



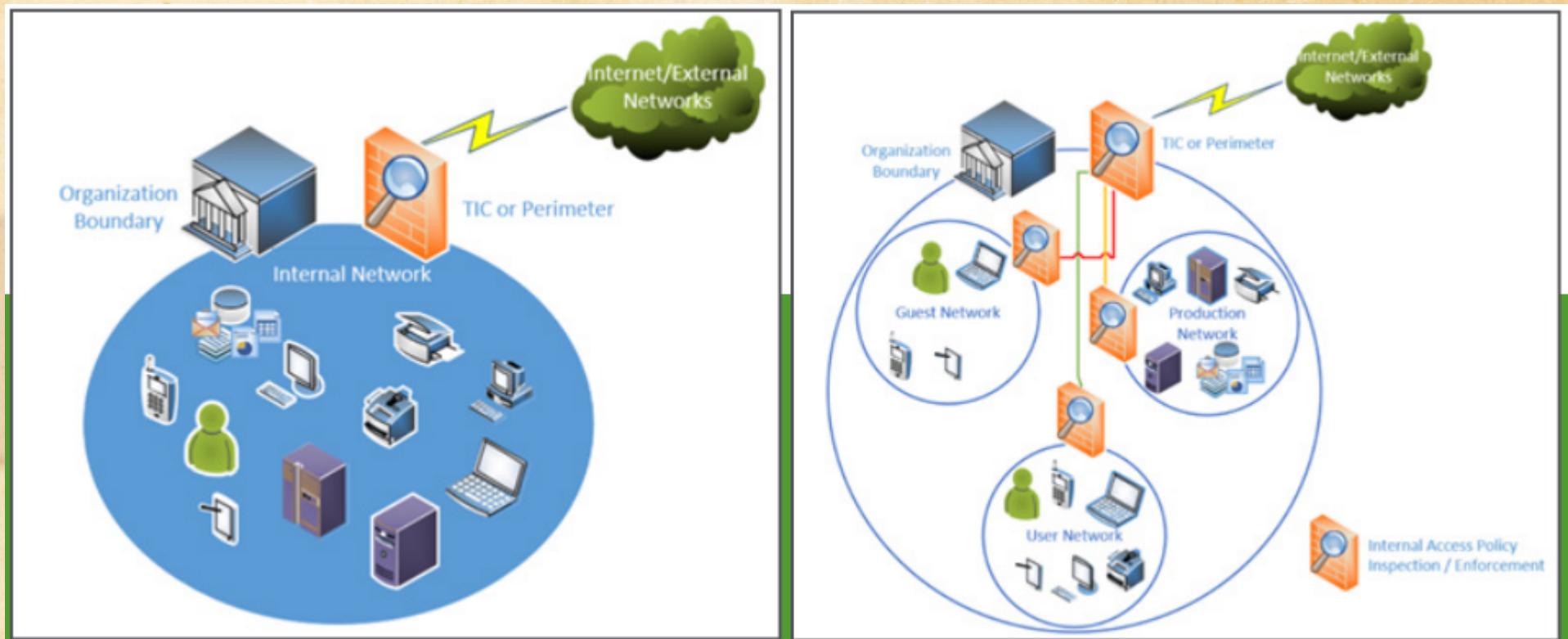
# **Leadership in Cybersecurity: You Are the Firewall**

Silicon Valley  
Engineering Leadership Community  
Thursday, August 18, 2022

Matthew C. Bascom  
[mcbascom@arizona.edu](mailto:mcbascom@arizona.edu)  
<https://www.linkedin.com/in/bascom>



- Threat – circumstances that could result in harm to an asset.
- Vulnerability – weaknesses that are subject to exploitation and may be caused by poor software design, improper software implementation, or improper software configuration.
- Harm – an actualized threat.
- Residual Risk – Risk that is not addressed.



*Figure. Flat (less secure) and Segmented (more secure) Networks*

Source: CISA MS-ISAC, “Ransomware Guide” (September 2020).

(MS-ISAC: Multi-State Info Sharing and Analysis Center)

# CIA-triad

Confidentiality

Integrity

Availability

# Types of Adversaries

Hacktivists

Script-Kiddies

Nation-State Actors (APTs)

Malicious Insiders

Criminals

Terrorists



*Figure.* Top five of  
25 Common Weakness Enumeration  
 (CWE), updated June 28, 2022.

Rank	ID	Name
1	<a href="#">CWE-787</a>	Out-of-bounds Write
2	<a href="#">CWE-79</a>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
3	<a href="#">CWE-89</a>	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
4	<a href="#">CWE-20</a>	Improper Input Validation
5	<a href="#">CWE-125</a>	Out-of-bounds Read

Score	KEV Count (CVEs)	Rank Change vs. 2021
64.20	62	0
45.97	2	0
22.11	7	+3 ▲
20.63	20	0
17.67	1	-2 ▼

*Example Language:* C

```
void host_lookup(char *user_supplied_addr){
    struct hostent *hp;
    in_addr_t *addr;
    char hostname[64];
    in_addr_t inet_addr(const char *cp);

    /*routine that ensures user_supplied_addr is in the right format for conversion */

    validate_addr_form(user_supplied_addr);
    addr = inet_addr(user_supplied_addr);
    hp = gethostbyaddr( addr, sizeof(struct in_addr), AF_INET);
    strcpy(hostname, hp->h_name);
}
```

*Figure.* Proof-of-concept code for  
CWE-787, Out-of-bounds Write.

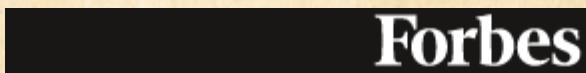
Reference	Description
<a href="#">CVE-2021-21220</a>	Chain: insufficient input validation ( <a href="#">CWE-20</a> ) in GPU kernel driver allows memory corruption [1].
<a href="#">CVE-2021-28664</a>	GPU kernel driver allows memory corruption [1].
<a href="#">CVE-2020-17087</a>	Chain: integer truncation ( <a href="#">CWE-197</a> ) causes stack-based buffer overflow [2]. See also <a href="#">CVE-2020-17088</a> . Per CISA KEV.
<a href="#">CVE-2020-1054</a>	Out-of-bounds write in kernel-mode driver, as part of a privilege escalation attack [3].
<a href="#">CVE-2020-0041</a>	Escape from browser sandbox using out-of-bounds write [4].
<a href="#">CVE-2020-0968</a>	Memory corruption in web browser scripting engine [5].
<a href="#">CVE-2020-0022</a>	Chain: mobile phone Bluetooth implementation [6].
<a href="#">CVE-2019-1010006</a>	Chain: compiler optimization ( <a href="#">CWE-733</a> ) removes bounds check [7].
<a href="#">CVE-2009-1532</a>	Malformed inputs cause accesses of uninitialized memory [8].
<a href="#">CVE-2009-0269</a>	Chain: -1 value from a function call was intended to be a length parameter [9].
<a href="#">CVE-2002-2227</a>	Unchecked length of SSLv2 challenge value [10].
<a href="#">CVE-2007-4580</a>	Buffer underflow from a small size value with large offset [11].
<a href="#">CVE-2007-4268</a>	Chain: integer signedness error ( <a href="#">CWE-195</a> ) plus integer truncation ( <a href="#">CWE-197</a> ) [12].
<a href="#">CVE-2009-2550</a>	Classic stack-based buffer overflow in media player [13].
<a href="#">CVE-2009-2403</a>	Heap-based buffer overflow in media player [14].

*Figure. The CWE-787 page includes a list of vulnerabilities caused by out-of-bounds writes.*

# What is NIST SP 800-207?

The NIST 800-series of special publications describes federal computer security policies and procedures, and guidelines for secure system design, system implementation, hardening, and secure system acquisition.

1. Identify legitimate ***consumers of data***.
2. Identify the ***assets*** owned by the enterprise.
3. What processes influence ***data access*** and what are their associated risks?
4. Determine policies for assets, data, and consumers of data.
5. Identify solutions to implement those policies.
6. Deploy the solutions necessary to control data consumption and monitor the performance of the solutions.



BREAKING • BUSINESS

# Hacker Tried To Raise Chemicals In Drinking Water ‘To Dangerous Levels’ At Florida Treatment Plant

**Carlie Porterfield** Forbes Staff  
*I cover breaking news.*

Follow



CYBERSECURITY

# Florida Water Plant Hackers Exploited Old Software And Poor Password Habits

**Lee Mathews** Senior Contributor ©  
*Observing, pondering, and writing about tech.  
Generally in that order.*

Feb 15, 2021, 10:21am EST

Follow

*Figure.* Articles from February 2021.

## Chasing Bitcoin: Why North Korea Ransomware Attacks Target U.S. Health Care Providers

JASON BRETT Contributor

I write about blockchain regulation and policy.

Jul 23, 2022, 08:11am EDT

Follow

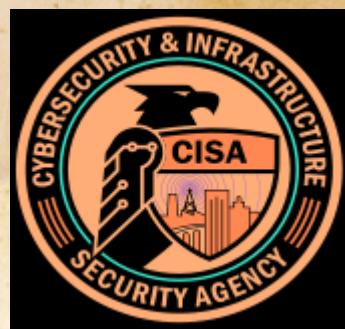
The U.S. Department of Justice (DOJ) announced this week that around \$500,000 in bitcoin BTC -3.8% has been seized from North Korean threat actors who were using Maui ransomware to attack healthcare organizations in the United States. DOJ filed a complaint in the District of Kansas asking for the forfeiture of the Bitcoin be returned to the victims of the attacks which were healthcare providers in Kansas and Colorado.

The attacks caused extensive disruption to IT systems and medical services and put patient safety at risk. The new

*“The combination of high-dollar rewards for breaching a U.S. hospital’s data records along with temporarily shutting down the technical services until a bitcoin ransom is paid is an outright attack on American citizens while they are in need of healthcare services.” - Jason Brett (2022).*

# Cybersecurity Incident & Vulnerability Response Playbooks

Operational Procedures for Planning and  
Conducting Cybersecurity Incident and Vulnerability  
Response Activities in FCEB Information Systems



*Figure. Incident Response Playbooks.*

FCEB – Federal Civilian Executive Branch, designed in accordance to Executive Order 14028:  
“Improving the Nation’s Cybersecurity”.

*Source: CISA (November 2021).*



# How can the enterprise secure against a cyber attack?

- Software Patching – implement recommended updates pushed out by vendors.
- System Hardening – close unused server ports and *uninstall unnecessary applications and services*.
- Separation of Privilege – This measure may prevent an attacker from moving laterally to other systems.

```
alert tcp any any -> any $HTTP_PORTS (msg:"TRICKBOT_ANCHOR:HTTP URI contains '/anchor'"; sid:1; rev:1; flow:established,to_server; content:"/anchor"; http_uri; fast_pattern:only; content:"GET"; nocase; http_method; pcre:"/^\/anchor_?.{3}\/[\\w_-]+\\.\\.[A-F0-9]+\\/?$/U"; classtype:bad-unknown; priority:1; metadata:service http;)
```

```
alert tcp any $SSL_PORTS -> any any (msg:"TRICKBOT:SSL/TLS Server X.509 Cert Field contains 'C=XX, L=Default City, O=Default Company Ltd'"; sid:1; rev:1; flow:established,from_server; ssl_state:server_hello; content:"|31 0b 30 09 06 03 55 04 06 13 02|XX"; nocase; content:"|31 15 30 13 06 03 55 04 07 13 0c|Default City"; nocase; content:"|31 1c 30 1a 06 03 55 04 0a 13 13|Default Company Ltd"; nocase; content:! "|31 0c 30 0a 06 03 55 04 03|"; classtype:bad-unknown; reference:url, www.virustotal.com/gui/file/e9600404ecc42cf86d38deedef94068db39b7a0fd06b3b8fb2d8a3c7002b650e/detection; metadata:service ssl;)
```

*Figure.* Snort IDS signatures for identifying Trickbot activity.

Source: “Best Practices for MITRE ATT&CK Mapping”, CISA, June 2021.

The image shows a screenshot of the VirusTotal analysis interface. At the top left, there is a circular progress bar with a red gradient, displaying the number '55' and '/ 69'. Below the progress bar, there is a red 'X' icon and a green checkmark icon next to the text 'Community Score'. On the right side, a large red warning icon with an exclamation mark is followed by the text '55 security vendors and 1 sandbox flagged this file as malicious'. Below this, the SHA256 hash of the file is shown: e9600404ecc42cf86d38deedef94068db39b7a0fd06b3b8fb2d8a3c7002b650e. Underneath the hash, the file name 'PORTABLEDEVICECLASSEXTENSION.DLL' is listed. Two tags are present: 'overlay' and 'peexe'. A horizontal line separates this from the vendor analysis section. The vendor analysis table has three columns: Vendor, Result, and Analysis. The first row shows 'VIPRE' with a red warning icon and 'Trojan.Win32.Generic!BT'. The second row shows 'Zillya' with a red warning icon and 'Trojan.Generic.Win32.894958'. The third row shows 'Acronis (Static ML)' with a green checkmark icon and 'Undetected'. The fourth row shows 'Baidu' with a green checkmark icon and 'Undetected'. To the right of the table, a section titled 'Security Vendors' Analysis' is visible, showing results for 'Ad-Aware' (red warning icon, 'Trojan.Mint.Zamg.X'), 'AhnLab-V3' (red warning icon, 'Malware/Win32.Generic.C3338281'), and another entry partially visible.

Vendor	Result	Analysis
VIPRE	!( Trojan.Win32.Generic!BT )	
Zillya	!( Trojan.Generic.Win32.894958 )	Ad-Aware !( Trojan.Mint.Zamg.X )
Acronis (Static ML)	✓ Undetected	AhnLab-V3 !( Malware/Win32.Generic.C3338281 )
Baidu	✓ Undetected	

*Figure.* Partial VirusTotal result for DLL with SHA256 of  
e9600404ecc42cf86d38deedef94068db39b7a0fd06b3b8fb2  
d8a3c7002b650e



National  
Security  
Agency



Cybersecurity &  
Infrastructure  
Security Agency



Federal Bureau  
of Investigation

TLP:W

## Cybersecurity Advisory

# People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices

### Summary

This joint Cybersecurity Advisory describes the ways in which People's Republic of China (PRC) state-sponsored cyber actors continue to exploit publicly known vulnerabilities in order to establish a broad network of compromised infrastructure. These actors use the network to exploit a wide variety of targets worldwide, including public and private sector organizations. The advisory

### Best Practices

- Apply patches as soon as possible
- Disable unnecessary ports and protocols
- Replace end-of-life infrastructure

*Figure.* Cybersecurity Advisory describing APT activity attributed to PRC that leverages vulnerable SOHO devices to route C2 communications. This particular report highlights Mimikatz, an open source technology for credential harvesting.

Source: "Cybersecurity Advisory" v1, NSA, CISA, FBI, June 2022.

SECURITY MARKET VALIDATION

## Amanda Rousseau, Endgame – Hack Naked News #124



Paul Asadoorian

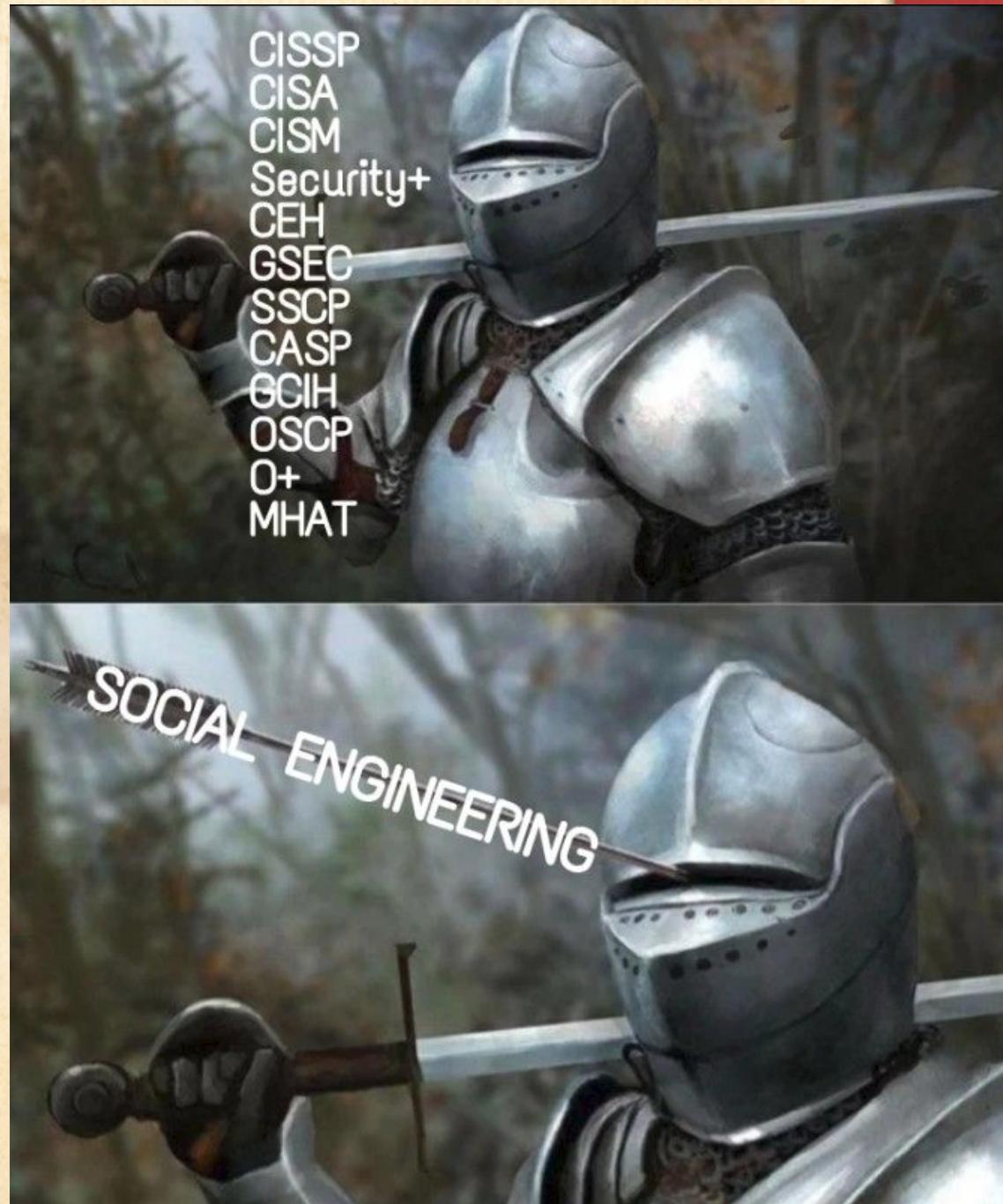
124, Amanda Rousseau, Endgame, Episode 124, Hack Naked, Hack Naked News, Hack Naked News 124, hacking news, asadoorian, ransomware, security weekly, Special Segment

May 17, 2017



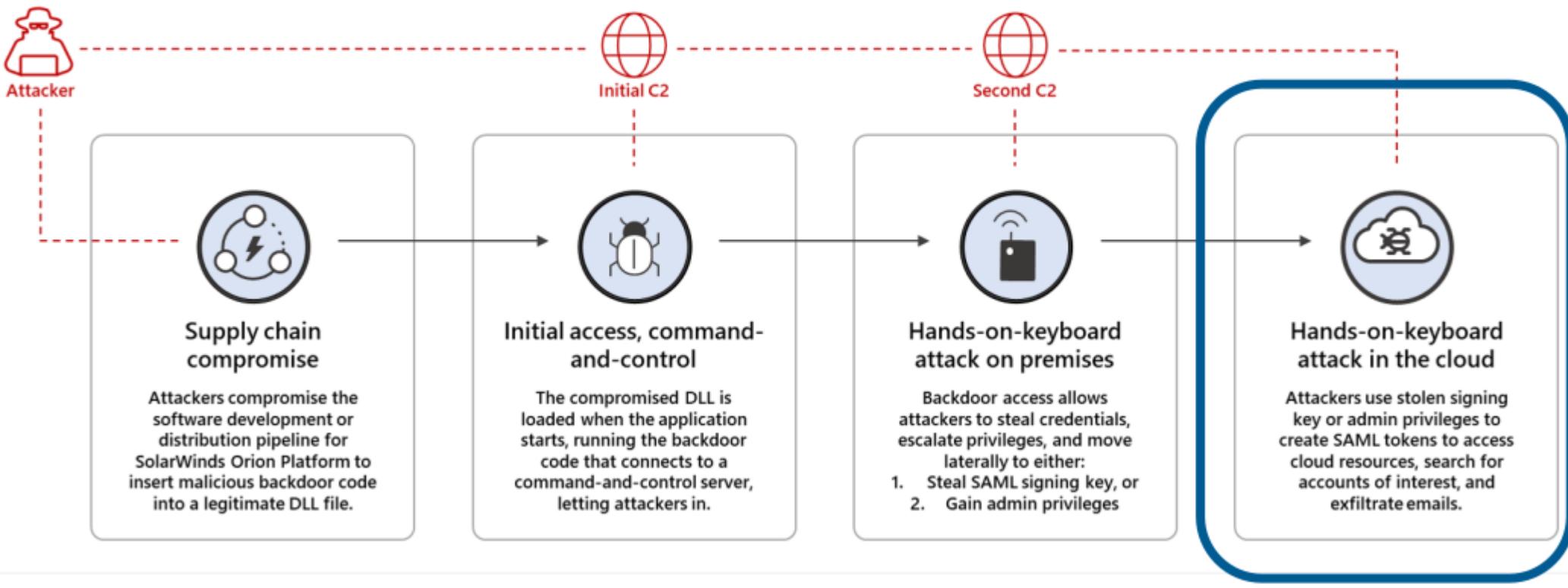
*Figure. Security Weekly Interview with Amanda Rousseau (Facebook) on Mimikatz.*

*Figure.* All the technical preparation in the world can still fail because of an effective social engineering attack.



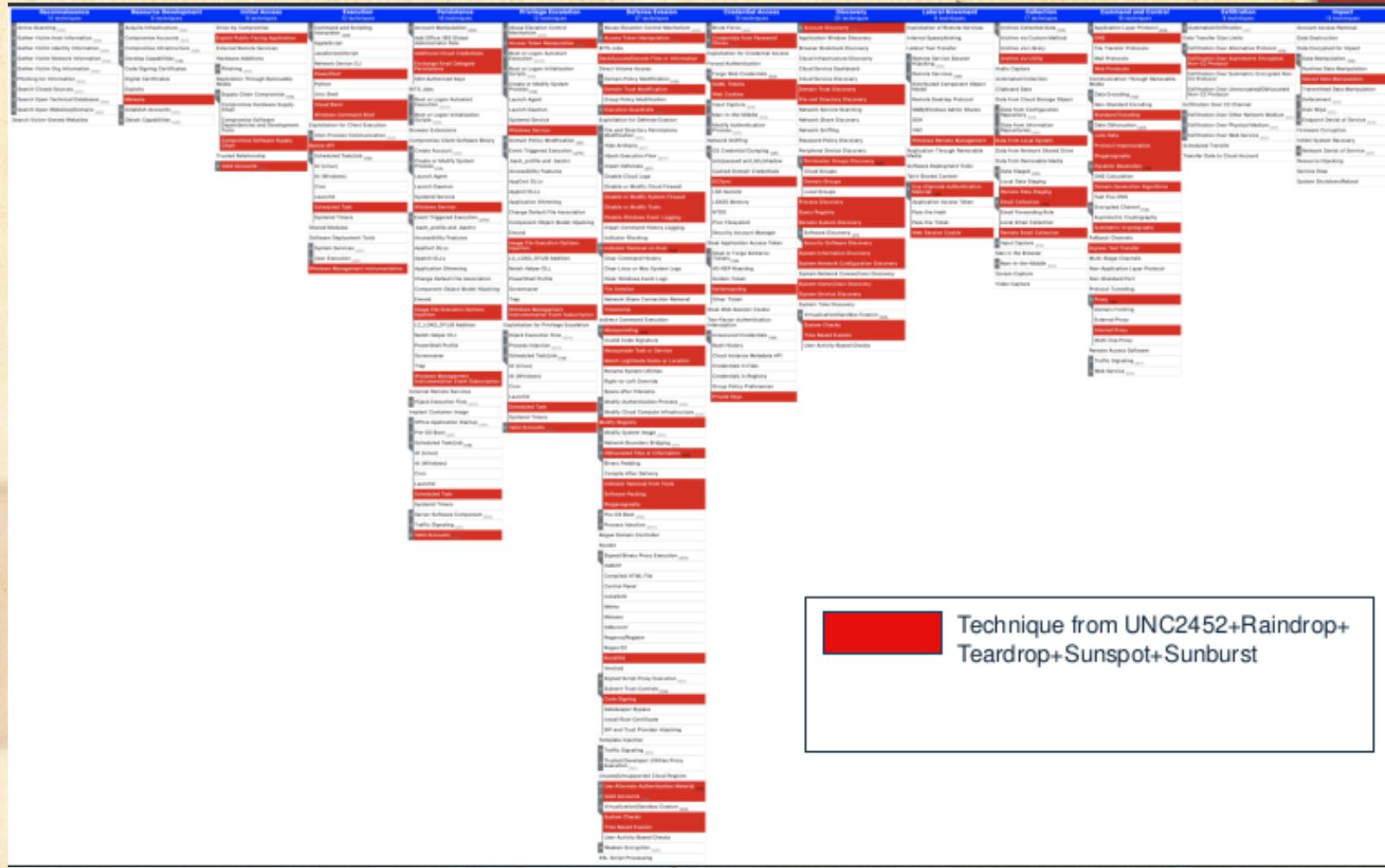
## SOLORIGATE ATTACK

### High-level end-to-end attack chain



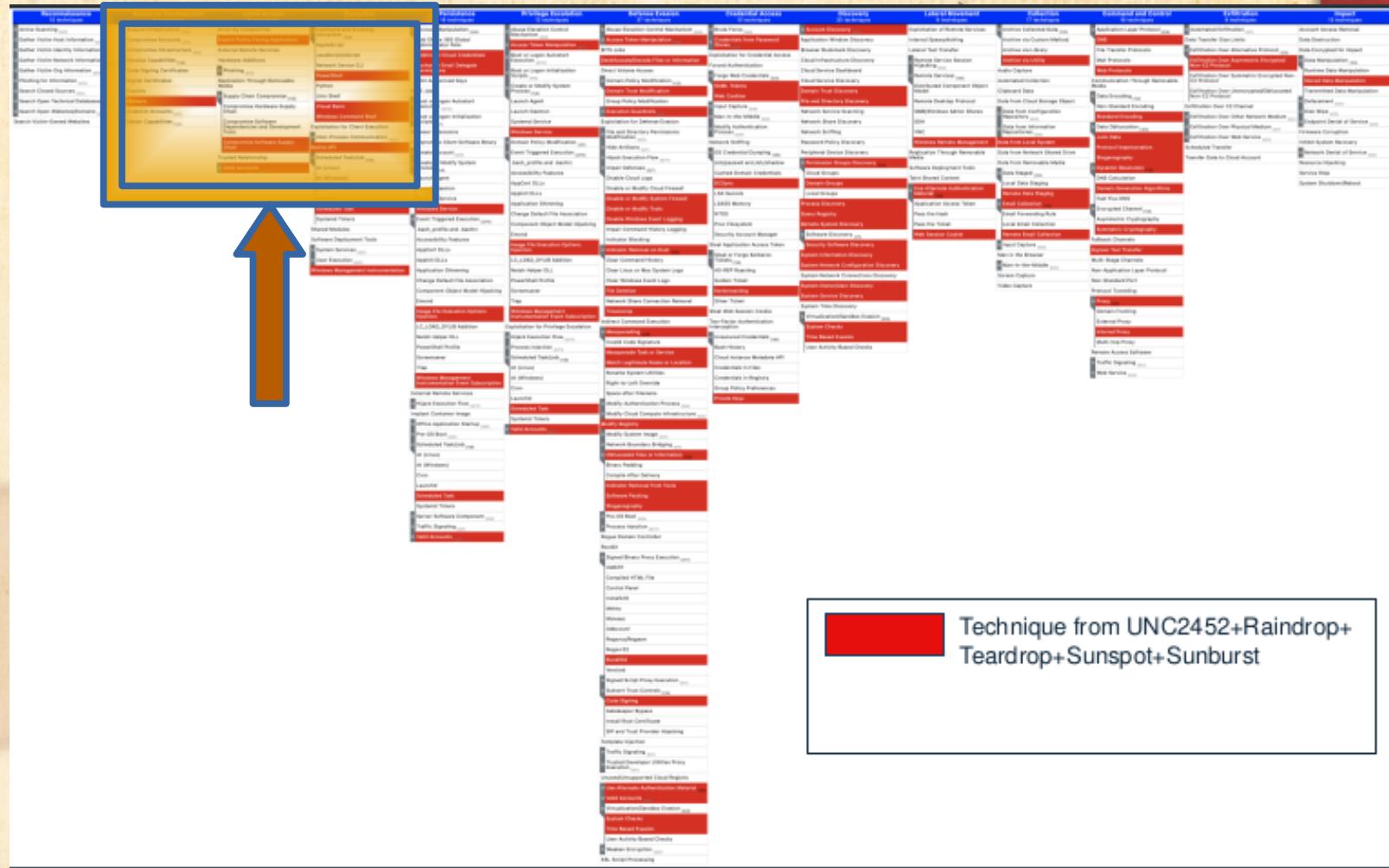
*Figure.* High-level end-to-end attack chain of the Solarwinds Solorigate attack.

Source: Jen Burns & Adam Pennington, “Quantifying Threat Actor Assessments”, MITRE, 2021.



*Figure.* High-level view of MITRE ATT&CK for enterprises and the December 2020 Solarwinds Solorigate attack.

Source: Jen Burns & Adam Pennington, “Quantifying Threat Actor Assessments”, MITRE, 2021.



*Figure.* High-level view of MITRE ATT&CK for enterprises and the December 2020 Solarwinds Solorigate attack.

Source: Jen Burns & Adam Pennington, “Quantifying Threat Actor Assessments”, MITRE, 2021.

Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques
Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (3/8)
Compromise Accounts (0/2)	Exploit Public-Facing Application	AppleScript
Compromise Infrastructure (0/6)	External Remote Services	JavaScript/JScript
Develop Capabilities (1/4)	Hardware Additions	Network Device CLI
Code Signing Certificates	II Phishing (0/3)	PowerShell
Digital Certificates	Replication Through Removable Media	Python
Exploits	II Supply Chain Compromise (1/3)	Unix Shell
Malware	Compromise Hardware Supply Chain	Visual Basic
Establish Accounts (0/2)	Compromise Software Dependencies and Development Tools	Windows Command Shell
Obtain Capabilities (0/6)	Compromise Software Supply Chain	Exploitation for Client Execution
	Trusted Relationship	II Inter-Process Communication (0/2)
	II Valid Accounts (0/4)	Native API
		II Scheduled Task/Job (1/6)
		At (Linux)

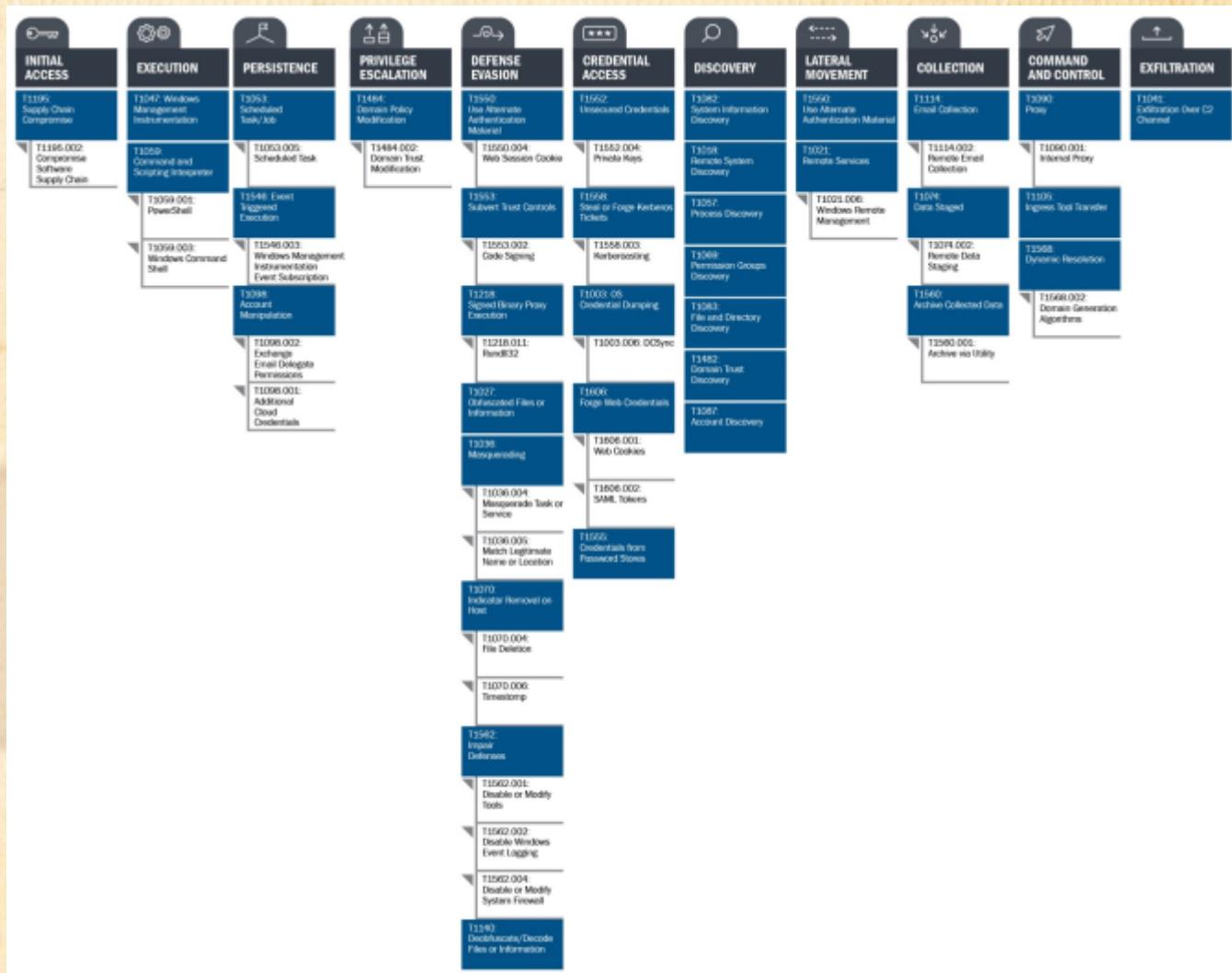
Figure. Top left portion of MITRE ATT&CK for Solarwinds Solorigate.

Source: Jen Burns & Adam Pennington, “Quantifying Threat Actor Assessments”, MITRE, 2021.

<ul style="list-style-type: none"> <li>• Reconnaissance</li> <li>• Resource Development</li> <li>• Initial Access</li> <li>• Execution</li> <li>• Discovery</li> </ul>	<ul style="list-style-type: none"> <li>• Persistence</li> <li>• Privilege Escalation</li> <li>• Defense Evasion</li> <li>• Credential Access</li> </ul>	<ul style="list-style-type: none"> <li>• Lateral Movement</li> <li>• Collection</li> <li>• Command &amp; Control</li> <li>• Exfiltration</li> <li>• Impact</li> </ul>
--	---	---

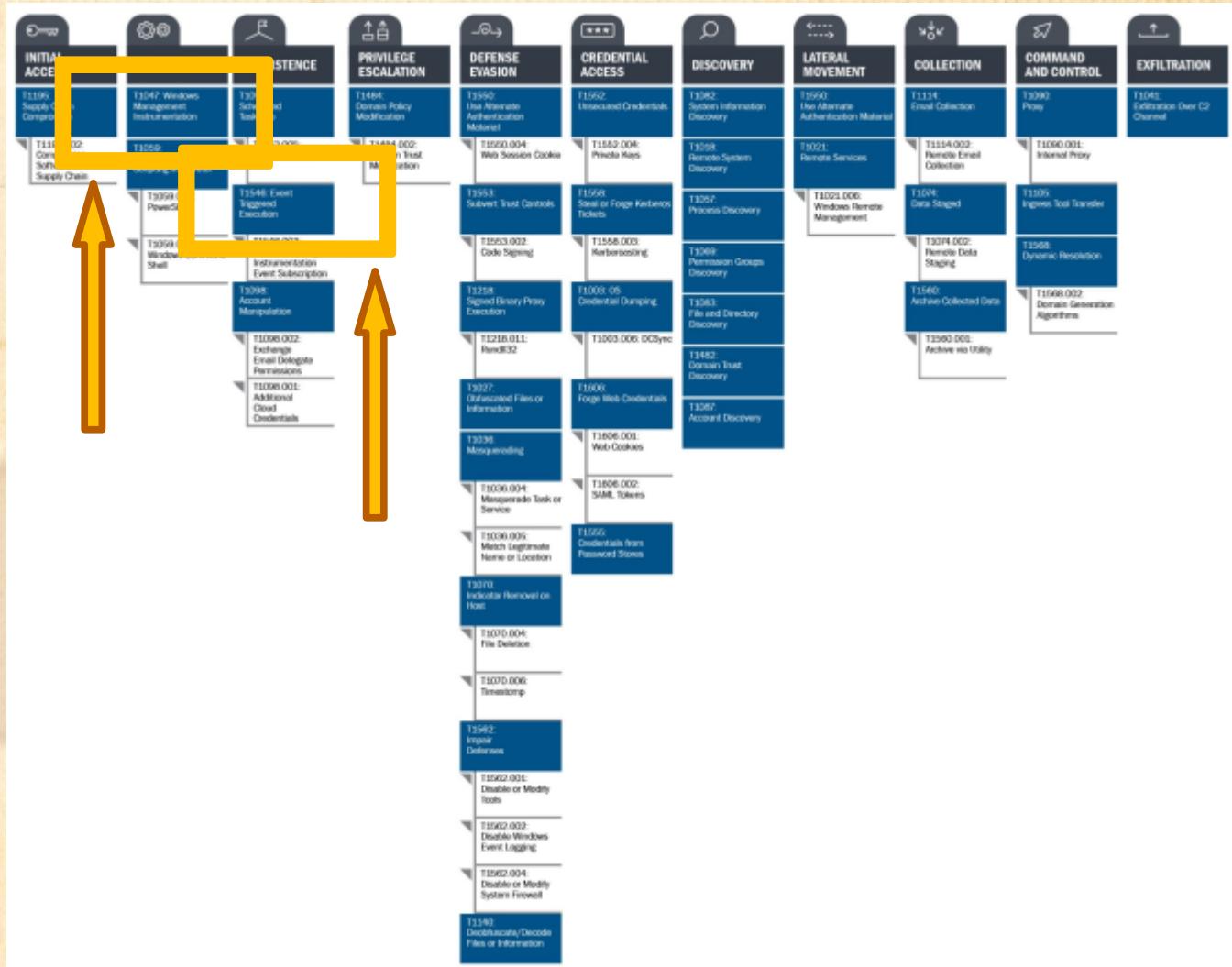
*Table.* List of MITRE Enterprise ATT&CK Framework Techniques. Each heading in the framework is a generalization of several detailed tactics & techniques.

Source: Jen Burns & Adam Pennington, “Quantifying Threat Actor Assessments”, MITRE, 2021.



*Figure.* An illustration of Solarwinds using MITRE ATT&CK .

Source: CISA, “SolarWinds and Active Directory/M365 Compromise: Detecting Advanced Persistent Threat Activity from Known Tactics, Techniques, and Procedures’, 2021.



*Figure.* An illustration of Solarwinds using MITRE ATT&CK .

Source: CISA, “SolarWinds and Active Directory/M365 Compromise: Detecting Advanced Persistent Threat Activity from Known Tactics, Techniques, and Procedures”, 2021.

Execution [TA0002] 	Windows Management Instrumentation [T1047]	The threat actor used Windows Management Instrumentation (WMI) for the remote execution of files for lateral movement. <sup>14,15,16</sup>	Monitor network traffic for WMI connections. WMI connections in environments that do not usually use WMI may be an indicator of compromise. Capture command-line arguments of wmic via process monitoring and look for commands that are used for remote behavior. <sup>17</sup> According to Microsoft, the following was used for lateral movement via WMI: <code>wmic /node:[target] process call create "rundll32 c:\windows\[folder]\[beacon].dll [export]"</code> . <sup>18</sup> <b>Note:</b> detecting WMI connections for execution requires detecting it at the time it happens.
Lateral Movement [TA0008] 			
Persistence [TA0003] 	Event Triggered Execution: Windows Management Instrumentation Event Subscription [T1546.003]	The threat actor used WMI event subscriptions for persistence. <sup>19,20</sup>	

*Table.* Solarwinds techniques T1047 and T1546 (both are techniques that perform Windows Management Instrumentation).

Source: CISA, “SolarWinds and Active Directory/M365 Compromise: Detecting Advanced Persistent Threat Activity from Known Tactics, Techniques, and Procedures”, 2021.

Execution [TA0002] 	Windows Management Instrumentation [T1047] 	The threat actor used Windows Management Instrumentation (WMI) for the remote execution of files for lateral movement. <sup>14,15,16</sup>	Monitor network traffic for WMI connections. WMI connections in environments that do not usually use WMI may be an indicator of compromise. Capture command-line arguments of wmic via process monitoring and look for commands that are used for remote behavior. <sup>17</sup> According to Microsoft, the following was used for lateral movement via WMI: <code>wmic /node:[target] process call create "rundll32 c:\windows\[folder]\[beacon].dll [export]"</code> . <sup>18</sup> <b>Note:</b> detecting WMI connections for execution requires detecting it at the time it happens.
Lateral Movement [TA0008] 			
Persistence [TA0003] 	Event Triggered Execution: Windows Management Instrumentation Event Subscription [T1546.003]	The threat actor used WMI event subscriptions for persistence. <sup>19,20</sup>	

*Table.* Solarwinds techniques T1047 and T1546 (both are techniques that perform Windows Management Instrumentation).

Source: CISA, “SolarWinds and Active Directory/M365 Compromise: Detecting Advanced Persistent Threat Activity from Known Tactics, Techniques, and Procedures”, 2021.

## Windows Management Instrumentation

Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform environment to access Windows system components. The WMI service enables both local and remote access, though the latter is facilitated by [Remote Services](#) such as [Distributed Component Object Model \(DCOM\)](#) and [Windows Remote Management \(WinRM\)](#).<sup>[1]</sup> Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.<sup>[1][2]</sup>

An adversary can use WMI to interact with local and remote systems and use it as a means to execute various behaviors, such as gathering information for Discovery as well as remote Execution of files as part of Lateral Movement.<sup>[3]</sup> [2]

*Figure.* MITRE's [Technique T1047](#) page includes detection aids, mitigations, and 87 examples where T1047 has been used in the wild including the well known exploits REvil, Stuxnet, NotPetya, Emotet, Empire, and WannaCry.



## **SolarWinds and Active Directory/M365 Compromise: Detecting Advanced Persistent Threat Activity from Known Tactics, Techniques, and Procedures**

**March 17, 2021**

**Cybersecurity and Infrastructure Security Agency**



*Figure.* The Solarwinds attack was attributed to the Russian Foreign Intelligence Service.

The screenshot shows a web browser window with the URL <https://trustfoundry.net/using-iodine-for-dns-tunneling-c2-to-bypass-egress-filtering/>. The page features a large orange and grey logo on the left. The main title is "Using Iodine for DNS Tunneling C2 to Bypass Egress Filtering". Below the title, there is a section titled "Intro" which contains text about egress filtering. The page has a dark background with a grid pattern.

TrustFoundry

# Using Iodine for DNS Tunneling C2 to Bypass Egress Filtering

## Intro

Security-conscious organizations will often restrict the types of traffic allowed out of their networks. Protocols or ports deemed unnecessary for the majority of the organization's users will simply be blocked, with whitelists established for the few users who may have a business need to get around those restrictions. Restricting outbound traffic in this manner is a practice known as egress filtering, and it can be an effective security control that makes establishing Command and Control (C2) channels much more difficult for attackers.

*Figure.* Toolkits are widely available that will take advantage of system vulnerabilities. For example, login portals will often block HTTP/S (ports 80/443) but not DNS (port 53).

Source: [TrustFoundry](#)



Open questions for the enterprise CISO (Chief Information Security Officer), according to Palo Alto Networks:

- How can cybersecurity help generate, protect, and ensure revenue?
- How can cybersecurity help retain existing customers?
- How can cybersecurity help differentiate against competitors?
- How can cybersecurity drive operational efficiencies and effectiveness?

(It's a cross-functional role: sales, operations, finance...)

Source: “Navigating the Digital Age” v3, Palo Alto Networks.



# Lockheed Martin's Cyber Kill Chain ® Seven Phase Framework

Reconnaissance	Installation
Weaponization	Command & Control
Delivery	Actions & Objectives
Exploitation	

WHAT  
DOES THE  
DATA  
TELL US  
TO DO?



WE ONLY  
HAVE BAD  
DATA ON  
THIS.



©SCOTTADAMSAYS  
DILBERT.COM.  
DOES THE BAD DATA  
SUGGEST WE SHOULD DO  
WHAT WE WANTED TO  
DO ANYWAY?

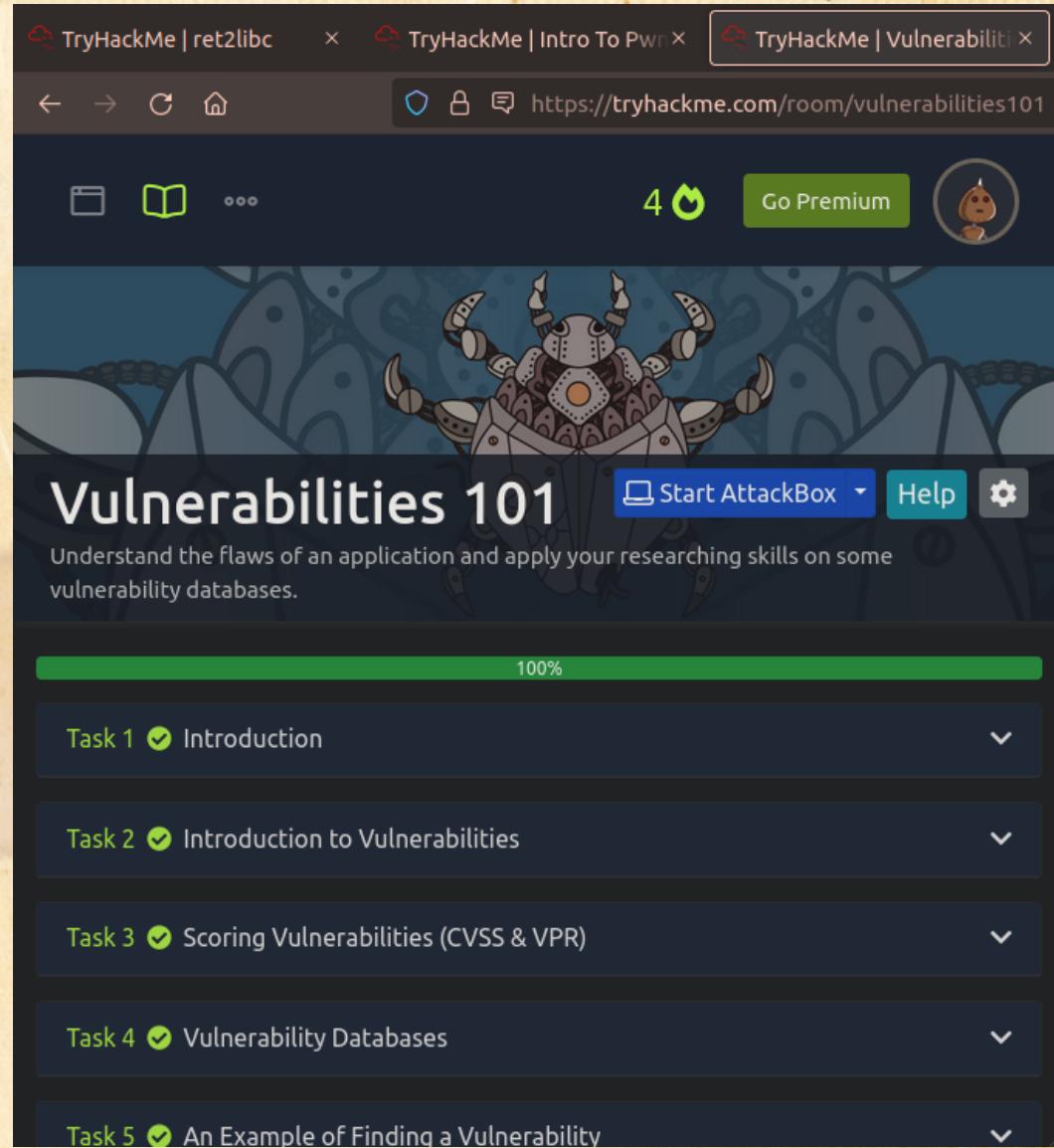


WELL,  
YES.

4-3-18 ©2018 Scott Adams, Inc./Cart. by Andrews McMeel

THAT'S CALLED  
"GOOD DATA."





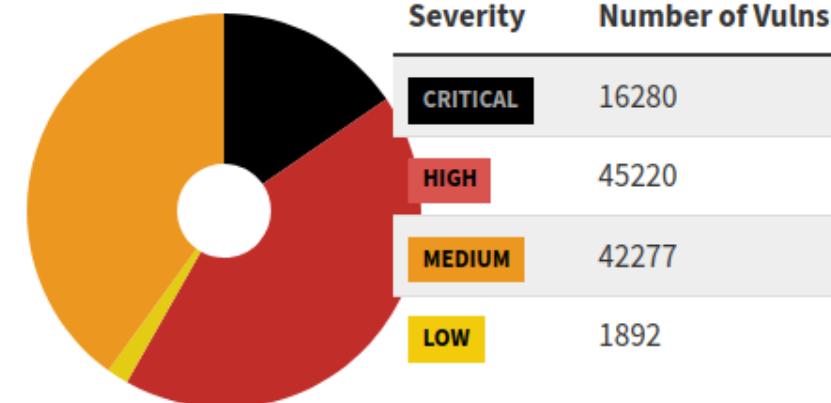
*Figure.* The gamification of hacking tools makes practice accessible to anyone willing to run a remote desktop (RDP) and a VPN.  
Image: TryHackMe.com



*Figure.* CTF spiderplot used to track aptitude for practicing cyber professionals. This plot shows relative performance in several domains including web app exploitation, log analysis, and password cracking. 35

**NATIONAL VULNERABILITY DATABASE****NVD Dashboard****CVEs Received and Processed**

Time Period	New CVEs Received by NVD	New CVEs Analyzed by NVD	Modified CVEs Received by NVD	Modified CVEs Re-analyzed by NVD
Today	0	0	0	0
This Week	46	75	14	9
This Month	534	538	170	91
Last Month	1959	2060	889	676
This Year	14920	15177	5587	6036

**CVSS V3 Score Distribution**

*Figure. NIST's National Vulnerability Database – Statistics for the week of August 7, 2022.*

Information Technology Laboratory

## NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

### CVE-2022-2274 Detail

#### AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

#### Description

The OpenSSL 3.0.4 release introduced a serious bug in the RSA implementation for X86\_64 CPUs supporting the AVX512IFMA instructions. This issue makes the RSA implementation with 2048 bit private keys incorrect on such

#### QUICK INFO

**CVE Dictionary Entry:**  
CVE-2022-2274

**NVD Published Date:**  
07/01/2022

**NVD Last Modified:**  
07/05/2022

*Figure. [CVE-2022-2274](#), an RSA encryption vulnerability that was published in July and affects x86-64 CPU architecture.*

CVE: Common Vulnerabilities & Exposures. See: [www.cve.org](http://www.cve.org), by <sup>37</sup> MITRE and sponsored by Dept. of Homeland Security & CISA.

The screenshot shows the Exploit Database homepage. On the left is a vertical sidebar with orange icons: a spider, a TV, a magnifying glass, a folder, a film strip, a search icon, a book, an upward arrow, and a graduation cap. The main content area has a dark blue header with the "EXPLOIT DATABASE" logo, which features a stylized spider icon and the text "EXPLOIT DATABASE". Below the header is a search bar with two checkboxes: "Verified" and "Has App", and buttons for "Filters" and "Reset All". A "Show 15" dropdown is also present. To the right is a search bar labeled "Search: [ ]". The main table lists vulnerabilities with columns for Date, Title, Type, Platform, and Author. The first entry is "WiFi Mouse 1.7.8.5 - Remote Code Execution(v2)" by RedHatAugust. The other entries are from June 14, 2022, and include "Mailhog 1.0.1 - Stored Cross-Site Scripting (XSS)", "WSO2 Management Console (Multiple Products) - Unauthenticated Reflected Cross-Site Scripting (XSS)", "WordPress Plugin Weblizar 8.9 - Backdoor", "SolarView Compact 6.00 - 'pow' Cross-Site Scripting (XSS)", "SolarView Compact 6.00 - 'time\_begin' Cross-Site Scripting (XSS)", "Old Age Home Management System 1.0 - SQLi Authentication Bypass", "ChurchCRM 4.4.5 - SQLi", and "Sourcegraph Gitserver 3.36.3 - Remote Code Execution (RCE)".

Date	Title	Type	Platform	Author
2022-07-01	WiFi Mouse 1.7.8.5 - Remote Code Execution(v2)	Remote	Windows	RedHatAugust
2022-06-27	Mailhog 1.0.1 - Stored Cross-Site Scripting (XSS)	WebApps	Multiple	Vulnz
2022-06-27	WSO2 Management Console (Multiple Products) - Unauthenticated Reflected Cross-Site Scripting (XSS)	WebApps	PHP	cxosmo
2022-06-27	WordPress Plugin Weblizar 8.9 - Backdoor	WebApps	PHP	Sobhan Mahmoodi
2022-06-14	SolarView Compact 6.00 - 'pow' Cross-Site Scripting (XSS)	WebApps	Hardware	Ahmed Alroky
2022-06-14	SolarView Compact 6.00 - 'time_begin' Cross-Site Scripting (XSS)	WebApps	Hardware	Ahmed Alroky
2022-06-14	Old Age Home Management System 1.0 - SQLi Authentication Bypass	WebApps	PHP	twseptian
2022-06-14	ChurchCRM 4.4.5 - SQLi	WebApps	PHP	nu11secur1ty
2022-06-14	Sourcegraph Gitserver 3.36.3 - Remote Code Execution (RCE)	Remote	Multiple	Altelus

*Figure.* Exploit Database publishes proof of concepts against vulnerabilities as they become publicly available. The top reads, “WiFi Mouse Remote Code Execution” remotely runs code on Windows. The others, from the previous 15 days, include web application exploits that leverage vulnerabilities in PHP.

The screenshot shows a browser window with several tabs open, including "TryHackMe | ret2libc", "TryHackMe | Intro To Pwn", "TryHackMe | Vulnerabiliti", "NVD - CVE-2022-2274", and "WiFi Mouse 1.7.8.5 - Rem". The main content area displays a Python exploit script for WiFi Mouse 1.7.8.5. The script includes comments about the exploit title, date, author, vendor, software link, version, and test environment. It also notes that Python 3 was used and references an original exploit from exploit-db. The script itself uses socket programming to connect to a target host and port, handling command-line arguments for the remote host, local host, and payload.

```
# Exploit Title: WiFi Mouse 1.7.8.5 - Remote Code Execution
# Date: 25-02-2021
# Author: H4rk3nz0
# Vendor Homepage: http://necta.us/
# Software Link: http://wifimouse.necta.us/#download
# Version: 1.7.8.5
# Tested on: Windows Enterprise Build 17763

# Python 3 port done by RedHatAugust
# Original exploit: https://www.exploit-db.com/exploits/49601
# Tested on: Windows 10 Pro Build 15063

# Desktop Server software used by mobile app has PIN option which does not prevent command input.
# Connection response will be 'needpassword' which is only interpreted by mobile app and prompts for PIN input.

#!/usr/bin/env python3

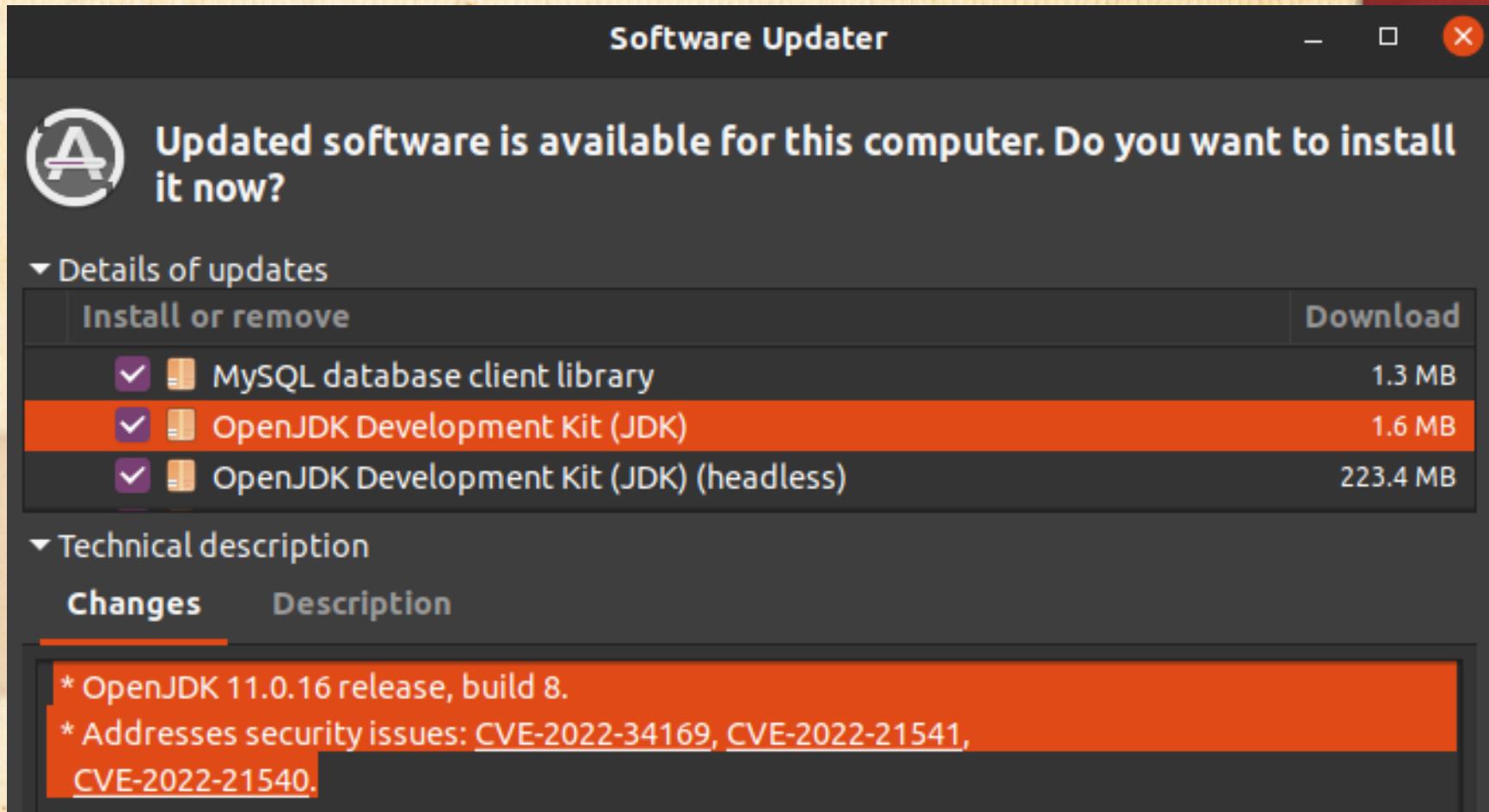
from socket import socket, AF_INET, SOCK_STREAM
from time import sleep
import sys
import string

target = socket(AF_INET, SOCK_STREAM)
port = 1978

try:
    rhost = sys.argv[1]
    lhost = sys.argv[2]
    payload = sys.argv[3]
```

*Figure.* Proof-of-concept Python code that leverages the vulnerability discovered in WiFi mouse devices. Note that this vulnerability does not have a corresponding CVE entry on NIST's NVD database.

Source: [www.exploit-db.com/exploits/50972](https://www.exploit-db.com/exploits/50972)



*Figure. [CVE-2022-34169](#). “The Apache Xalan Java XSLT library is vulnerable to an integer truncation issue when processing malicious XSLT stylesheets. This can be used to corrupt Java class files generated by the internal XSLTC compiler and execute arbitrary Java bytecode.”*

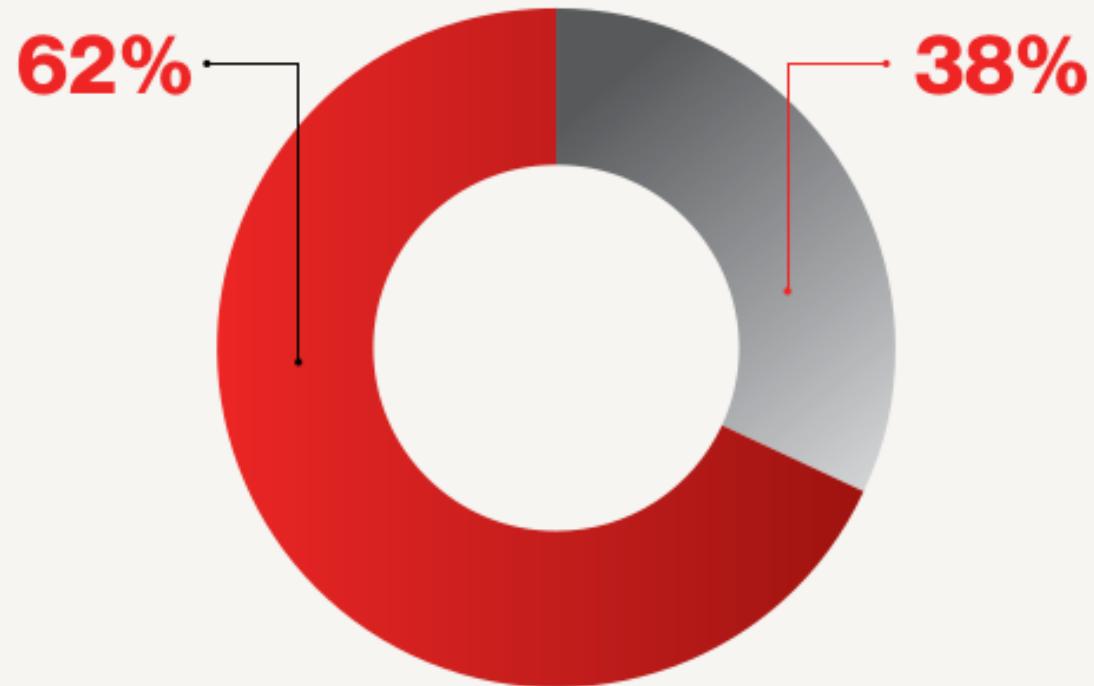
## Adversary Tactics

Detections indexed by the CrowdStrike Security Cloud in Q4 2021

Malware-Free Malware

**Adversaries continue to show  
that they have moved beyond malware.**

Attackers are increasingly attempting to accomplish their objectives without writing malware to the endpoint. Rather, they have been observed using legitimate credentials and built-in tools — an approach known as “living off the land” (LOTL) — in a deliberate effort to evade detection by legacy antivirus products. Of all detections indexed by the CrowdStrike Security Cloud in the fourth quarter of 2021, 62% were malware-free.



*Figure.* According to CrowdStrike, evidence of adversary activity systems monitored by Crowdstrike, 38% involved the use of malware; 62% of activity was due to LOTL and stolen credentials.

Source: CrowdStrike 2022 Global Threat Report

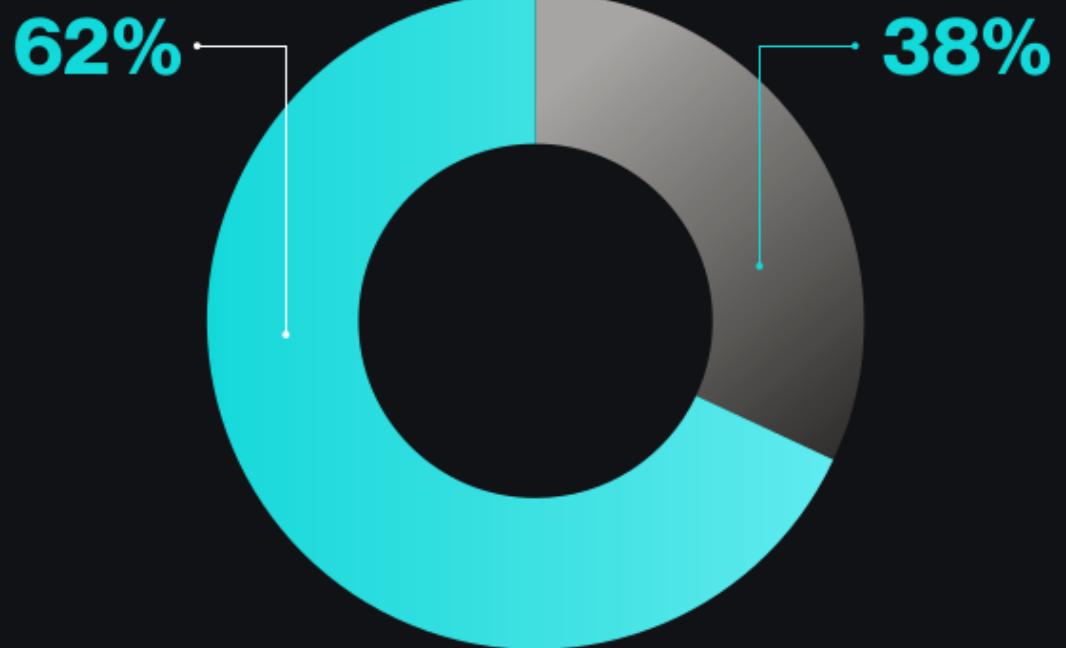
## Adversary Tactics

Detections indexed by the CrowdStrike Security Cloud in Q4 2021

Malware-Free      Malware

**Adversaries continue to show  
that they have moved beyond malware.**

Attackers are increasingly attempting to accomplish their objectives without writing malware to the endpoint. Rather, they have been observed using legitimate credentials and built-in tools — an approach known as “living off the land” (LOTL) — in a deliberate effort to evade detection by legacy antivirus products. Of all detections indexed by the CrowdStrike Security Cloud in the fourth quarter of 2021, 62% were malware-free.



*Figure.* According to CrowdStrike, evidence of adversary activity systems monitored by Crowdstrike, 38% involved the use of malware; 62% of activity was due to LOTL and stolen credentials.

Adversary	Nation-state or Category
 BEAR	RUSSIA
 BUFFALO	VIETNAM
 CHOLLIMA	DPRK (NORTH KOREA)
 CRANE	ROK (REPUBLIC OF KOREA)
 JACKAL	HACKTIVIST
 KITTEN	IRAN

*Figure.* Crowdstrike APT naming convention, Part 1.

Source: CrowdStrike 2022 Global Threat Report

	LEOPARD	PAKISTAN
	LYNX	GEORGIA
	OCELOT	COLOMBIA
	PANDA	PEOPLE'S REPUBLIC OF CHINA
	SPIDER	ECRIME
	TIGER	INDIA
	WOLF	TURKEY

*Figure.* Crowdstrike APT naming convention, Part 2.

Source: CrowdStrike 2022 Global Threat Report

# APT29

APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).  
[1][2] They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. APT29 reportedly compromised the Democratic National Committee starting in the summer of 2015.[3][4][5][6]

In April 2021, the US and UK governments attributed the SolarWinds supply chain compromise cyber operation to the SVR; public statements included citations to APT29, Cozy Bear, and The Dukes.[7][8] Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, and Dark Halo.[9][10][11][12][13]

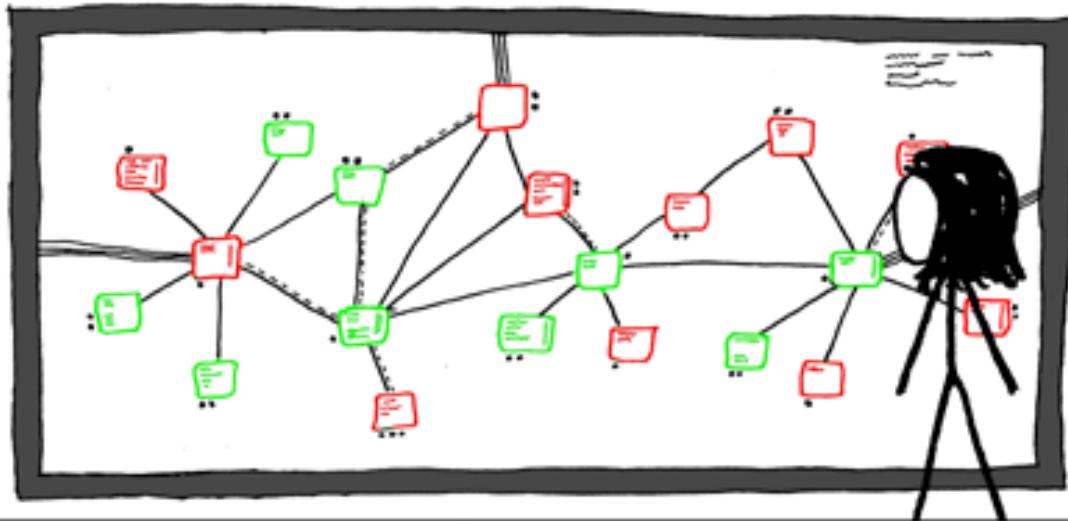


*Figure.* The MITRE ATT&CK website uses some of the same naming conventions provided by Crowdstrike, such as Cozy Bear, to denote a Russian APT.

Source: <https://attack.mitre.org/groups/G0016/>



*Figure. Billy the Puppet* movie image used by Jigsaw ransomware. Many recent malware, like Jigsaw (2016), are compatible with 32-bit architecture. Countdown...



PRETTY, ISN'T IT?

WHAT IS IT?



I'VE GOT A BUNCH OF VIRTUAL WINDOWS MACHINES NETWORKED TOGETHER, HOOKED UP TO AN INCOMING PIPE FROM THE NET. THEY EXECUTE EMAIL ATTACHMENTS, SHARE FILES, AND HAVE NO SECURITY PATCHES.



BETWEEN THEM THEY HAVE PRACTICALLY EVERY VIRUS..

THERE ARE MAIL TROJANS, WARHOL WORMS, AND ALL SORTS OF EXOTIC POLYMORPHICS. A MONITORING SYSTEM ADDS AND WIPES MACHINES AT RANDOM. THE DISPLAY SHOWS THE VIRUSES AS THEY MOVE THROUGH THE NETWORK.



GROWING AND STRUGGLING.

YOU KNOW, NORMAL PEOPLE JUST HAVE AQUARIUMS.

GOOD MORNING, BLASTER. ARE YOU AND W32.WELCHIA GETTING ALONG?



WHO'S A GOOD VIRUS? YOU ARE! YES, YOU ARE!

Figure. XKCD Malware Aquarium

<https://xkcd.com/350>

# **A<sub>D</sub>V<sub>E</sub>R<sub>S</sub>A<sub>R</sub>I<sub>A</sub>L<sub>C</sub>uscator: An Adversarial-DRL based Obfuscator and Metamorphic Malware Swarm Generator**

Mohit Sewak

Microsoft R&D, India

[mohit.sewak@microsoft.com](mailto:mohit.sewak@microsoft.com)

Sanjay K. Sahay, Hemant Rathore

BITS Pilani, Goa, India

[{ssahay, hemantr}@goa.bits-pilani.ac.in](mailto:{ssahay, hemantr}@goa.bits-pilani.ac.in)

## **DOOM: A Novel Adversarial-DRL-based Op-Code Level Metamorphic Malware Obfuscator for the enhancement of IDS**

Mohit Sewak

Department of CS & IS, Goa Campus  
BITS Pilani, Goa, India.

[p20150023@goa.bits-pilani.ac.in](mailto:p20150023@goa.bits-pilani.ac.in)

Sanjay K. Sahay

Department of CS & IS, Goa Campus,  
BITS Pilani, Goa, India.

[ssahay@goa.bits-pilani.ac.in](mailto:ssahay@goa.bits-pilani.ac.in)

Hemant Rathore

Department of CS & IS, Goa Campus  
BITS Pilani, Goa, India.

[hemantr@goa.bits-pilani.ac.in](mailto:hemantr@goa.bits-pilani.ac.in)

*Figure.* New works in offense and defense with Deep RL.

<https://arxiv.org/abs/2010.08608> (2020) and

<https://arxiv.org/abs/2109.11542> (2021)

# 403

## 403 Forbidden В доступе на страницу отказано

server248.hosting.reg.ru 27 Apr 2022 11:14

### Что случилось и как исправить?

- Неверные права на каталоги или файлы  
Верные права на папки: **755**, на файлы: **644**. Если у вас назначены другие, исправьте по инструкции.
- Ограничение доступа через **.htaccess**  
Переименуйте файл **.htaccess**. Например, в **.htaccess\_old**. После проверьте, работает ли сайт.



## Questions?