Advanced Security Threats
Some important principles

Digital crime is a massive multinational industry, which is constantly “innovating”

Aiming for more security than your organization needs generally makes you less safe

Perfect security is neither possible nor desirable

Security is a core element of your organizational mission
What are folks most worried about?
**Custom Attacks**
- Politically-motivated attacks
- Attacks on specific infrastructure
- Often leverage extensive organizational profiling and/or insider information

**Templatized attacks**
- Attacks follow predictable patterns, but leverage organization-specific details
- Often “sent by” ED of organization
- Financial spearphishing

**Low-effort/low-skill generic attacks**
- Non-targeted phishing
- Crypto malware / ransomware
Phishing / Business Email Compromise

Perhaps the most common attack targeting non-profits at the moment

Attacks range in sophistication from generic mass mailings to highly-tailored schemes incorporating significant background research on the target organization (including names of leadership team; watering holes that staff tend to frequent, etc.)

Attacks often involve burner email accounts set up solely for the purpose of facilitating this attack. More sophisticated attackers will set up email address(es) that incorporate organizational info

Phishing emails increasingly come from valid accounts that traditional spam checking won’t flag, courtesy of either clever SPF bypass tricks or true compromise of a trusted contact
From: Administrators Team [mailto:ms-ompro@mssimple.apcprd01.prdechangepe11.net]
Sent: Thursday, September 27, 2018 7:16 AM
To: HealthEquityValue <HealthEquityValue@
Subject: Account Verification

Hi HealthEquityValue

Your account of healthequityvalue@ will be disconnected from sending or receiving mails from other users because you failed to resolve errors on your mail.

Please resolve now

Regards,
Microsoft Security Team
Hi scheduling@techimpact.org

You Have a New Voice Message
From: WIRELESS CALLER (317) 696-0438
Received: Wednesday, August 26, 2018 at 03:20 PM
Length: 00:13
To: scheduling@techimpact.org

Play Voicemail <https://tanyurl.com/ylmgc4yp?z=++%db%4b%4b%>

Microsoft VMS 🎧🎧

Please consider the environment before printing this.
You have a secure document via One Drive pending your signature.

View File <https://1drv.ms/w/s!Att1_hAx49Emg2K7_DUwhFoI3NvM>

Your document is ready for download.

If you are having trouble signing the document, please visit the Help with Signing page on our Support Center.


Virus-free, www.aviq.com <https://1drv.ms/w/s!Att1_hAx49Emg2K7_DUwhFoI3NvM>
Step 1: Identify a Target
Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Step 2: Grooming
Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).
Perpetrators use persuasion and pressure to manipulate and exploit human nature.
Grooming may occur over a few days or weeks.

Step 3: Exchange of Information
The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4: Wire Transfer
Upon transfer, the funds are steered to a bank account controlled by the organized crime group.

*Note: Perpetrators may continue to groom the victim into transferring more funds.

Source: FBI
<table>
<thead>
<tr>
<th>Phishing Defenses</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Threat Protection anti-phishing rules</td>
<td></td>
</tr>
<tr>
<td>Mail processing rules that look for inconsistencies and flag them</td>
<td></td>
</tr>
<tr>
<td>Remove staff email address from your website</td>
<td></td>
</tr>
<tr>
<td>DKIM enforcement</td>
<td></td>
</tr>
<tr>
<td>Security training (Wombat / KnowBe4)</td>
<td></td>
</tr>
</tbody>
</table>
Core infrastructure spoofing attack

Often powered by standardized attack toolkits which are bought and sold as commodities

Can be installed on any compromised webserver (especially Wordpress / Drupal)

Attacks often leverage corporate branding, trusted service providers, link shorteners, other dirty tricks
Hi info@twoten.org,

Attention: info@twoten.org. We detected you have [6] undelivered incoming emails on 21-Aug-2018. This is because your account storage is full. Your action is required for them to be delivered.

Kindly follow the self-service instructions below to rectify the issue:

Release pending messages to inbox

Source: info@twoten.org Office365 Support.
Enter password

Because you're accessing sensitive info, you need to verify your password

Your account or password is incorrect. Try Again.

Password

Sign In

Forgot Password
<table>
<thead>
<tr>
<th>Infrastructure spoofing defenses</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Multi Factor Authentication</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Suspicious login monitoring and alerting</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Endpoint DNS defenses, to prevent PCs from accessing attack domains</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Password managers and/or certificate pinning utilities that flag when a site isn’t what it claims to be</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Security Training (Wombat / KnowBe4)</th>
</tr>
</thead>
</table>
Crypto ransomware

Searches PCs for any files that look like user-generated data, puts those files into an encrypted zip archive, and deletes the originals.

Often employed by more sophisticated groups with specific agendas, targeting larger organizations.

Especially in these situations, the crypto ransomware can be outfitted with self-replication capabilities, enabling it to infect an entire network.
Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don’t pay in 7 days, you won’t be able to recover your files forever.
We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address: [Address]
Atlanta Working 'Around The Clock' To Fight Off Ransomware Attack

March 27, 2018 - 7:47 AM ET

DOREEN MOCALISTER

AT&T Live

Atlanta's Computers Held Hostage, With A $50K Ransom

Now

NEWSCASTER: JENN GIDMAN

Atlanta is being held hostage, by computer hackers who want more than $50,000 in bitcoin to stop their siege. "This is much bigger than a ransomware attack, this really is an attack on our government," Mayor Keisha Lance Bottoms said at a Monday presser about the e-attack, per Reuters, adding, "We are dealing with a [hostage] situation." Bitcoinist reports the hack began Thursday morning, and it has taken down Atlanta's online bill payment system from some remote location, says Bottoms, who's staying mum over whether the ransom will be paid.

(Bitcoinist notes, however, the city has "no plans" to pay up.) The FBI, Homeland Security, Cisco, and Microsoft are all teaming up to help the city figure out what data has been breached and what steps to take next in what Bottoms has deemed a "massive inconvenience," reports ABC News.
<table>
<thead>
<tr>
<th>Crypto Ransomware Defenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily backups</td>
</tr>
<tr>
<td>Move all critical data off of self-hosted servers</td>
</tr>
<tr>
<td>Centrally-managed software updates and antivirus</td>
</tr>
<tr>
<td>High-grade Deep Packet Inspection</td>
</tr>
<tr>
<td>High-grade email security, such as Advanced Threat Protection, Barracuda, etc.</td>
</tr>
</tbody>
</table>
Domain squatting

Buying domain names that are “adjacent” to the target domain of Interest

Can be based on likely typos, different domain suffixes, common misspellings, etc.

Can be used to divert visitor traffic, publish misinformation, or for simple extortion

Famously, in 2001 Peta.org was purchased by a troll claiming to be the founder of “People Eating Tasty Animals”
Windows 10 PC Repair

System Information:
Your machine is currently running Windows 10
Reimage Repair is compatible with your operating system

Download Time: Under 1 minute
Manufacturer: Reimage
Designed for: Windows XP, Vista, 7, 8, 8.1 & 10

Start Download

Download the PC Repair Utility to scan and identify Windows Errors on Windows 10.
Update your PC and eliminate potential threats:
- Scan your PC for Windows errors with 1 click
- Remove Viruses and repair damage caused
- Eliminate all Malware from your PC

Step 1
Click "Run" or "Save" button when dialog appears

Step 2
Scan your PC for Free with one click!
Most DNS registrar accounts are not well-secured

Few organizations have Registrar Lock directives in place with

Making changes to DNS records is often sufficient to “prove” ownership of a website or cloud services account

Many organizations don’t even have direct admin control over their own DNS records!
<table>
<thead>
<tr>
<th>DNS Defenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registrar locks</td>
</tr>
<tr>
<td>Multi Factor Authentication for DNS Registrar admin login</td>
</tr>
<tr>
<td>Auto-renewal</td>
</tr>
<tr>
<td>Endpoint DNS protection (eg Cisco Umbrella)</td>
</tr>
</tbody>
</table>
A number of core Internet technologies can be used to **amplify** and **reflect** small amounts of specially-crafted attack traffic, resulting in the bombardment of the target(s) with tens to hundreds of times the initial volume of data.

| Router protocols such as NTP and DNS are the most common targets | Any UDP protocol is theoretically susceptible |

Only organizations with sophisticated adversaries are likely to be targeted by one of these attacks – but anyone with publicly-exposed infrastructure could be enlisted into one of them.

**Botnet / DDoS**
DDoS / Botnet Defenses

Centrally-managed antivirus and software update engine

Infrastructure penetration testing

If you think you might be a target of the attacks themselves: put all of your web assets behind Cloudflare
Watering Hole Attacks
Rather than attacking a target directly, attack a commonly-used resource hub that’s easier to compromise.

Sites that are compromised are often chosen based on extensive research / surveillance of target populations’ behaviors, and often involve more than one site.

Forbes.com’s “Quote of the Day” was hijacked in 2015, with the end goal of attacking visitors from financial and defense firms.
<table>
<thead>
<tr>
<th>Evil Maid Defenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Training</td>
</tr>
<tr>
<td>Script blockers</td>
</tr>
<tr>
<td>System segmentation for sensitive resources</td>
</tr>
<tr>
<td>Virtualization</td>
</tr>
</tbody>
</table>
Side-channel exploits
Side-Channel Attacks

Physical proximity to devices allows for a much wider range of attacks

Spectre & Meltdown

We haven’t seen the last of these attacks yet

Monitoring subtle side-effects of operations involving private data to partially or fully expose that data

Monitoring electrical noise and/or power fluctuations emitted by CPU during cryptographic operations to expose private keys
## Side-Channel Defenses

- Centrally managed software updates

- Rigorous policies for applying firmware upgrades to both endpoint devices and critical network infrastructure (i.e., all devices should be checked for available firmware updates on a quarterly basis)

- Policies limiting what kinds of materials can be accessed on mobile devices

- Policies limiting locations in which people can work on sensitive information
Evil Maid

Any attack that can be performed by a malicious party with physical access to a device

Cold boot attacks

ROM tampering

Bottom line: physical access + motivation + skill = GAME OVER
<table>
<thead>
<tr>
<th>Evil Maid Defenses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Escort polices for office guests</strong></td>
</tr>
<tr>
<td><strong>Machines storing highly sensitive limits should be physically locked up, with all ports rendered inaccessible</strong></td>
</tr>
<tr>
<td><strong>Policies limiting what kinds of materials can be accessed on mobile devices</strong></td>
</tr>
<tr>
<td><strong>Policies limiting locations in which people can work on sensitive information</strong></td>
</tr>
<tr>
<td><strong>Policies mandating that devices containing sensitive information be turned off, not put to sleep</strong></td>
</tr>
</tbody>
</table>
Man-In-The-Middle
<table>
<thead>
<tr>
<th>Man-in-the-Middle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Point compromise</td>
</tr>
<tr>
<td>Certificate theft and/or bogus issuance – often coupled with domain squatting techniques</td>
</tr>
<tr>
<td>Installing trusted certificate on local devices</td>
</tr>
<tr>
<td>SSL stripping</td>
</tr>
</tbody>
</table>
Man-in-the-Middle Defenses

- Policies mandating the use of VPN tools on all untrusted networks
- Centrally-managed antivirus and software updates
- Policies limiting locations in which people can work on sensitive information
<table>
<thead>
<tr>
<th>Mobile phone identity theft</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phone numbers have become digital IDs and means for verifying those identities</strong></td>
</tr>
<tr>
<td>Foiling MFA defenses (e.g., Reddit)</td>
</tr>
<tr>
<td>Confirmation for password resets</td>
</tr>
<tr>
<td>3rd-party billing fraud</td>
</tr>
</tbody>
</table>
Mobile Phone Identity Defenses

- Treat your mobile phone number like a Social Security number
- Carrier PINs
- Disable 3rd-party billing
- Google Voice redirection
Threats on the Horizon

- Further refinement and professionalization of high-volume phishing attack toolkits
- Crypto ransomware that specifically targets cloud infrastructure
- More creative and destructive post-breach protocols
- Crypto mining malware
- Using more legitimate sites as part of attack
- More phone number attacks
What did I miss? Any favorite horror stories?
Thanks – and good luck out there!

jordan@techimpact.org