Identifying Cybersecurity Challenges

How to Protect Organizations in a Dynamic Environment

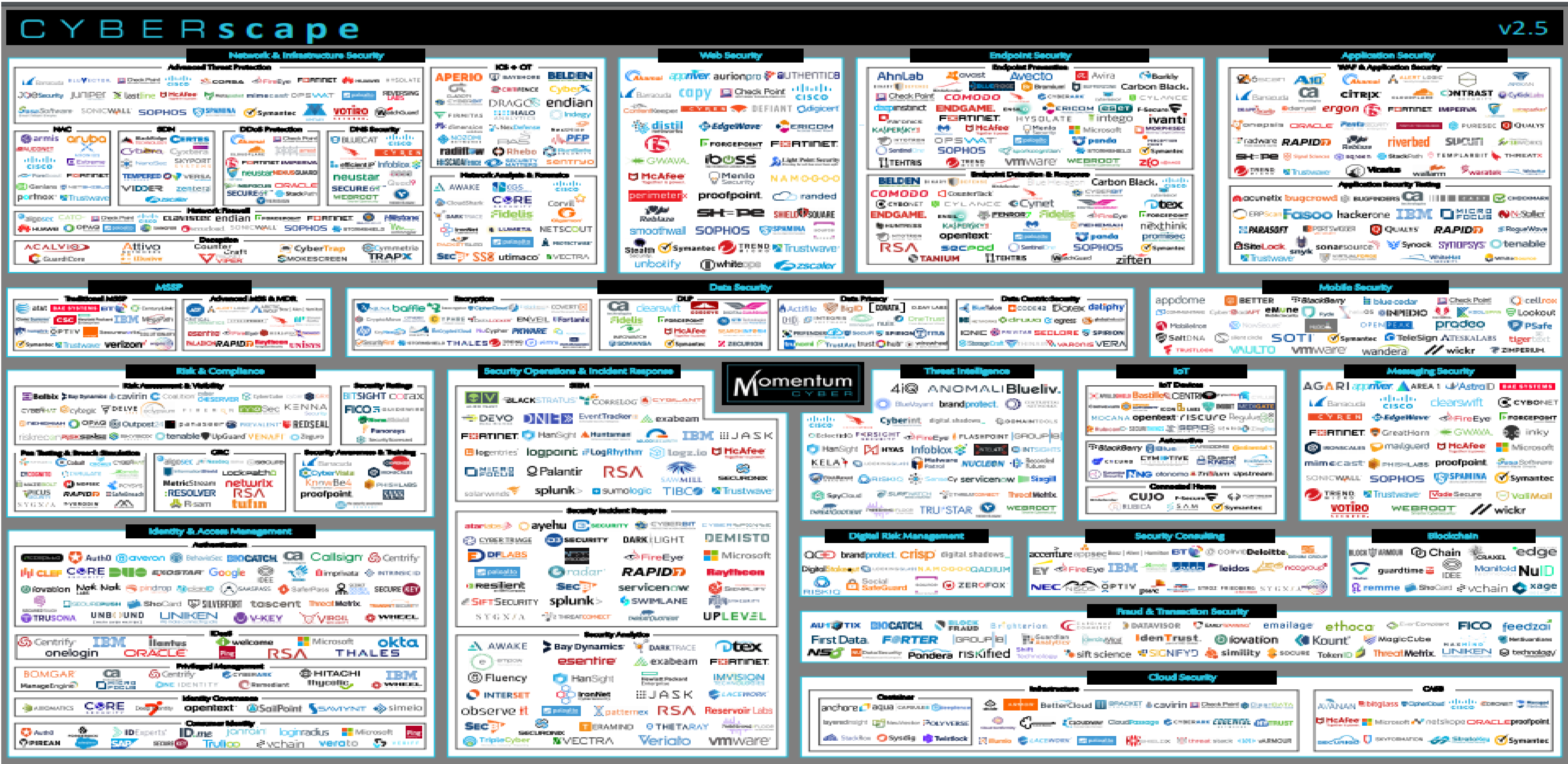
Chris Richmond- Sales Engineering Leader for Canada and Northeast US

Cyber-Security Landscape

What are we really up against?

proofpoint.

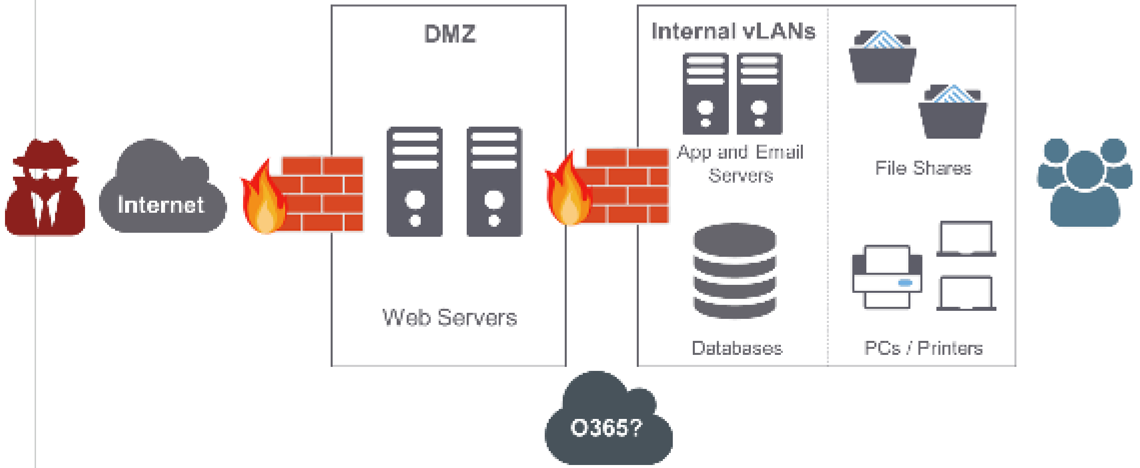
How can they all have the answer?



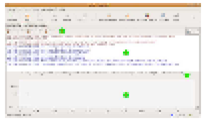
The Real Problem

LEGACY APPROACH

Protect channels, devices, data

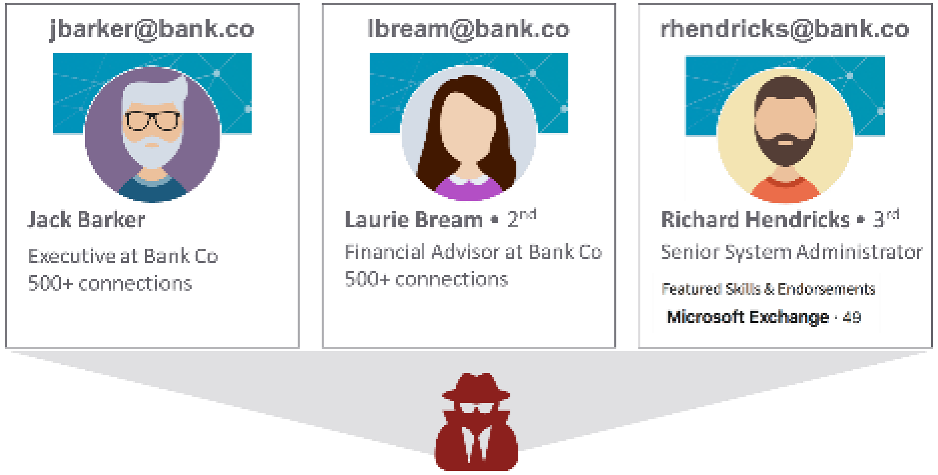


Vulnerability Assessment Tools



CURRENT ATTACKER TACTICS

Target people, across all channels



Vulnerability Assessment Tools

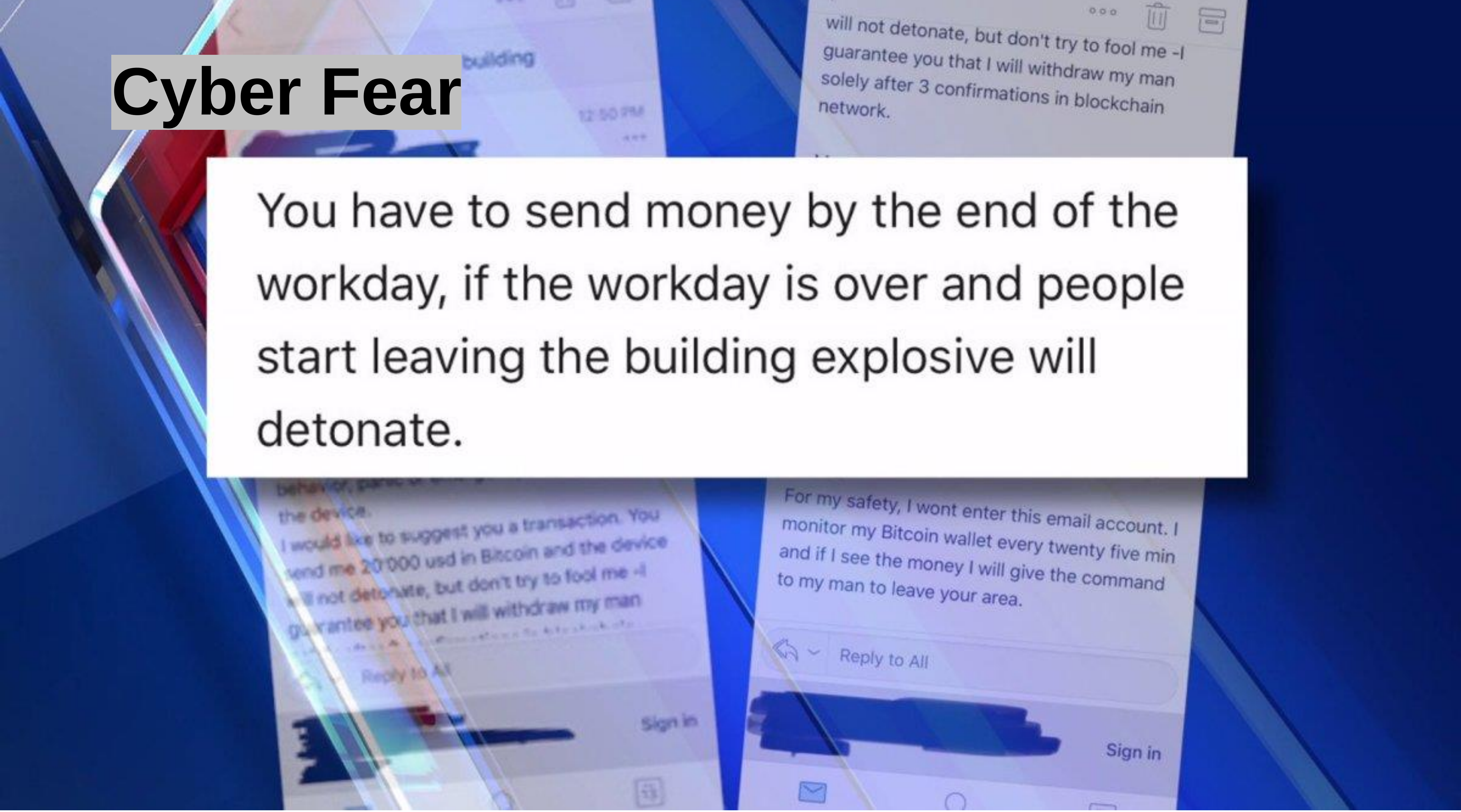
What is the Hacker Motivation?

	Nuisance	Data Theft	Cyber Crime	Hacktivism	Network Attack
Objective	**Access & Propagation**	**Economic, Political Advantage**	**Financial Gain**	**Defamation, Press & Policy**	**Escalation, Destruction**
Example	Botnets & Spam	Advanced Persistent Threat	Ransomware	Data Disclosure	Destroy Critical Infrastructure

Seehotel Jaegerwirt

- Beautiful 4 STAR hotel
- Can pay C$634 per night
- Locked out key function and removed the capability of the hotel to open doors to rooms and make new keys
- Paid Bitcoin 2,367 C$
- It happened 4 times……
- Went back to manual keys ☹

Cyber Fear



You have to send money by the end of the workday, if the workday is over and people start leaving the building explosive will detonate.

will not detonate, but don't try to fool me -I guarantee you that I will withdraw my man solely after 3 confirmations in blockchain network.

behavior, panic or

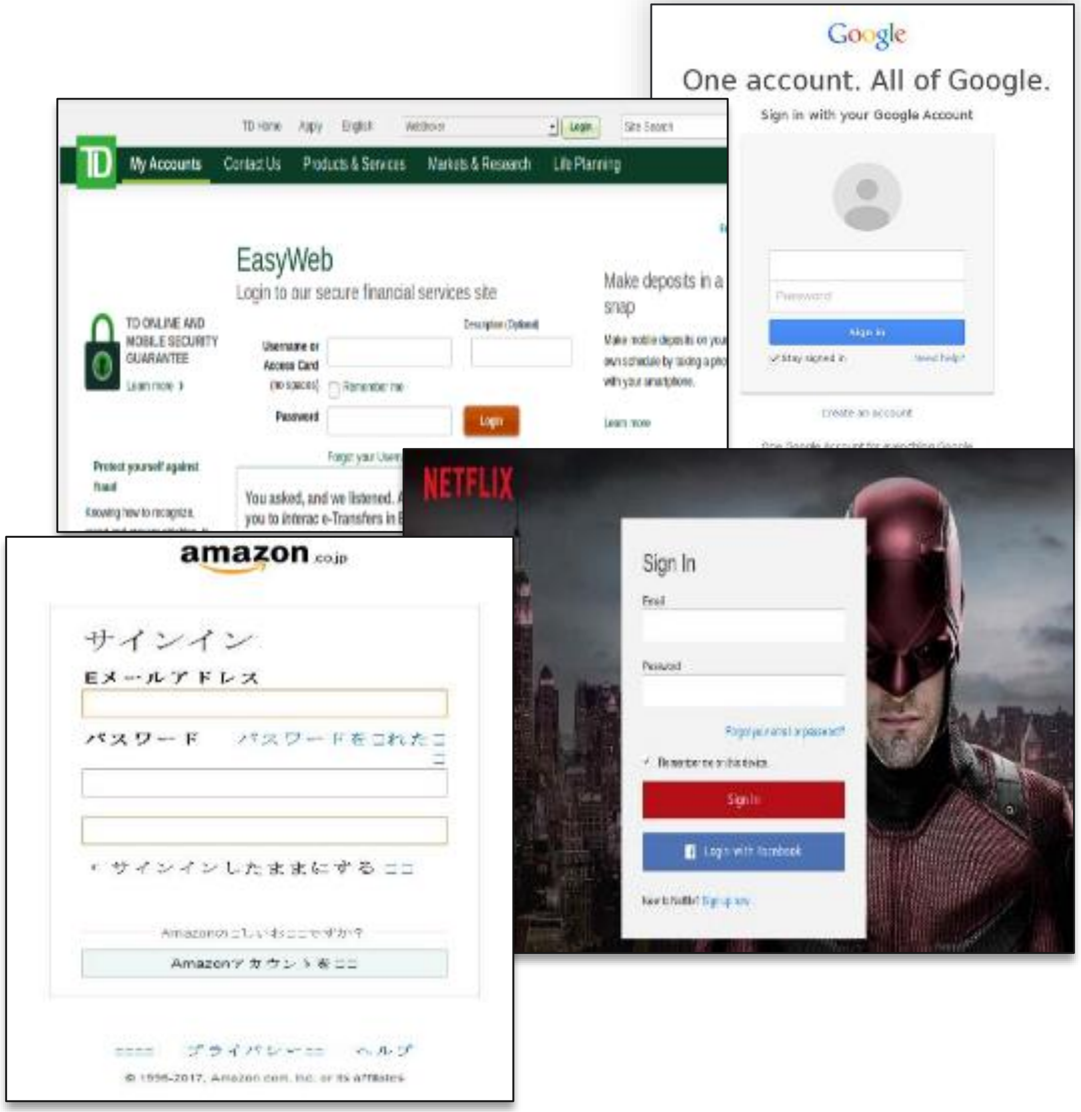
the device.

I would like to suggest you a transaction. You send me 20'000 usd in Bitcoin and the device will not detonate, but don't try to fool me -I guarantee you that I will withdraw my man

For my safety, I wont enter this email account. I monitor my Bitcoin wallet every twenty five min and if I see the money I will give the command to my man to leave your area.

Cred Phishing Always Active

- Increase in phishing of enterprise cloud services
  - *dropbox, box, onedrive, salesforce…*
  - O365 phishing is a major issue
- PDFs containing links
- Not limited to email
  - *SMS, Social, etc.*
- Often the first stage of a larger attack
  - *DNC compromise*
  - *Recon for Impostor phishing*



proofpoint.

Biggest trend: Rising Wave of O365 Attacks

- Significant increase in organized attacks on O365 accounts
- Allows for INTERNAL Social manipulation
- Increasing as the Cloud move becomes larger
- Variety of techniques
  - *Brute-force appears to be the most common initial vector*
  - *Use botnets to scale across many O365 tenants*
  - *Password reuse from mega-breaches*
  - *Phishing*
- Managed Cloud - centralized data for attacker
- Rapidly developing different techniques

Partner Network Exposure

- This is a **HUGE** risk
- Global business demands partner interaction
- Partners are connected to us
- Segmented out
- For how long?
- Why doesn't it have the same level of security as the internet?

Protecting

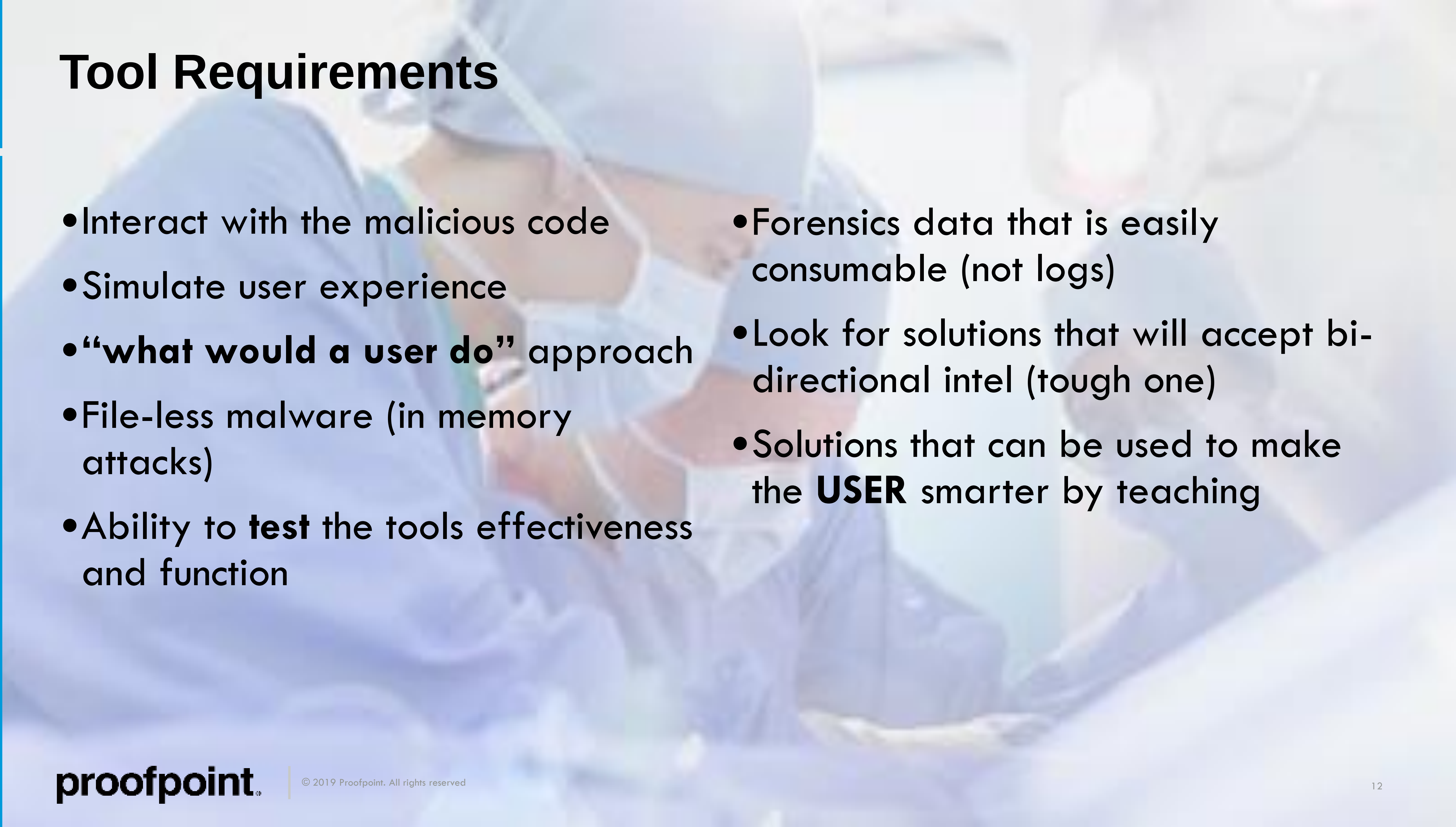
Building Blocks

- Firewall
- Email protection and phishing
- Privileged Access Management
- Patch/Asset mgt tools
- Password management
  - Two factor
- CASB
- DLP network, mail, endpoint
- VPN
- SIEM
- Proxies
- Sandboxing

Encryption/Decryption –data and network

- Endpoint AV, EDR, Advanced Protection
  - DLP, asset mgt, and more
- NAC
- UEAB
- DNS
- Orchestration
- IDS/IPS
- Backups
- Business Continuity
- Packet Capture
- Data classifiers
- Mobile and MDM
- Intel feeds

Tool Requirements



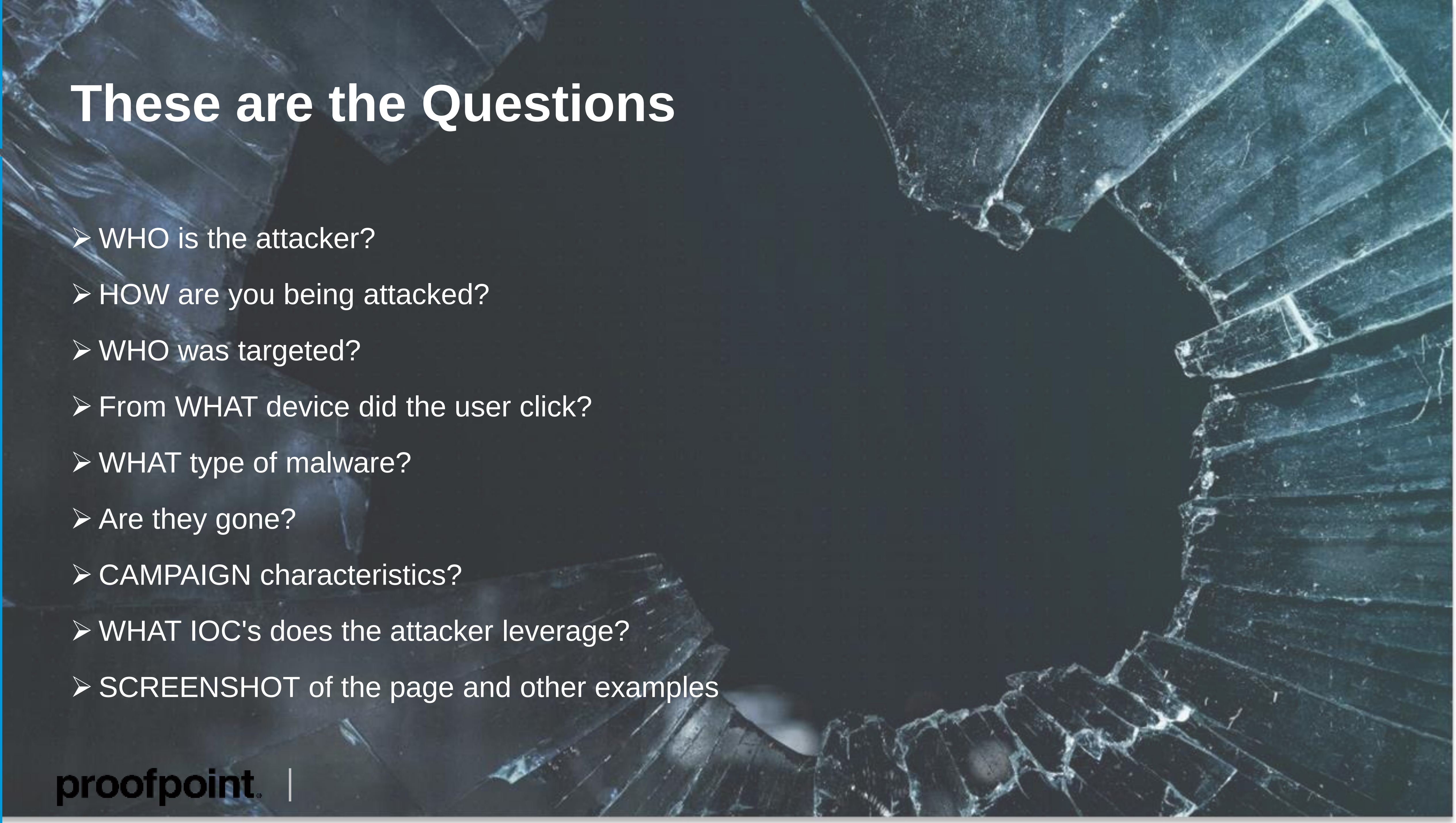
- Interact with the malicious code
- Simulate user experience
- **“what would a user do”** approach
- File-less malware (in memory attacks)
- Ability to **test** the tools effectiveness and function

- Forensics data that is easily consumable (not logs)
- Look for solutions that will accept bi-directional intel (tough one)
- Solutions that can be used to make the **USER** smarter by teaching

Visibility

- **See**
- **Correlate**
- **Validate**
- Find other **IOC’s**
- **Hunt**

These are the Questions



- WHO is the attacker?
- HOW are you being attacked?
- WHO was targeted?
- From WHAT device did the user click?
- WHAT type of malware?
- Are they gone?
- CAMPAIGN characteristics?
- WHAT IOC's does the attacker leverage?
- SCREENSHOT of the page and other examples

So what’s working?

War-time mindset
Acceptance of the new normal

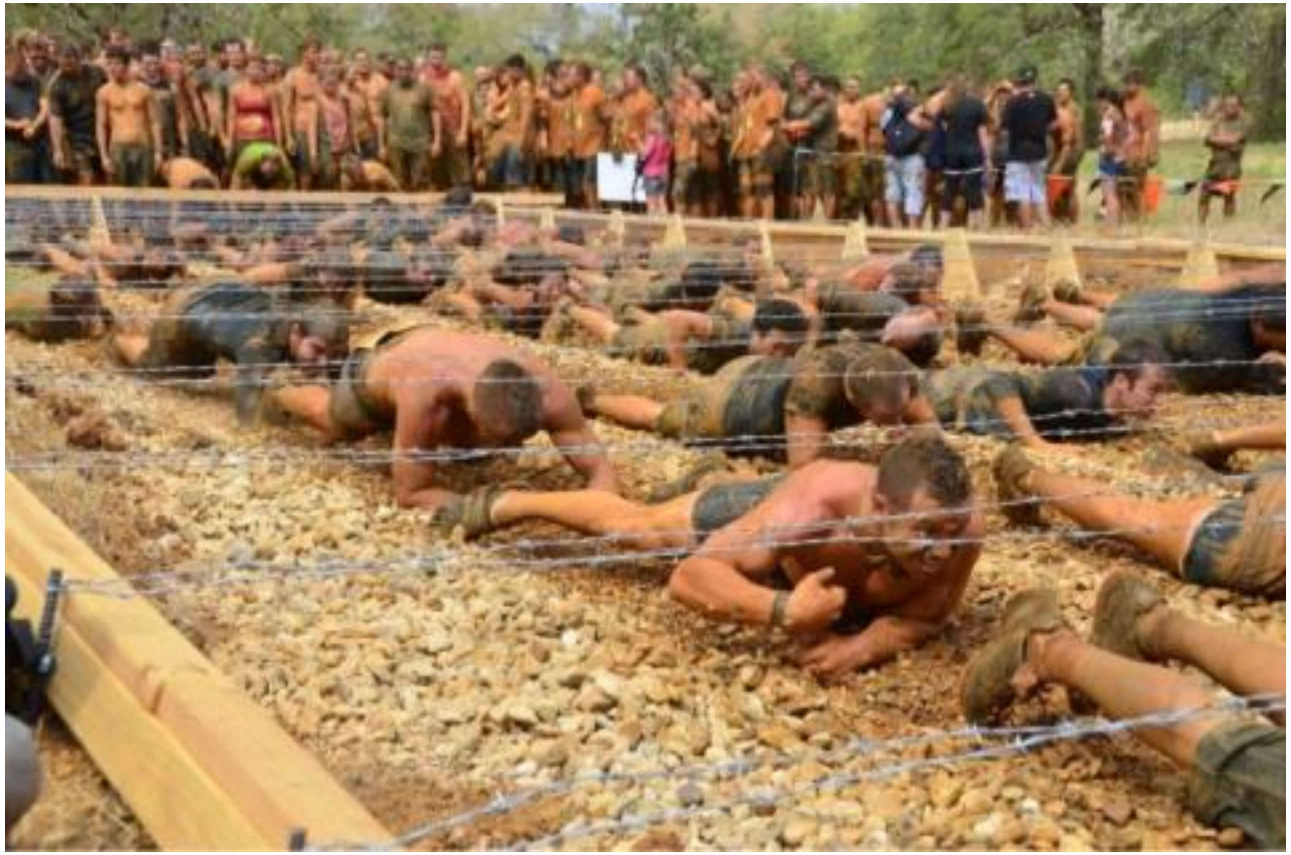
Tools only go so Far
Ensure that staffing can manage tools effectively

Resilience
Ability to operate through the breach

Focus on the basics first

90% of attack come via mail

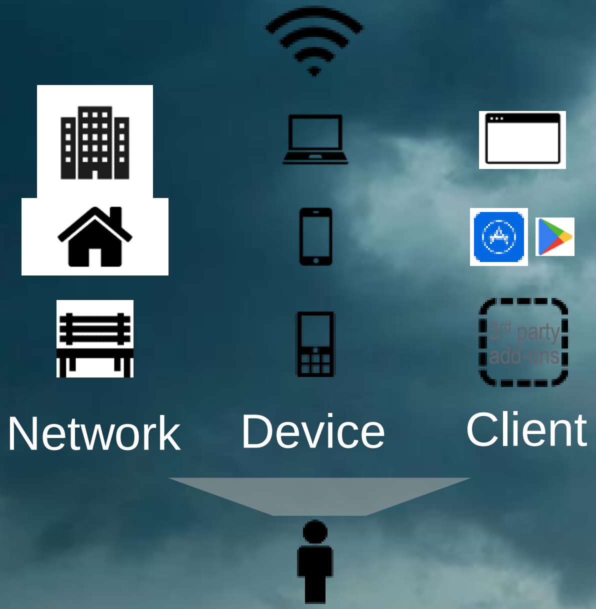
Educating the user
Users must become part of the solution



The Move to the Cloud - It’s Here…..

Office 365 | G Suite | box | amazon web services S3 | Dropbox | salesforce

Email | Collaborate | Share Files
Download & Upload Files | Use external facing portals



Network

Device

Client

Attacks

Mistakes

PCI HIPAA GDPR

Regulations

THANK YOU!

Chris Richmond

917-617-0361

crichmond@Proofpoint.com