130.156.31:3126 -> $ 15:59:31:08
Decoding TDSS

2011-03-04 14:26:59 - 129.130.36.12 -> 248.118
GET /zGkhDDI8r6zFekDnJ6wNV+veXyUMD5h7q7d2YZtVo5PIG2NVui7McCYi1o4fm74s3wD5D06YX1Inmk850DcQbltBNZDKH4pS77w7NeEbwLDAD3h5K/KLexpatm2to816R4
0XE0KlvqG57tpl31g4WXV\GYiEoTfBK5Waa5n7qUMN11MF7H+2zWtrxm6Pm73B05pchdx/61PHlv1key1ZGqOvbMJzZ+5d0SgZ52SKNies5ncHe5ws5zVH/0sZs3xda6MyDKj
b5kl6D40Wv8eg/RS5LjTPbejPyPpRmRN3Hv4Q45fV3PYxy7gCMc enrichedU65s5W1A7k/jgj/PavX0h3UFbOMw== HTTP/1.1
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; GTB6.6; SearchToolbar 1.2; SLCC2; .NET CLR 2.0.50727
 ; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; HPNTDF; .NET4.0C; BRI/1)
Host: crj71k1813ck.com
Cache-Control: no-cache

$request1 = rc4crypt::decrypt($hostname, base64_decode ( substr ($uri, 1)));