Leadership in Cybersecurity: You Are the Firewall

Silicon Valley
Engineering Leadership Community
Thursday, August 18, 2022

Matthew C. Bascom
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.

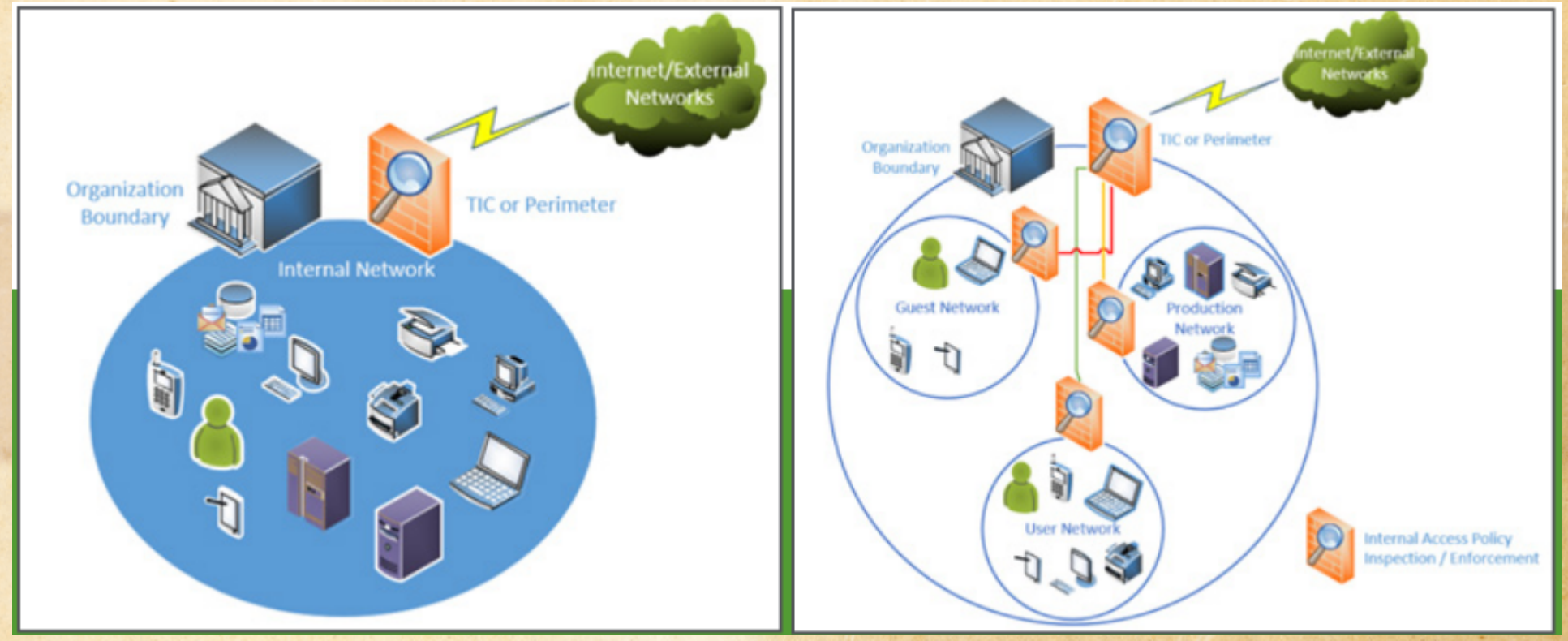


Figure. Flat (less secure) and Segmented (more secure) Networks

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	Score	KEV Count (CVEs)	Rank Change vs. 2021
1	CWE-787	Out-of-bounds Write	64.20	62	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.97	2	0
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22.11	7	+3 ▲
4	CWE-20	Improper Input Validation	20.63	20	0
5	CWE-125	Out-of-bounds Read	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
CVE-2021-21220	Chain: insufficient input validation (CWE-20) i
CVE-2021-28664	GPU kernel driver allows memory corruption l
CVE-2020-17087	Chain: integer truncation (CWE-197) causes s per CISA KEV.
CVE-2020-1054	Out-of-bounds write in kernel-mode driver, as
CVE-2020-0041	Escape from browser sandbox using out-of-b
CVE-2020-0968	Memory corruption in web browser scripting e
CVE-2020-0022	chain: mobile phone Bluetooth implementatio
CVE-2019-1010006	Chain: compiler optimization (CWE-733) remo
CVE-2009-1532	malformed inputs cause accesses of uninitiali
CVE-2009-0269	chain: -1 value from a function call was intenc
CVE-2002-2227	Unchecked length of SSLv2 challenge value l
CVE-2007-4580	Buffer underflow from a small size value with
CVE-2007-4268	Chain: integer signedness error (CWE-195) p
CVE-2009-2550	Classic stack-based buffer overflow in media
CVE-2009-2403	Heap-based buffer overflow in media player u

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.

Figure. Articles from February 2021.

Forbes

FORBES DIGITAL ASSETS

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

Jason Brett Contributor ⓘ
I write about blockchain regulation and policy.

Follow

Jul 23, 2022, 08:11am EDT

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 $HTTP_PORTS (msg:"TRICKBOT_ANCHOR:HTTP URI GET contains
'/anchor'"; sid:1; rev:1; flow:established,to_server; content:"/anchor";
http_uri; fast_pattern:only; content:"GET"; nocase; http_method;
pcre:"/^\/anchor_?.{3}\/[\w_-]+\.[A-F0-9]+\/?$/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/e9600404ecc42cf86d38deedef94068db39b7a0
fd06b3b8fb2d8a3c7002b650e/detection; metadata:service ssl;)
```

Figure. Snort IDS signatures for identifying Trickbot activity.

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

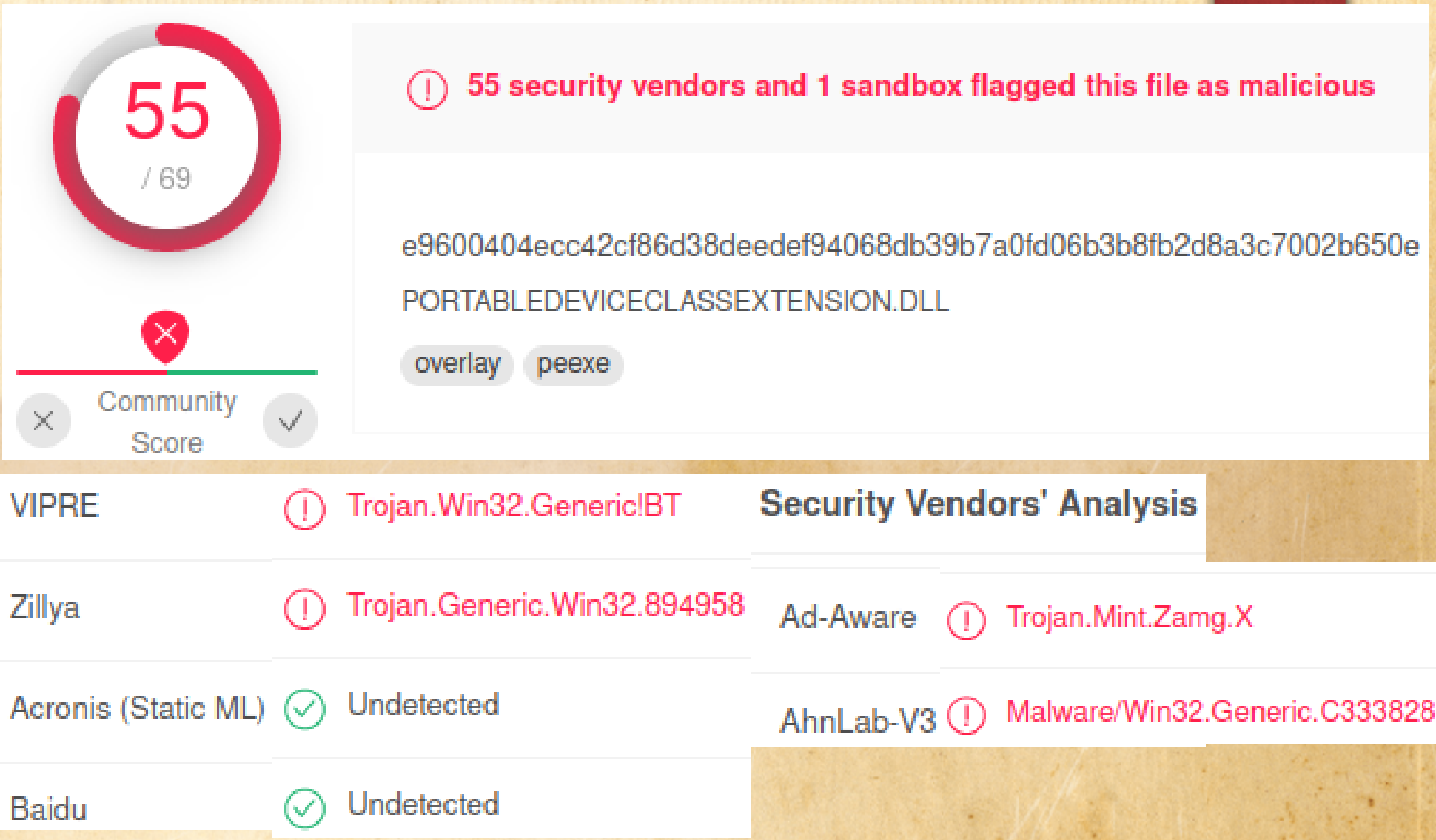


Figure. Partial VirusTotal result for DLL with SHA256 of e9600404ecc42cf86d38deedef94068db39b7a0fd06b3b8fb2d8a3c7002b650e

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.

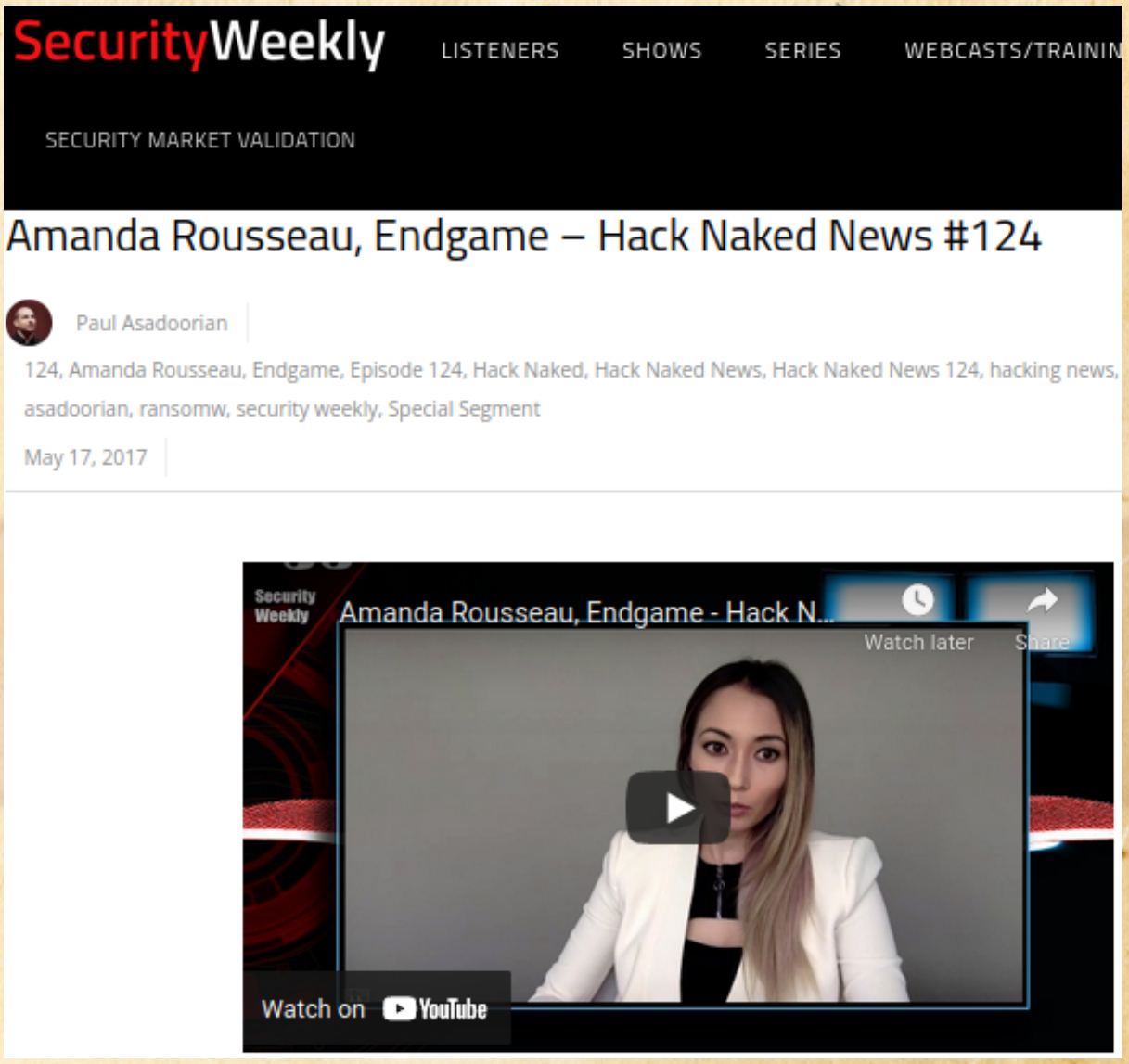


Figure. Security Weekly Interview with Amanda Rousseau (*Facebook) on Mimikatz.*

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

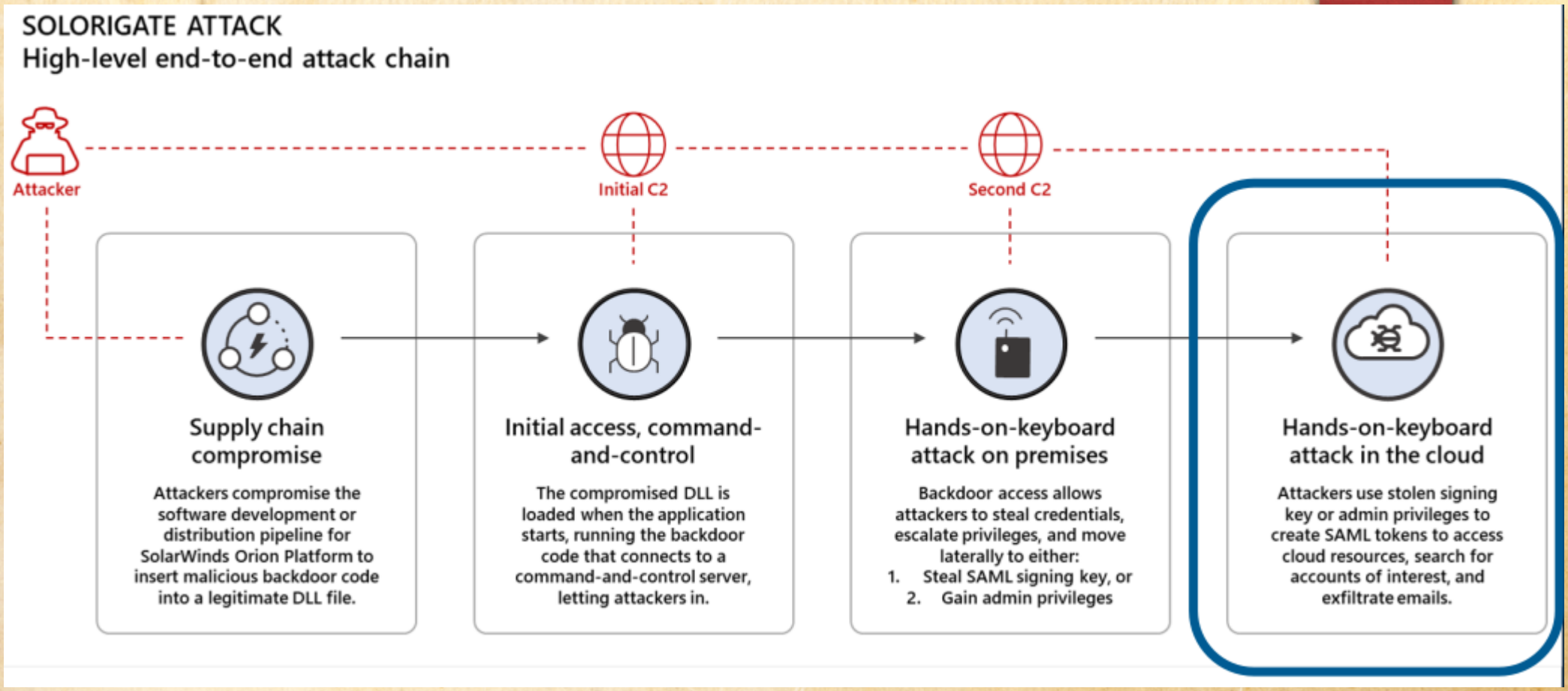


Figure. High-level end-to-end attack chain of the Solarwinds Solorigate attack.

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.

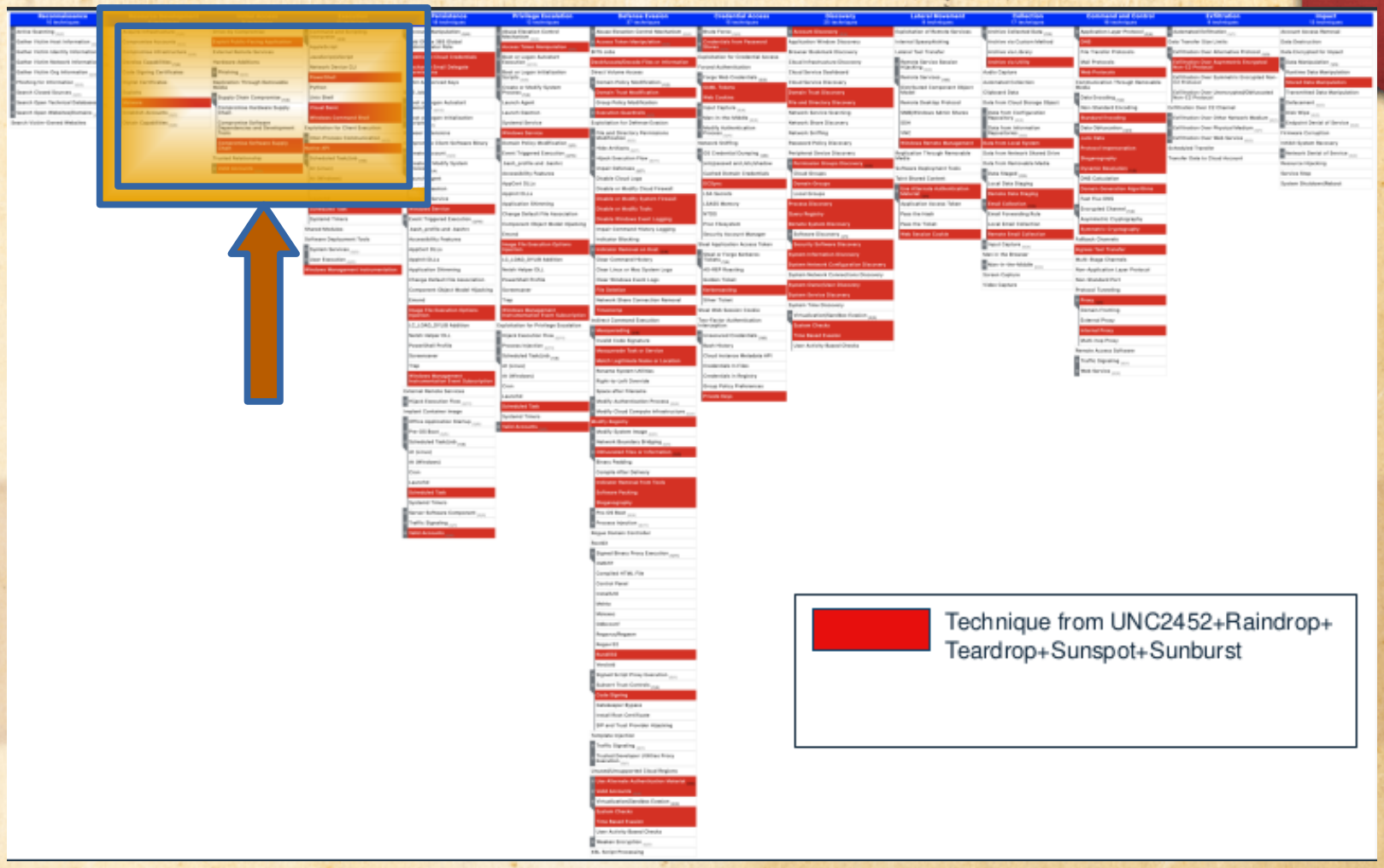


Figure. High-level view of MITRE ATT&CK for enterprises and the December 2020 Solarwinds Solorigate attack.

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

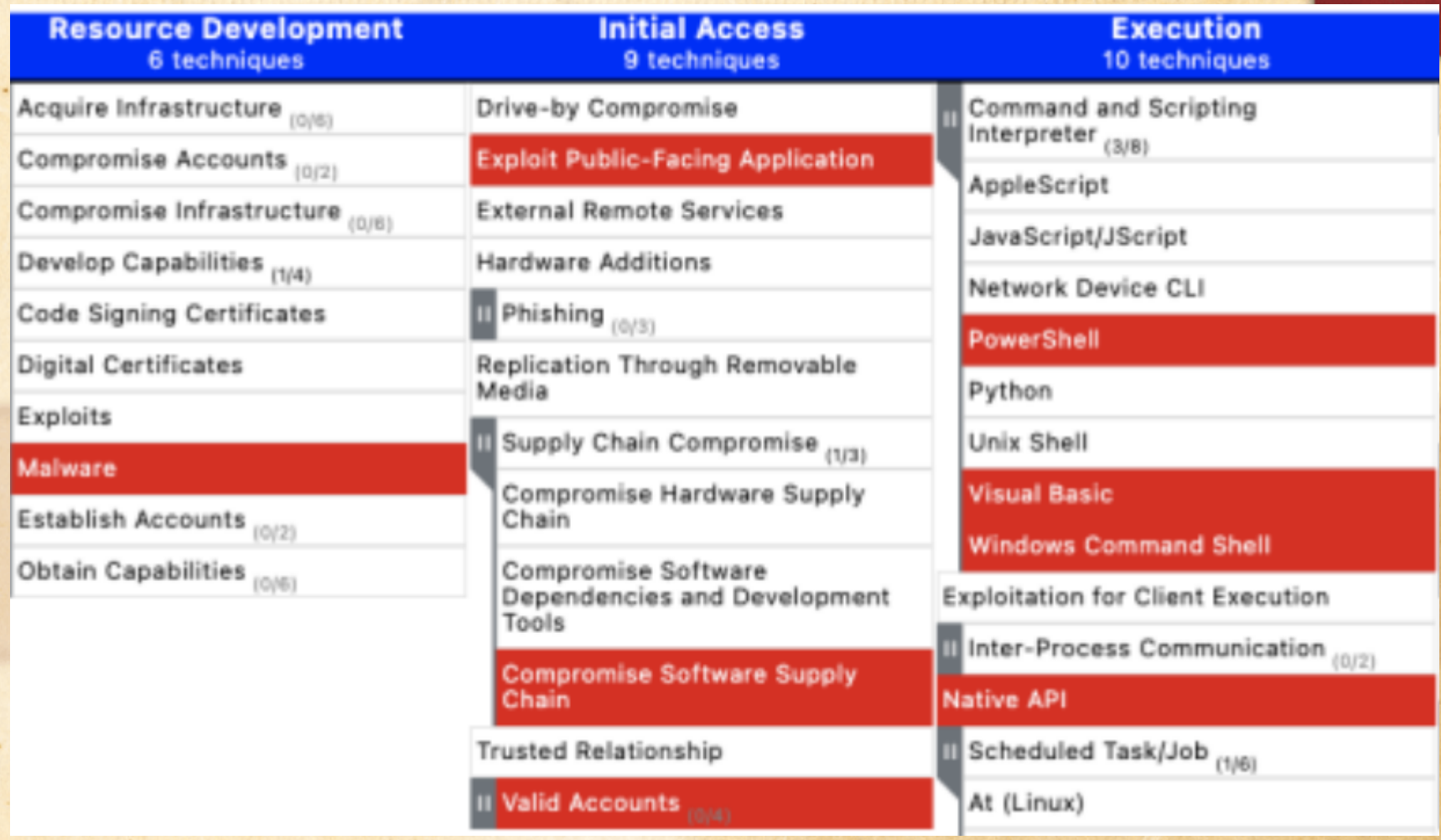


Figure. Top left portion of MITRE ATT&CK for Solarwinds Solorigate.

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

• Reconnaissance • Resource Development • Initial Access • Execution • Discovery	• Persistence • Privilege Escalation • Defense Evasion • Credential Access	• Lateral Movement • Collection • Command & Control • Exfiltration • Impact

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.

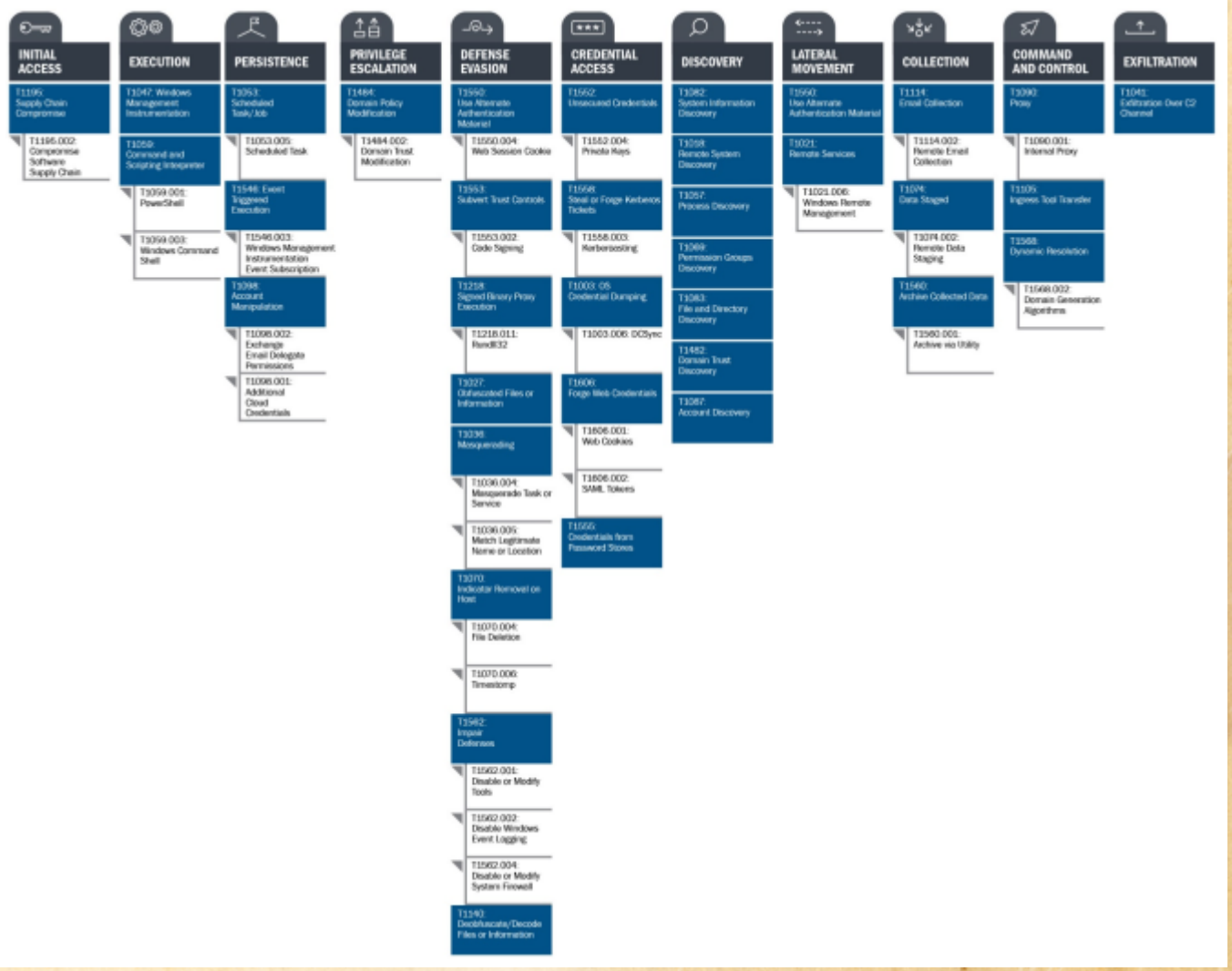


Figure. An illustration of Solarwinds using MITRE ATT&CK .

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

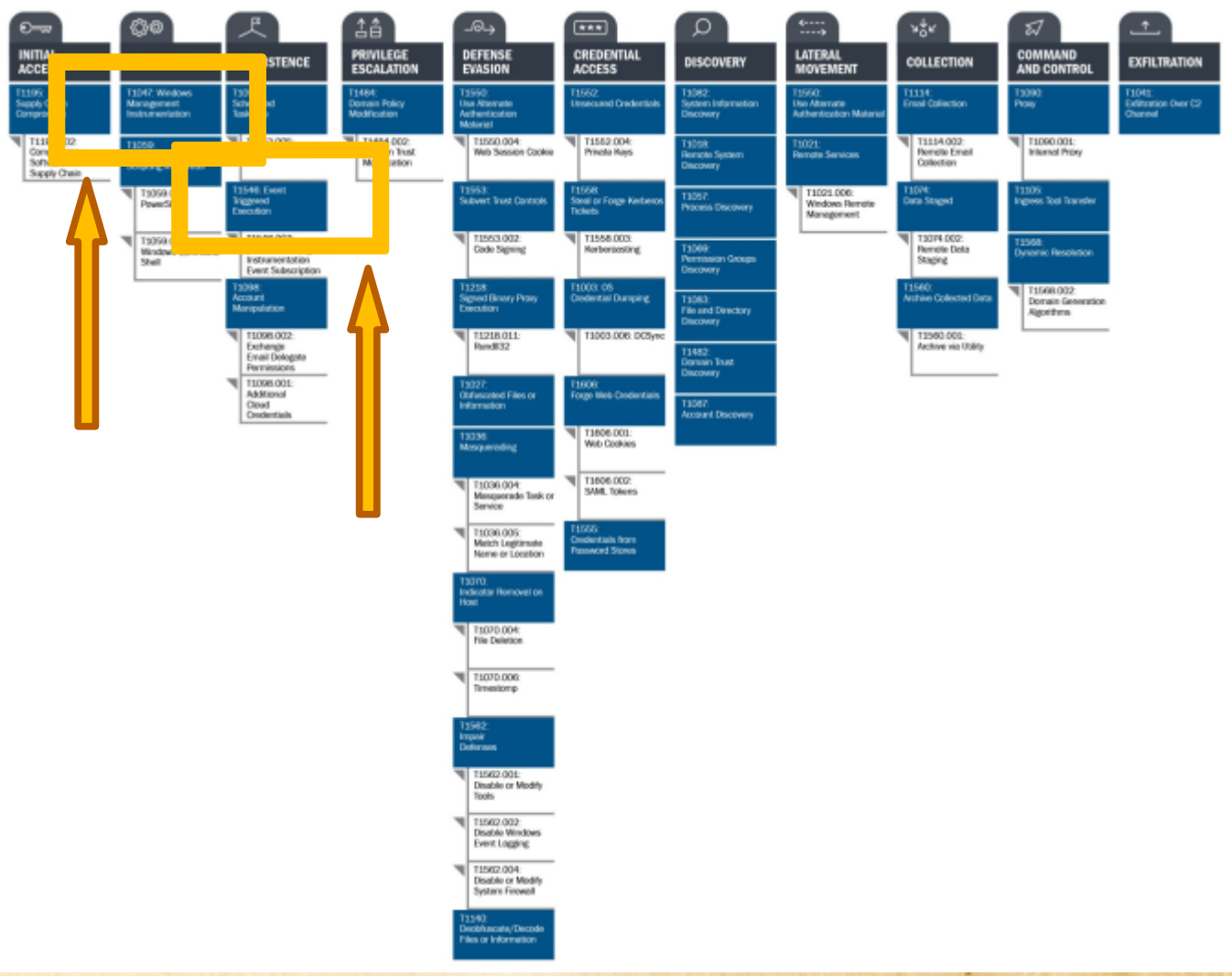


Figure. An illustration of Solarwinds using MITRE ATT&CK .

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.[14,15,16]	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.[17] According to Microsoft, the following was used for lateral movement via WMI: `wmic /node:[target] process call create "rundll32 c:\windows\[folder]\[beacon].dll [export]"`.[18] **Note**: 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.[19,20]	

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]	he threat actor used Windows anagement Instrumentation (WMI) for e remote execution of files for lateral ovement.[14,15,16]	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.[17] According to Microsoft, the following was used for lateral movement via WMI: `wmic /node:[target] process call create "rundll32 c:\windows\[folder]\[beacon].dll [export]"`.[18] **Note**: 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.[19,20]	

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.

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.

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

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.
DILBERT.COM
@SCOTTADAMSSAYS
DOES THE BAD DATA SUGGEST WE SHOULD DO WHAT WE WANTED TO DO ANYWAY?
WELL, YES.
9-3-18
©2018 Scott Adams, Inc./Dist. by Andrews McMeel
THAT'S CALLED "GOOD DATA."

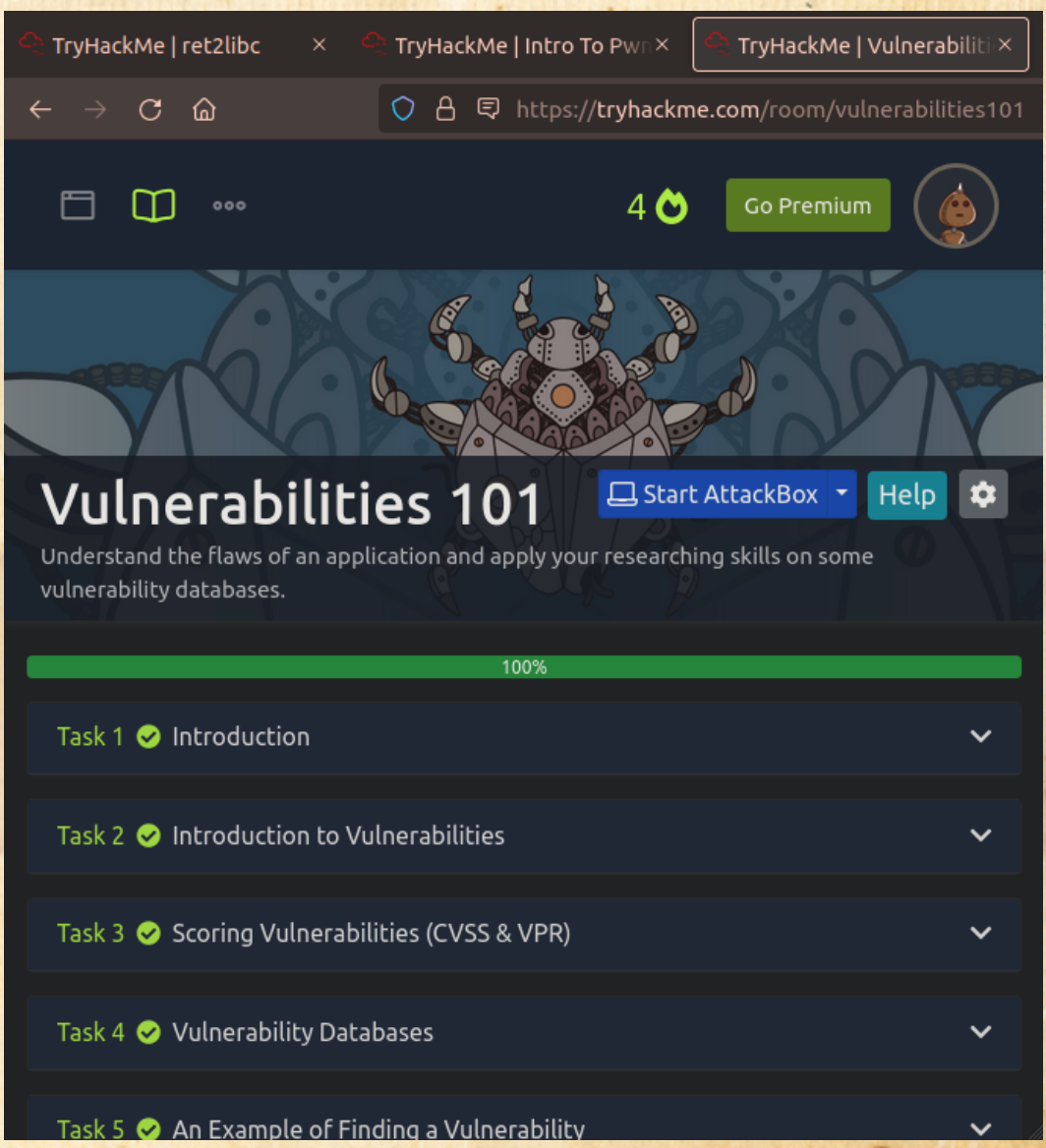


Figure. The gamification of hacking tools makes practice accessible to anyone willing to run a remote desktop (RDP) and a VPN. Image: TryHackMe.com

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.

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

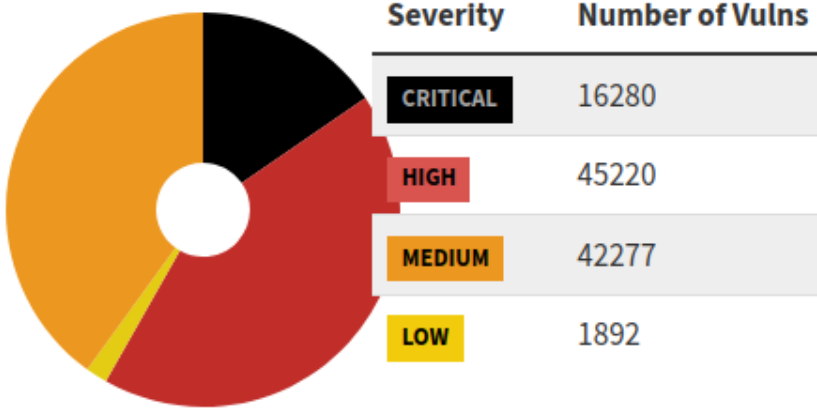
NVD

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



Severity	Number of Vulns
CRITICAL	16280
HIGH	45220
MEDIUM	42277
LOW	1892

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

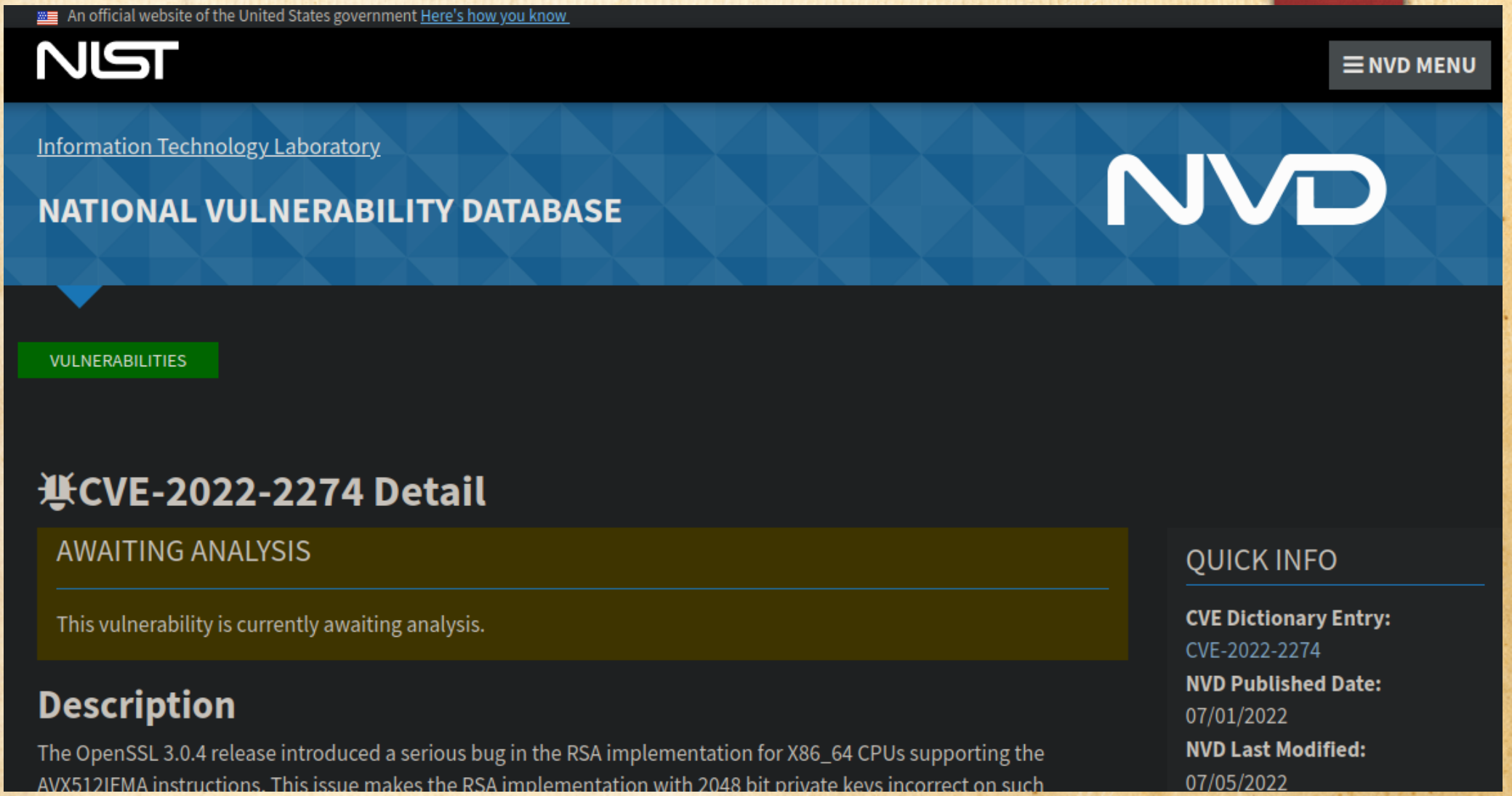


Figure. CVE-2022-2274, an RSA encryption vulnerability that was published in July and affects x86-64 CPU architecture.

CVE: Common Vulnerabilities & Exposures. See: www.cve.org, by MITRE and sponsored by Dept. of Homeland Security & CISA.

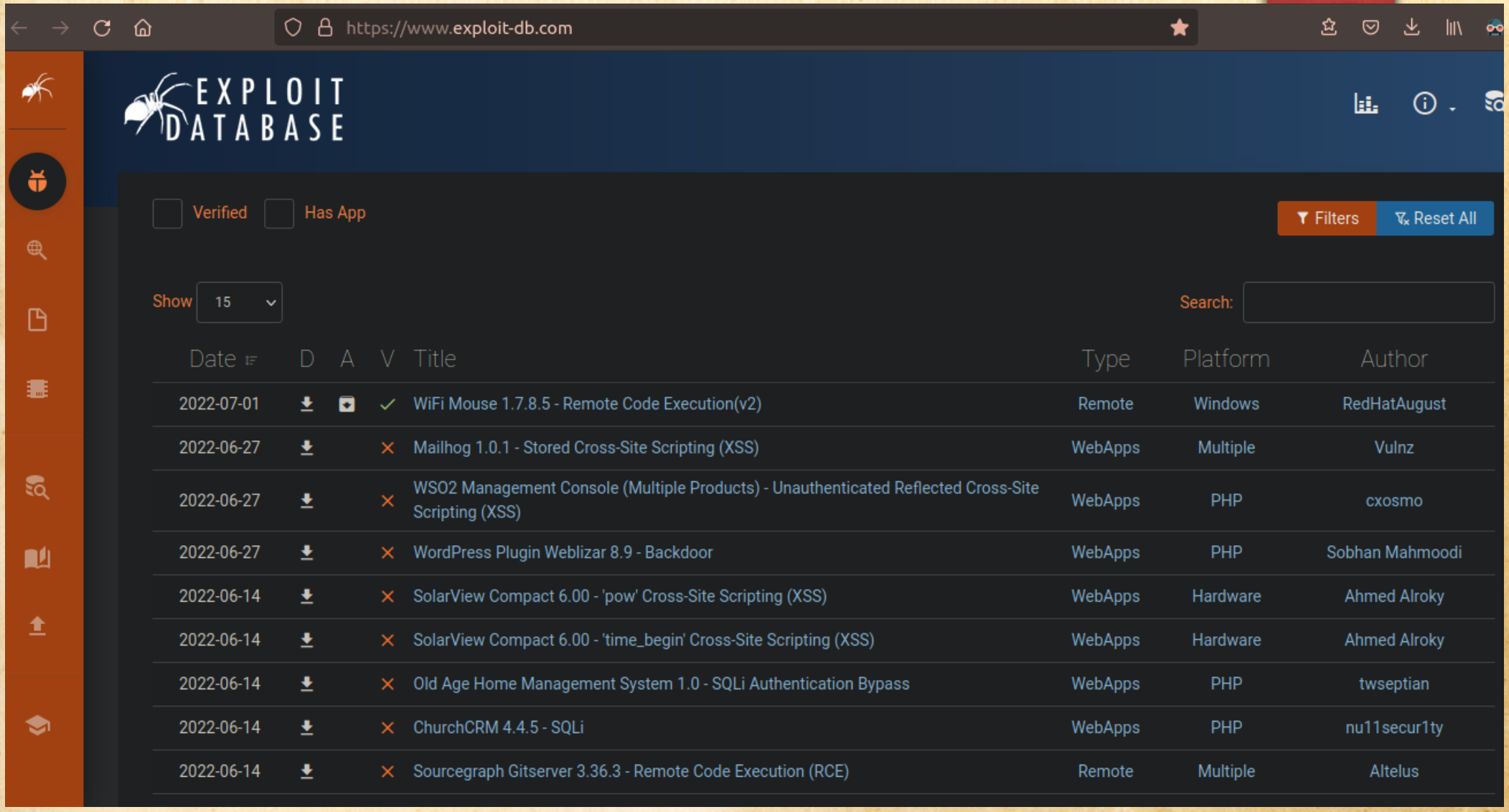


Figure. Exploit Database publishes proof of concepts against vulnerabilities as they become publicly available. The top reads, “WiFi Mouse Remote Code Execution” remotely runs code on Windows. The others, from the previous 15 days, include web application exploits that leverage vulnerabilities in PHP.

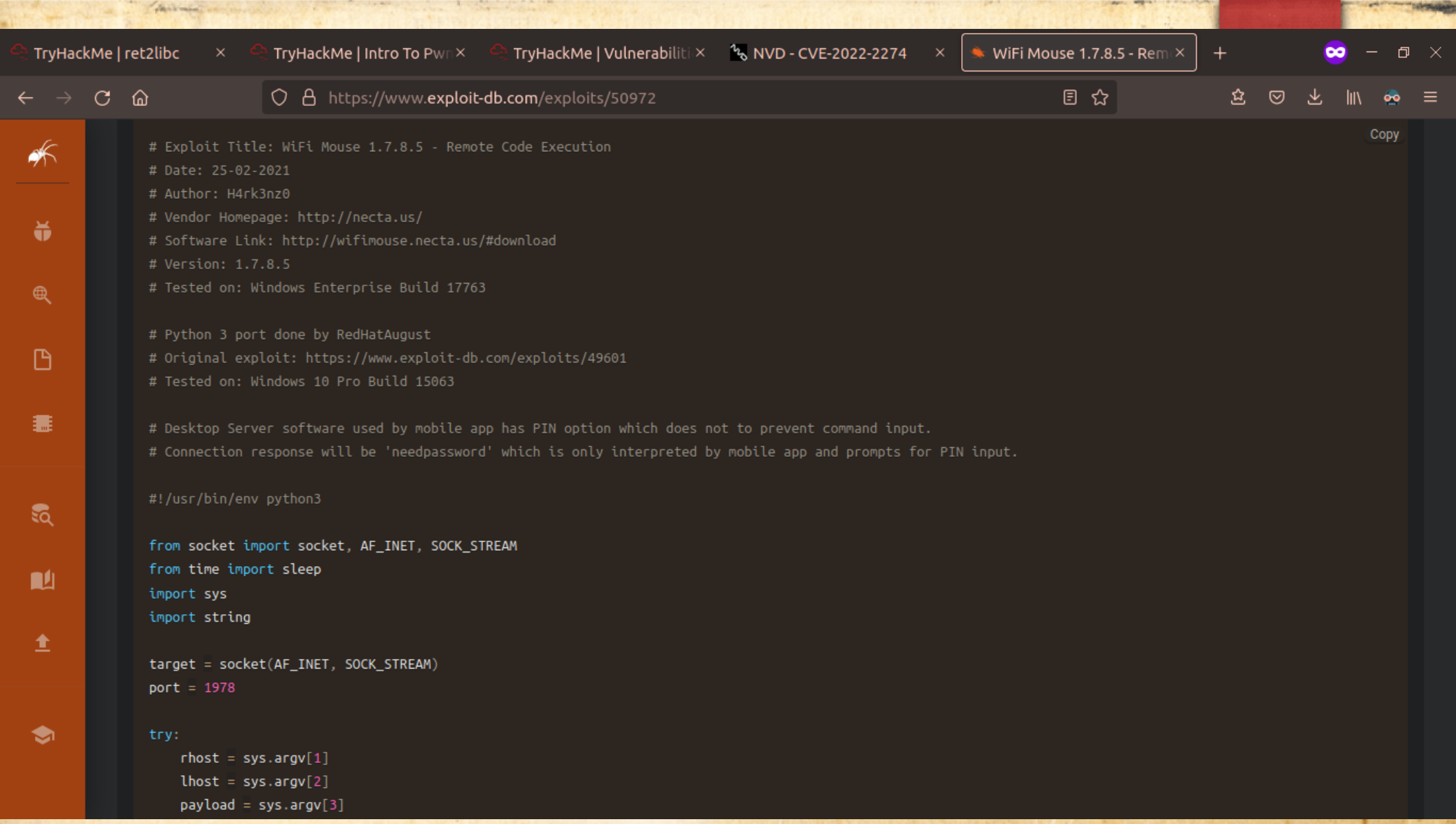


Figure. Proof-of-concept Python code that leverages the vulnerability discovered in WiFi mouse devices. Note that this vulnerability does not have a corresponding CVE entry on NIST's NVD database.

Source: www.exploit-db.com/exploits/50972

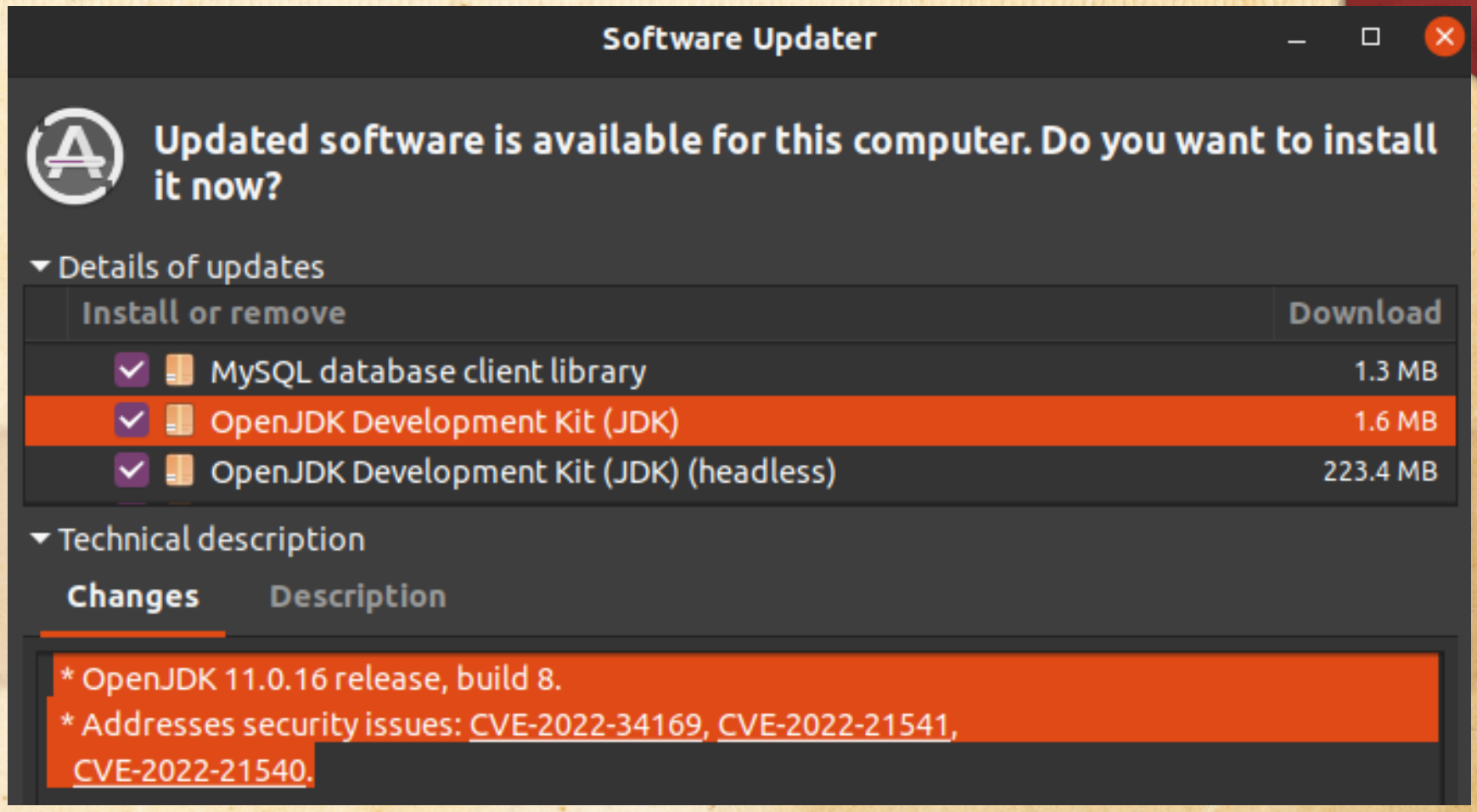
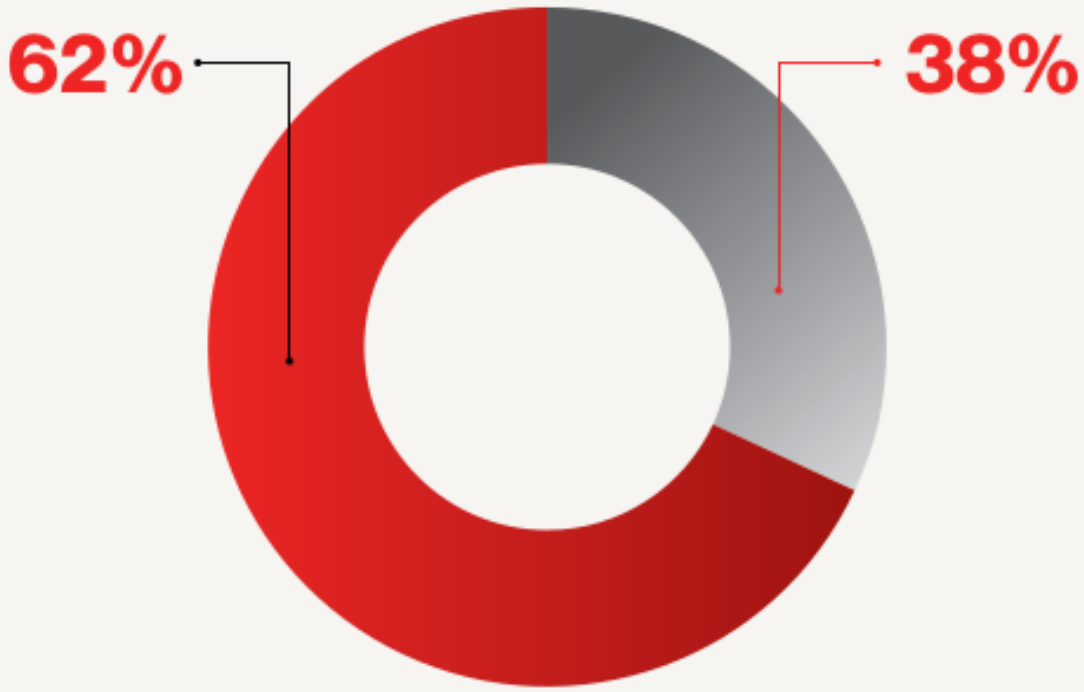


Figure. CVE-2022-34169. *"The Apache Xalan Java XSLT library is vulnerable to an integer truncation issue when processing malicious XSLT stylesheets. This can be used to corrupt Java class files generated by the internal XSLTC compiler and execute arbitrary Java bytecode."*

Adversary Tactics

Detections indexed by the CrowdStrike Security Cloud in Q4 2021



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

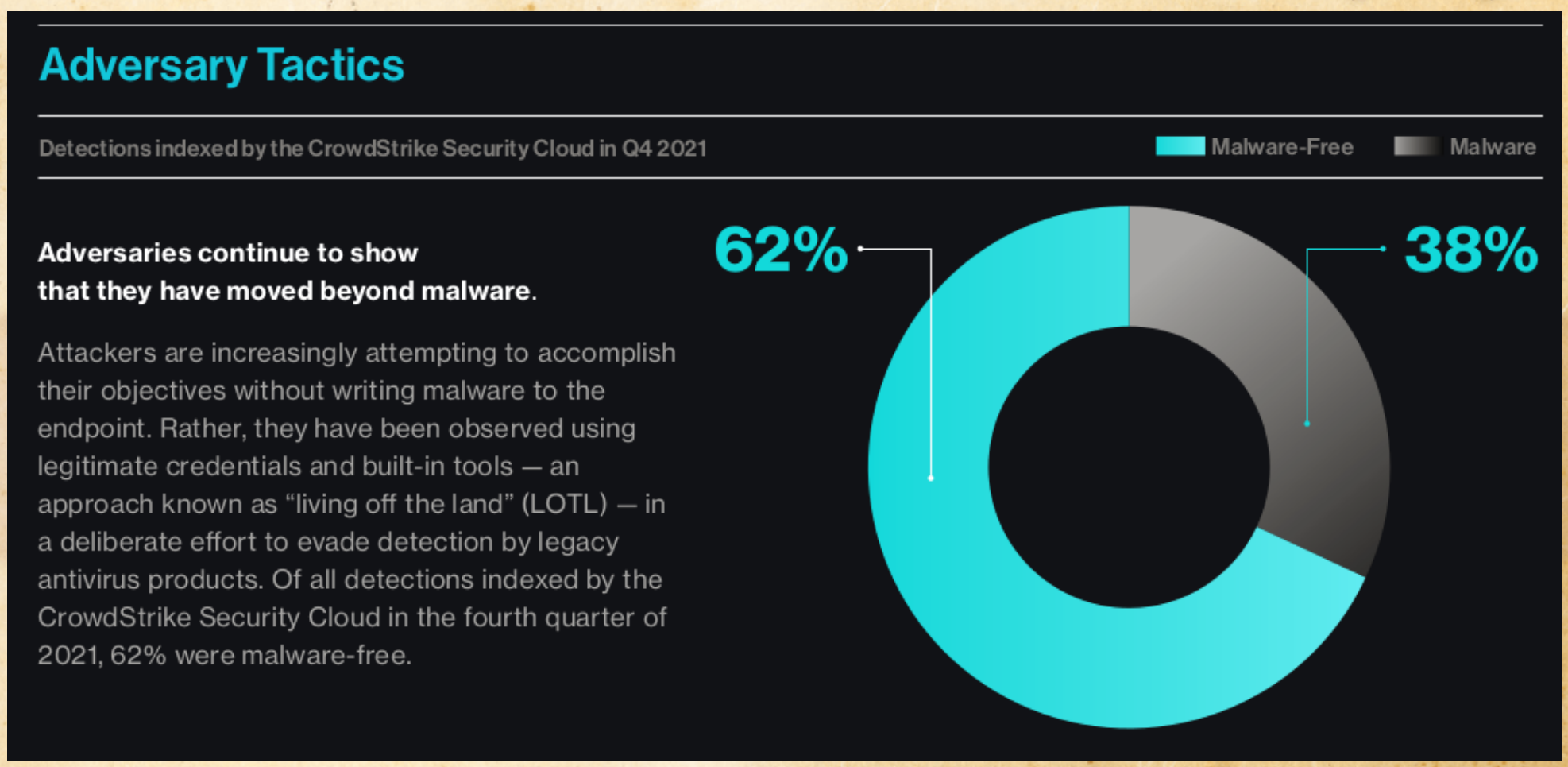


Figure. According to CrowdStrike, evidence of adversary activity systems monitored by Crowdstrike, 38% involved the use of malware; 62% of activity was due to LOTL and stolen credentials.

Source: CrowdStrike 2022 Global Threat Report

Adversary	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

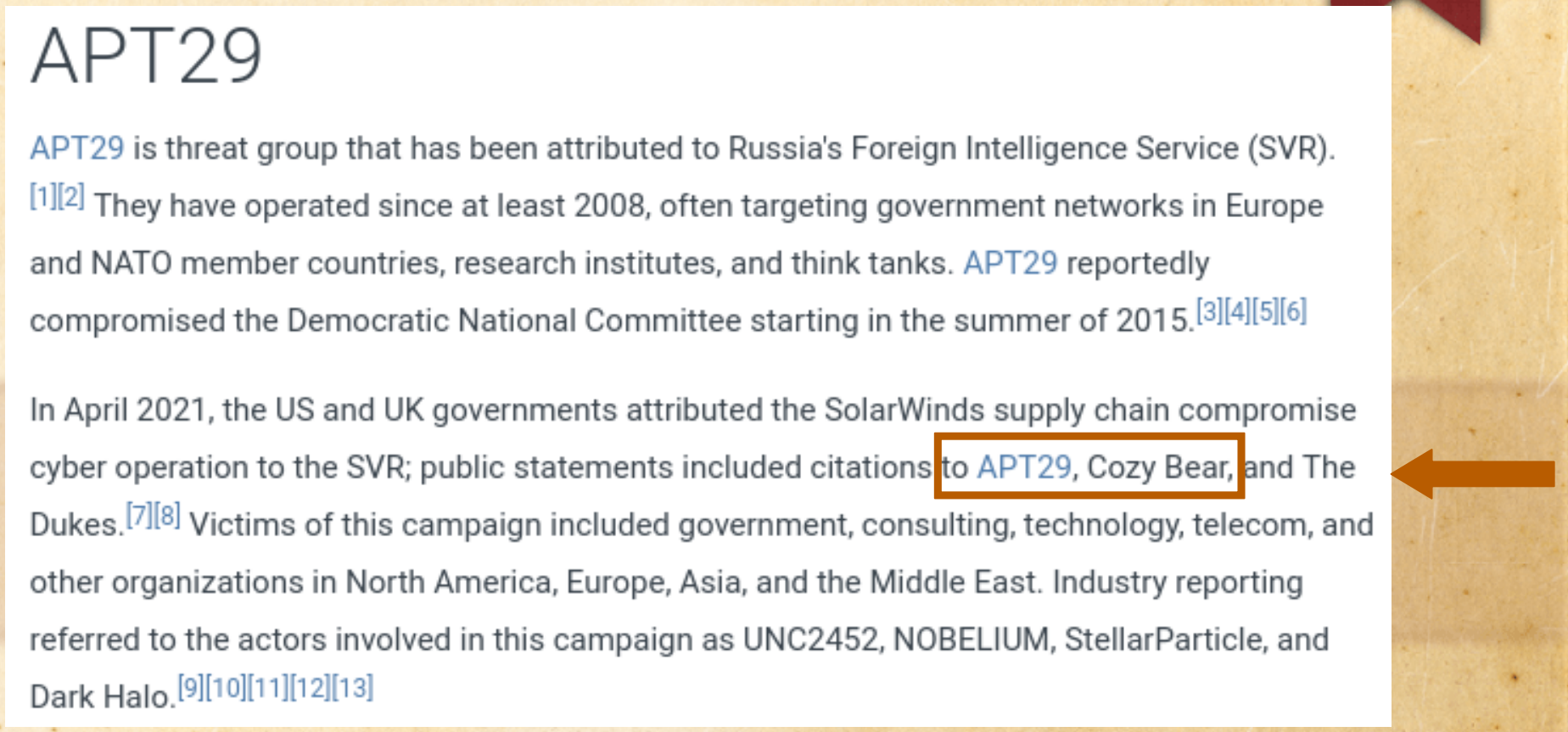


Figure. The MITRE ATT&CK website uses some of the same naming conventions provided by Crowdstrike, such as Cozy Bear, to denote a Russian APT.

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...

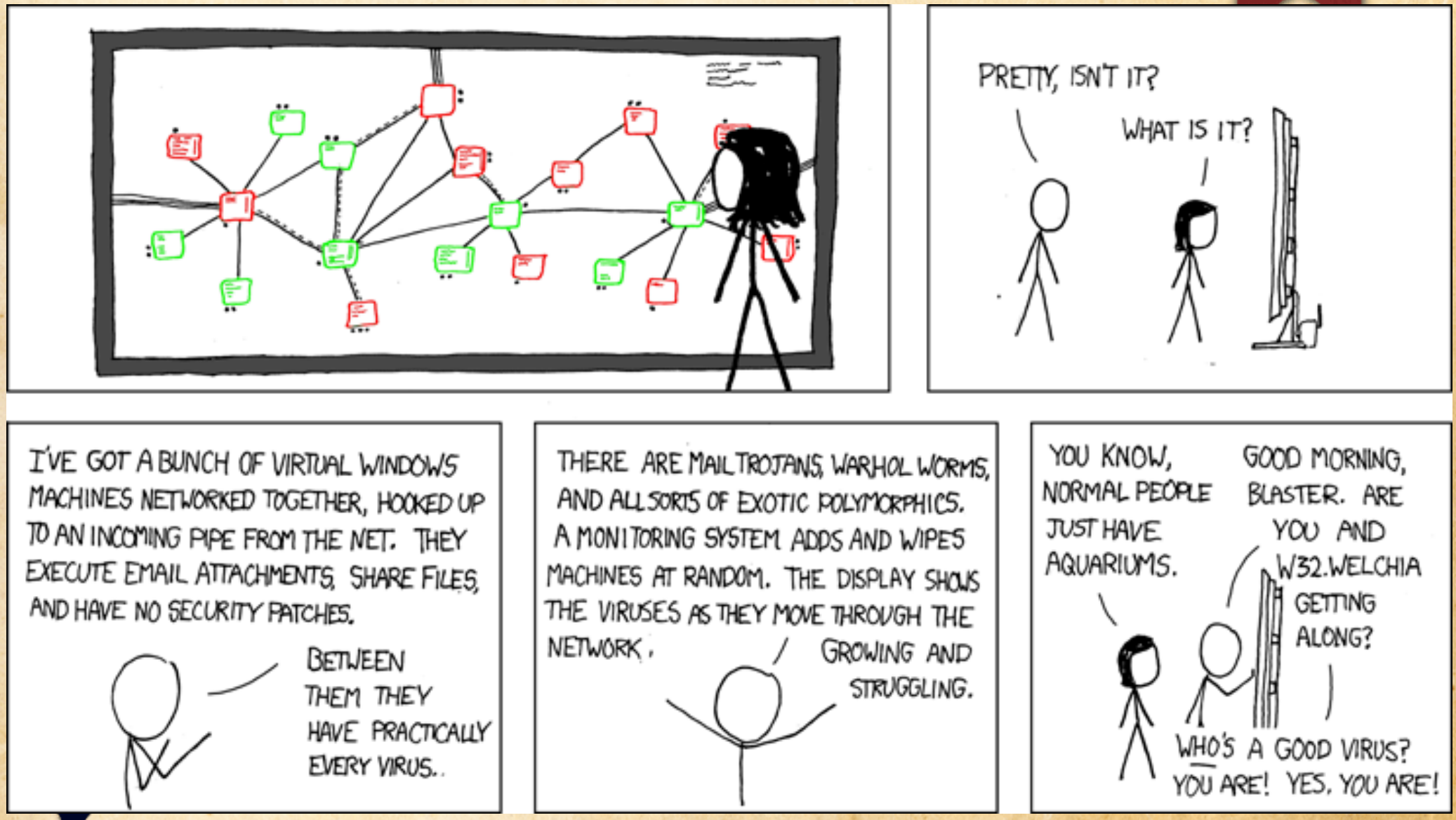
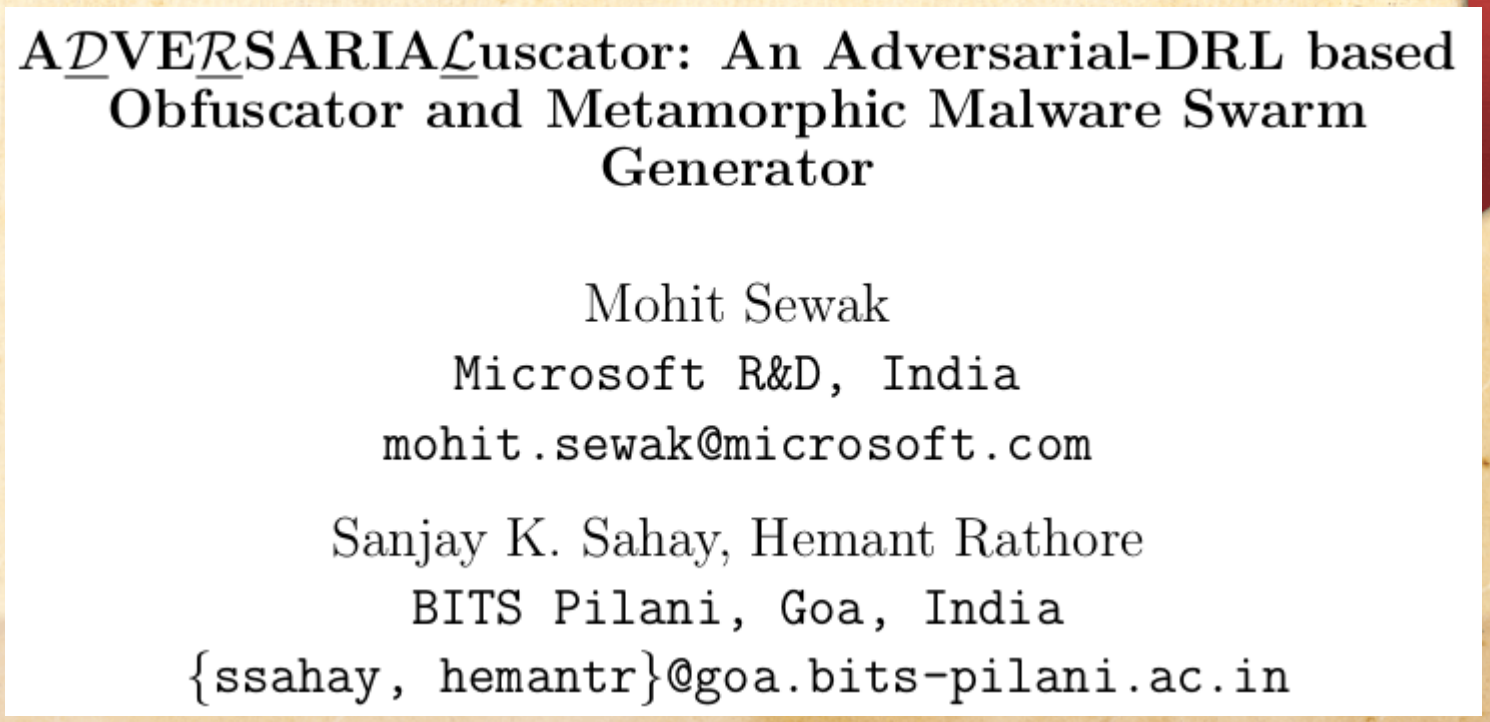


Figure. XKCD Malware Aquarium

https://xkcd.com/350



A$\underline{D}$VE$\underline{R}$SARIA$\underline{L}$uscator: An Adversarial-DRL based Obfuscator and Metamorphic Malware Swarm Generator

Mohit Sewak
Microsoft R&D, India
mohit.sewak@microsoft.com

Sanjay K. Sahay, Hemant Rathore
BITS Pilani, Goa, India
{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

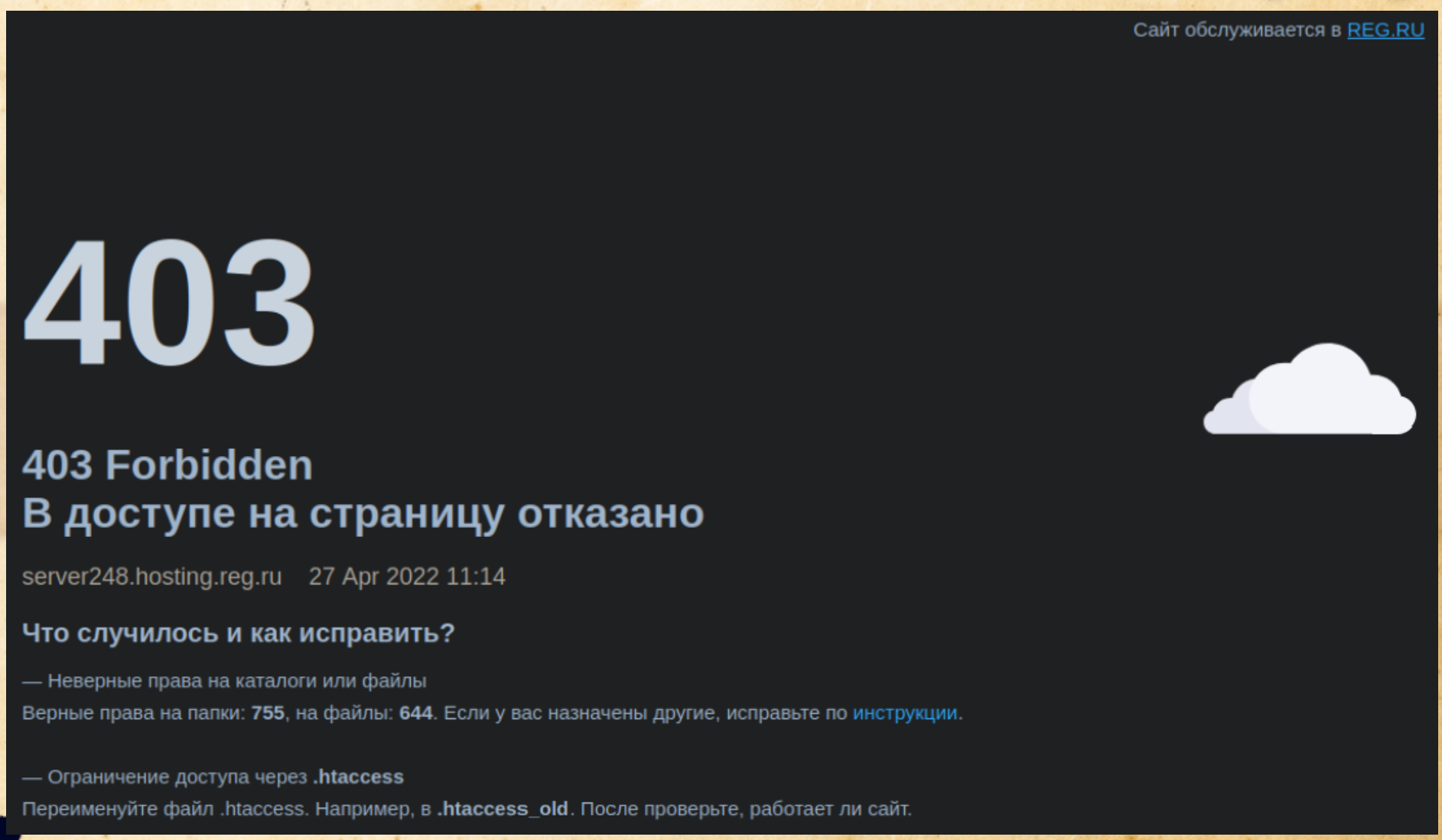
Sanjay K. Sahay
Department of CS & IS, Goa Campus,
BITS Pilani, Goa, India.
ssahay@goa.bits-pilani.ac.in

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


Сайт обслуживается в REG.RU
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?