

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?



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



♀ Reply ♀ Reply All ♀ Forward ♀ IM



VOICEMAIL <pendingvoicemail_noreply@simermeyer.onmicrosoft.com>

Scheduling

Wmv received from (8328990209) (8328990209)

Retention Policy Junk Email (30 days)

Expires 10/26/2018

This item will expire in 25 days. To keep this item longer apply a different Retention Policy. Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox. This message was marked as spam using a junk filter other than the Outlook Junk Email filter. We converted this message into plain text format.

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://tinyurl.com/y8mqcdyp??==++%4b%4b%4b%>>

Microsoft VMS 🎵 🗍

Please consider the environment before printing this.

Reply Reply All Sorward Star ADMIN <accountpayable@lakelandrx.com> O no_user@admin.com Wed 9/26 Successfully Payment Confirmation -Wednesday, September 26, 2018 Expires 10/26/2018 Retention Policy Junk Email (30 days) This item will expire in 25 days. To keep this item longer apply a different Retention Policy. Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox. This message was marked as spam using a junk filter other than the Outlook Junk Email filter. This message was sent with High importance. \sim You have a secure document via One Drive pending your signature. View File <https://1drv.ms/w/s!Att1 hAx49EmgzK7 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.

<http://www.avg.com/email-signature?utm_medium=email&utm_source=link&utm_campaign=sig-email&utm_content=webmail>

Virus-free. www.avg.com <https://ldrv.ms/w/s!Att1 hAx49EmgzK7 DUwhFoi3NvM>

Step 1: Identify a Target

REPOR



Step 2:

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.







The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.



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

nation available op a profile on d its executives. Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

identified in the finance department).

Grooming may occur over a few days or weeks.

Phishing Defenses

Advanced Threat Protection antiphishing rules

Mail processing rules that look for inconsistencies and flag them

Remove staff email address from your website

DKIM enforcement

Security training (Wombat / KnowBe4) 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

RE: You have 6 Incoming Messages

MICROSOFT

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

Microsoft respects your privacy. Please read our online <u>Privacy Statement</u>. MicrosoftCorporation, One Microsoft Way, Redmond, WA 98052 Send us <u>feedback</u>.





info@twoten.org

8

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



Infrastructure spoofing defenses

Multi Factor Authentication

Suspicious login monitoring and alerting

Endpoint DNS defenses, to prevent PCs from accessing attack domains

Password managers and/or certificate pinning utilities that flag when a site isn't what it claims to be

Security Training (Wombat / KnowBe4)

Crypto ransomware

Searches PCs for any files that look like usergenerated 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 selfreplication capabilities, enabling it to infect an entire network





Mayor Keisha Lance Bottoms speaks at a press conference in Atlanta ir David Goldman/AP

Officials in Atlanta say the city's computer systems a ransomware attack hit the city last week and locked encryption.

Tasnim Shamma of member station WABE in Atlan cybersecurity experts are working around the clock

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

NOW NEWSER BY 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 [cyberhostage] 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.

Atlanta still feeling the effects of ransomware cyberattack

1

DAVID GOLDMAN/ASSOCIATED PRESS

ongoing troubles caused by a cyberattack.

ork last week.

ty continues to operate despite ongoing troubles

ty's computer network had been attacked by

Crypto Ransomware Defenses

Daily backups

Move all critical data off of self-hosted servers

Centrally-managed software updates and antivirus

High-grade Deep Packet Inspection

High-grade email security, such as Advanced Threat Protection, Barracuda, etc.

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"

goooogle.com

Reimage Repair

Windows 10 PC Repair



System Information: Your machine is currently running: Windows 10

Reimage Repair is compatible with your operating system

Start Download

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

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







ussaa.com



PSA: DNS Security is a Big Deal

Most DNS registrar accounts are not wellsecured

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!

DNS Defenses

Registrar locks

Multi Factor Authentication for DNS Registrar admin login

Auto-renewal

Endpoint DNS protection (eg Cisco Umbrella)

Botnet / DDoS

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

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

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

Evil Maid Defenses

Security Training

Script blockers

System segmentation for sensitive resources

Virtualization

Side-channel exploits



SPECTRE

Side-Channel Attacks 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

Spectre & Meltdown

We haven't seen the last of these attacks yet

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



Side-Channel Defenses

Centrally managed software updates

Rigorous policies for applying firmware upgrades to both endpoint devices and critical network infrastructure (ie, 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



Evil Maid Defenses

Escort polices for office guests

Machines storing highly sensitive limits should be physically locked up, with all ports rendered inaccessible

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

Policies limiting locations in which people can work on sensitive information

Policies mandating that devices containing sensitive information be turned off, not put to sleep

Man-In-The-Middle



Man-in-the-Middle

Access Point compromise

Certificate theft and/or bogus issuance – often coupled with domain squatting techniques

Installing trusted certificate on local devices

SSL stripping

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 Mobile phone identity theft Phone numbers have become digital IDs and means for verifying those identities

Foiling MFA defenses (eg, Reddit)

Confirmation for password resets

3rd-party billing fraud

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 highvolume 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