Home Is Where The Hack Is:

Attacks & Defenses for a Workforce Quarantined at Home

Jason Nickola
Jason@pulsarsecurity.com

Tim Connell
tim@pulsarsecurity.com

PULSAR SECURITY

HOME IS WHERE THE HACK IS

Jason Nickola – COO, Senior Security Consultant

- Hacker who likes building teams, culture
- GIAC Security Expert (GSE) & Offensive Security Expert (OSCE)
- SANS instructor for Penetration Testing & Ethical Hacking
- 'Trust Me, I'm Certified' podcast host
- Tech and security opportunities to anyone I can
  - TechRamp nonprofit
  - NHTA Workforce Development Committee
  - BSidesNH Conference

Tim Connell – Head of Enterprise Products, Security Consultant

- 10 years experience in sales, marketing and product development for early stage technology companies
- Hold Certifications as an OSCP, GIAC 4x and CompTIA 2x
- Play the role of business professional during the day and cyber security professional at night from 10pm-2am, or when my two daughters and wife let me :)

PULSAR SECURITY

HOME IS WHERE THE HACK IS

The stats – before the pandemic

- Organized crime with a financial motive is still most the common threat actor
- Business email compromise three times more lucrative at median than computer data breach
- Phishing and use of stolen credentials #1 and #2 actions associated with a breach
- 94% of all malware delivered via email

The stats – during the pandemic

- RiskIQ analyzed its spam box feed for the time period of 04/03/2020-04/06/2020.
  - **262,902** spam emails containing either "*corona*" or "*covid*" in the subject line
  - **6,835** unique subject lines
  - **3,887** unique sending email domains and **10,242** unique IP Addresses
  - **1,532** emails sent an executable file for Windows machines.

Source: 2019 Verizon Data Breach Investigations Report (https://enterprise.verizon.com/resources/reports/dbir/)

Source: Investigate | COVID-19 Cybercrime Daily Update(https://www.riskiq.com/blog/analyst/covid19-cybercrime-update/)

PULSAR SECURITY

HOME IS WHERE THE HACK IS

Most Businesses Didn't Anticipate Mandated WFH

- Misconfigurations and poor planning for legitimate access to corporate resources remotely creates risk
- Hackers and opportunistic vendors preying on fear
    - Cheap devices and software with vulnerabilities(malicious or mistakes)
    - Phishing under the guise of helping or informing
- Employee home networks have become a more attractive target
    - Most are not doing anything to secure their home networks and personal devices
        - Now a more concentrated source of risk for organizational assets
    - How many vulnerability assessments have you run on your employee's home network?

PULSAR SECURITY

HOME IS WHERE THE HACK IS

Accessing Corporate Resources

- Easy to get this wrong, especially with hasty transitions
- Directly connecting services (file shares, RDP & SSH, etc.) is easy but a largely terrible idea
- WannaCry (2017) exploited file sharing (SMBv1) connected to the public internet.
  - 1/3 of all corporate networks are supporting Windows XP, which has SMBv1 enabled by default
  - Three years later, we certainly aren't connecting SMB to the public internet anymore, right?

PULSAR SECURITY

HOME IS WHERE THE HACK IS

PULSAR SECURITY

HOME IS WHERE THE HACK IS

VPN

- A few key benefits:
  - Protects your traffic from sniffing
  - Multiple services to be exposed behind a single connection, rather than a hole at the edge for each service
  - **Great choke point for monitoring and securing the network, too**
- Can be annoying to manage and use as an end user, but is necessary
- But not a panacea:
  - VPN services can have their own vulnerabilities and misconfigurations, too
  - When compromised, an attacker can typically access anything the user can…

PULSAR SECURITY

HOME IS WHERE THE HACK IS

Home Networks as a Gateway to Corporate Assets

- Phishing to harvest credentials or exploit devices
  - Malicious intent hidden behind the "Save" or "Submit" link
- It's not just ransomware or capturing login credentials
  - Invasion of privacy via keylogger, screen grab, audio and video, clipboard, etc.
- Attacking home wireless networks
  - Wigle, sniffing traffic, cracking wireless passwords, Wifi Pineapple, etc.
- Once home network and devices are owned, attackers can use legitimate accounts and apps to access corporate environment
  - Difficult to detect without mature monitoring, behavioral & geographical analytics, etc.

PULSAR SECURITY

Videoconferencing and Recent Zoom Developments

- Zoom has received a lot of attention due to recent research and high-profile incidents
  - Some mistakes and sloppy practices, but not unique to Zoom
- Don't look for the service that doesn't have any issues
  - Really just means no one is looking
  - Pay more attention to response, patching, and trending approach to security
- "Zoom Bombing" and "hacking" are really just trolling due to misconfiguration
  - Take the time to research and learn how to use the product
  - Follow best-practice guidance from vendor and trusted third parties

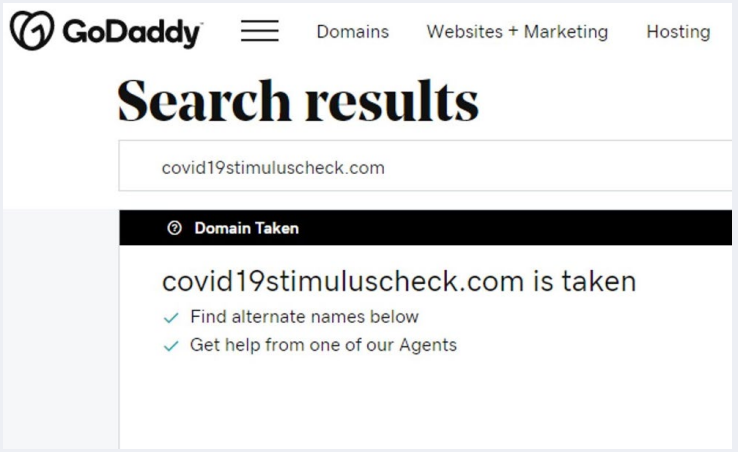
HOME IS WHERE THE HACK IS

PULSAR SECURITY

HOME IS WHERE THE HACK IS

Fear and Scarcity Creates Opportunity

- Malicious domains and sites created posing as pandemic help / resources
- Increase in phishing activity taking advantage of FUD, both health and economic
- Entire world working from home? Gonna need a webcam...
  - "Good" ones are all sold out or price gouged
  - Many "cheap" alternatives suddenly available
  - Should you trust these brands? How do you know what the device actually does?
    - Can easily be backdoored or vulnerable thanks to sloppy code or poor hardware
- Buy from trusted brands, and make sure default configurations are hardened to limit attacking surface



Simulated Phishing Attack
& Compromise

DEMO

PULSAR SECURITY

HOME IS WHERE THE HACK IS

Defenses: Great Account/Password Practices

- Use a password manager
  - The best password is one you can't remember (and don't need to)
  - LastPass, DashLane, 1Password, etc.
- Long passphrases when you can't use a password manager
  - 'a long time ago in a galaxy far, far away' is better than Spring2020$
- Turn on Multi-Factor Authentication wherever you can
  - Severely limits the ability for your password to be guessed or used when found via a breach dump

PULSAR SECURITY

HOME IS WHERE THE HACK IS

Defenses: Patching

- Not news to most, even if you are not an IT or security professional
  - A vendor's vulnerability fix doesn't protect you if you don't apply the patch…
- Automatically applying patches is safe for most home environments
  - Some devices – modems and WiFi access points especially – don't offer great support
- Some devices require more complicated processes for applying updates
  - Especially device firmware
  - Best to have a trusted resource (more on this in a minute) to help if you are unsure of the process

PULSAR SECURITY

HOME IS WHERE THE HACK IS

Defenses: Secure Configuration

- Lots of devices come with insecure defaults
- Even secure configurations can change over time as a result of troubleshooting or mistakes
- Hardening guides, if you are up for the challenge
    - NIST, Center for Internet Security, etc.
    - Another area where trusted advisors helps
- In general, turn off everything you don't actively use
    - "Reduce the attack surface"
    - Universal Plug n' Play and WPS are high-value
    - Most home networks don't need anything to be allowed in from the public internet
    - Another great spot for a trusted advisor to help with

PULSAR SECURITY

HOME IS WHERE THE HACK IS

Defenses: Stick to Trusted Sites, Vendors

- You don't need work-from-home tips from that site you've never heard of
  - Major news media, government, and well-known private entities are the safest bet
    - Have lots of their own issues, but are not (usually) trying to hack you
- The $10 webcam is cheap for a reason
  - Popular brands and products are typically subject to more vetting and review
  - Remember this if you have a hand in purchasing or setting expense policies
- The IRS is not emailing you to threaten jail
- That link from the alternative medicine Facebook group is not going to show you how to self-vaccinate

PULSAR SECURITY

HOME IS WHERE THE HACK IS

Defenses: Support Your Employees

- Hyper concentrated at the moment, but work from home is not new and isn't going away
- Orgs must evolve and offer more resources to help employees configure and secure personal resources
    - Difficult to mandate, but typically well-received where we've seen it
- Help with configuration, patching, security best-practice review, and whatever else you can do
    - Fill their need for a trusted advisor
- Shedding responsibility at your firewall doesn't make you more secure, it just means you don't know the ways in which you are not

THANKS!

PULSAR SECURITY

www.pulsarsecurity.com

tim@pulsarsecurity.com
jason@pulsarsecurity.com