Someone wants your stuff!

- Where are the threats coming from?
- What are they looking to gain?
- Reducing the risk and impacts
### Major Threat Areas into the Future

- Targeted attacks – Nation-state
- Ransomware
- Distributed Denial of Service (DDoS) Attacks
- The Internet of Things (IoT) and Cloud
- Social Engineering and Human Error

---

**Major Threat Areas into the Future**

- Targeted attacks – Nation-state

  - Nation-state cyber attacks refer to foreign government (or government-directed) organizations targeting other countries’ government or commercial institutions or infrastructure.
  - Possible motivations for these attacks include eroding rivals’ economic and military competitiveness; influencing the political and diplomatic landscape; obtaining intelligence to advance weapons proliferation programs; and cyber warfare to create an advantage in armed conflict.

- Nopsec, [https://www.nopsec.com](https://www.nopsec.com)
Major Threat Areas into the Future

• Targeted attacks – Nation-state (cont.)

✓ Alleged attempt by Russia to tamper with US elections in 2016
✓ Malware linked to the NSA, stolen possibly by Russian hackers (Shadow Brokers) and offered for auction
✓ Yahoo claimed the data breach that occurred in 2014 but reported late last year may have been state sponsored
✓ Disk-wiping malware against Ukraine in Jan and Feb 2016, resulting in power outages

Major Threat Areas into the Future

• Targeted attacks – Nation-state (cont.)

✓ China and US signed a 2015 agreement – not to conduct economic espionage, resulting in significant drop, but other groups still use this practice
✓ Simple spear-phishing email was used to gain access to Hillary Clinton’s campaign chairman’s (John Podesta) Gmail account – a non-software related method (Living off the land)
Major Threat Areas into the Future

• Ransomware - Definition

✓ Ransomware is a type of malware program that infects, locks or takes control of a system and demands ransom to undo it. Ransomware attacks and infects a computer with the intention of extorting money from its owner.

*S techopedia.com

Major Threat Areas into the Future

• Ransomware (cont.)

✓ Top security threat for healthcare in 2016 and expected to continue to rise in 2017
✓ Healthcare data breach cost $355 per record – more than 2x the mean across all industries of $158 per record*
✓ Like other hacking tools – Ransonware as a service (RaaS) is now being sold on the Dark Web
✓ According to an IBM survey (Dec 2016) – 70% of business executives that were victims had paid to get data back. More than ½ paying over $10k and 1 in 5 paying > $40k

* IBM Security 2016 Cost of Data Breach Study
Major Threat Areas into the Future

• Ransomware (cont.)
  ✓ Is a form of malware with numerous variants
  ✓ Typically spread via email attachment or malicious webpages
  ✓ A successful technique – due to success, more sophisticated attacks being developed
  ✓ Ransom for data is typically demanded in Bitcoin since many broker services now exist
  ✓ Only 47% of victims who paid the ransom reported getting their files back - according to Norton Cyber Security Insight team

Major Threat Areas into the Future

• Ransomware – WannaCry
  ✓ Initiated on Friday, May 12, 2017
  ✓ Digital clues point to North Korea as origin
  ✓ Exploit created by US National Security Agency (NSA), then stolen and leaked a month prior
  ✓ Carried out by penetrating network defense or spear-phishing
  ✓ Microsoft (MS) released a patch 2 months prior
  ✓ MS operating system was vulnerable if not patched along with older versions of the OS
  ✓ Vulnerability with Microsoft Server Message Block (SMBv1) server that allows remote code execution
  ✓ Domain name used in WannaCry was registered and used as temporary “kill switch”
Major Threat Areas into the Future

- Ransomware – WannaCry (Impact)
  - Infecting more than 230,000 computers in 150 countries
  - Britain’s National Health Service (NHS) was a victim
  - NHS greatly publicized - 48 trusts were affected
  - Able to identify bitcoin accounts receiving the ransom payments
  - Approximately 291 payments - $93,000 (May 19, 2017)
  - PCs still vulnerable that haven’t applied the patch
WannaCry Encryption Notice

How Ransomware Works
Major Threat Areas into the Future

- Distributed Denial of Service (DDoS) Attacks – Definition

✓ A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.

* techtarget.com
Major Threat Areas into the Future

• Distributed Denial of Service (DDoS) Attacks – (Cont.)

- Infamous DDoS attack on Dyn in Oct 2016
- Dyn is a DNS website – directs/maps internet traffic
- Highly distributed attack involving 10s of millions of IP addresses
- Site is overwhelmed by traffic and can’t respond to valid requests
- World’s leading websites affected – Netflix, Paypal, Twitter
- Mirai malware was the culprit – more on this in IoT

Major Threat Areas into the Future

• The Internet of Things (IoT) – Definition

- The Internet of Things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data.

* wikipedia.com
Major Threat Areas into the Future

• The Internet of Things (IoT) and Cloud (Cont.)

 ✓ Is a big concern in healthcare with medical devices and information stored on them
 ✓ DDoS attack on Dyn last year was made possible by a botnet that targeted IoT devices
 ✓ Smart TVs and “intelligent assistant” devices (Amazon Echo, Google Home, etc.)
 ✓ Explosion of Cloud services – harder to control what information is stored where
 ✓ 25% of all shadow data (business data stored in the cloud without IT’s knowledge or consent) is “broadly shared” – internally, externally and/or with the public*

* Symantec Internet Threat Report April 2017

Major Threat Areas into the Future

• The Internet of Things (IoT) and Cloud (Cont.)

 ✓ Can’t fully mitigate risks to cloud-stored data from employee misuse or account compromise by hackers
 ✓ Companies’ data governance being eroded and susceptible to outside-the-company weakness
 ✓ Some cloud providers build their services using other cloud providers’ services – extending risk

* Symantec Internet Threat Report April 2017
**Major Threat Areas into the Future**

- **Social Engineering and Human Error**
  - Humans are your biggest cybersecurity vulnerability
  - Breach can be caused by a single employee (intentional or unintentional)
  - Social attacks are becoming more sophisticated – tailored to specific employees
  - Spear-phishing
  - IoT vulnerability due to human error
  - Busy, high volume businesses like healthcare - difficulty managing privileged users effectively, leading to inappropriate access

* Nopsec https://www.nopsec.com

---

**Spear-phishing email used in DNC attacks**

Text of spear-phishing email sent to John Podesta, the chairman of the 2016 Clinton presidential campaign.

*From:* google-one-reply@accounts.google.com

*Date:* March 30, 2016 at 12:34:19 PM EST

*From:* **********@gmail.com

*Subject:* Someone has your password

Someone has your password

Hi John

Someone just used your password to try to sign into your Google Account **********@gmail.com.

Details:

- **Date:** Saturday, March 30, 2016, 12:34:19 PM UTC
- **IP Address:** 183.230.136.200
- **Location:** Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

[CHANGE PASSWORD](https://bit.ly/3pUcnu)

Best,
The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.

* Symantec, Internet Threat Report, April 2017
Cyber Crime Pays

• The Dark Web – Definition

✓ The Dark Web is the portion of the Deep Web that has been intentionally hidden and is inaccessible through standard Web browsers. Dark Web sites serve as a platform for Internet users for whom anonymity is essential, since they not only provide protection from unauthorized users, but also usually include encryption to prevent monitoring.*

*THE IMPACT OF THE DARK WEB ON INTERNET GOVERNANCE AND CYBER SECURITY, Michael Chertoff and Tobby Simon, Global Commission on Internet Governance, Feb. 2015

---

Underground marketplace price list

<table>
<thead>
<tr>
<th>Payment Cards</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single credit card</td>
<td>$0.5 - $30</td>
</tr>
<tr>
<td>Single credit card with full details (Full)</td>
<td>$20 - $60</td>
</tr>
<tr>
<td>Dump of magnetic strip data (16 &amp; PIN)</td>
<td>$600 - $1,200</td>
</tr>
</tbody>
</table>

Malware

| Basic banking trojan kit with support | $100 |
| Password stealing trojan | $20 - $100 |
| Android banking trojan | $200 |
| Account macro downloader generator | $5 |
| Malware crytaler service (make hard to detect) | $20 - $40 |
| Ransomware kit | $10 - $1,800 |

Services

| Media streaming services | $0.10 - $10 |
| Hotel reward program accounts (100K points) | $10 - $200 |
| Airline frequent flyer miles account (10K miles) | $5 - $30 |
| Tax preparation accounts with credit | $5 - $100 |
| Online retail gift cards | 20% - 40% of face value |
| Restaurant gift cards | 20% - 40% of face value |
| Airline ticket and hotel bookings | 10% of face-value |
| DDoS service, < 1 hr duration, medium target | $5 - $20 |
| DDoS service, > 2 hr duration, medium & strong target | $10 - $1,000 |
| Dedicated bulletproof hosting (per month) | $1,000 - $2,000 |
| Money transfer services | |
| Cash-out service | 10% - 20% |

Accounts

| Online bank accounts | 0.5% - 10% of account balance |
| Retailer accounts | $20 - $40 |
| Cloud service provider accounts | $6 - $10 |
| Identity (Name, SSN & DOB) | $0.1 - $1.5 |
| Scanned passports and other documents (e.g., utility bill) | $1 - $2 |

* Symantec, Internet Threat Report, Apr. 2017
Reducing the Risk and Impact

• Healthcare Industry

✓ Healthcare data is a treasure trove - credit card numbers, Social Security numbers, email addresses, bank account information, and birth dates
✓ Compliance is not the same as security
✓ Need to leverage each to support and enhance the other
✓ Healthcare stills lags in IT spending compared to other industries, particularly other regulated industries like finance or government
✓ Needs to keep up with the rapidly changing threat landscape
✓ With the increasing digital transformation and connectivity in the industry comes increased risk

* Symantec Internet Threat Report, April 2017

Cybersecurity Domains

• Henry Jiang, CISO, CISO/CEO and Managing Director at Oppenheimer & Co. Inc.
Reducing the Risk and Impact

• Healthcare Small to Medium Business (SMB) Security Tips

  ✓ Employ firewalls, desktop antivirus software, antivirus software on email servers, antivirus and anti-malware protection on employee inboxes, and content filtering for the Internet and email.
  ✓ Have a strong password policy – require changing of passwords often (at least once a quarter), use password strength techniques
  ✓ Send email containing PHI – software to encrypt email body and attachments
  ✓ Restrict access for employees – least privilege model
Reducing the Risk and Impact

• Healthcare SMB Security Tips (Cont.)

✓ Secure mobile devices – encrypt smartphones, laptops, tablets, etc. Patch, password protect, require virus protection for access to systems, perhaps utilize a VPN.
✓ Cyber security policy – develop and maintain
✓ Third party vendors – make sure security controls are in place

Someone wants your stuff!

<table>
<thead>
<tr>
<th>Bibliography and Web Links</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Ways Small Practices Can Thwart Cybercrime</td>
<td><a href="http://www.physicianspractice.com/hipaa/6-ways-small-practices-can-thwart-cybercrime/">http://www.physicianspractice.com/hipaa/6-ways-small-practices-can-thwart-cybercrime/</a></td>
</tr>
<tr>
<td>Ten ways to stop a ransomware threat targeting healthcare data</td>
<td><a href="http://searchhealthit.techtarget.com/tip/Ten-ways-to-stop-a-ransomware-threat-targeting-healthcare-data">http://searchhealthit.techtarget.com/tip/Ten-ways-to-stop-a-ransomware-threat-targeting-healthcare-data</a></td>
</tr>
<tr>
<td>Carbonite: A Cornerstone For Ransomware Protection And Recovery</td>
<td><a href="http://www.bitpipe.com/detail/RES/1482960493_91.html">http://www.bitpipe.com/detail/RES/1482960493_91.html</a></td>
</tr>
</tbody>
</table>