Cybersecurity Update: Phishing to Ransomware – Looking ahead to 2019

Kevin J. Murphy, CISSP, CISM, CGEIT
A very interactive discussion – We learn from each other!

- *Who is in the room?*
- *Lessons from 2018*
- *Looking ahead to 2019*
- *Vendor verification*
- *Quick review*
Who is in the room?

- Provincial Government
- Federal Government
- Municipal
- Retail
- Technology
- Transportation
- Law Enforcement
- Healthcare
- Energy
- Telecom
- Financial
- Manufacturing
- Education
- Services
Who is attacking? 

North Korea were held responsible for the NotPetya attack, which was widely thought to have been carried out by Russia, an allegation Moscow denies.

The Canadian government's computer networks have been hit by state-sponsored cyberattacks about 50 times a week — and at least one of them usually succeeded.

On October 24th, BadRabbit targeted Windows machines, impersonating as an Adobe Flash update. The cyber attack has seen computers go down in Russia, Ukraine, Germany and Turkey.

"The new Cold War with less rules"
2017 Canadian Companies

- Phishing: 58%
- Malware: 45%
- Network scanning: 20%
- Brute force attack: 9%
- Man in the middle: 9%
- Other technique: 5%
- Yes, but unsure of technique: 11%

2018 Notable Cyber Breaches

Risk Based Security in Richmond, Va. reported data as of June 30 showing the United States had, by far, the most incidents per country at 1,074. United Kingdom was second with 62 and Canada third with 48 incidents.
2018 Reality

CyberAttacks:

• Data breaches have hit 36 per cent of Canadian businesses.

• Cyber-attacks on Canadian municipalities increasing
  – https://auma.ca/news/cyber-attacks-canadian-municipalities-increasing
New Breach Regulations

• Commencing November 1, 2018, Canada’s federal Personal Information Protection and Electronic Documents Act (“PIPEDA”) will require an organization that suffers a “breach of security safeguards” involving personal information under its control to keep prescribed records of the breach and, if the breach presents a “real risk of significant harm to an individual”, to promptly report the breach to the Privacy Commissioner and give notice of the breach to affected individuals and certain other organizations and government institutions.

2018 Reality

**Malware**
- Up 102% in 2018 from 2017
- Also more threats via smart malware and file-less malware
- Malware attacks on non-profits as staging areas for attacks on business
  - Youth activity, charities, social sites, the arts, etc. generally have marginal security

**Ransomware**
- Up 229% in 2018 from 2017
- West Jet, City of Atlanta, Univ of Calgary, Colorado, Alaska, etc, etc.

**Attackers leveraging encryption (SSL/TLS) to bypass your security controls**
- Up 275% in 2018 from 2017
- 2/3rd of City of Seattle Internet traffic is now Https
- Attackers can leverage free SSL certificates using “Let’s Encrypt” to disguise their traffic.
- Our City non-encrypted traffic now ~8% and getting smaller. Your network traffic monitoring is blind if you are only inspecting port 80 traffic
Who is attacking?
2018 Reality

Phishing

• Employee Awareness
  – Nearly 1.5 million phishing URLs are created each month just to trick users into thinking an email is indeed originating from their employer, Microsoft, the CRA, their bank, Facebook page, insurance claim form, PayPal, Apple, etc.

• Cloud Applications: e.g O365
  – Base subscriptions has insufficient security as standalone product; think “Defense in Depth”

• Outnumbered by Malicious Actors
  – They are right once and win; we have to be right 100% of the time
  – And they are using AI against you.
Quiz

• Which country hosts the most malicious web addresses?

<table>
<thead>
<tr>
<th>Ranking in Q2</th>
<th>Country/region</th>
<th>Number of domains in Q2</th>
<th>Number of domains in Q1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>US United States</td>
<td>248</td>
<td>257</td>
</tr>
<tr>
<td>2.</td>
<td>NL Netherlands</td>
<td>31</td>
<td>13</td>
</tr>
<tr>
<td>3.</td>
<td>HK Hong Kong</td>
<td>9</td>
<td>41</td>
</tr>
<tr>
<td>4.</td>
<td>AU Australia</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>5.</td>
<td>DE Germany</td>
<td>5</td>
<td>12</td>
</tr>
<tr>
<td>6 (tied)</td>
<td>GB United Kingdom</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>6 (tied)</td>
<td>IT Italy</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>7 (tied)</td>
<td>CN China</td>
<td>2</td>
<td>106</td>
</tr>
<tr>
<td>7 (tied)</td>
<td>RU Russian</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>8 (tied)</td>
<td>CA Canada</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>8 (tied)</td>
<td>ES Spain</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>8 (tied)</td>
<td>FR France</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>8 (tied)</td>
<td>IE Ireland</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>8 (tied)</td>
<td>KG Kyrgyzstan</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 2. country/region distribution graph of malicious domains
Phishing

Dear Customer

Your account make a order on Apps Store, please visit your attachment

Billing Information

Sincerely,

Apple Support
Dear Client,

We just processed the payment for your John LaMunyon account and charged your credit card for $848.00. You will see “John LaMunyon” as recipient on your card statement.

Any question, please do contact us and we will be delighted to help.

Thank you for choosing John LaMunyon

Thank you in advance

**Invoice 2019-0120**

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sender:</strong></td>
<td>John LaMunyon</td>
</tr>
<tr>
<td><strong>Invoice date:</strong></td>
<td>01-30-2019</td>
</tr>
<tr>
<td><strong>Due date:</strong></td>
<td>02-01-2019</td>
</tr>
<tr>
<td><strong>Amount due:</strong></td>
<td>$0.00 (Amount paid: $848.00)</td>
</tr>
</tbody>
</table>
2018 Reality

Phishing

• Openly Shared Public Data e.g. email addresses
  – Address Book and other data can be used for “spoofing” and password spraying
  – Common passwords used in the local Seattle area
    • Fall2018
    • Winter2019
    • Seahawks12!
    • GoHawks!
    • Christmas2018

Vancouver area?
  • Canucks2019!
  • Lions2019!
  • Winter2019
  • Cannabis@@
  • Whistler2019

Don’t fall for this!
Ransomware

- WannaCry worm traveled between unpatched computers without user interaction.
- March 14, 2017 - Microsoft issued **critical** security bulletin MS17-010
- May 12, 2017 - WannaCry launched

*Lessons Learned:*

“The answer is to patch systems earlier!”
2018 Attack Chain Example

1. Attacker continuously scanning external systems of target looking for new servers

2. Developer created virtual server in the cloud

3. Default settings not disabled, leaving it vulnerable to brute forcing

4. Attacker guesses password and logs into server

5. Attacker uses existing link to access internal network

6. Attacker spends a day mapping out network

7. Uses ‘pass-the-hash’ to log into multiple servers and workstations

8. Holds files for ransom
2018

CYBER WARFARE
Attacks cities are seeing

- 400,000 cyberattacks blocked per month
- 70+% of incoming mail is SPAM or Phishing
- Outbound phishing from compromised internal accounts is a problem
- 10-15 successful phishing attacks per month
2018 Reality - A cyber-breach is inevitable

• Prepare for your breach:
• Test your recovery plan
• What you can do now to recover quickly?
Looking ahead to 2019: Geopolitical Threats

• Hostile Nation States will use AI to manipulate your personalized news sources.

• Nation state will increase Disinformation Operations against trusted democratic institutions.
  – This is modern propaganda that is so tailored to the individual user that it becomes that persons reality.
  – Our political leaders are not trained to counter this threat and will struggle to discover truth from fiction.
    • Mob mentality, Brexit lies, American election candidate lies
Looking ahead to 2019: Geopolitical Threats

• “Research has shown that 6 out of 10 of us will share an article just based on its title, which means in all of those cases, we're prone to fall for a hoax”

• Click bait sells ads. That is how the internet based information model works
2019 Geopolitical Threats: Your best defense

• Seek out the logical opposing view
  – When our news feeds show the opposing view as “idiots” be very cautious.
  – The opposition are logical people and they will present well thought out views. Always look for views that are presented as logical arguments.

• Most of life is not sensational.
  – Daily life is generally mundane. However it is the sensational that gets us to click on the link. Clicking on the link is what sells ads. That’s how the social media model works.
2019 Geopolitical Threats

• Nation-states have attacks on the shelf ready for cyberwar
  – PressTV-Iran foils Israeli cyber attacks on communications ...
    • https://www.presstv.com/Detail/2018/11/05/579125/Iran-Israel-Cyber...
    • 2018-11-05 · Iran says it has successfully staved off a wave of cyber attacks apparently by Israel targeting its communications infrastructure, vowing to pursue the ...
  – Iran has laid groundwork for extensive cyberattacks on U.S ...
    • https://www.nbcnews.com/news/us-news/iran-has-laid-groundwork...
    • July 20, 2018 - Iran has positioned cyber weapons to hit private firms and infrastructure, but there is no suggestion an attack is imminent, say U.S. officials.
2019 Predictions

Threats Landscape: Looking ahead to 2019

• Cyber-attacks will become more methodical using AI
• Critical infrastructure ransomware attacks: OT, SCADA
• SPAM and phishing mails will rise to over 90% of total email received.
• Phishing will become very hard for a humans to detect.
• Cloud providers will continue to be slow for taking down malicious URLs.
• Legacy Applications risk increasing
  – Speed and ability to patch

• What else? Room discussion

Next year let’s see what we missed. 😊
So where do we go from here?
Information Security IndustryScape

Lots of Choices
Security Controls and security tool effectiveness

“So how will we know if all of this is working as the various vendors have promised?”
Visibility

- Are tools seeing traffic between zones as expected?
- Are comm direction and port/protocols allowed expected?
- Inline vs. tapped/spanned expected?

Prevention

- What tests are being blocked and by which technology?
- Which technologies are preventing the most?
- Are the company’s expectations of what will be blocked inline with the results?

Detection

- What detection events are generated?
- What is generating high fidelity events vs. noise or false positives?
- Where am I detecting tests with high fidelity and can quickly reconfigure to blocking?

Event Flow

- Are the detection events going from Sensor > Mgmt. Console > SIEM?
- Are they being correctly parsed?
- Is all the anticipated data present?
- Are the timestamps correct?

Alerting

- Are alerts firing?
- Where can context be increased to make the alert more actionable?
- Are high fidelity/priority detection events alerting?
POC At-a-Glance:

June 19-20, on-site at Seattle Municipal Tower

- 149 Actions ran
- 53% Block Rate
- 89% Events logged with Qradar
- Of those events, 11% triggered correlation alerts

Controls tested: QRadar*, FireEye*, Websense, Checkpoint, Trend, Malware Bytes, InfoBlox

Numbers may shift slightly once POC is complete

*Indicates Verodin integrations for purpose of POC
Call to Action

• Learn from other industries as they might get hit before yours.
  – Attend information network opportunities such as Privacy & Security Conferences, BC Provincial Cybersecurity events, VanSecSig monthly broadcast meetings, AGORA and SecureWorld

• Know your IT Inventory and patch status

• Evaluate your threat models with the latest attack vectors. Ask, “Can that happen here?”

• Evaluate the effectiveness of your security controls

• Test your business continuity plans with a cyber attack scenario

• Cybersecurity risks needs to be part of the overall risk report delivered to your corporate Board of Directors.
Call to Action: Specific Actions

1. Know your IT Inventory
2. Test and apply patches within the vendor & government guidelines. Critical patches ASAP
3. Implement SSL Inspection
4. Don’t allow default passwords
5. Implement an anti-phishing solution that blocks outbound phishing from compromised internal accounts
6. Have threat hunting tools that are adaptive and use AI
7. Use a tool that verifies that your security tools are actually working.
Your Board of Directors

The Cyberresilient Enterprise: What the Board of Directors Needs to Ask

Move Beyond Standalone Risk Protection to Enterprise Wide Risk Management and Operational Sustainability

Advances in the digital marketplace are creating more opportunities for value—and risk. As organizations leverage cloud computing, the Internet of Things, mobile computing and social media, digital risk management takes on greater importance. Theft of personal information and private business information, misappropriation of resources, denial of service, and cybertheft are more common for enterprises large and small.

In the past, businesses used separate approaches to information security, business continuity and incident response. Today, a new comprehensive approach is required. The urgency of providing continuously available services for customers and business partners in a digital economy requires organizations to be resilient.

Learn how to make the important transition to becoming a cyberresilient enterprise with this thought-provoking resource that will help you:
You can name her whatever you like but be sure it's something you can remember. You'll be using it as a security question answer for the rest of your life.

My contact info:
kevinmur@Hotmail.com
References:

• baseStriker: Office 365 Security Fails to Secure 100 Million Email Users

• How can Office 365 phishing threats be addressed?

• Threat Spotlight: Cybercriminals Working Hard to Take Over Email Accounts
  – https://blog.barracuda.com/2018/05/03/threat-spotlight-cybercriminals-working-hard-to-take-over-email-accounts/

• baseStriker attack technique allow to bypass Microsoft Office 365 anti-phishing filter

• Fake Invoices: Why Does Office 365 Keep Missing These Phishing Attacks?

• ZeroFont Phishing: Manipulating Font Size to Get Past Office 365 Security
  – https://www.avanan.com/resources/zerofont-phishing-attack
References:

- BC Office of information security
  - http://www.gov.bc.ca/informationsecurity
- VanSecSig
  - http://www.infosecbc.org/events/
- AGORA: http://gallery.mailchimp.com/771fca6487cf0869f0a463e92/files/Agora_Acknowledgement.pdf
- SecureWorld Expo Seattle Nov13-14, 2019
  - https://www.secureworldexpo.com/
- UBC Cybersecurity Summit: http://konstantin.beznosov.net/professional/
- UK National Cyber Security Centre: https://www.ncsc.gov.uk/
What is your company doing?

• Thank You
Defence Strategy

Cybersecurity Operations Tool Suite:

- **Threat Hunting** – Threat intelligence from the security ecosystems community. Monitoring known bad URLs as they evolve.
- **Security focused SIEM and EDR** - integrates A/D and strong user/machine based analytics (UBA, UEBA, ABA).
- **Anti-phishing** – Scans outbound email, Leverages AI, Integrates with FireEye Email Security.
- **Log Correlation** – to reduce Events per Second Cost.
- **Verification** - Test the effectiveness of our controls.

Defense in “Mesh”
The following slides are not intended as an endorsement for any particular product nor should in be considered a benchmark evaluation of the performance of any specific product. The performance results of your implementation will vary based on many factors within your company’s IT ecosystem.
Helix Security Operations Platform

**Network Security & Cloud MVX:**
- Automated Inline Blocking
- Multi-stage & Multi-Vector Detection
- Broad Coverage (Windows, OSX, many OS/file/app permutations)
- **SmartVision:** Protects from threats moving laterally within the network
  - Reduces the time to detection
  - Helps minimize risk of data theft
  - Helps reduce the spread of malware throughout the network

**Cloud Email Security:**
- Correlation of stopped email-borne threats and attacks across environment
- Enhanced detection and alert fidelity
- Intelligence and rule books
- Alert prioritization
- Contextual intelligence
- Investigative tools

**Endpoint Security:**
- EDR + EPP Capabilities; single agent
- Automated threat indicator sharing and context from Email & Network platforms
- Investigative tools and rapid remote containment for endpoints, even when outside of the enterprise
- Validate and analyze network traffic alerts
- Rapid interrogation of all endpoints
insightIDR

• Detect stealthy behavior behind breaches.

• Key Features:
  – User Behavior Analytics (UBA)
  – Attacker Behavior Analytics (ABA)
  – Endpoint Detection and Visibility (EDR)
  – Centralized Log Management
  – Visual Investigation Timeline
  – Deception Technology
Elastic Search

- Log collection/filtration to reduce Events per Second (EPS) cost
- Endpoint log collection
- Collection of O365 audit logs making them much more searchable
- Reduce the number of logging systems within the City. Reducing overall cost for the City.
Avanan Anti-phishing solution

• Scans **outbound** email looking for phishing from compromised internal accounts
• Scans inbound mail like everyone else
• Incorporates with FireEye
1. Incoming email from Internet reaches FireEye Email Security Cloud.

2. FireEye Email Security Cloud analyzes email, quarantines malicious emails, and alerts admin.

3. Safe emails forwarded to customer MTA for end user delivery.

4. Admin can manage alerts/release emails via the FireEye Email Security Cloud portal.
6 Cyber Attacks Business Networks will Face in 2018

1. **Malware**
   - A malicious program installed on a PC, i.e., Trojans, worms, or adware.
   - 18% come from clicking malicious links in emails.

2. **Phishing**
   - Uses social engineering to learn a user's password or personal data.

3. **Brute Force Password Attacks**
   - A computer tries every possible combination for a password until successful.

4. **Denial of Service (DoS) Attacks**
   - Overwhelms the network or servers with high volumes of traffic which disrupts all services.

5. **Man in the Middle (MITM) Attacks**
   - The hardest to find. Pretends to be the destination for the information, copies it all, and then passes the information on to the real destination.

6. **Rogue Software**
   - Installs itself to do something that wasn't originally intended, often posing as something beneficial, like security software or a movie player.

**Cyber Attacks by the Numbers**

- 43% of cyber attacks target small businesses.
- 64% of companies have experienced web-based attacks.
- 62% experienced phishing & social engineering attacks.
- 59% of companies experienced malicious code.
- 51% experienced denial of service attacks.

*Statistics courtesy of www.itspmagazine.com*