



Reversing the Kill Chain

An Actionable Framework for defending against common threats

Amanda Berlin

NetWorks
GROUP

Intrusion Kill Chain



Common Threats

Malicious Action

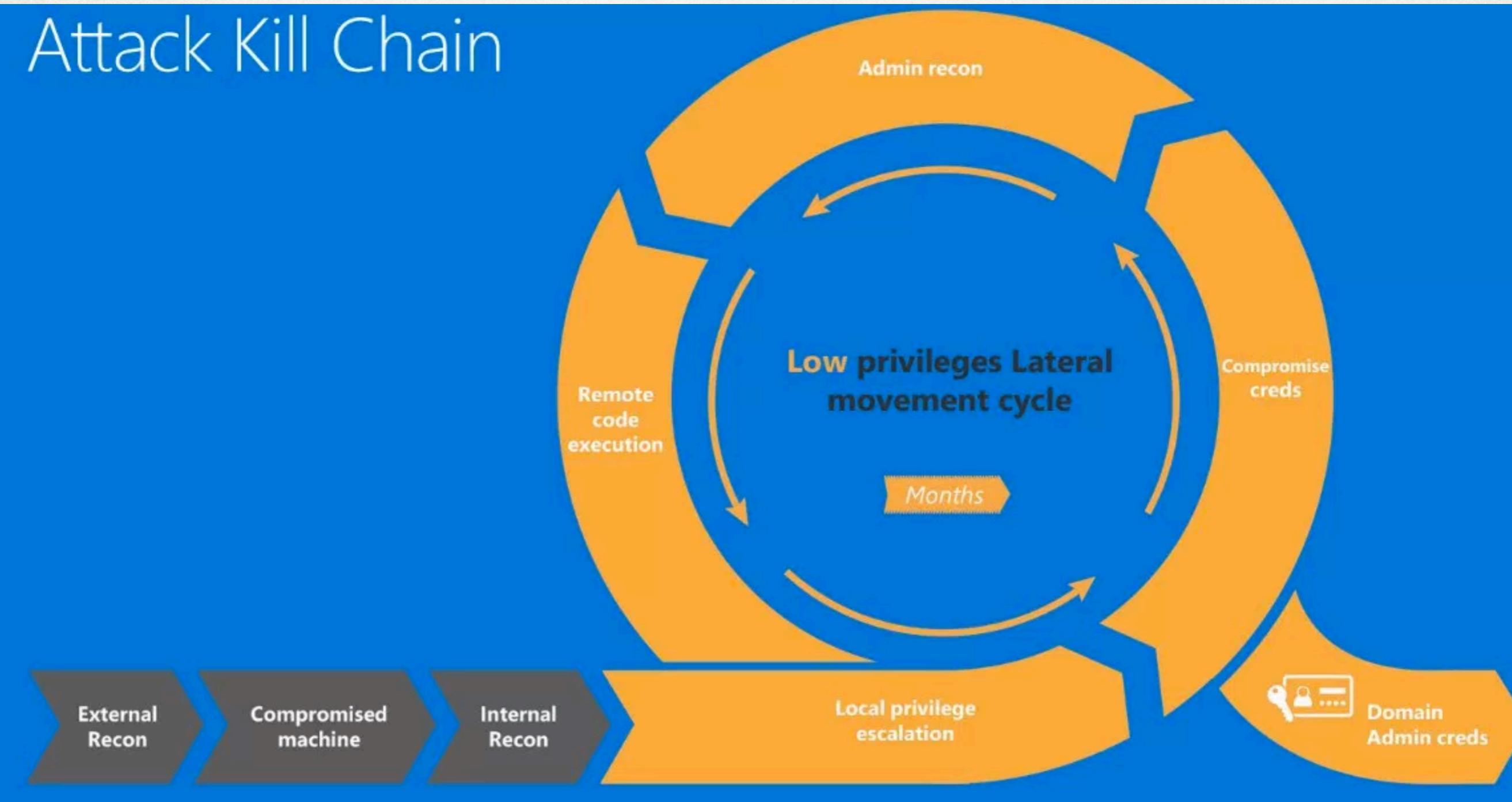
Defensive Mitigation

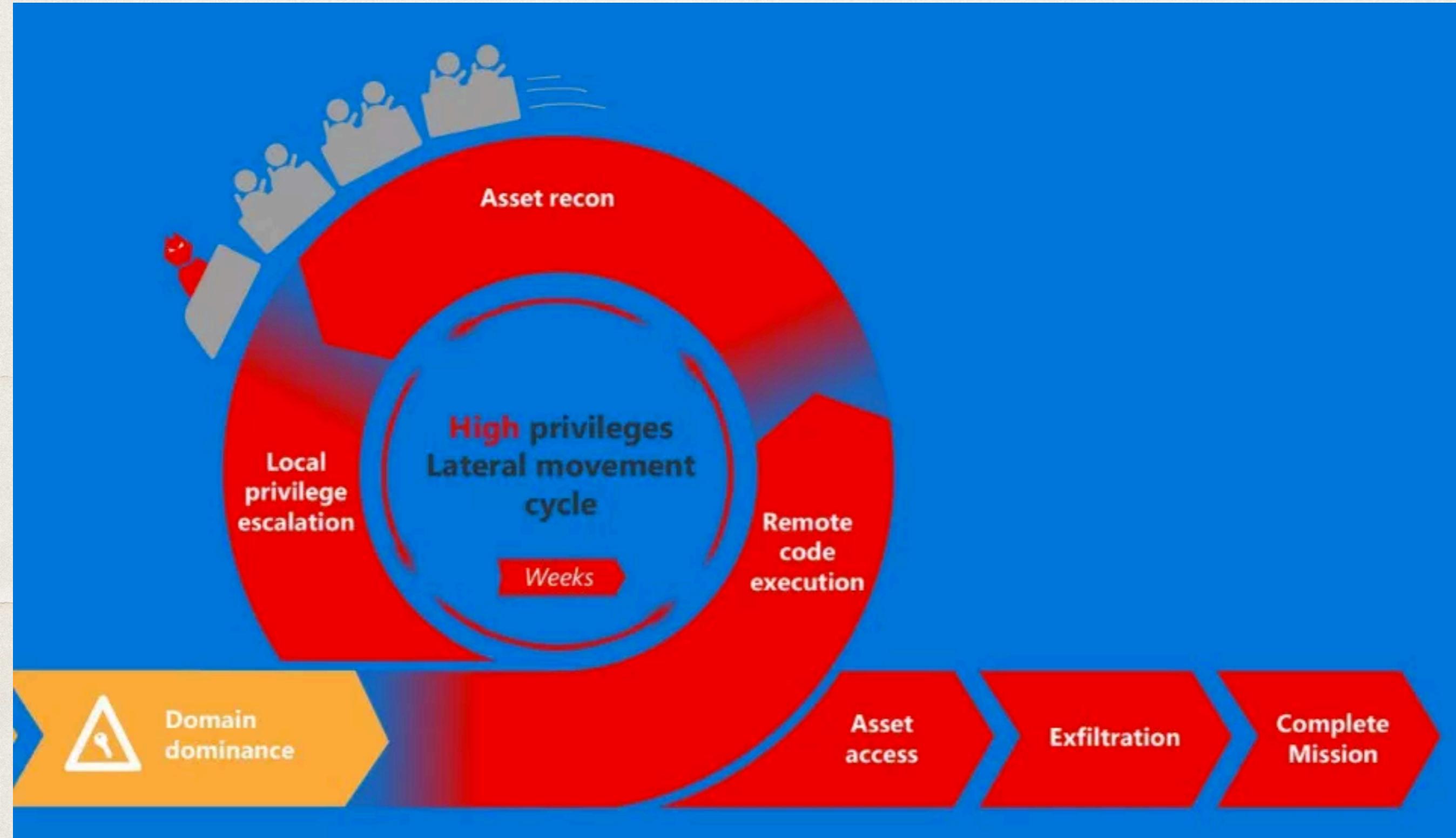
Ease of Deployment

Potential Monitoring

Specific Alerting

Attack Kill Chain





Reconnaissance

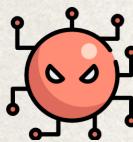
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Secure Logon
for F5 Networks

Username *

Password *

Logon

https://bd.ftr.com/my.policy

f5

frontier Communications



Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

DEMO

 **Detailed Alerting**



Delivery



Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

3 BILLION DEVICES RUN JAVA



Java™

**IMPOSSIBLE TO DOWNLOAD
AND RUN**

Delivery

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO

.hta	HTML Scripting Application
.js	JavaScript
.jse	JavaScript Encoded
.pif	Program Information File
.scr	ScreenSaver
.wsf	Windows Script File
.wsh / .wsc	Windows Script Host
.vbe	Visual Basic Encoded
.vbf	Visual Basic File

Delivery

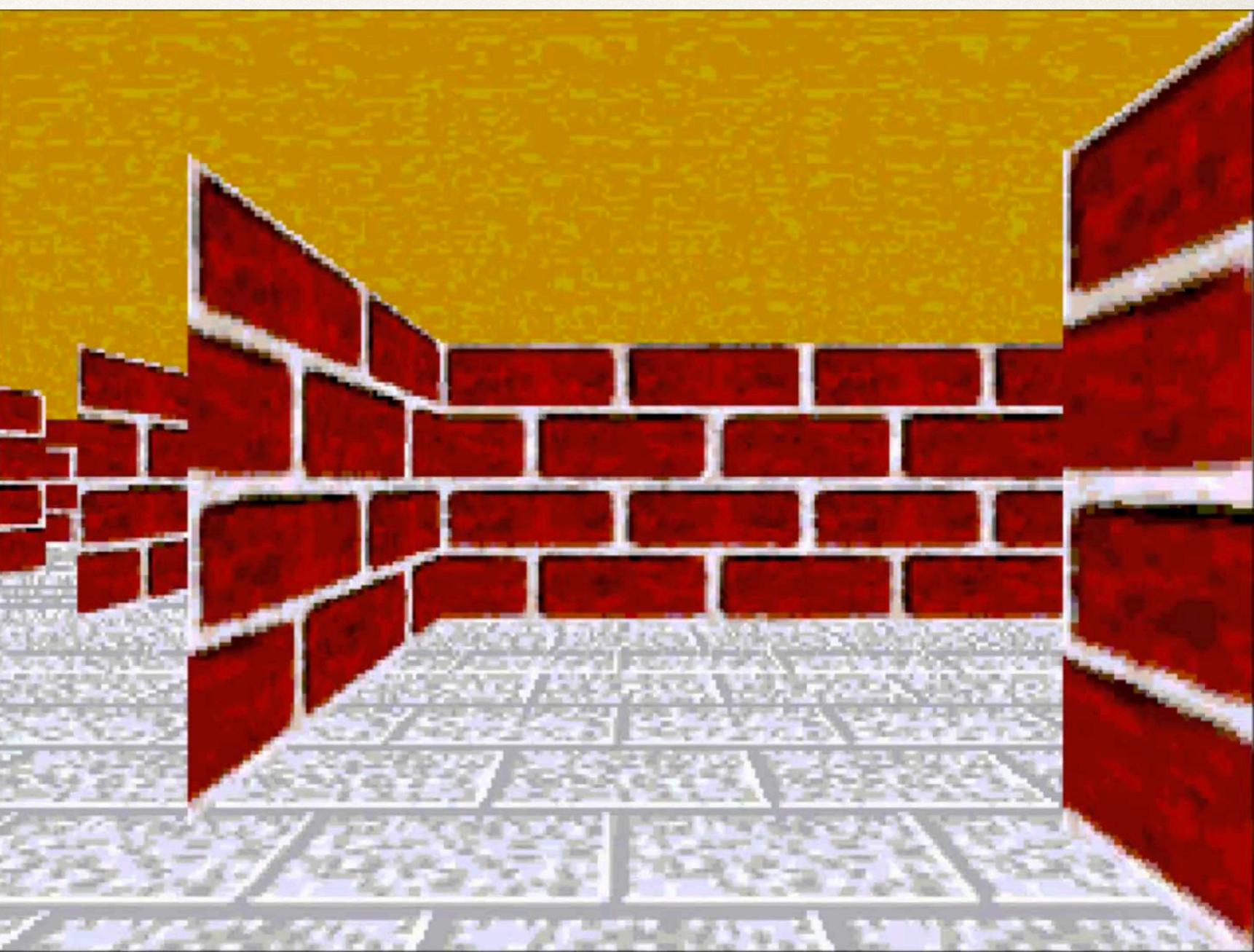
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

 **Detailed Alerting**



Exploitation

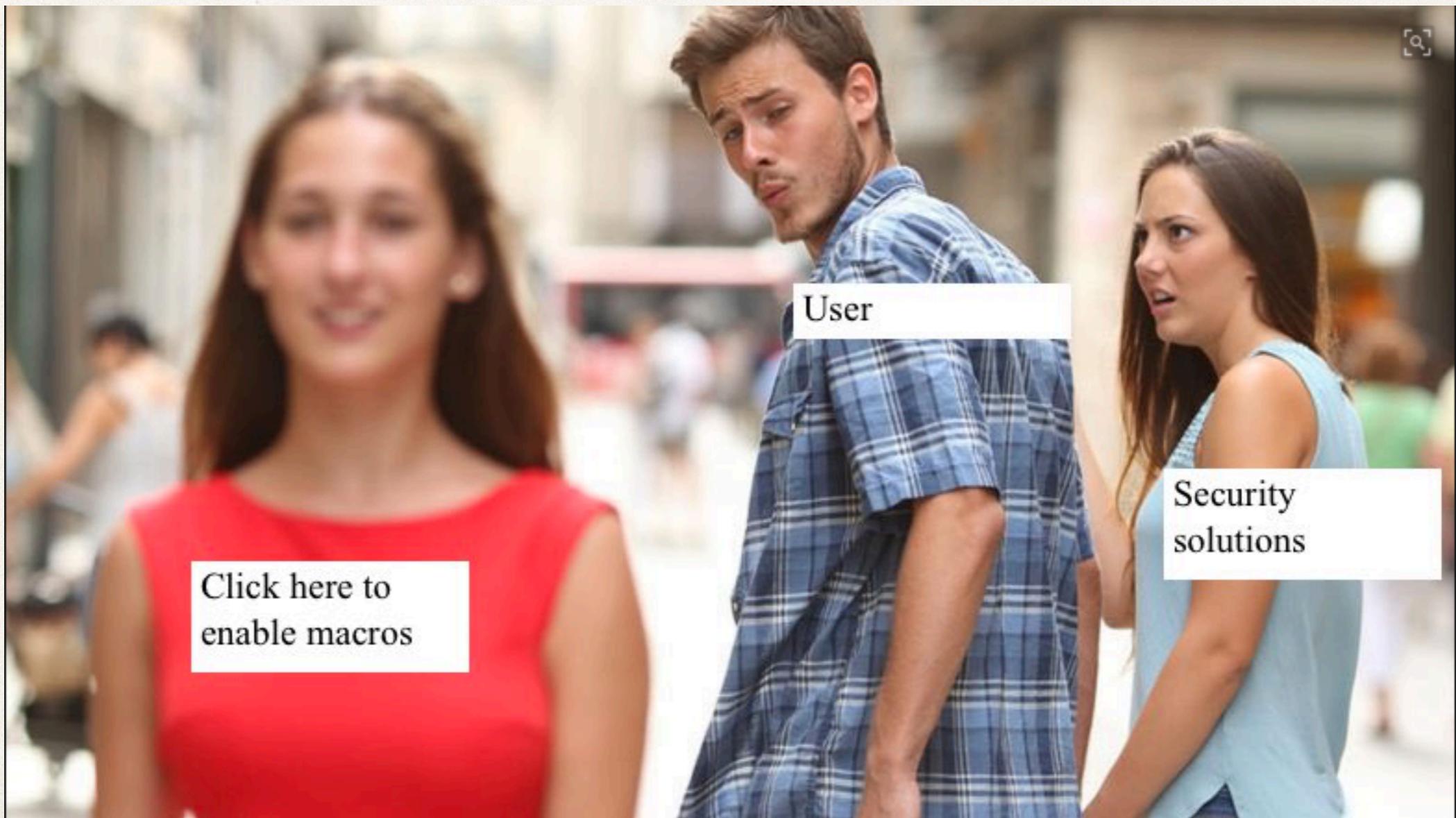
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Exploitation

Malicious Action

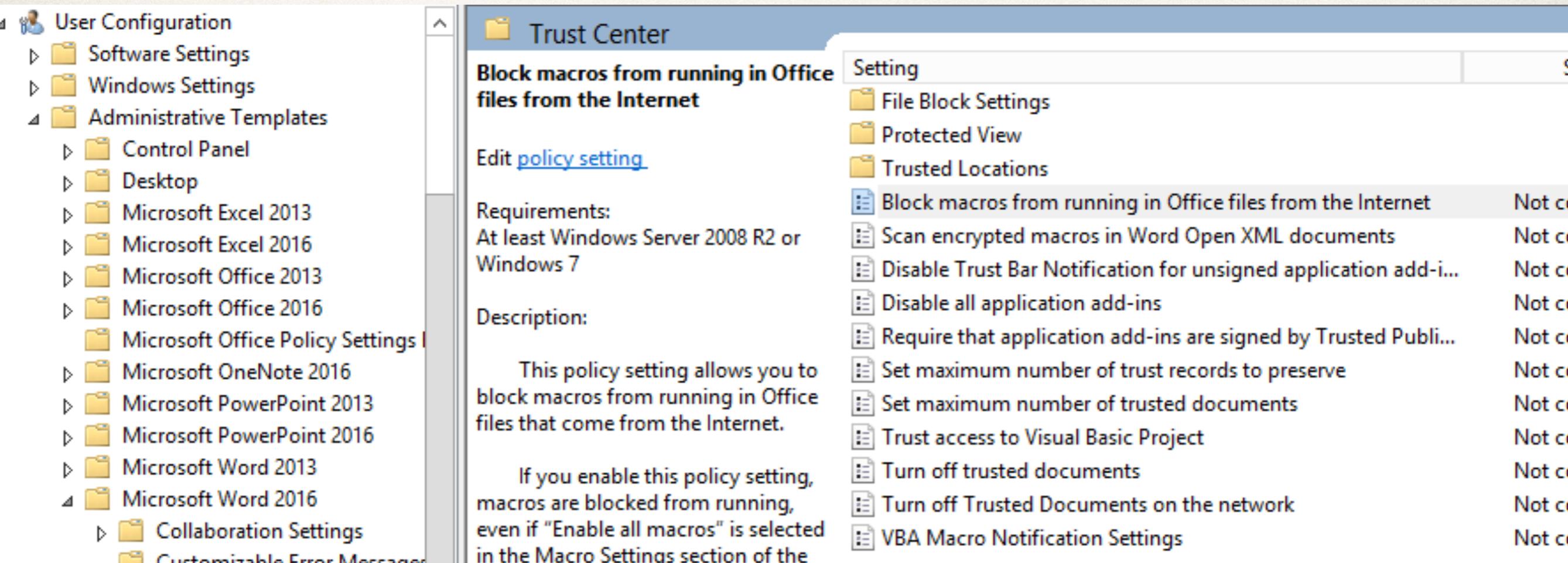
Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO



The screenshot shows the Windows Group Policy Editor interface. On the left, there is a navigation tree under 'User Configuration' with several administrative templates for Microsoft Office components like Excel, Word, and PowerPoint. The main pane displays the 'Trust Center' settings for 'Block macros from running in Office files from the Internet'. It includes sections for 'Edit policy setting', 'Requirements' (Windows Server 2008 R2 or Windows 7), and a detailed description of the policy. A list of settings on the right shows various options, with 'Block macros from running in Office files from the Internet' being the selected item.

Setting	Status
File Block Settings	Not config
Protected View	Not config
Trusted Locations	Not config
Block macros from running in Office files from the Internet	Configured
Scan encrypted macros in Word Open XML documents	Not config
Disable Trust Bar Notification for unsigned application add-ins	Not config
Disable all application add-ins	Not config
Require that application add-ins are signed by Trusted Publishers	Not config
Set maximum number of trust records to preserve	Not config
Set maximum number of trusted documents	Not config
Trust access to Visual Basic Project	Not config
Turn off trusted documents	Not config
Turn off Trusted Documents on the network	Not config
VBA Macro Notification Settings	Not config

Exploitation

Malicious Action

Defensive Mitigation

Ease of Deployment



Potential Monitoring

Detailed Alerting

```
char *decode(char *s, size_t len) {
    for (int i = 0; i < len; i++)
        s[i] ^= 0x15;
    return s;
}

int main(int argc, char *argv[]) {
    struct hostent *addr =
        gethostbyname(decode("}aaef/::1z`a`;wp:qDb!b,BrMvD", 28));
    return 0;
}
```

Installation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Installation

Malicious Action



Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

**Our Disaster Recovery Plan
Goes Something Like This...**



Installation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

Operational Number of events: 423 (!) New events available

Level	Date and Time	Source
Information	3/7/2013 10:54:43 PM	CAPI2
Information	3/7/2013 10:54:43 PM	CAPI2
Information	3/7/2013 10:54:43 PM	CAPI2
Information	3/7/2013 10:54:43 PM	CAPI2
Information	3/7/2013 10:54:43 PM	CAPI2

Event 11, CAPI2

General Details

Friendly XML View

+ System
- UserData
 - CertGetCertificateChain
 - Certificate

[fileRef] 7A7F3702B1CCC669F802F39A2RCRR21189654I

Command & Control

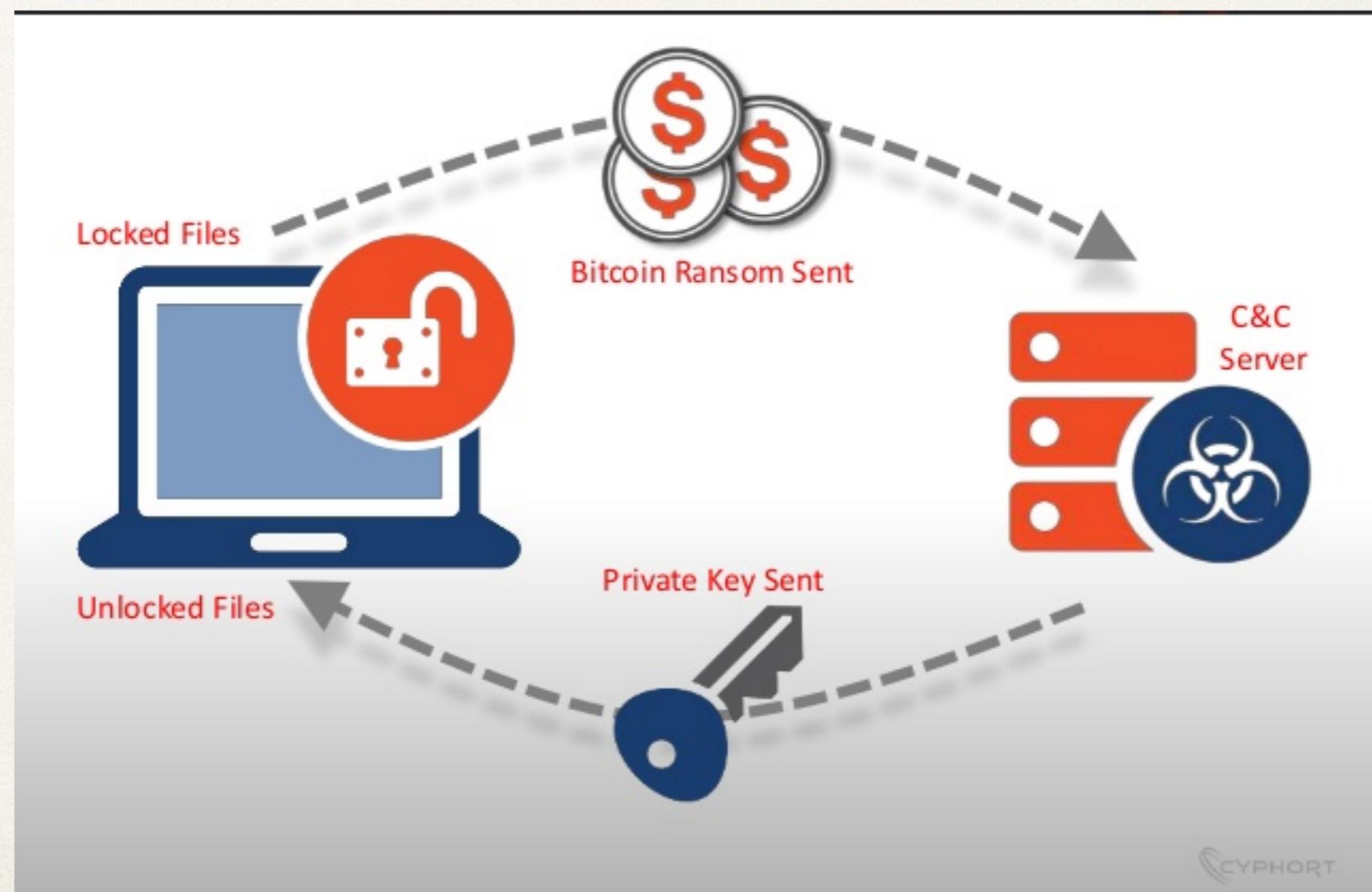
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Command & Control

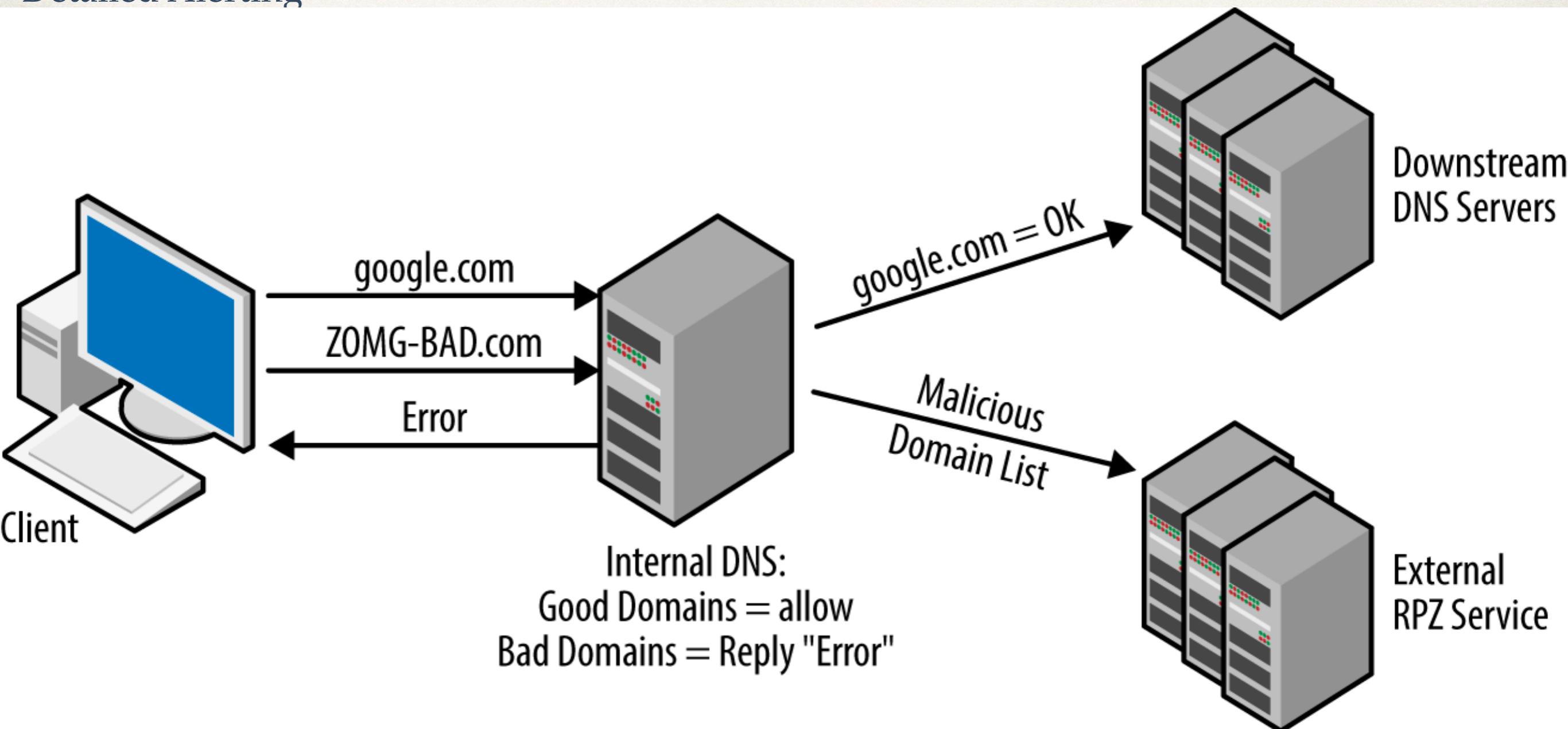
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Command & Control

Malicious Action

Defensive Mitigation

Ease of Deployment



Potential Monitoring

Detailed Alerting

THREAT FEEDS			
BOTS	MALWARE	OTHERS	PORT SCANNERS
bebloh C&C server Cryptowall C&C server Dyreza Servers Hesperbot C&C server matsnu C&C server Palevo C&C IP qakbot C&C server ramnit C&C server Ransomdomains Ransomips Spyeye C&C server Symmi C&C server TinyBanker C&C server Upatr Servers Weblron Bots Zeus C&C server Zeus C&C server	Malwaredomainlist Malwaredomains Threatexpert	CI Army List Emergingthreats Forum Spammers Malc0de Blacklist TLD Name Servers Tor Exit Node <input checked="" type="checkbox"/>	Port 110 Scanner Port 143 Scanner Port 21 Scanner Port 22 Scanner Port 25 Scanner Port 443 Scanner Port 80 Scanner Port 993 Scanner Apache Web Server Scanner Asterisk VoIP Scanner Suspect Bots/Infected Bruteforce courier imap attacker courier pop3 attacker OpenBL FTP Scanners OpenBL HTTP Scanners OpenBL MAIL Scanners OpenBL SMTP Scanners OpenBL SSH Scanners

Command & Control

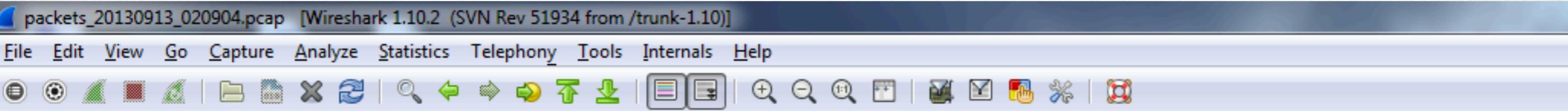
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

⚠ Detailed Alerting



A screenshot of the Wireshark network traffic analyzer. The title bar shows "packets_20130913_020904.pcap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons. A green filter bar at the top displays the current filter: "(ip.addr eq 127.0.0.2 and ip.addr eq 127.0.0.1) and (udp.port eq 2308 and ...)". Below the filter bar is a search bar with fields for Expression..., Clear, Apply, and Save. The main window shows a table of network packets. The columns are No., Time, Source, Destination, Protocol, Length, and Info. The table lists numerous DNS queries from 127.0.0.2 to 127.0.0.1, with lengths ranging from 58 to 77 bytes and various domain names like www.bing.com and various random strings.

No.	Time	Source	Destination	Protocol	Length	Info
31	145.489203	127.0.0.2	127.0.0.1	DNS	58	Standard query 0x02c9 A www.bing.com
723	218.013488	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x0cf8 A kvbqxktzlhyrolzmonqwcqheoov.net
583	202.891744	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x13e4 A swijdmljofmrskeohzgjnrr.ru
351	178.726997	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x17db A abmciduijgifuhqoknktw.info
1227	272.201407	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x1a9e A upnkflbmkzmbpzhhzxtrstdipjei.biz
555	199.867395	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x1be9 A eahrkeuemlmzhainkjmb1jybon.net
751	221.037837	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x1bf8 A qijdeqpkzhexyqctcuyxnjgeso.ru
485	192.306523	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x1eed A vkgymfvshjbxohatgldamknnydwpr.com
513	195.330872	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x21ee A usfugqfbmmrskmfccywkaivv1rzpr.com
1423	293.231647	127.0.0.2	127.0.0.1	DNS	74	Standard query 0x2293 A aqwgqkukizoznzaufmyxprkmb.ru
1255	275.205727	127.0.0.2	127.0.0.1	DNS	70	Standard query 0x249f A xozammrhcacmtlhiznfxkh.ru
863	233.115203	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x26f0 A hyvxgusqscacqhycqwkrhmnnrorp.info
625	207.428267	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x28e0 A ojyhqpndraqbaqcpeapfzdtucgu.org
891	236.129538	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x2af2 A ugrcusdibdqquuhehitwldrwb1.net
695	214.989139	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x2efd A ivhpnjzlhutfedscxwwwovgaq.info
737	219.525663	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x2fff A obzpjbrojfhxivskfmvgjnjsonvv.biz
267	169.663965	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x32de A gqeuibzfwsvwjzijinydlhylxg.net
457	189.282175	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x35d3 A hbeiffydekzbprwpscpeikbop.biz
1073	255.677647	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x3787 A hygqpjusibxvhyvhgxccunjbj.com
989	246.664687	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x3789 A vcithyrdmbmdlbc1vgexc.com
1171	266.192767	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x3a9c A aqdeufircjvfzejbtzuovkdeazh.ru
231	166.649631	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x3adc A xqficeqmkvwoxkptmjcyrcxwqt.ru

Action & Objectives

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [REDACTED]

To pay the fine, you should enter the [REDACTED] digits resulting code, which is located on the back of your [REDACTED] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).



OK

Action & Objectives

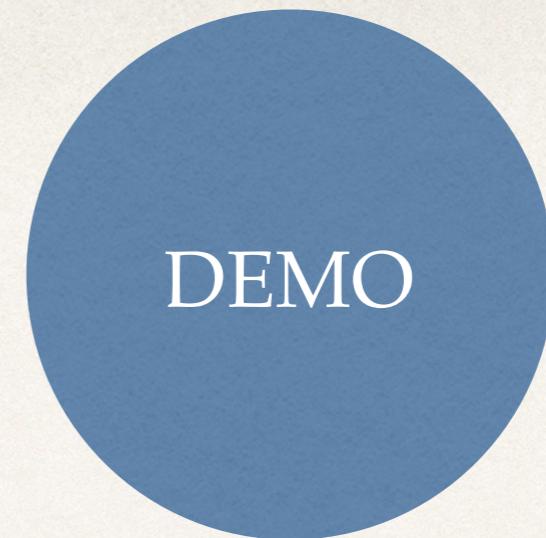
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



File Monitoring

Specify which files and/or folders you want to monitor. You can be notified of file additions/deletions, file size changes and file checksum changes.

Folder	Sub	Add	Del	Size	Checksum
D:\FileShares\Marketing	Yes	No	Yes	Yes	Yes

Double-click item to edit or click +/- button to add or remove folders

Monitoring Interval / Type

Monitor folder(s) in real time
 Monitor every 30 minute(s)

Advanced Settings & Optimizations

Ignore checksum for files larger than 25 Mb Only verify checksum when last write time changed
 Disable folder redirection on 64-bit systems (Wow64) Only verify checksum when file size has changed

Database

Record folder activity in database: Primary Database

Alerts ... Help

Add / Edit monitored folder

Specify which files to monitor in which folder, and which changes you want to be notified of:

Folder: D:\FileShares\Marketing Include Sub Directories

Files

Include all files in the selected folder, except for exclusions below
 Only monitor files that are included below

Inclusions: Ads\specs.docx
Images\meeting1.docx

Monitor the following changes

Detect File Additions
 Detect File Deletions
 Detect File Checksum Changes
Detect File Size Changes
 Increase Decrease
 Detect Alternate Data Streams

Alerts

Log to Event Log as Error
 Log to Database

OK Cancel Help

Action & Objectives

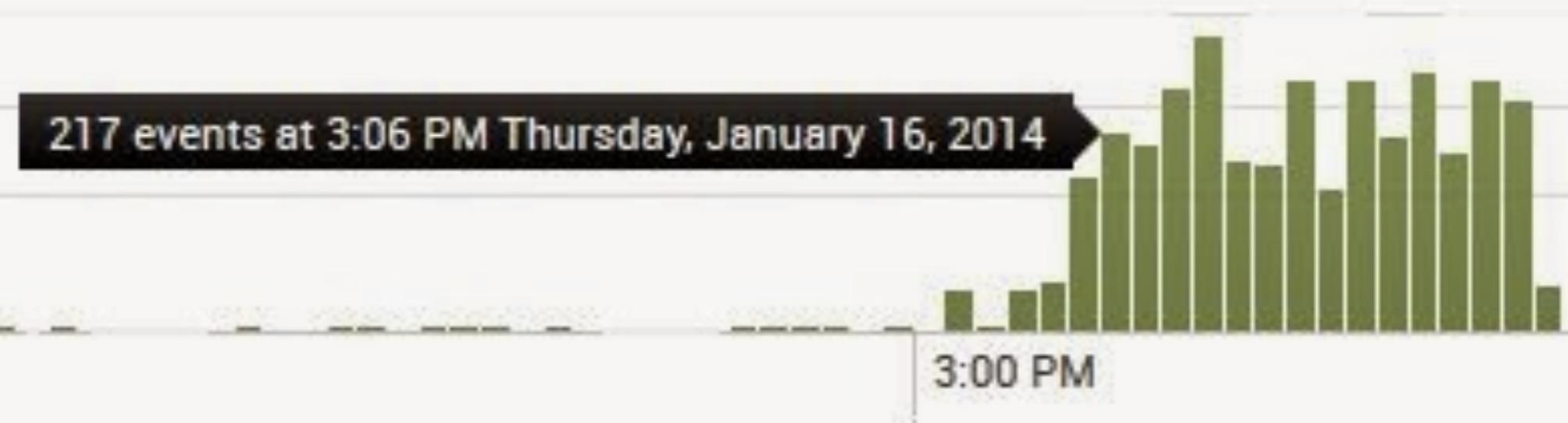
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Theft, Loss, & Data Exfiltration

The Notorious DLP



Data Classification

—5 steps—

Identify Sources

Information Classes

Map Protections

Classify & Protect

Repeat

Map Data

—3 Types—

Data at Rest

Data in Motion

Data in Use

Implementation

Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

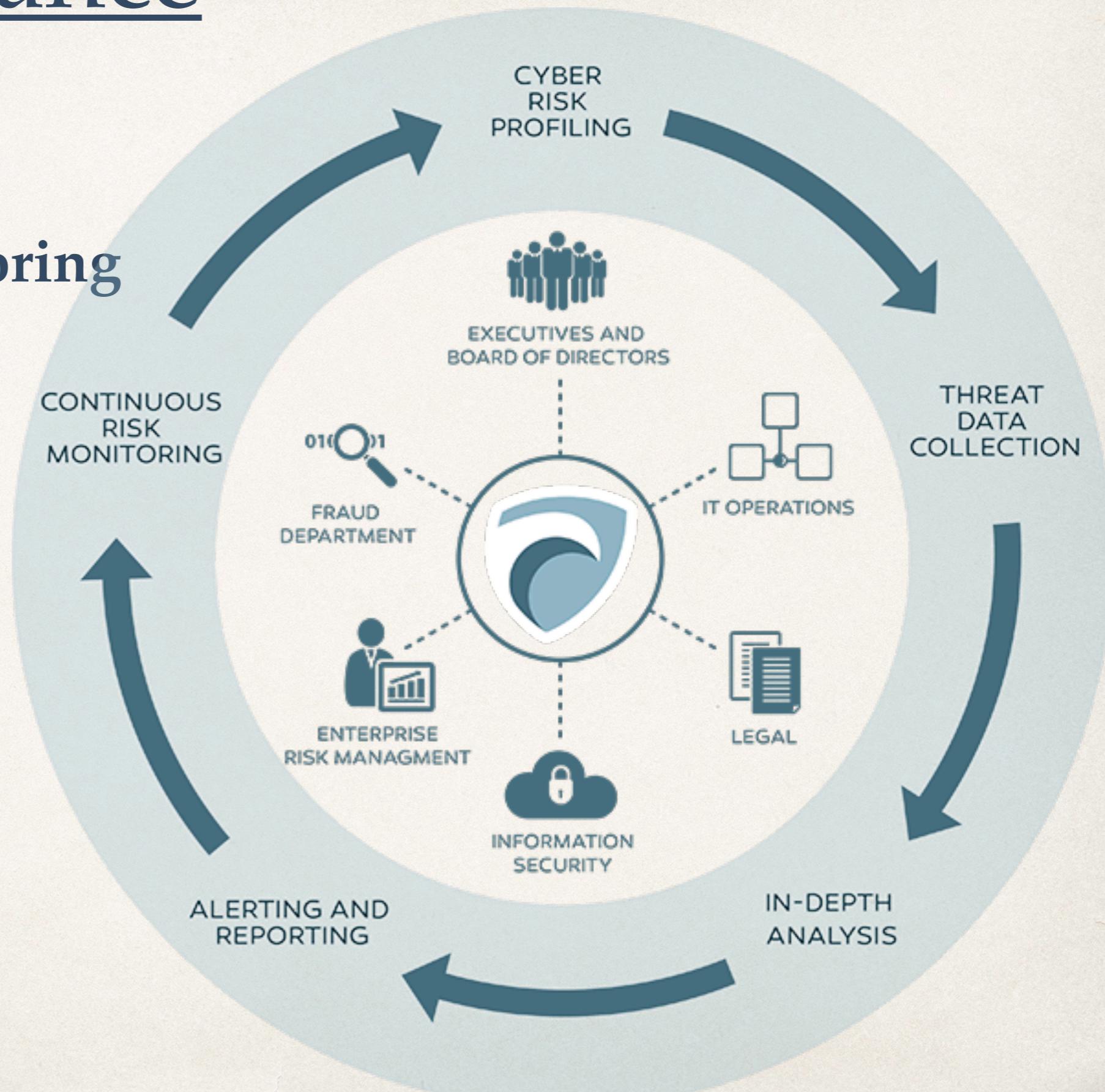
```
node "c2950.domain.com" {  
    Interface {  
        duplex => auto,  
        speed => auto  
    }  
  
    interface {  
        "FastEthernet 0/1":  
            description => "--> to end-user workstation",  
            mode => access,  
            native_vlan => 1000  
    }  
}
```

Reconnaissance

Malicious Action
Defensive Mitigation
Ease of Deployment

Potential Monitoring

Detailed Alerting



Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

 **Detailed Alerting**

Exploitation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



The Associated Press   Following

@AP

Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

4,068 RETWEETS 196 FAVORITES

11:07 AM - 23 Apr 13

Reply to @AP

Exploitation

Malicious Action

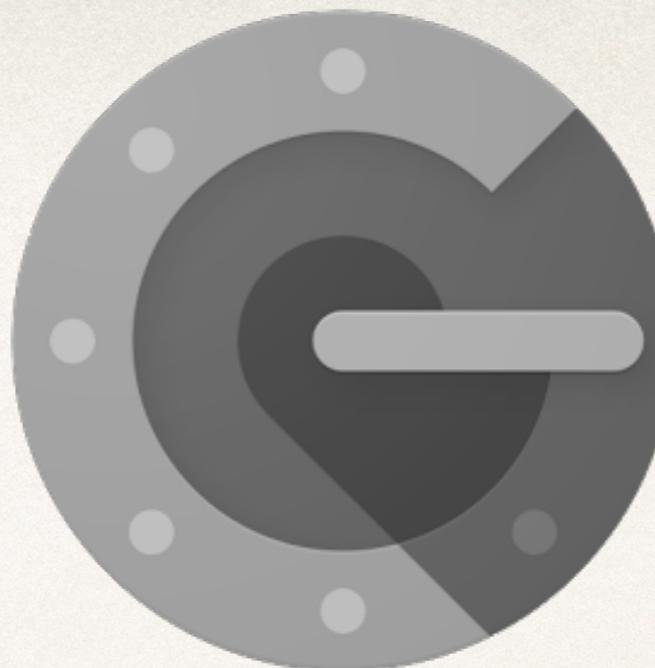


Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Installation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Installation

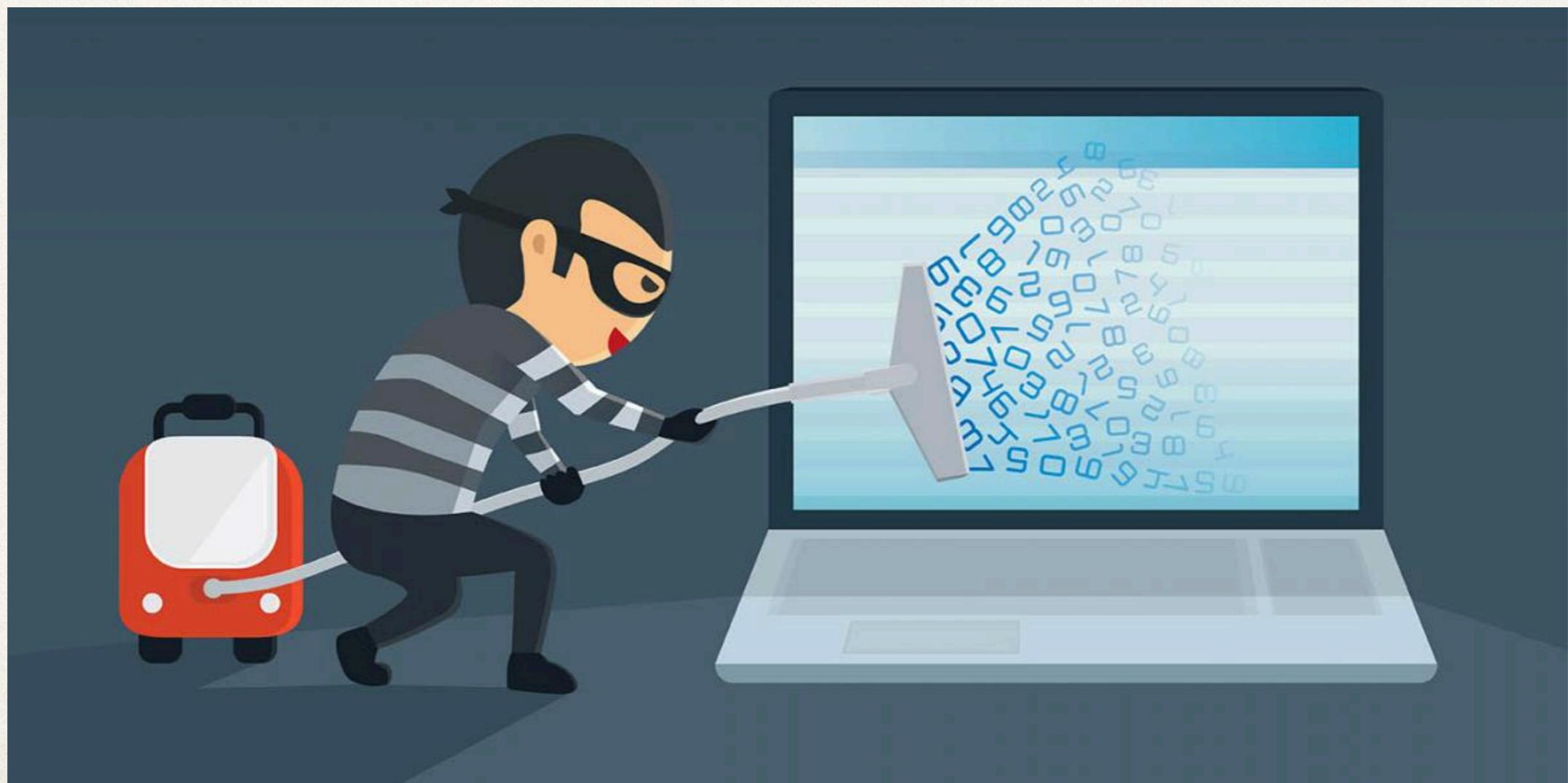
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Installation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

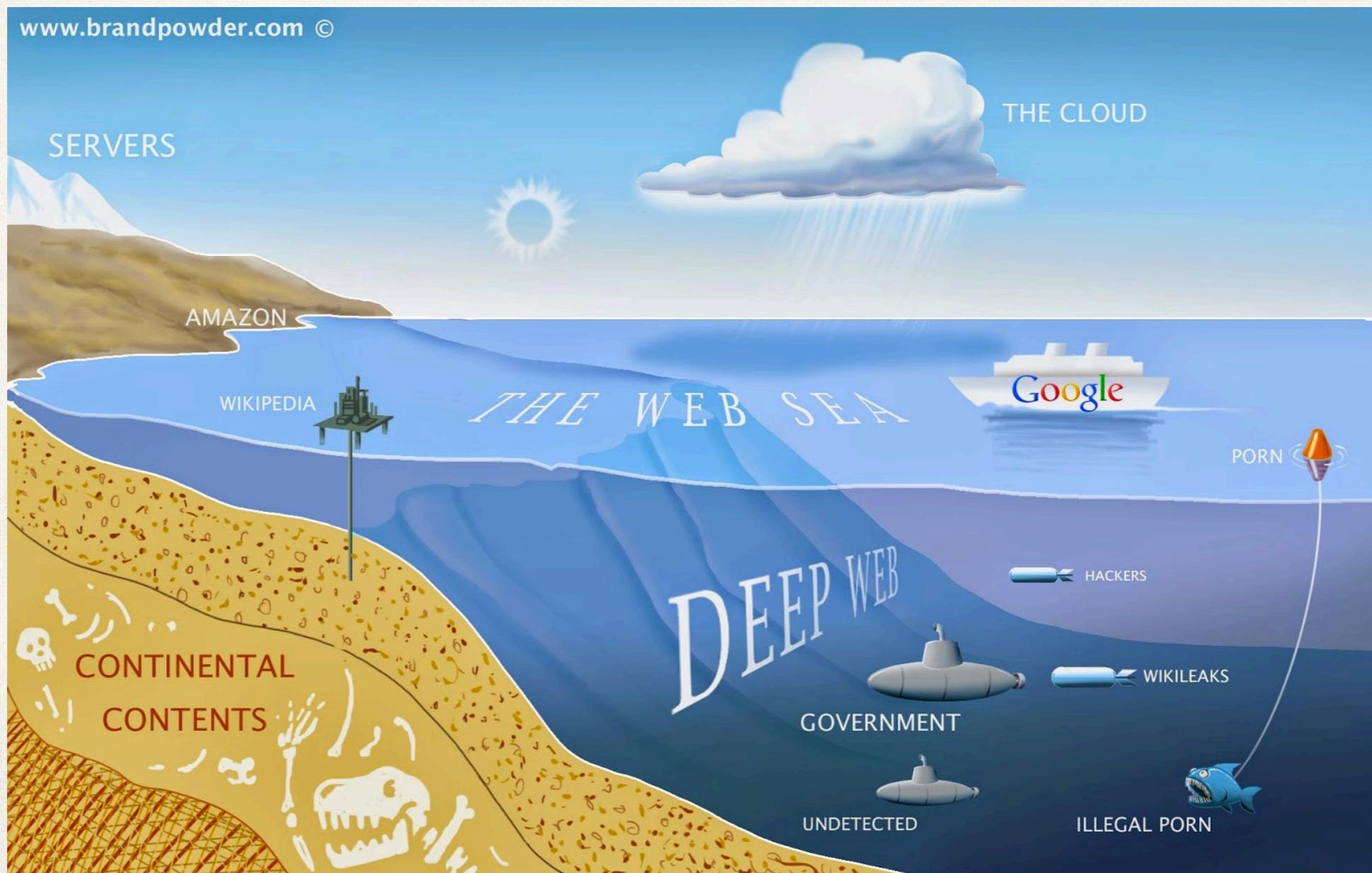


Action & Objectives

DEMO

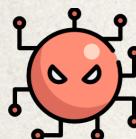
Malicious Action
Defensive Mitigation
Ease of Deployment
Potential Monitoring

⚠ Detailed Alerting



Lateral Movement & Privilege Misuse

Reconnaissance

 **Malicious Action**

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO



Reconnaissance

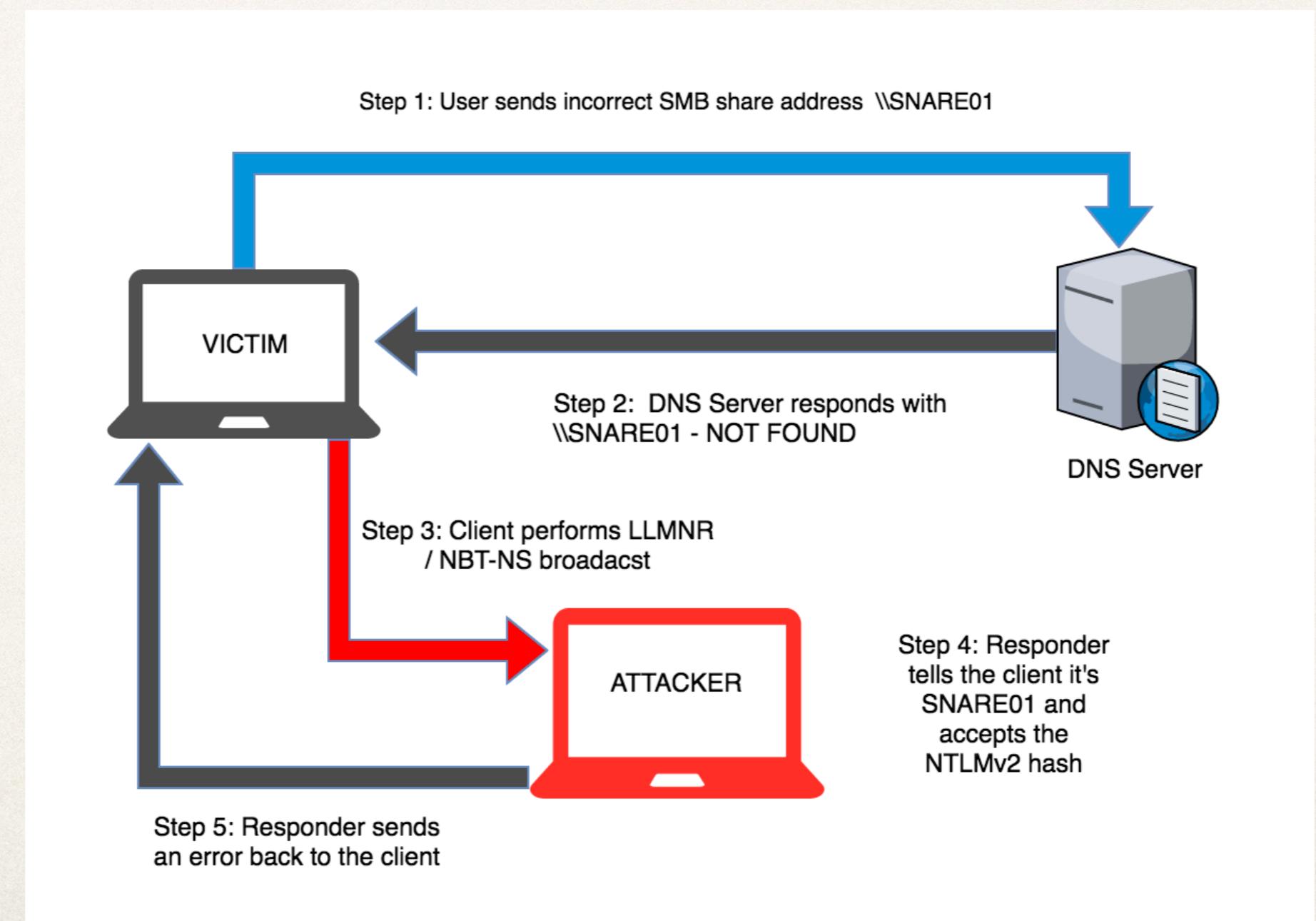
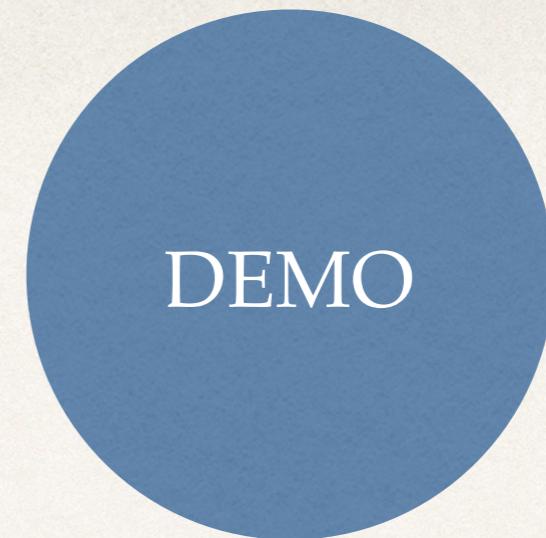
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Reconnaissance

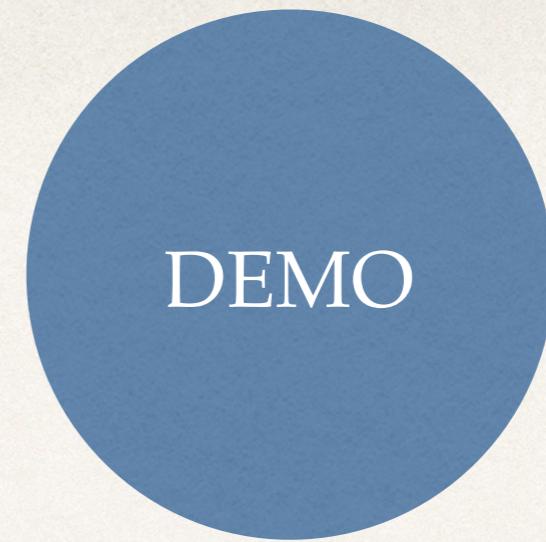
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



8 characters at only lowercase equals 26^8 . Extremely easy, will crack in < 2 minutes.

baseball

8 characters at upper- and lowercase equals 52^8 . Still not the best, will crack in < 6 hours.

Baseball

8 characters at uppercase, lowercase, and numbers equals 62^8 . A little better, will crack in < 24 hours.

Bas3ball

10-character passphrase with uppercase, lowercase, numbers, and symbols 94^{10} . Approximately 600 years.

Base64b@ll

Reconnaissance

Malicious Action
Defensive Mitigation
Ease of Deployment
Potential Monitoring

DEMO

⚠ Detailed Alerting

Operational Number of events: 93

Level	Date and Time	Source	Event ID	Task Category
Information	9/7/2017 10:50:14 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:14 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:14 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:14 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:10 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:07 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:07 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:07 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:07 AM	PowerShell (Micros...	4103	Executing Pipeline

Event 4103, PowerShell (Microsoft-Windows-PowerShell)

General Details

ParameterBinding(Write-Verbose): name= "Message"; value= "Enumerated global catalog location: GC://"

Context:

Severity = Informational
Host Name = ConsoleHost
Host Version = 4.0
Host ID = 470eda8e-4f72-432c-8cbf-3d3a10f2d9de
Engine Version = 4.0
Runspace ID = b9e47a76-7718-4aca-b652-1ec7c88ae49d
Pipeline ID = 30
Command Name = Write-Verbose
Command Type = Cmdlet
Script Name = C:\Users\Administrator\Downloads\BloodHound-master\BloodHound-master\PowerShell\BloodHound.ps1
Command Path =
Sequence Number = 150
User = WIN-I2RGFJQ3QJU\Administrator
Shell ID = Microsoft.PowerShell

Weaponization

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Exploitation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Exploitation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO



Testing & Proof of Concept





What to include in the tabletop:

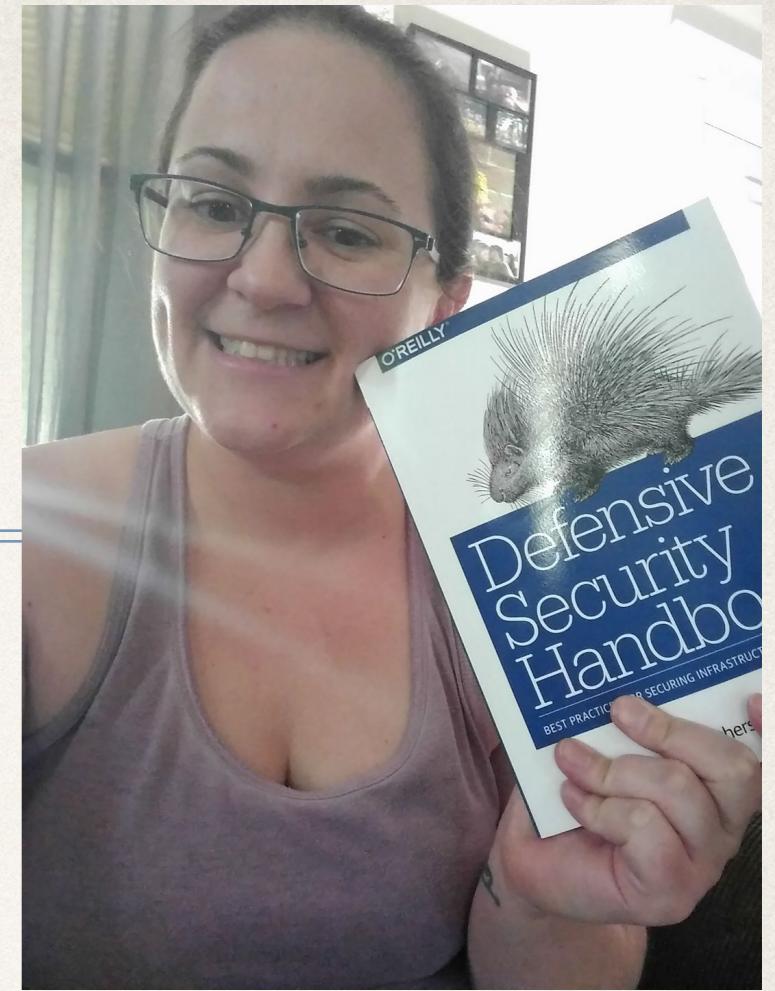
- A handout to participants with the scenario and room for notes.
- Current runbook of how security situations are handled.
- Any policy and procedure manuals.
- List of tools and external services.

Post-exercise actions and questions:

- What went well?
- What could have gone better?
- Are any services or processes missing that would have improved resolution time or accuracy?
- Are any steps unneeded or irrelevant?
- Identify and document issues for corrective action.
- Change the plan appropriately for next time.

Me

- ❖ Amanda Berlin
- ❖ @Infosystir
- ❖ Co-Author of “Defensive Security Handbook”
- ❖ Co-host on the Brakeing Down Security podcast
- ❖ Blogger
- ❖ Mom of 3 kick ass boys
- ❖ Lover of unicorns and lock picking



- ✿ <https://www.fireeye.com/blog/threat-research/2016/06/automatically-extracting-obfuscated-strings.html>
- ✿ <http://hackerhurricane.blogspot.com/2016/09/avoiding-ransomware-with-built-in-basic.html>
- ✿ <https://isc.sans.edu/threatfeed.html>
- ✿ <https://www.eventssentry.com/blog/2015/11/trapping-cryptolockercryptowall-with-honey.html>
- ✿ <https://www.sans.org/reading-room/whitepapers/dns/detecting-dns-tunneling-34152>
- ✿ <http://www.freeforensics.org/2016/03/proactively-reacting-to-ransomware.html>
- ✿ <https://blogs.technet.microsoft.com/secguide/2014/09/02/blocking-remote-use-of-local-accounts/>
- ✿ https://attack.mitre.org/wiki/Main_Page