DIGITAL HAPKIDO

REDIRECTING THE ATTACKER’S ENERGY

Secure Iowa October 6th , 2021

ANDY NELLER

PRESENTER BIOGRAPHY

Andrew Neller - (CISSP, CRISC, C|CISO, CCE)
Director Cybersecurity Risk & Operations + Security Official

- Andy is a strategic leader with over 25 years in cybersecurity. His qualifications include a BS in Cybersecurity and the CISSP, C|CISO, CRISC, and CCE certifications. He has extensive experience in helping organizations securely transition to the cloud in highly regulated environments. He focuses on best-in-class security through the creation of sound security programs; ensuring governance and regulation compliance, and IT security risk management strategies that enable delivery of secure solutions for business stakeholders.
- He has provided forensic case information to Law Enforcement, the Iowa Attorney General, and the United States Congress.
- An active mentor in the Iowa STEM Hyperstream cyberdefense program, Mr. Neller is also a member of the Technology Association of Iowa (TAI) CISO workgroup and the Blue Cross Blue Shield (BCBSA) CISO Cybersecurity Subcommittee.
- Mr. Neller is also co-founder of Digital Revelation, a security research and award winning competitive hacking team.

AGENDA

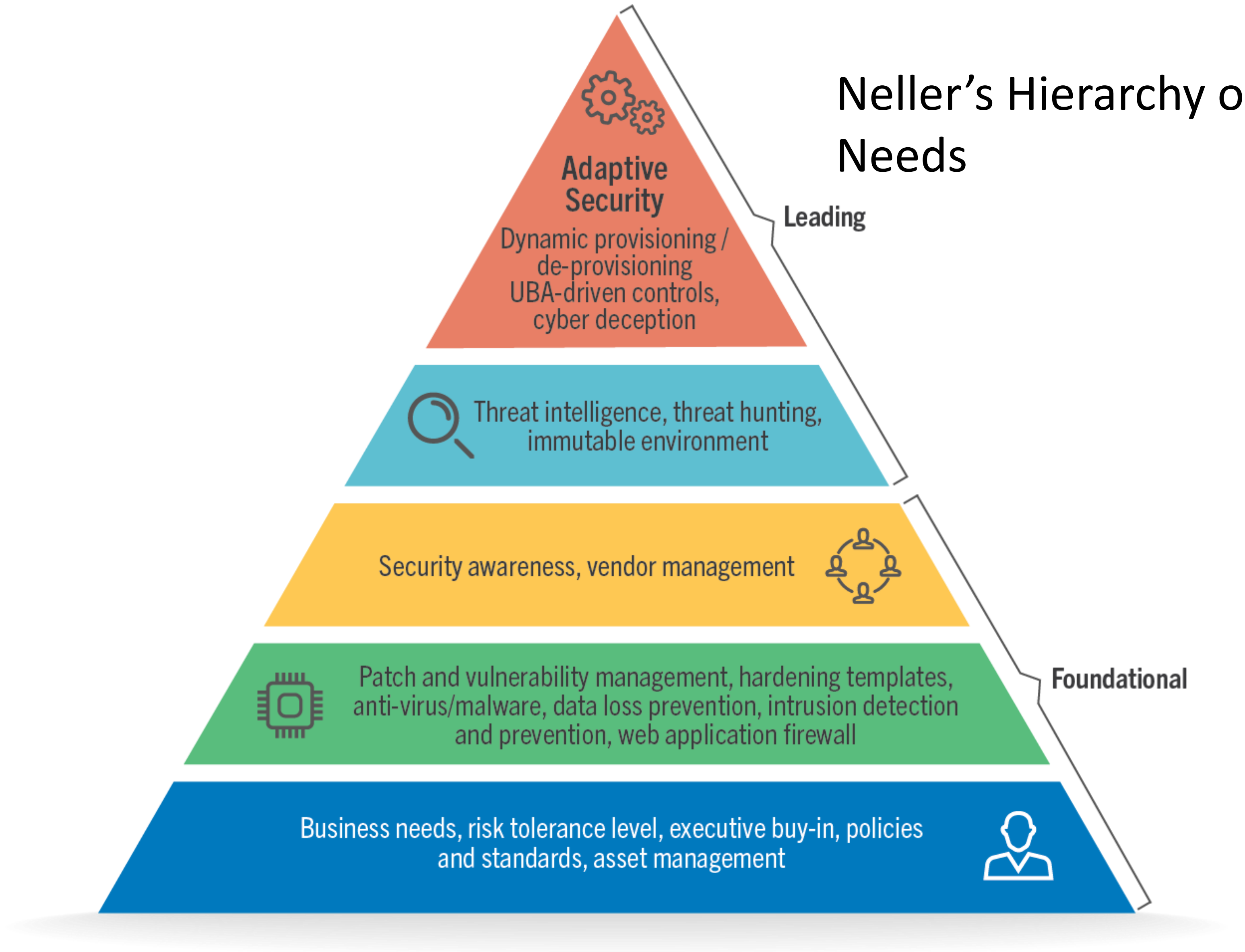
- Key foundational tenants
- Neller’s hierarchy of Cyber Security needs
- Cyber Security kill chain
- AOA (Anatomy of Attack)
- MITRE ATT&CK ™
- Adversary Obstruction examples
- Cyber Deception & Vendor based solutions (Deception in a box)
- Conversation and Questions

KEY FOUNDATIONAL TENANTS

- Focus on the journey to win the war.
- **Breaches are not inevitable, control failures are.**
- You have the home field advantage. (Even against insider threats)
- Validate and verify what is critical (Metrics)
- Good security doesn’t have to be expensive (traditional tradeoffs)
- The song changes, but the dance remains the same
- Compliance ≠ Security

SECURE FRAMEWORK

Neller's Hierarchy of Cyber Security Needs



Adaptive Security

Dynamic provisioning / de-provisioning UBA-driven controls, cyber deception

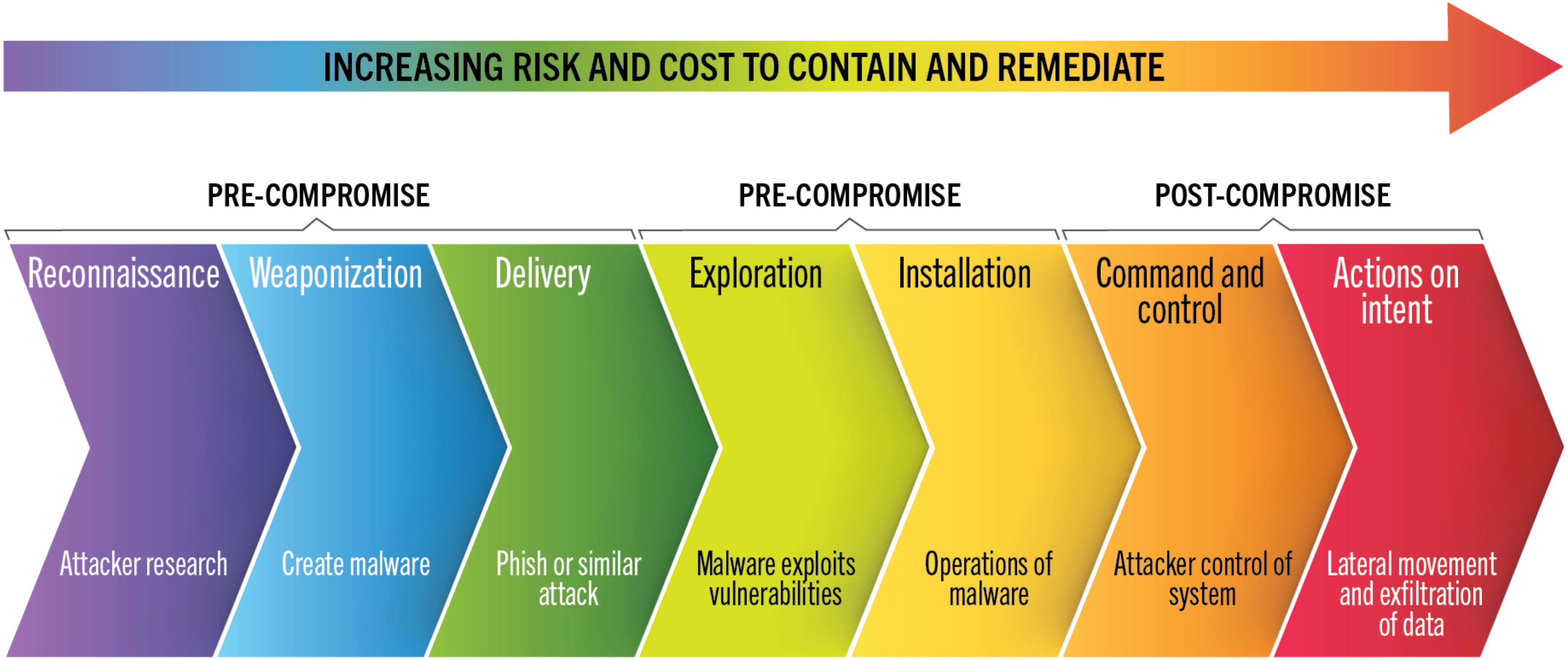
Threat intelligence, threat hunting, immutable environment

Security awareness, vendor management

Patch and vulnerability management, hardening templates, anti-virus/malware, data loss prevention, intrusion detection and prevention, web application firewall

Business needs, risk tolerance level, executive buy-in, policies and standards, asset management

CYBER SECURITY KILL CHAIN



INCREASING RISK AND COST TO CONTAIN AND REMEDIATE

PRE-COMPROMISE

- Reconnaissance: Attacker research
- Weaponization: Create malware
- Delivery: Phish or similar attack

PRE-COMPROMISE

- Exploration: Malware exploits vulnerabilities
- Installation: Operations of malware

POST-COMPROMISE

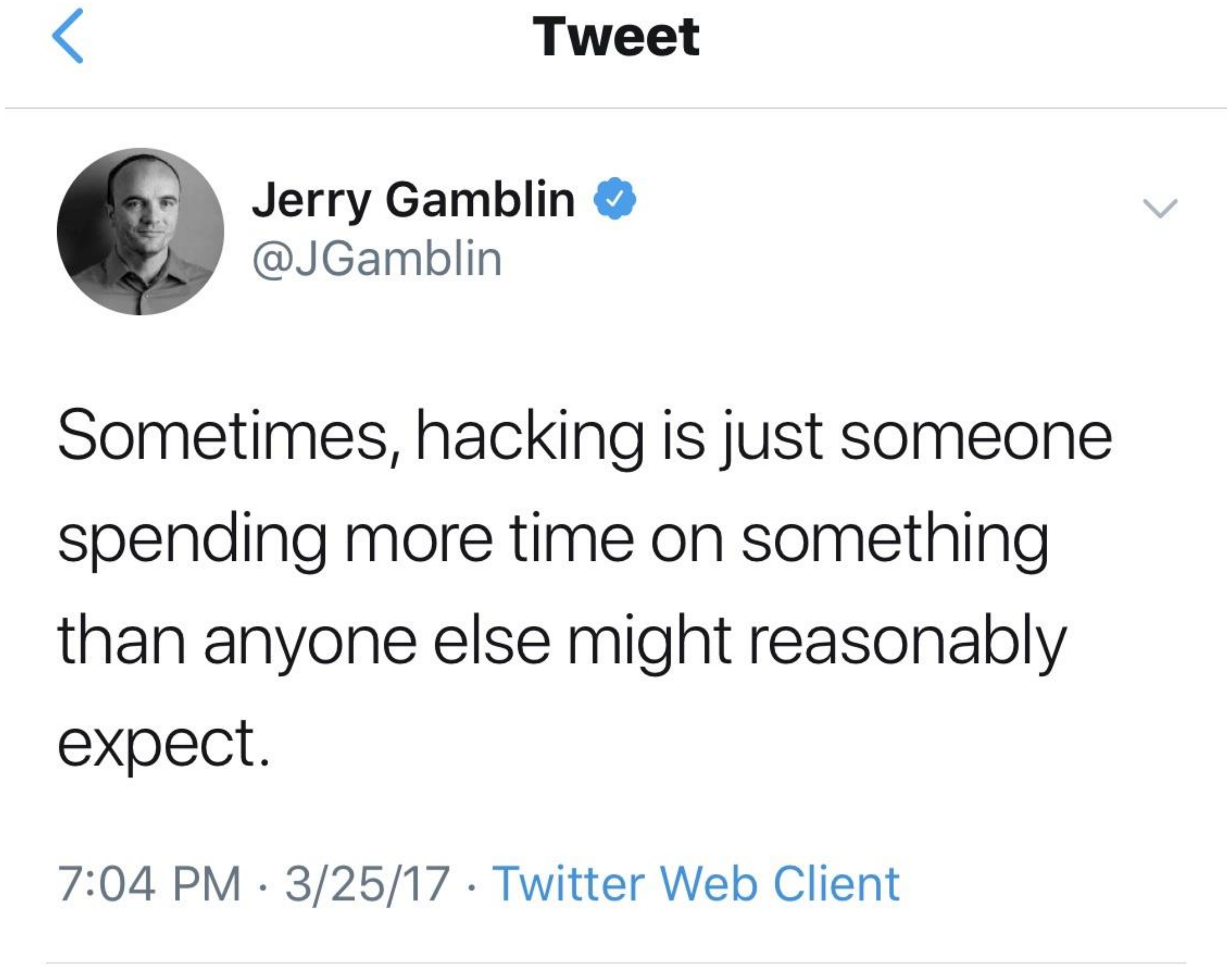
- Command and control: Attacker control of system
- Actions on intent: Lateral movement and exfiltration of data

Cyber Kill Chain

Sequential chain of events in order to successfully complete its targeted mission ~ Lockheed Martin CIRT

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

UNDERSTAND YOUR ADVERSARY



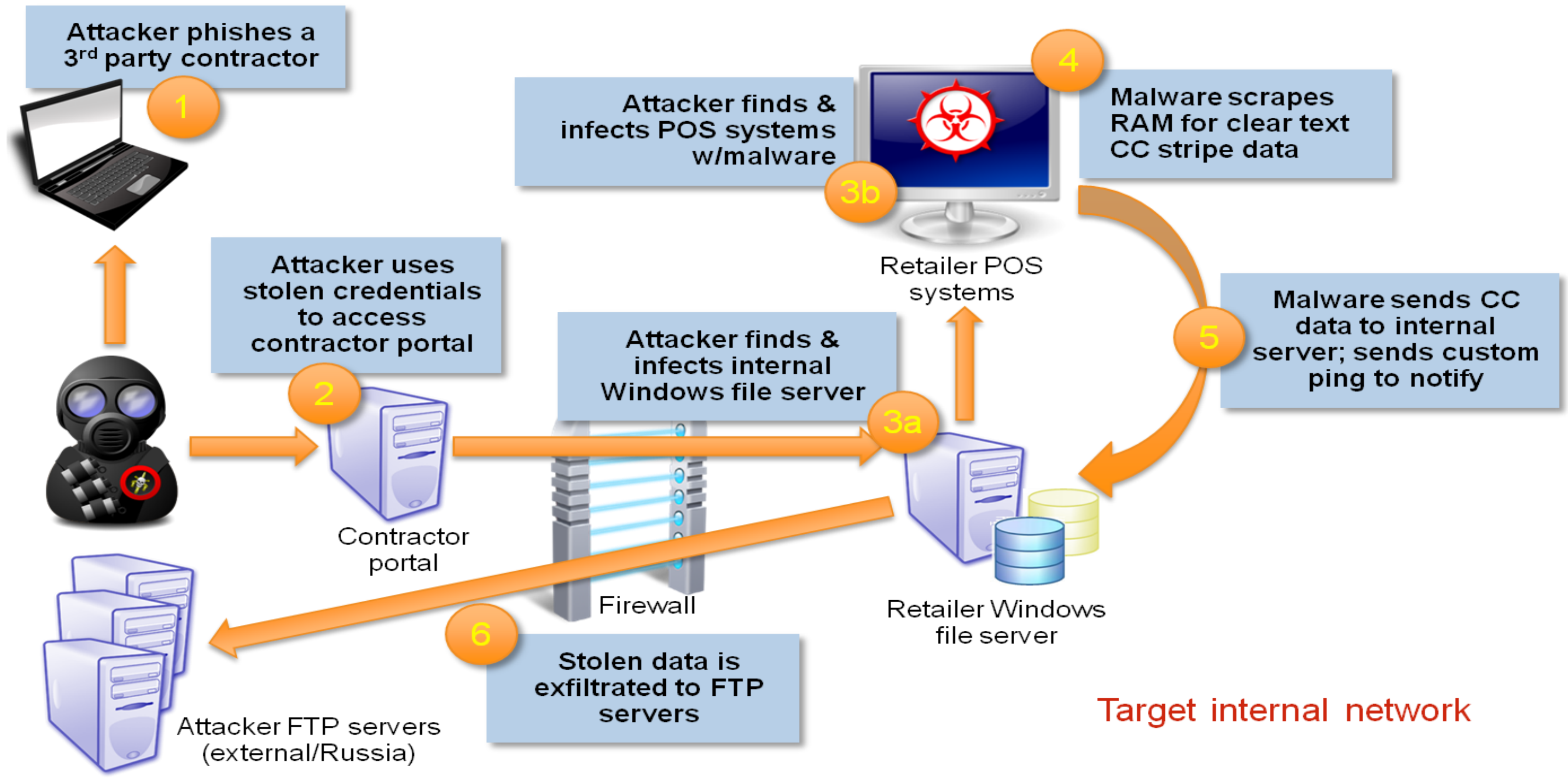
Jerry Gamblin
@JGamblin

Sometimes, hacking is just someone spending more time on something than anyone else might reasonably expect.

7:04 PM · 3/25/17 · Twitter Web Client

ANATOMY OF ATTACK (AOA)

Anatomy of the Target Retailer Breach



1 Attacker phishes a 3rd party contractor

2 Attacker uses stolen credentials to access contractor portal

3a Attacker finds & infects internal Windows file server

3b Attacker finds & infects POS systems w/malware

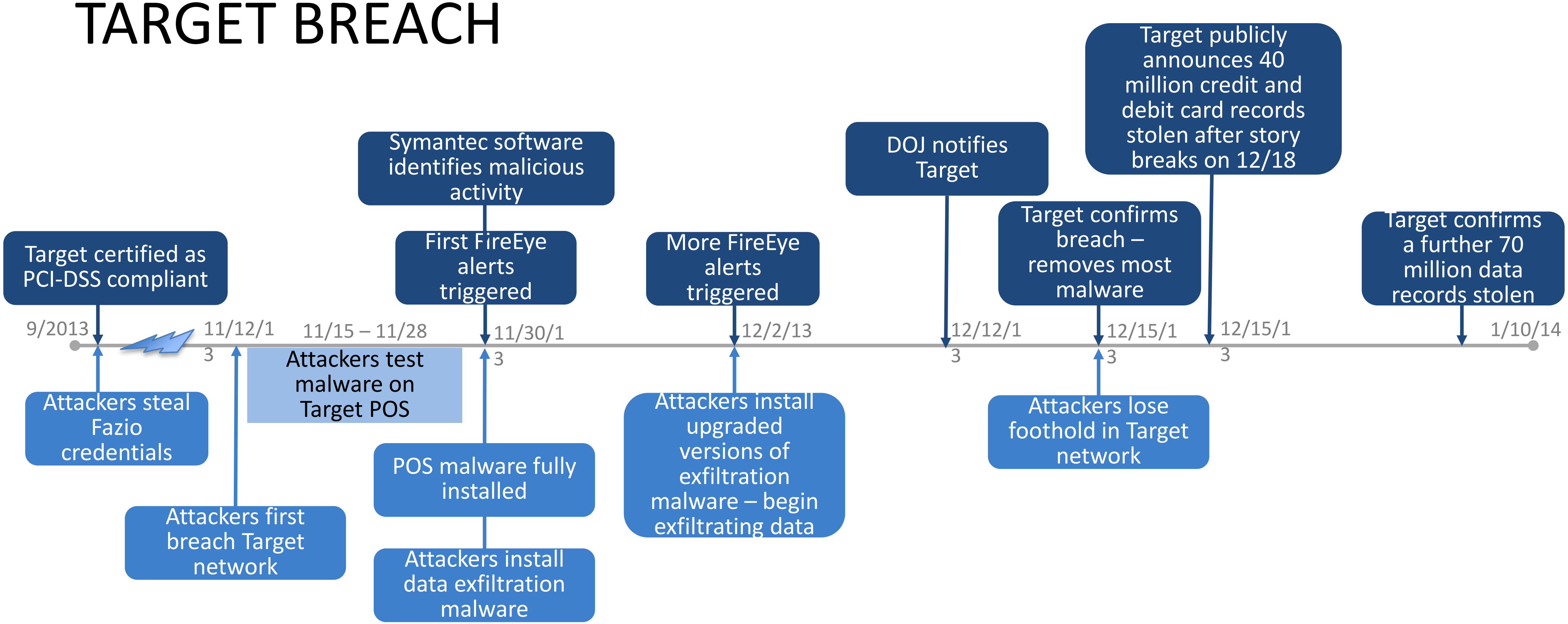
4 Malware scrapes RAM for clear text CC stripe data

5 Malware sends CC data to internal server; sends custom ping to notify

6 Stolen data is exfiltrated to FTP servers

https://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/
January 31, 2014 | By Chris Poulin

TARGET BREACH



9/2013

Target certified as PCI-DSS compliant

Attackers steal Fazio credentials

11/12/13

Attackers first breach Target network

11/15 – 11/28

Attackers test malware on Target POS

11/30/13

Symantec software identifies malicious activity

First FireEye alerts triggered

POS malware fully installed

Attackers install data exfiltration malware

12/2/13

More FireEye alerts triggered

Attackers install upgraded versions of exfiltration malware – begin exfiltrating data

12/12/13

DOJ notifies Target

12/15/13

Target confirms breach – removes most malware

Attackers lose foothold in Target network

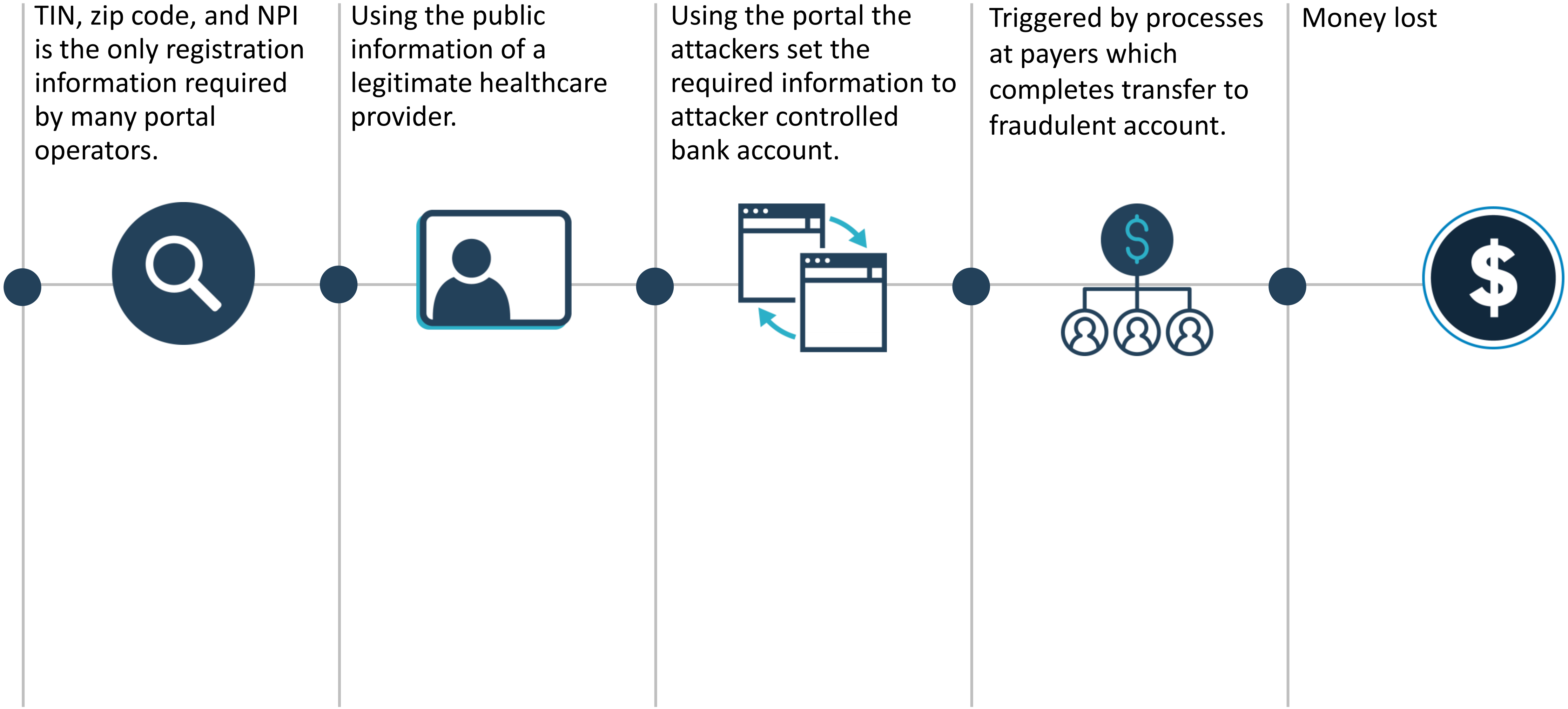
12/15/13

Target publicly announces 40 million credit and debit card records stolen after story breaks on 12/18

1/10/14

Target confirms a further 70 million data records stolen

FUND REDIRECTION — ANATOMY OF ATTACK ACA/HEALTH (AOA)



TIN, zip code, and NPI is the only registration information required by many portal operators.

Using the public information of a legitimate healthcare provider.

Using the portal the attackers set the required information to attacker controlled bank account.

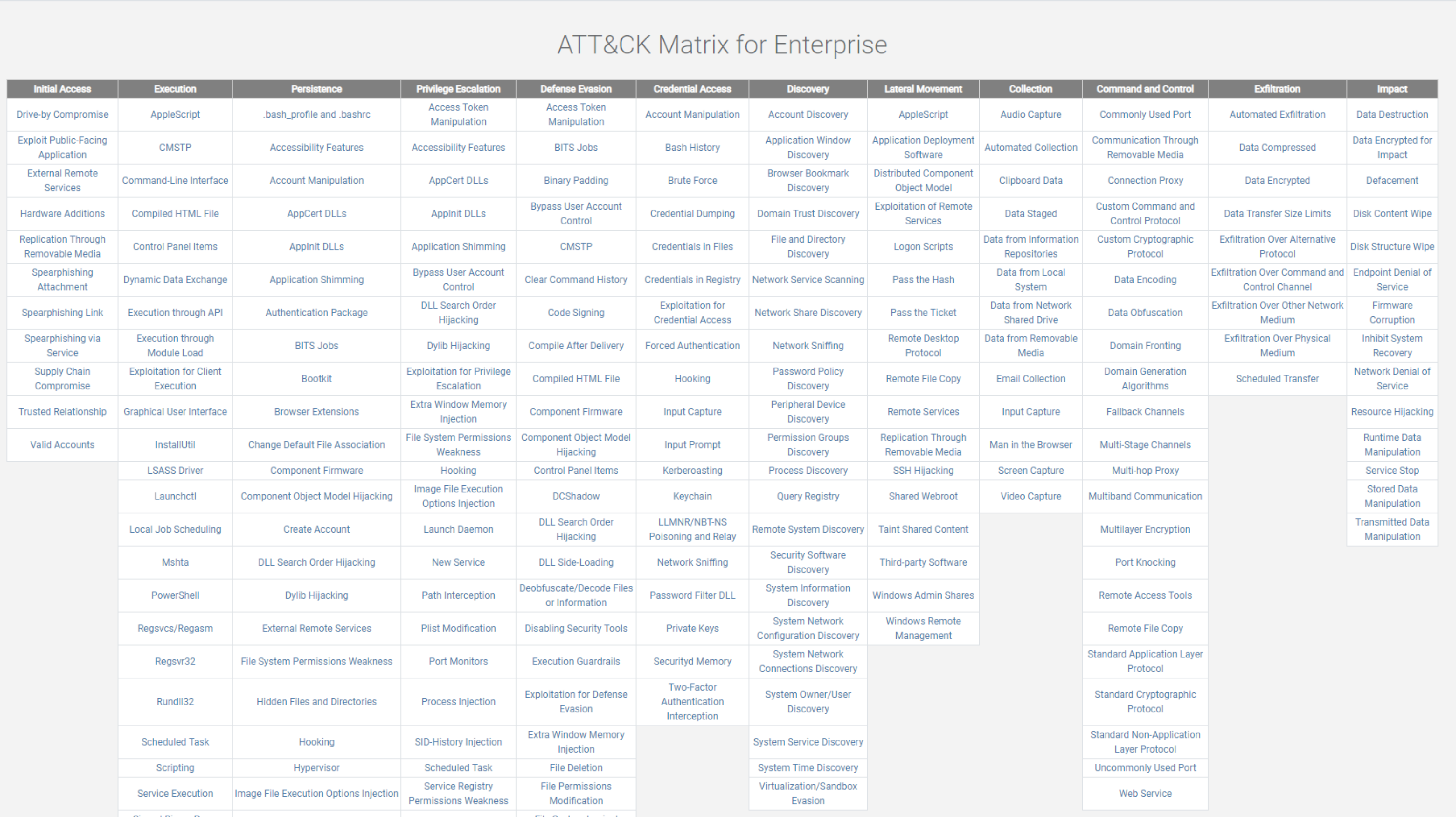
Triggered by processes at payers which completes transfer to fraudulent account.

Money lost

MITRE ATT&CK ™

- MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

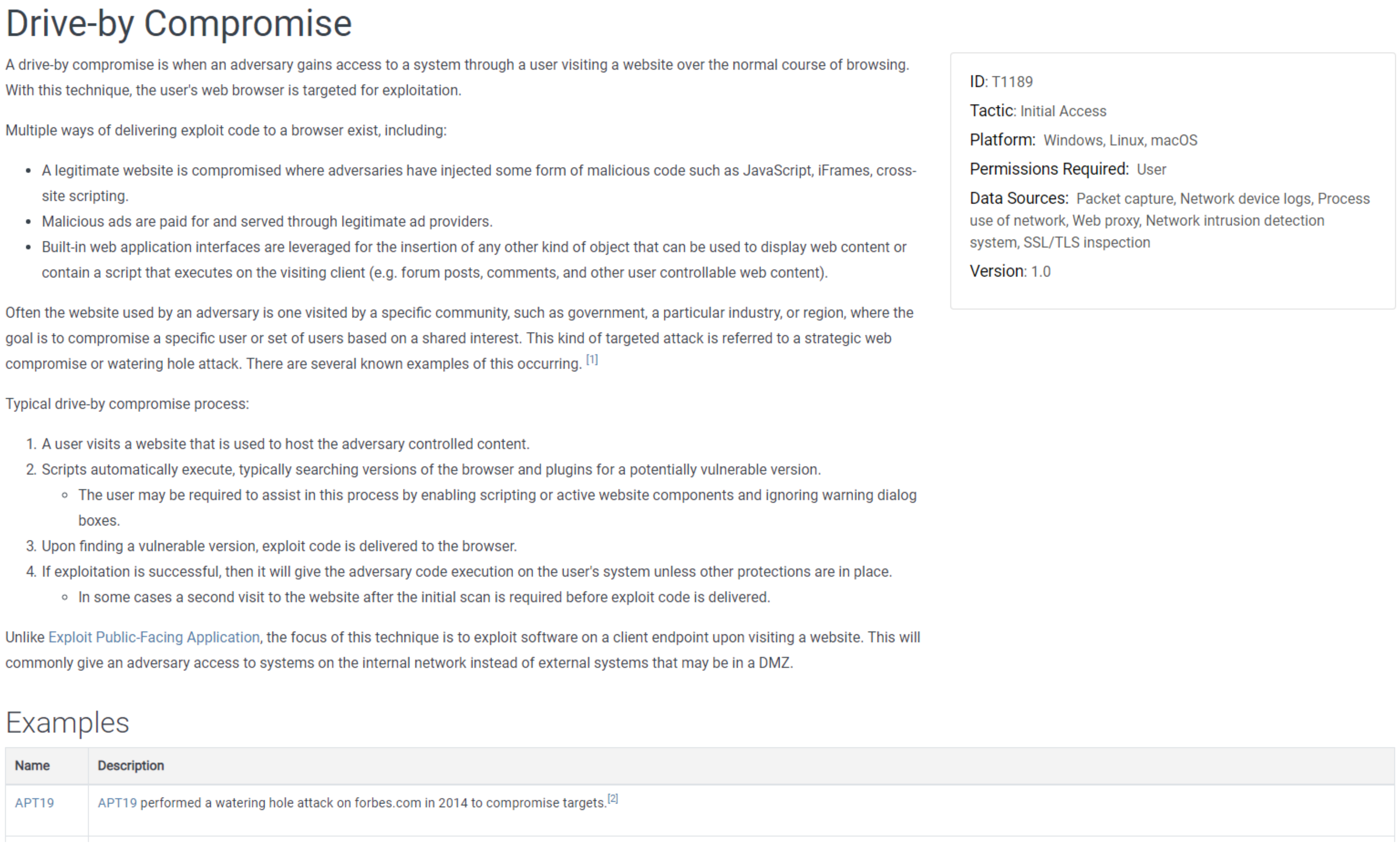
https://attack.mitre.org/



ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture	Multi-hop Proxy		Service Stop
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Stored Data Manipulation
	Local Job Scheduling	Create Account	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	DLL Side-Loading	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	Deobfuscate/Decode Files or Information	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	Disabling Security Tools	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	SID-History Injection	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Scheduled Task	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		

https://attack.mitre.org/



Drive-by Compromise

A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation.

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring. [1]

Typical drive-by compromise process:

1. A user visits a website that is used to host the adversary controlled content.
2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version.
    - The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes.
3. Upon finding a vulnerable version, exploit code is delivered to the browser.
4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place.
    - In some cases a second visit to the website after the initial scan is required before exploit code is delivered.

Unlike Exploit Public-Facing Application, the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ.

ID: T1189

Tactic: Initial Access

Platform: Windows, Linux, macOS

Permissions Required: User

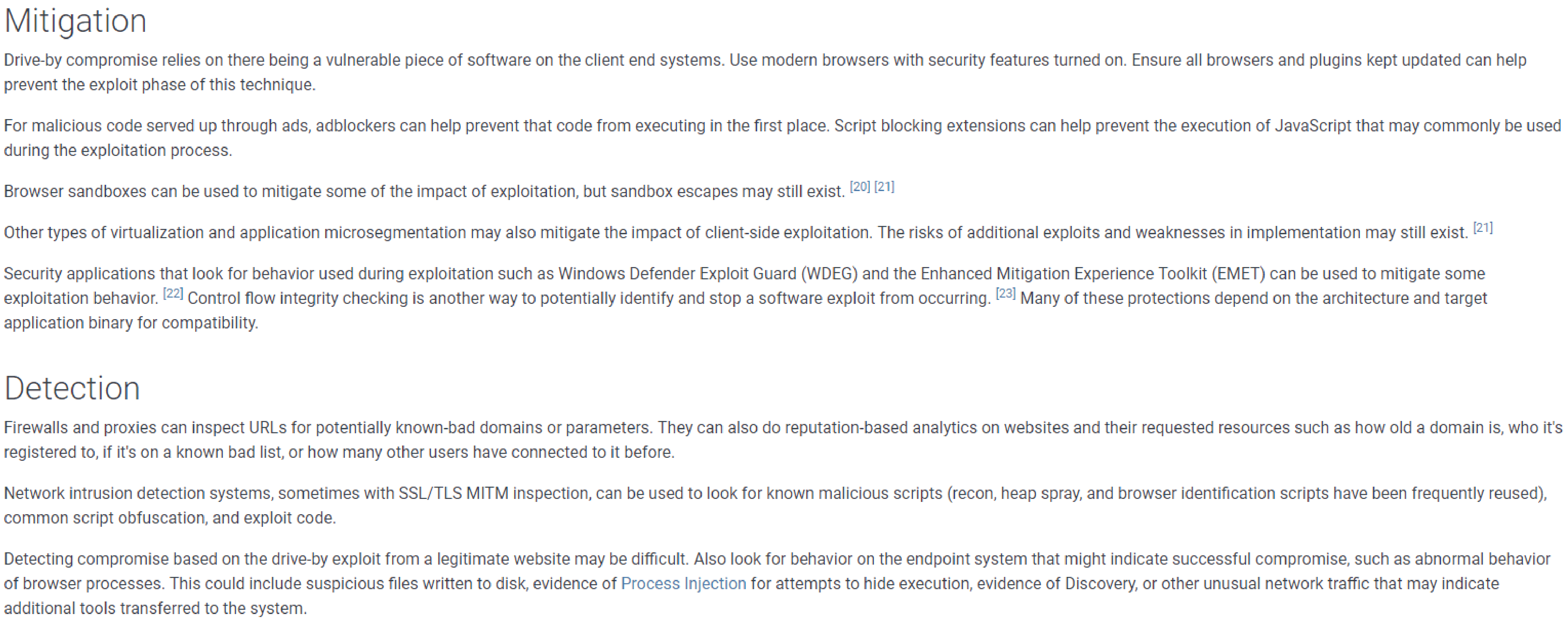
Data Sources: Packet capture, Network device logs, Process use of network, Web proxy, Network intrusion detection system, SSL/TLS inspection

Version: 1.0

Examples

Name	Description
APT19	APT19 performed a watering hole attack on forbes.com in 2014 to compromise targets.[2]

https://attack.mitre.org/



Mitigation

Drive-by compromise relies on there being a vulnerable piece of software on the client end systems. Use modern browsers with security features turned on. Ensure all browsers and plugins kept updated can help prevent the exploit phase of this technique.

For malicious code served up through ads, adblockers can help prevent that code from executing in the first place. Script blocking extensions can help prevent the execution of JavaScript that may commonly be used during the exploitation process.

Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist. [20] [21]

Other types of virtualization and application microsegmentation may also mitigate the impact of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist. [21]

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. [22] Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. [23] Many of these protections depend on the architecture and target application binary for compatibility.

Detection

Firewalls and proxies can inspect URLs for potentially known-bad domains or parameters. They can also do reputation-based analytics on websites and their requested resources such as how old a domain is, who it's registered to, if it's on a known bad list, or how many other users have connected to it before.

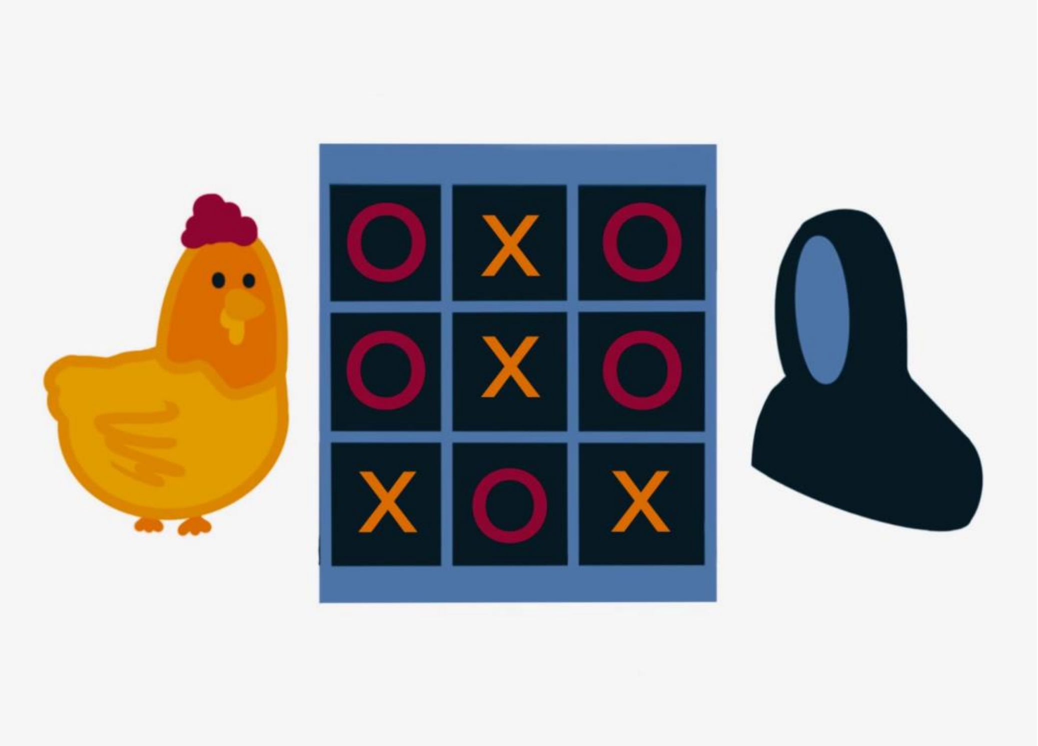
Network intrusion detection systems, sometimes with SSL/TLS MITM inspection, can be used to look for known malicious scripts (recon, heap spray, and browser identification scripts have been frequently reused), common script obfuscation, and exploit code.

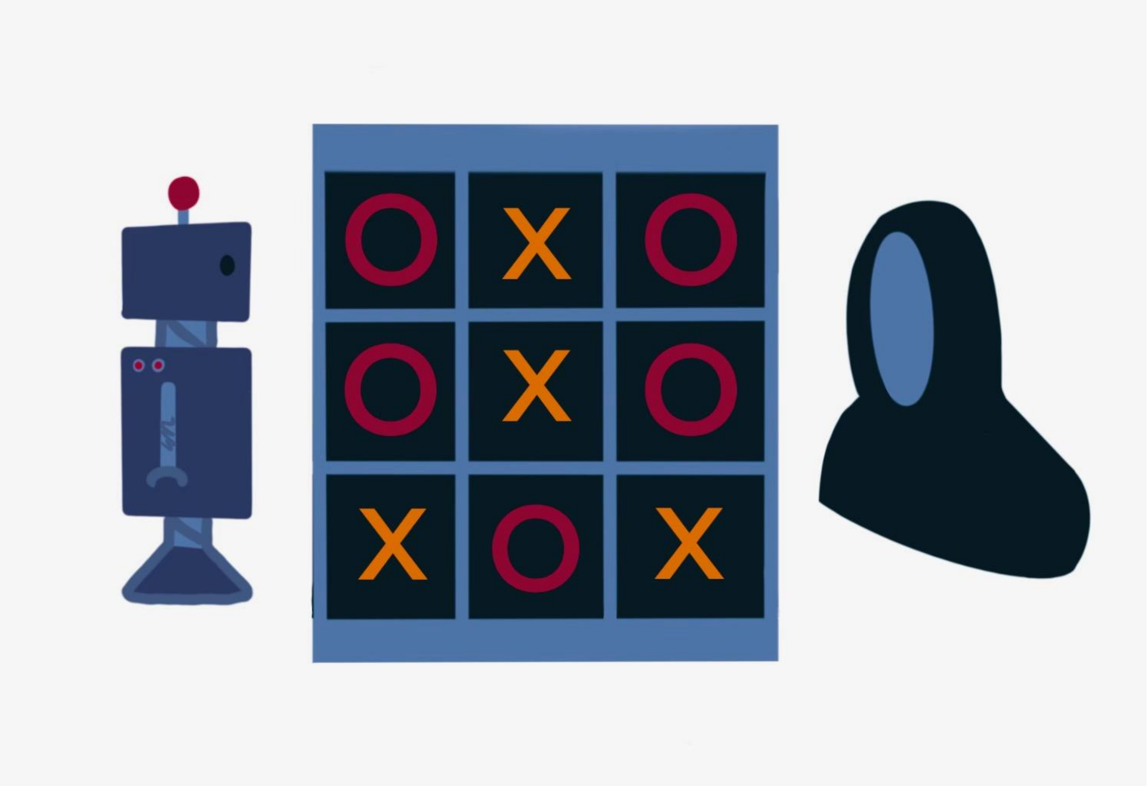
Detecting compromise based on the drive-by exploit from a legitimate website may be difficult. Also look for behavior on the endpoint system that might indicate successful compromise, such as abnormal behavior of browser processes. This could include suspicious files written to disk, evidence of Process Injection for attempts to hide execution, evidence of Discovery, or other unusual network traffic that may indicate additional tools transferred to the system.

https://attack.mitre.org/

ADVERSARY OBSTRUCTION

INTRO TO CYBER ADVERSARY OBSTRUCTION





ADVERSARY OBSTRUCTION

- Layers are your friend
- Allows Blue team to flip-the-script
- High fidelity based off your environment
- Typically low/no cost to put in place
- Setting alarms that should never/rarely go off
- Additive to an established InfoSec program
- Metrics and Testing (Critical)
- Take it to the next level with deception tech

ADVERSARY OBSTRUCTION EXAMPLES

- Segmentation Rules (Especially from user land)
- Peer-to-Peer
- Volume of traffic
- Types of traffic
- Operating systems (more difficult in BYOD)
- Take advantage of host based firewalls / free solutions (Microsoft ATA)

ADVERSARY OBSTRUCTION EXAMPLES

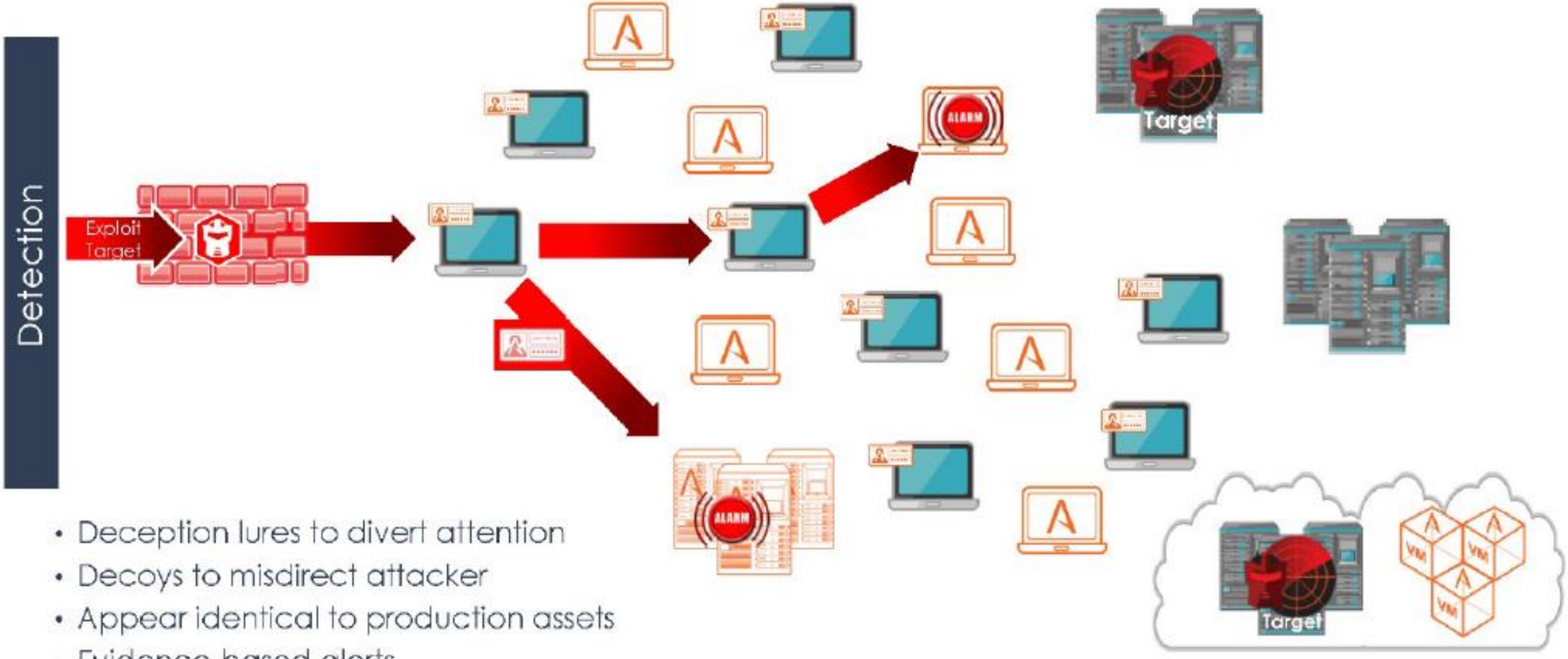
- Do you really need to talk to China/Russia/?
- Keyboard Layouts (Non-Us)
- DNS Blackhole *

CYBER DECEPTION

INTRO TO CYBER DECEPTION

Changing the Game with Deception and Decoys

Deception Obscures the Attack Surface and Disrupts Attacks



- Deception lures to divert attention
- Decoys to misdirect attacker
- Appear identical to production assets
- Evidence-based alerts

https://www.linkedin.com/pulse/deception-technology-aditya-mukherjee-phd-information-security-/

WHY?

Rationale: Adversaries have evolved, Controls will eventually fail (weakest link).

Can your environment serve as a detection network?

If employees use reports and GUIs, adversaries seek raw data stores, CLIs and APIs.

Adversaries seek to move inside an environment without detection.

Lateral Movement is a key indicator of a security event…but what about files/instances/tokens that should never be touched?

LOW / NO COST OPTIONS

- API security value example , DNS example, Web Cookie example, and AWS Key example , Microsoft ATA

COMMERCIAL OPTIONS

- MazeRunner (Cymmetria – Gadi Everon)
- Smokescreen
- Javelin Networks (Symantec)
- Thinkst Canaries (Check your Cyber Insurance)*

THINKST CANARIES

Deployed quickly

Signal/Noise ratio in your favor

High-interaction honeypots are a lot of work

Low-interaction honeypots aren't very interesting

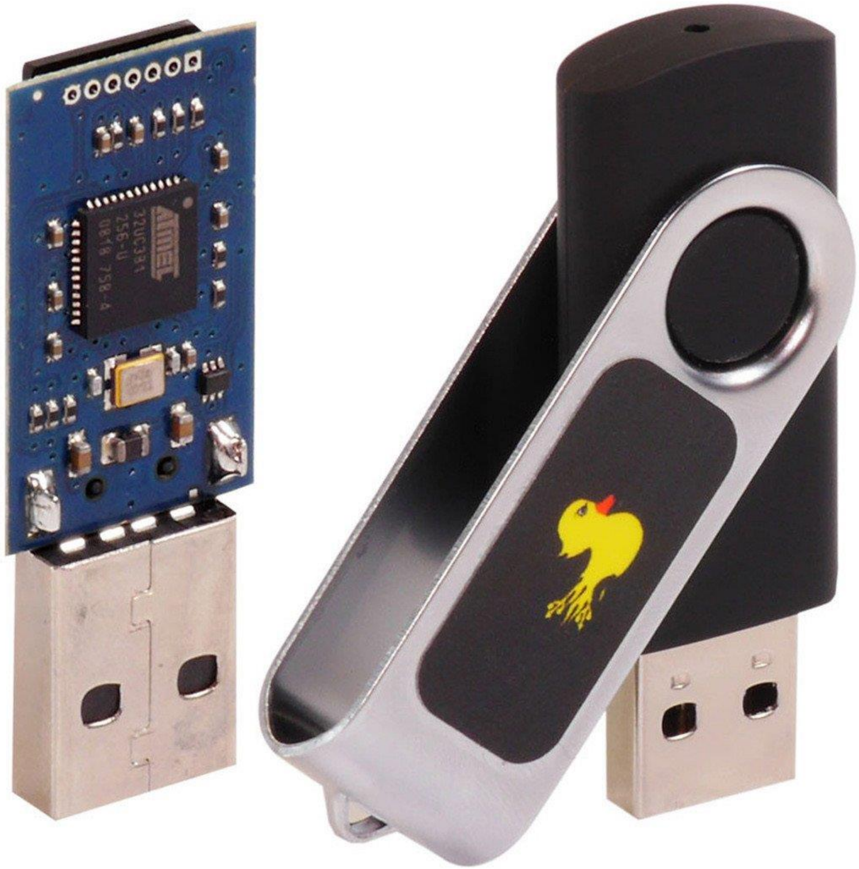
WINNING

- Non-persistence (not immutable)
- Solid Update Process
- Measure and Report
- Automate

CONVERSATIONS AND QUESTIONS

DEMO

USB RUBBER DUCK

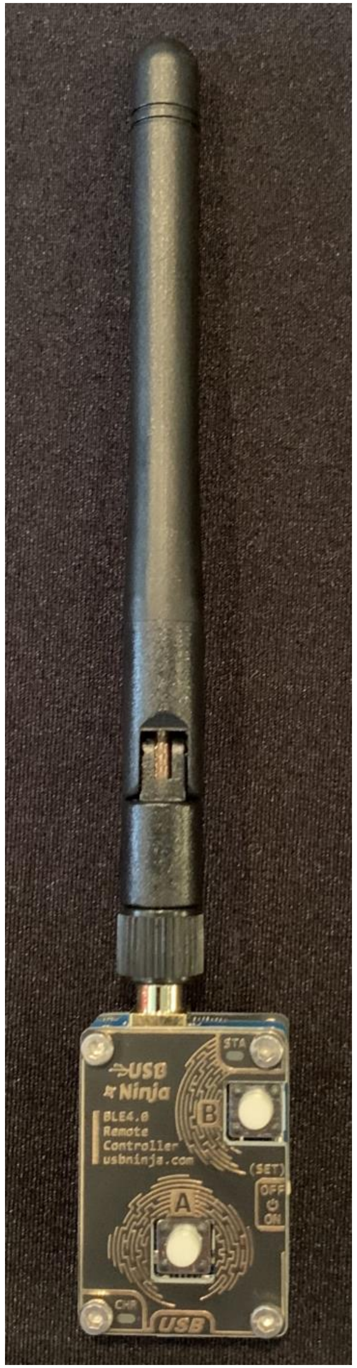


REALLY BAD USB (USBNINJA)

- The USBNinja is a USB Cable that embedded an BADUSB in it. It has 6KB Flash Memory in it to store your own payload. These payloads can be triggered by a Bluetooth Remote Control or this Application. The Cable can simulate itself to an HID-Keyboard or an HID-Mouse to Control .your computer

REALLY BAD USB (USBNINJA)

REALLY BAD USB (USBNINJA)



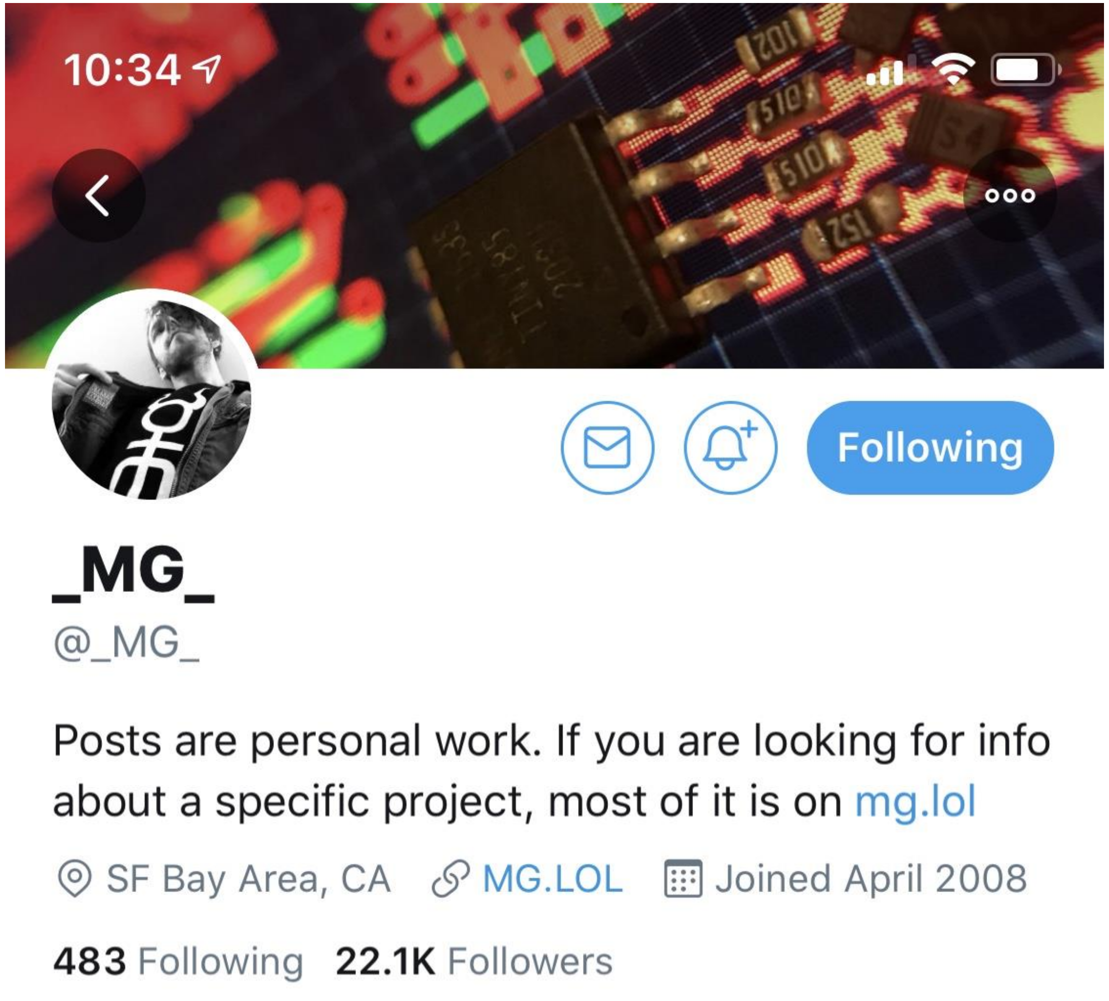
O.MG CABLE

The O.MG Cable allows you to wirelessly create, save, and execute payloads. The Cable is built for Red Teams, with features that enhance remote execution, stealth, forensics evasion, all while being able to quickly and dynamically change your tooling with minimal effort.

setup info: https://o.mg.lol/setup

8 11342 03064 4

Package Contents: O.MG Cable + Programmer
Made in China. Mak3 LLC, 548 Market ST, #39371, San Francisco, CA 94104 https://o.mg.lol



_MG_

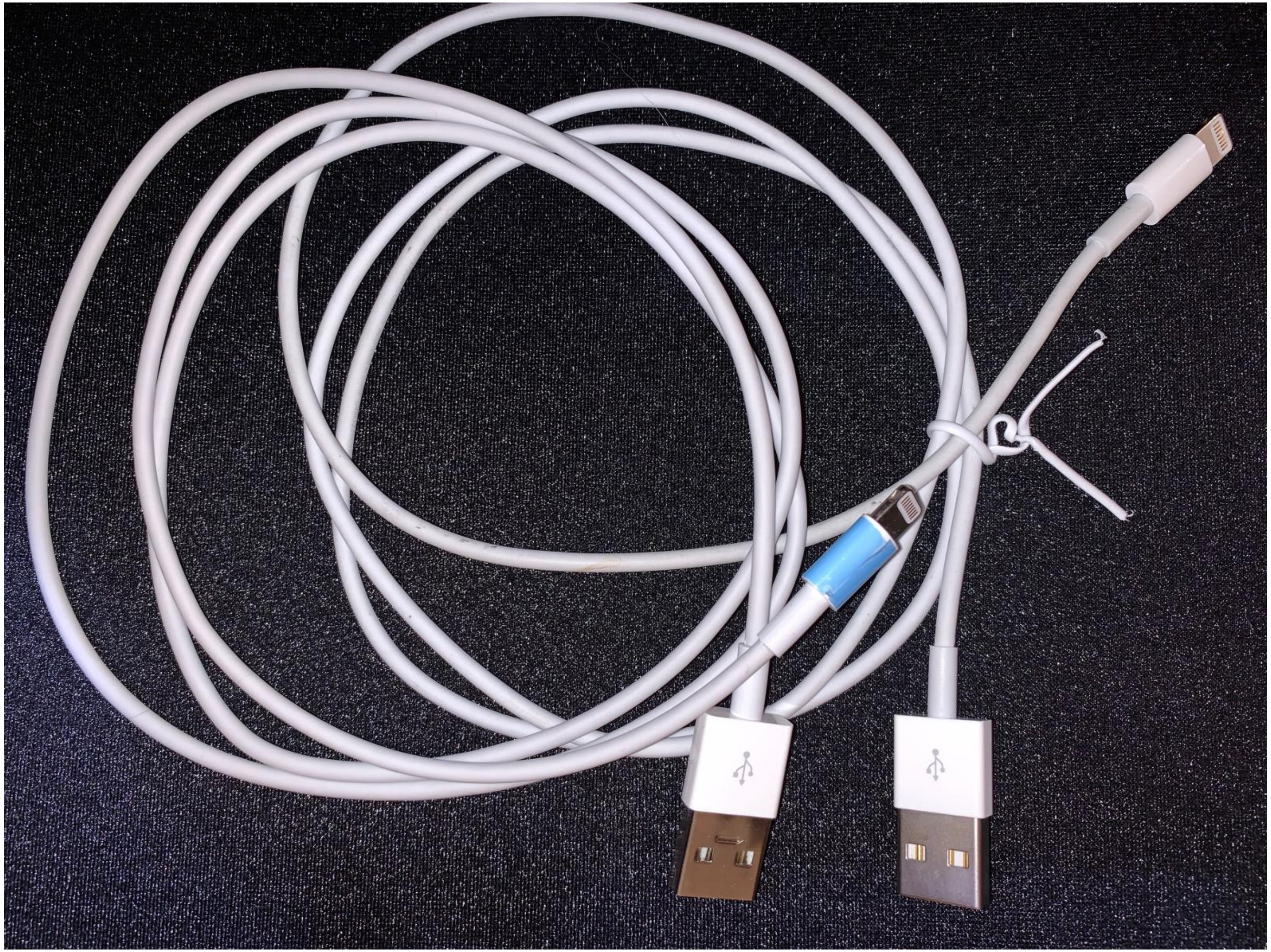
@_MG_

Posts are personal work. If you are looking for info about a specific project, most of it is on mg.lol

SF Bay Area, CA   MG.LOL   Joined April 2008

483 Following   22.1K Followers

O.MG CABLE



Tuesday
7
Calendar
Photos
Camera
Maps
Clock
Weather
News
Wallet
Notes
1
Reminders
tv
TV
Books
iTunes Store
App Store
Home
Health
Settings
Chrome
Safari
30
5,281
Downloads

THANK YOU

@ORACLE_52
NELLERAE@WELLMARK.COM
ANELLER52@GMAIL.COM