CYBERSECURITY BEST PRACTICES AND CONSIDERATIONS

Andrew Weidenhamer, Security & Privacy Director, RSM US, LLP
Today’s presenters

Bob Feldmann
National State & Local Government Industry Leader

Andrew Weidenhamer
Director, Security & Privacy Services
Agenda

• Introductions
• Public sector threat modeling
• Phishing
• Ransomware
• Insecure wireless
• Protections
PUBLIC SECTOR
THREAT MODELING
Who, What, and How

External actor varieties within Public
- State-affiliated: 61
- Unaffiliated: 30
- Nation-state: 16
- Organized crime: 11
- Activist: 2
- Acquaintance: 1
- Customer: 1

Data compromised in Public
- Personal: 103
- Secrets: 60
- Medical: 34
- Credentials: 32
- Internal: 32
- System: 23
- Classified: 19
- Payment: 7
- Bank: 4

Cyber-Espionage action varieties within Public
- Phishing: 74
- Use of backdoor or C2: 61
- Backdoor: 59
- C2: 49
- Spyware/keylogger: 35
- Password dumper: 20
- Downloader: 16
- Exploit vulnerability: 16
- Other: 15
- Capture app data: 15

PHISHING
Definition

• Social engineering is a technique employed by threat actors to manipulate people in doing something against their best interest (i.e. providing sensitive data, etc).

• Phishing is a form of social engineering and technical deceit to gain access to user credentials, identity and financial information. Usually delivered through email.

• Vishing is similar to phishing except attacks are delivered over the phone.
Spear phishing

• Sending emails from a trusted sender in order to induce targeted individuals to perform an action on behalf of the attacker
The lookalike

- A phishing email that looks like something the recipient already trusts

Your T-Mobile bill is now available

T-Mobile USA <leewill217@gmail.com>  Thu, Sep 17, 2015, 9:02 AM

to me

T-Mobile

Go to My T-Mobile

Your T-Mobile bill is available for review.

Dear ANDREW,

Your bill for account number 941412228 for bill close date on 09/10/15 is ready. You may view it here anytime.

<table>
<thead>
<tr>
<th>BALANCE</th>
<th>DUE DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>$117.98</td>
<td>10/03/15</td>
</tr>
</tbody>
</table>

Thank you,
T-Mobile Customer Care
This is an automated message; please do not reply to this email.
Wire transfer fraud

- Email typically comes from an executive who is usually tied up and needs an immediate wire transfer to pay for a service before close of business.

![Email example](https://isc.sans.edu/forums/diary/A+recent+example+of+wire+transfer+fraud/20581)

Spoofed email address

---

Image Source: [https://isc.sans.edu/forums/diary/A+recent+example+of+wire+transfer+fraud/20581](https://isc.sans.edu/forums/diary/A+recent+example+of+wire+transfer+fraud/20581)
Smishing

• Phishing through SMS

Dear Walmart shopper,
Congratulations you have just won a $1000 Walmart Gift Card. Click here to claim your gift.
www.WmartClick.com
(cancel: reply STOP)

Image Source: https://www.oneclickroot.com/how-to/how-to-protect-your-android-against-smishing/
RANSOMWARE
Definition

- Type of malware that prevents users from accessing their system or personal files
- Once installed, the attackers request payment usually in the form of bitcoin to obtain the encryption key
Threat Research from Insikt Group

Phishing Campaign Delivers Trickbot via Fake Advertisement for Royal Bank of Scotland – Cyber Threat Analysis

On April 16, 2018, security researchers observed a phishing email campaign with the subject of “Advice of Service Charge.” The email comes from either Garry[] T@rbs-commercial[.]com or Garry.T@rbscommercial[.]com. The email addresses have typo-squatted domains, giving them the appearance of coming from the Royal Bank of Scotland. The email contains a message telling the user that their account has a large service charge due on their account. A malicious attachment named “scotiabank_completed_confirmation.docx” contains malicious macros that download the Trickbot banking Trojan. Researchers believe that the actors behind this campaign are using ThreadKit, a new exploit kit which targets Microsoft Office Equation Editor vulnerabilities CVE-2017-11882 and CVE-2017-8570.

First sightings of the new ThreadKit exploit builder spreading an updated Trickbot variant were reported by security researchers from multiple firms in late March 2018. More details about ThreadKit and related entities are available in the Insikt Group Analyst Note linked above. This phishing campaign is relatively sophisticated in its use of typosquatting domains in the sender email address. Users should remain vigilant and verify the sender address of emails claiming to be from financial institutions. Additionally, organizations should consider adding the indicators of compromise (IOCs) from the query linked above to their intrusion detection processes.
This automated message has been sent because

bsclcm@scotiabank.com

has attempted to send you a secure, encrypted e-mail message.

To view this e-mail, please download attached file and log in with your existing account.

Please note that a self-password-reset feature has been added to the Scotiabank Secure Email Service.

Once you login to the Scotiabank secure email service you will be prompted to select a challenge question and enter your answer to the question.

You will use the selected challenge question and answer during a password reset.

For further information on how to use this service please refer to the Secure Email User Guide.
INSECURE WIRELESS
What is it?

• Networks with no authentication
What is it? – continued

- Wired Equivalent Privacy (WEP) Encryption
What is it? – continued

- Home wireless routers with default credentials

Image Source: https://www.routerpasswords.com
• Wi-Fi Protected Access (WPA) with weak pre-shared key (PSK)

Image Source: http://lifeofpentester.blogspot.com/2013/12/wpa-wpa2-handshake-cracking-with.html
What can a hacker do?

• Redirect you to a malicious website
• Attempt to exploit a vulnerability on your system
• Steal your credentials
Polling Question

When you receive an email with a Microsoft Office attachment and open it and see a message like this you should?

A) Click “enable content” as it provides additional security features for the document?

B) Never enable the content as malicious code run in the background compromising the computer.

C) Depends on who sent the email and whether or not you trust the person and the attachment.
PROTECTIONS
Phishing

• Don’t fall for any cheesy scams. If it sounds too good to be true, it usually is.

• Implement sender policy framework (SPF) records

• Evaluate domain name of sender

• Evaluate the URL to ensure that the domain name matches what you would expect.
  – https://www.bankofamerica.com: Correct
  – http://www.bankofmerica.com: Incorrect

• Instead of clicking on links, open a browser and manually navigate

• Use website scanning websites (i.e. sitecheck.secure.net)
Ransomware – Computer

• MalwareBytes – Runs alongside your anti-virus solution to detect and prevent 0-day malware

  ![Malwarebytes Logo](https://www.gamersnexus.net/industry/1997-mbam-free-license-for-pirates-amnesty)

• Don’t run as administrator on your computer
• Patch systems frequently including third party software (i.e. Secunia)
Ransomware – Mobile devices

• Only install apps from trusted sources (i.e. GooglePlay, Apple Store, etc.)


• Backup your information to a storage device / cloud (i.e. iCloud) to mitigate mobile ransomware attacks

• Update software
Virustotal

Virustotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

By clicking "Scan it", you consent to our Terms of Service and allow Virustotal to share this file with the security community. See our Privacy Policy for details.

Scan it!
Wireless protection

- Corporate – Configure infrastructure using 802.1x authentication with both server and client side certificates
- Home - Configure your wireless network for WPA2
Wireless protection – continued

• Use a strong wireless password

2.4 GHz Wi-Fi Status

<table>
<thead>
<tr>
<th>Wi-Fi:</th>
<th>On</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID:</td>
<td>FiOS-VR8C0</td>
</tr>
<tr>
<td>Wi-Fi Password:</td>
<td>da[redacted]</td>
</tr>
<tr>
<td>Channel:</td>
<td>Automatic</td>
</tr>
<tr>
<td>SSID Broadcast:</td>
<td>Enabled</td>
</tr>
<tr>
<td>MAC Authentication:</td>
<td>Disabled</td>
</tr>
<tr>
<td>Wi-Fi Mode:</td>
<td>Compatibility Mode(802.11b/g/n)</td>
</tr>
<tr>
<td>Packets Sent:</td>
<td>30252363</td>
</tr>
<tr>
<td>Packets Received:</td>
<td>15596879</td>
</tr>
</tbody>
</table>
Wireless protection – continued

• Home - Change default or preset admin password on administrator interfaces

![User Settings form](image)
Wireless protection – continued

• Turn off Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup is an easy way to add wireless devices to your network. To use this feature, your wireless client device needs to support WPS.

Warning: Wireless devices may briefly lose connectivity when turning WPS ON or OFF

Wi-Fi Protected Setup: 

• Update firmware

Image source: http://it-answer.blogspot.com/2013/04/how-to-upgrade-linksys-wrt54g-wireless.html
Mobile wireless protections – Corporate

• Mobile Device Policy

2. Scope

1. All mobile devices, whether owned by <Company X> or owned by employees, inclusive of smartphones and tablet computers, that have access to corporate networks, data and systems are governed by this mobile device security policy. The scope of this policy does not include corporate IT-managed laptops.

2. Exemptions. Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk authorized by security management must be conducted.

3. Applications used by employees on their own personal devices which store or access corporate data, such as cloud storage applications, are also subject to this policy.

3. Policy

3.1 Technical Requirements

1. Devices must use the following Operating Systems: Android 2.2 or later, iOS 4.x or later, "add or remove as necessary."

2. Devices must store all user-saved passwords in an encrypted password store.

3. Devices must be configured with a secure password that complies with <Company X>'s password policy. This password must not be the same as any other credentials used within the organization.

4. Only devices managed by IT will be allowed to connect directly to the internal corporate network.

5. These devices will be subject to the valid compliance rules on security features such as encryption, password, key lock, etc. These policies will be enforced by the IT department using Mobile Device Management software.

3.2 User Requirements

1. Users may only load corporate data that is essential to their role onto their mobile device(s).
Mobile wireless protections – Corporate

- Mobile Device Management (MDM) Solution
  - Remote wipe
  - Control security settings
  - Manage apps
Mobile wireless protections - Home

• Disable Wi-Fi when you aren’t using it

![iOS](image1.png) ![Droid](image2.png)

Mobile wireless protections - Home

- Use a VPN solution once connecting to the open WiFi
Mobile wireless protections - Home

• Forget wireless network
QUESTIONS AND ANSWERS
Thank you

Bob Feldmann
National State & Local Government Industry Leader
+1 954 356 5600
Bob.Feldmann@rsmus.com

Andrew Weidenhamer
Director, Security and Privacy Consulting
+1 703 336 6572
Andrew.Weidenhamer@rsmus.com
THANK YOU FOR YOUR TIME AND ATTENTION