FBI and REN-ISAC Briefing: New and Pervasive Threats in Cybersecurity
FBI and REN-ISAC Briefing: New and Pervasive Threats in Cybersecurity

Laz Andino, SSA FBI Cyber Division
Kim Milford, REN-ISAC
Threat Briefing

- Overview from attendees
- What we’re seeing: FBI
- What we’re seeing: REN-ISAC
- Trends
- Protection and Mitigation
**Threats**

**HACKTIVISM**  
Hacktivists might use computer network exploitation to advance their political or social causes.

**CRIME**  
Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.

**INSIDER**  
Insider threat actors typically steal proprietary information for personal, financial, or ideological reasons.

**ESPIONAGE**  
Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.

**TERRORISM**  
Terrorist groups might seek to sabotage the computer systems that operate our critical infrastructure.

**WARFARE**  
Nation-state actors might attempt to sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.
Recent Trends in Crimes Targeting Academia

July 2016 – December 2017

Source: FBI IC3

- Fake purchase order: 356
- Employment scam: 202
- Spoofed FBI/IRS call extorting student: 131
- Business e-mail compromise (BEC): 117
- Data breach: 37
- Ransomware attack: 18
- Fake Online University: 17
- Phishing e-mail sent to student: 16
Recent Trends in Crimes Targeting Academia

May 2017 – December 2017

Source: FBI IC3
Additional Techniques, Tactics and Procedures (TTPs):

- Adversaries using VPN/VPS (Burnable infrastructure)
- Utilizing free, non-reputable Certificate Authority
- Social Media as Vector (similar to Spearphish)
- Credential harvesting (illegitimate use of legitimate credentials)

Over 3 Billion Username/passwords leaked
Mabna Institute Spearphishing Campaign

A. Intrusion Activity

• The investigation has revealed that the actors responsible for the spearphishing campaign intruded into university networks in approximately 22 countries via spearphishing.

• The FBI observed in excess of 107,000 spearphishing emails being sent resulting in the harvest of nearly 8,000 usernames and passwords worldwide in a campaign most active between 2014 and 2016.

• Approximately 144 US universities and 176 foreign universities had professor email accounts compromised.

• Professors were targeted with spearphishing e-mails which sought to lure them to click on a link similar to the following example link, which would redirect the victim to a malicious Internet domain, such as eduo.in, registered and operated by the perpetrators of the scheme:

B. Spearphishing Messages

- Typically, spearphishing messages sent as part of the campaign purport to be sent from a professor from a different university, who has read, and has interest in an article authored by the professor. The sender requests that the victim send other articles to aid in research, which includes links that incorporate the malicious domains and falsely appear to be associated with the victim's university domain.

- Consistently, the spearphishing messages appear to be sent from professors at Canadian or other foreign universities. The actors use real professor names to send the spearphishing emails to help their messages appear to be more authentic.

- The sending e-mail addresses are consistently from fraudulently registered Internet domains that are confusingly similar to authentic university domains, to appear to be associated with the actual institution of the sender.

- To date, the investigation has revealed that the following domains have been used to send spearphishing messages as part of the campaign:

  - Uturonto.ca (Canada)
  - Umontreall.ca
  - Mcgiil.ca
  - Ulberta.ca
  - Concordia.cc (Cocos – Australian terrority)
  - Lakeheadu.ca
  - Macmaster.cc
  - Umantuba.ca
  - Lakeheadiu.ca
  - Ddal.co (Colombia)
  - Uottawa.cc
  - Uiwo.cc
  - Uoguelph.cc
  - Sfiu.co
  - Queensu.cc
C. Targeted Materials/Motivation:

The investigation has confirmed that the perpetrators were targeting, in part, access to and data from online academic databases available through University library.

D. Sample Spearphishing Message:

Hi

Dear Dr. [REDACTED]:

I recently read your good article: "[REDACTED]"
It's very useful in my field of research.
I wonder, if possible, to send me these articles to use in my current research:


Thanks for you Cooperation in Advance.

Assoc. Prof. [REDACTED]
For additional information, read the following Phishlabs links:

https://info.phishlabs.com/blog/post-iran-indictment-mabna-institute-what-next
Enterprise Security considerations:

- **Frameworks:**
  - ISO 27001
    - The ISO/IEC 27000 family of standards helps organizations keep information assets secure

- **NIST:**
  - Combination of multiple frameworks including ISO
Enterprise Security considerations: Challenges

• Frameworks are voluntary
• No Regulatory Requirements
  – PCI Compliance, HIPAA Compliance
• Cultural change
  – Security vs Feasibility
• Expensive to implement
• Executive Level Buy in
• Resource Allocation
Enterprise Security Control considerations:

- Patch, patch, patch
- Two Factor Authentication
- Application White Listing
- Separation of networks (physically and logically)
- Consolidated IT Security Strategy
- Principle of Least Privilege (even among executives and network admins)
- Define an incident response plan and test that plan internally and with partners
- Develop relationships, reporting, and information sharing plans before a breach
- Report early
Security considerations (cont’d):

• Physical access to mission critical servers:
  – Risk not worth the reward, easily exposed unless server is located in an adversary country.
    • Data centers generally have good physical controls unless located in adversary country.
  – Easier to introduce malware logically.

• Logical access to mission critical servers:
  – System hardening: disable all unnecessary services, remove unused software and disable guest account.
  – Disable uncontrolled activity to the internet from these servers
**RENS-ISAC: What we’re seeing**

<table>
<thead>
<tr>
<th>Type of Incident</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compromised Machines</td>
<td>66,692</td>
</tr>
<tr>
<td>Compromised Credentials</td>
<td>11,222</td>
</tr>
<tr>
<td>Spam or Phish</td>
<td>367</td>
</tr>
<tr>
<td>Vulnerable Machines</td>
<td>33,134</td>
</tr>
<tr>
<td>Open Recursive DNS Resolvers</td>
<td>135</td>
</tr>
<tr>
<td>Open Mail Relays</td>
<td>86</td>
</tr>
</tbody>
</table>
REN-ISAC CSIRT Activities

- 2017
  - SOC Interactions (except for password resets): 3,184
  - Unique Institutions per quarter, averaged 802
# REN-ISAC CSIRT Activities

<table>
<thead>
<tr>
<th></th>
<th>2018</th>
<th>2017</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compromised Machines</td>
<td>16,083</td>
<td>14,376</td>
<td>112%</td>
</tr>
<tr>
<td>Compromised Credentials</td>
<td>5,008</td>
<td>1,483</td>
<td>338</td>
</tr>
<tr>
<td>Spam or Phish</td>
<td>78</td>
<td>178</td>
<td>66</td>
</tr>
<tr>
<td>Vulnerable Machines</td>
<td>0</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>Open Recursive DNS Resolvers</td>
<td>612</td>
<td>707</td>
<td>87</td>
</tr>
<tr>
<td>Open Mail Relays</td>
<td>22</td>
<td>43</td>
<td>51</td>
</tr>
</tbody>
</table>
REN-ISAC CSIRT Activities

Compromised Machines: Exploits

- Ramnit
- Avalanche - Nymaim
- Zeus
- Sinkhole
- Gozi
- Mirai
- Xcode Ghost
- Avalanche -Andromeda
- Conficker
- Wanna Cry

2017 2018
REN-ISAC CSIRT Activities: Malware by Class

- Ransomware: 1157
- Worms: 925
- Backdoor: 835
- Banking: 721
Dorkbot March Activity

- XSS 4,669
- SQLi 1,051
- LFI 74
- OS 57
- RFI 4
Trends

• Phishing, especially spear-phishing
• Ransomware
• Business Email Compromise
• Cryptojacking
• Supply Chain Threats
• Social Media Compromise
Protection and Mitigation

Protect Your Computer from Ransomware

- Make sure you have updated antivirus software on your computer.
- Enable automated patches for your operating system and web browser.
- Have strong passwords, and don’t use the same passwords for everything.
- Use a pop-up blocker.
- Only download software—especially free software—from sites you know and trust (malware can also come in downloadable games, file-sharing programs, and customized toolbars).
- Don’t open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if you think it looks safe. Instead, close out the e-mail and go to the organization’s website directly.
- Use the same precautions on your mobile phone as you would on your computer when using the Internet.
- To prevent the loss of essential files due to a ransomware infection, it’s recommended that individuals and businesses always conduct regular system back-ups and store the backed-up data offline.
Don’t Be a Victim

The business e-mail compromise scam has resulted in companies and organizations losing billions of dollars. But as sophisticated as the fraud is, there is an easy solution to thwart it: face-to-face or voice-to-voice communications.

“The best way to avoid being exploited is to verify the authenticity of requests to send money by walking into the CEO’s office or speaking to him or her directly on the phone,” said Special Agent Martin Licciardo. “Don’t rely on e-mail alone.”
Protection and Mitigation: BEC

Here are other methods businesses have employed to safeguard against BEC:

- Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, legitimate e-mail of abc_company.com would flag fraudulent e-mail of abc-company.com.
- Create an e-mail rule to flag e-mail communications where the “reply” e-mail address is different from the “from” e-mail address shown.
- Color code virtual correspondence so e-mails from employee/internal accounts are one color and e-mails from non-employee/external accounts are another.
- Verify changes in vendor payment location by adding additional two-factor authentication such as having secondary sign-off by company personnel.
- Confirm requests for transfers of funds by using phone verification as part of a two-factor authentication; use previously known numbers, not the numbers provided in the e-mail request.
- Carefully scrutinize all e-mail requests for transfer of funds to determine if the requests are out of the ordinary.
Protection and Mitigation

- Data
  - Disposal
  - Backups
- Users
  - Awareness and education (Be suspicious!)
  - Principle of least privilege
  - Multi-factor authentication
- Application management
  - Scanning and patching
Other Technical Controls

- Managed workstations
- System log management and review
- Passphrase vaults
- Set up Google alerts
- IP monitoring by geographic region
- Bad IP monitoring
- Software inspection & updating tools
Questions?

Thank you!

#Security18