ARIZONA HOUSE OF REPRESENTATIVES
Fifty-fifth Legislature - Second Regular Session

COMMITTEE ON COMMERCE

Report of Regular Meeting
Tuesday, January 11, 2022
House Hearing Room 3 -- 2 P.M. OR UPON ADJOURNMENT OF FLOOR

Convened 2:29 P.M.
Recessed
Reconvened
Adjourned 2:52 P.M.

MINUTES RECEIVED
CHIEF CLERK'S OFFICE
1-14-22

Members Present
Mr. Carter
Mr. Chávez
Mr. Cook
Mr. Espinoza
Mr. Kaiser
Mrs. Liguori
Mr. Meza
Mr. Wilmeth
Mr. Chaplik, Vice-Chairman
Mr. Weninger, Chairman

Members Absent

Agenda
Original Agenda – Attachment 1

Request to Speak
Report – Attachment 2

Committee Attendance
Report – Attachment 3

Presentations

Name	**Organization**	**Attachments** (Handouts)
Thomas MacLellan	Palo Alto Networks	4

Jacqueline Denlinger, Committee Secretary
January 14, 2022

(Original attachments on file in the Office of the Chief Clerk; video archives available at http://www.azleg.gov)

convened 2:29p
adjourned 2:52p

ARIZONA HOUSE OF REPRESENTATIVES
Fifty-fifth Legislature - Second Regular Session

REGULAR MEETING AGENDA

COMMITTEE ON COMMERCE

DATE Tuesday, January 11, 2022 ROOM HHR 3 TIME 2 P.M. or Upon Adjournment of Floor

Members of the public may access a livestream of the meeting here:
https://www.azleg.gov/videoplayer/?clientID=6361162879&eventID=2022011006

Members:

Mr. Carter	Mr. Kaiser	Mr. Wilmeth
Mr. Cook	Mrs. Liguori	Mr. Chaplik, Vice-Chairman
Mr. Chávez	Mr. Meza	Mr. Weninger, Chairman
Mr. Espinoza		

---

1. Call to Order
2. Introduction of Members & Staff
3. Presentation:
   - Thomas MacLellan, Cybersecurity 101
4. Public Testimony
5. Adjourn

DF
01/04/2022

People with disabilities may request reasonable accommodations such as interpreters, alternative formats, or assistance with physical accessibility. If you require accommodations, please contact the Chief Clerk's Office at (602) 926-3032 or through Arizona Relay Service 7-1-1.

Attachment 1

Information Registered on the Request to Speak System

House Commerce (1/11/2022)

4, Public Testimony

Attachment 2

ARIZONA STATE LEGISLATURE

Fifty-fifth Legislature - Second Regular Session

COMMITTEE ATTENDANCE RECORD

COMMITTEE ON **COMMERCE**

CHAIRMAN: Jeff Weninger VICE-CHAIRMAN: Joseph Chaplik

	DATE	01/11/22	/22	/22	/22	/22
	CONVENED	2:9pm	m	m	m	m
	RECESSED					
	RECONVENED					
	ADJOURNED	2:52pm				
MEMBERS						
Carter		✓				
Chávez		✓				
Cook		✓				
Espinoza		✓				
Kaiser		✓				
Liguori		✓				
Meza		✓				
Wilmeth		✓				
Chaplik, Vice-Chairman		✓				
Weninger, Chairman		✓				

√ Present --- Absent exc Excused

Attachment 3

Attachment 4

Presentation to Arizona House Commerce Committee

An Overview of Current and Emerging Cybersecurity Threats

Thomas MacLellan
Director
Government Affairs & Strategy
Palo Alto Networks
January 11, 2022

© 2022 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Current and Emerging Threats

- Ransomware
- Industrial Control System Attacks
- Supply Chain
- Vulnerability Exploitation

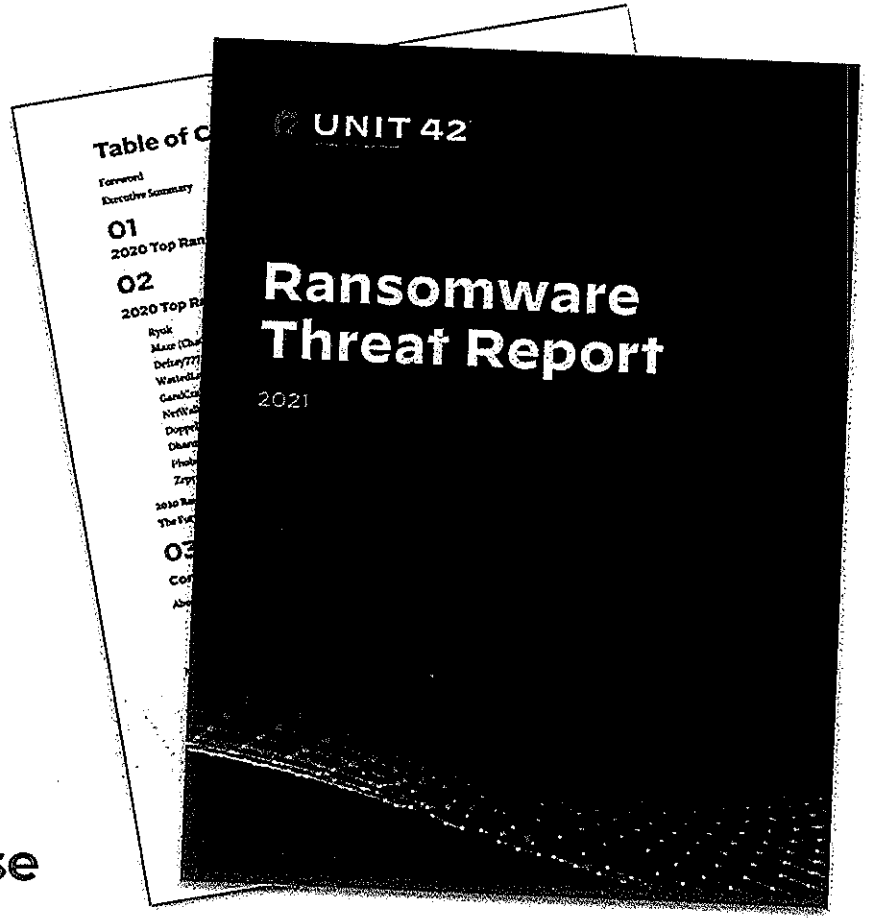
Key Trends: 2021

$2.1M average ransom demand in 2021

$461K average ransom paid in 2021

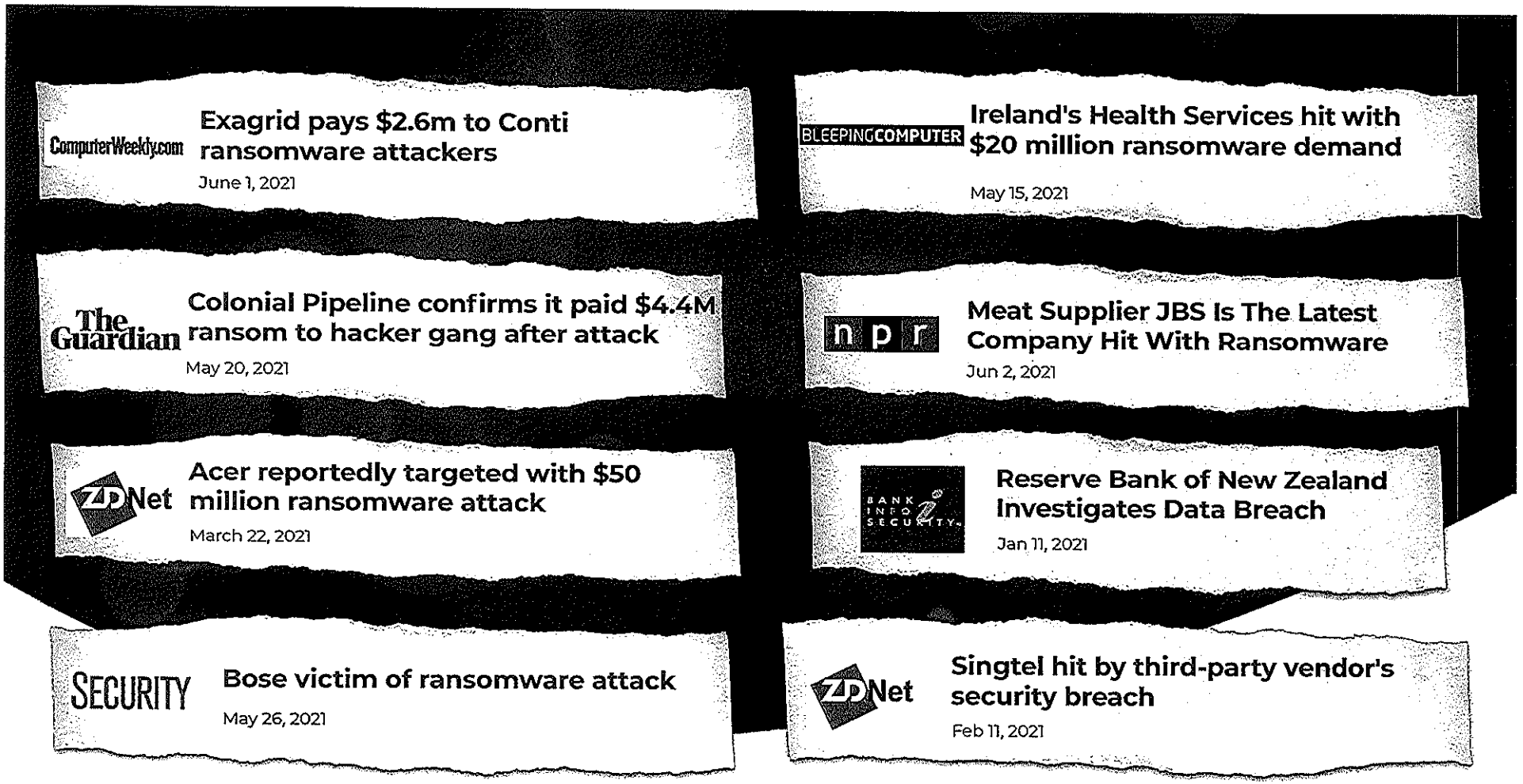
$11M highest ransom paid in 2021

$70M highest ransom demand in 2021



Quadruple Extortion on the Rise

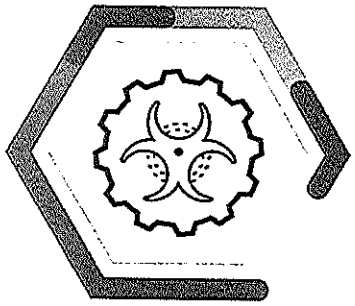
©2021 Palo Alto Networks, Inc. All rights reserved



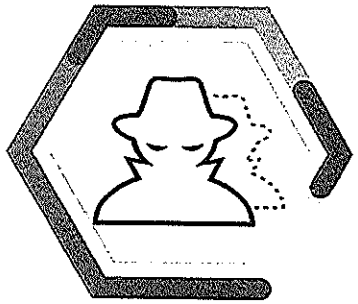
© 2022 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Unit 42: The Rise of Quadruple Extortion

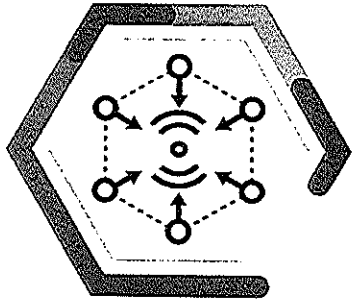
Ransomware operators now commonly use as many as four techniques for pressuring victims into paying.



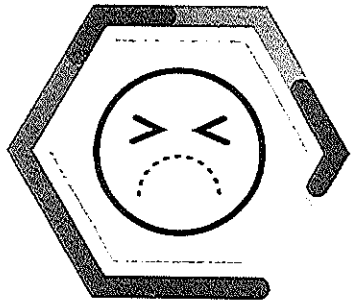
Encryption
Victims pay to regain access to encrypted data



Data Theft
Hackers threaten to release stolen data if ransom is unpaid



Denial of Service
DoS attacks shut down victim's public websites



Harassment
Customers, business partners, employees and media contacted

Extortion Payments Hit New Records as Ransomware Crisis Intensifies

© 2022 Palo Alto Networks, Inc. All rights reserved | Proprietary and Confidential Information

Colonial Pipeline

MAY 2021

What Happened:

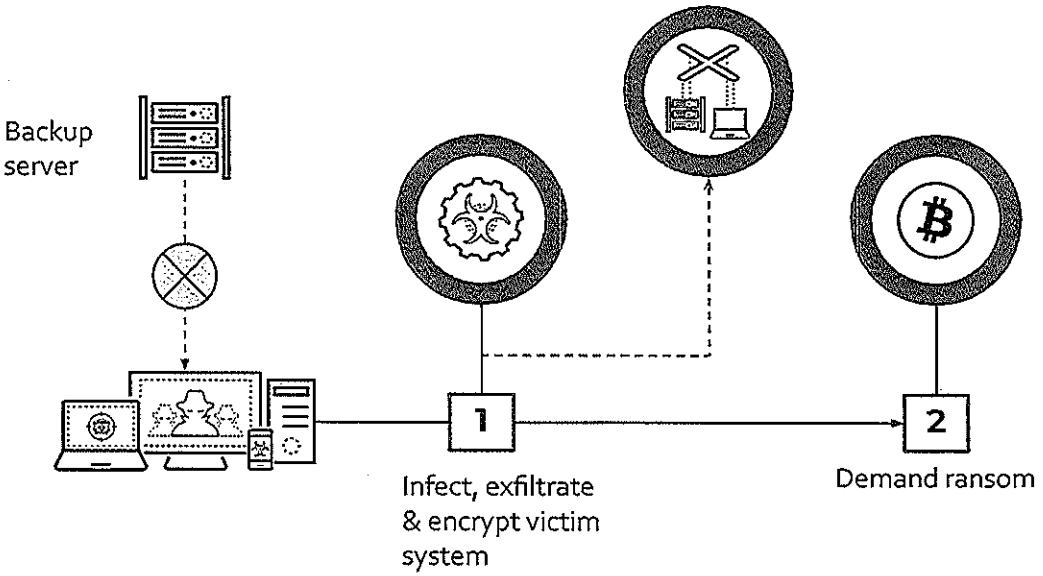
1. Gained access through compromised VPN credentials

2. Exfiltrated ~100GB of data before encrypting some business systems

3. Company shut down 5500 miles of pipeline as a precautionary measure

4. Company paid ~$4.4m ransom

5. DOJ Task Force recovered 85% of bitcoin / ~$2.3m



©2022 Palo Alto Networks, Inc. All rights reserved. Proprietary and Confidential Information.

Industrial Control Systems Attacks

Industrial control systems (ICS) are the physical systems like pumps that underpin the functions of critical infrastructure facilities like water, electricity, even hospitals. Attacks against ICS can have a kinetic impact in the real world.

© 2022 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

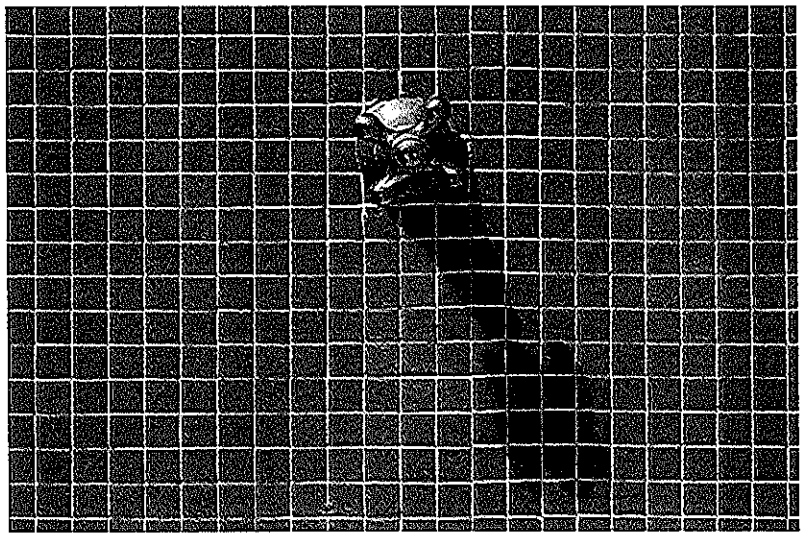
ICS Attacks Can Have Real World Impact

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

ANDY GREENBERG SECURITY 02.08.2021 06:54 PM

A Hacker Tried to Poison a Florida City's Water Supply, Officials Say

The attacker upped sodium hydroxide levels in the Oldsmar, Florida, water supply to extremely dangerous levels.

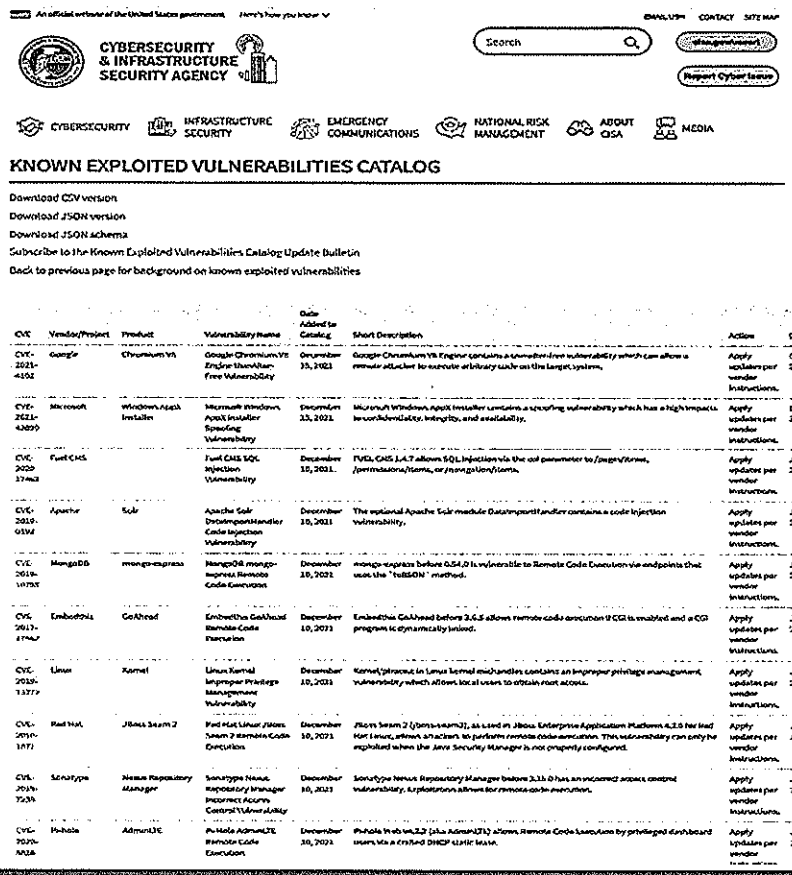


The cursor began clicking through the water treatment plant's controls. Within seconds, the intruder was attempting to change the water supply's levels of sodium hydroxide. PHOTOGRAPH: GETTY IMAGES

Exploitation of Known or Unknown Vulnerabilities

These are weaknesses in software or hardware that may not be known to anyone but the attacker, or a known vulnerability that an organization has not patched or mitigated. This can leave an organization's network extremely vulnerable.

Known Vulnerabilities



An official website of the United States government. Here's how you know

EMAIL US | CONTACT | SITE MAP

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Search

Report Cyber Issue

CYBERSECURITY | INFRASTRUCTURE SECURITY | EMERGENCY COMMUNICATIONS | NATIONAL RISK MANAGEMENT | ABOUT CISA | MEDIA

KNOWN EXPLOITED VULNERABILITIES CATALOG

Download CSV version

Download JSON version

Download JSON schema

Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin

Back to previous page for background on known exploited vulnerabilities

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
CVE-2021-4102	Google	Chromium V8	Google Chromium V8 Engine Use-After-Free Vulnerability	December 15, 2021	Google Chromium V8 Engine contains a use-after-free vulnerability which can allow a remote attacker to execute arbitrary code on the target system.	Apply updates per vendor instructions.	December 29, 2021	
CVE-2021-43890	Microsoft	Windows Appx Installer	Microsoft Windows Appx Installer Spoofing Vulnerability	December 15, 2021	Microsoft Windows Appx Installer contains a spoofing vulnerability which has a high impact to confidentiality, integrity, and availability.	Apply updates per vendor instructions.	December 29, 2021	
CVE-2020-17463	Fuel CMS		Fuel CMS SQL Injection Vulnerability	December 10, 2021	FUEL CMS 1.4.7 allows SQL injection via the col parameter to /page/filter/, /permissions/items, or /navigation/items.	Apply updates per vendor instructions.	June 10, 2022	
CVE-2019-0193	Apache	Solr	Apache Solr DataImportHandler Code Injection Vulnerability	December 10, 2021	The optional Apache Solr module DataImportHandler contains a code injection vulnerability.	Apply updates per vendor instructions.	June 10, 2022	
CVE-2019-10758	MongoDB	mongo-express	MongoDB mongo-express Remote Code Execution	December 10, 2021	mongo-express before 0.54.0 is vulnerable to Remote Code Execution via endpoints that use the `utilsSON` method.	Apply updates per vendor instructions.	June 10, 2022	
CVE-2017-17562	Embedthis	GoAhead	Embedthis GoAhead Remote Code Execution	December 10, 2021	Embedthis GoAhead before 2.4.5 allows remote code execution if CGI is enabled and a CGI program is dynamically linked.	Apply updates per vendor instructions.	June 10, 2022	
CVE-2019-13272	Linux	Kernel	Linux Kernel Improper Privilege Management Vulnerability	December 10, 2021	kernel/ptrace.c in Linux kernel mishandles certain unprivileged process-memory accesses, which allows local users to obtain root access.	Apply updates per vendor instructions.	June 10, 2022	
CVE-2016-1871	Red Hat	JBoss Seam 2	Red Hat Linux JBoss Seam 2 Remote Code Execution	December 10, 2021	JBoss Seam 2 (jboss-seam2), as used in JBoss Enterprise Application Platform 4.3.0 for Red Hat Linux, allows an actor to perform remote code execution. This vulnerability can only be exploited when the Java Security Manager is not properly configured.	Apply updates per vendor instructions.	June 10, 2022	
CVE-2019-7238	Sonatype	Nexus Repository Manager	Sonatype Nexus Repository Manager Incorrect Access Control Vulnerability	December 10, 2021	Sonatype Nexus Repository Manager before 3.15.0 has an incorrect access control vulnerability. Exploitations allow for remote code execution.	Apply updates per vendor instructions.	June 10, 2022	
CVE-2020-8516	Pi-hole	AdminLTE	Pi-hole AdminLTE Remote Code Execution	December 10, 2021	Pi-hole Web v4.3.2 (aka AdminLTE) allows Remote Code Execution by privileged dashboard users via a crafted DHCP static host.	Apply updates per vendor instructions.	June 10, 2022	

paloalto

Vulnerability Exploitation: Apache Log4j

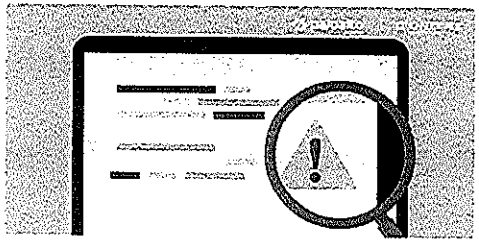
paloalto UNIT 42

Tools ATOMs Security Consulting About Us

Another Apache Log4j Vulnerability Is Actively Exploited in the Wild (CVE-2021-44228) (Updated Dec. 28)

196,342 people reacted | 380 | 15 min. read

SHARE



This post is also available in: 日本語 (Japanese)

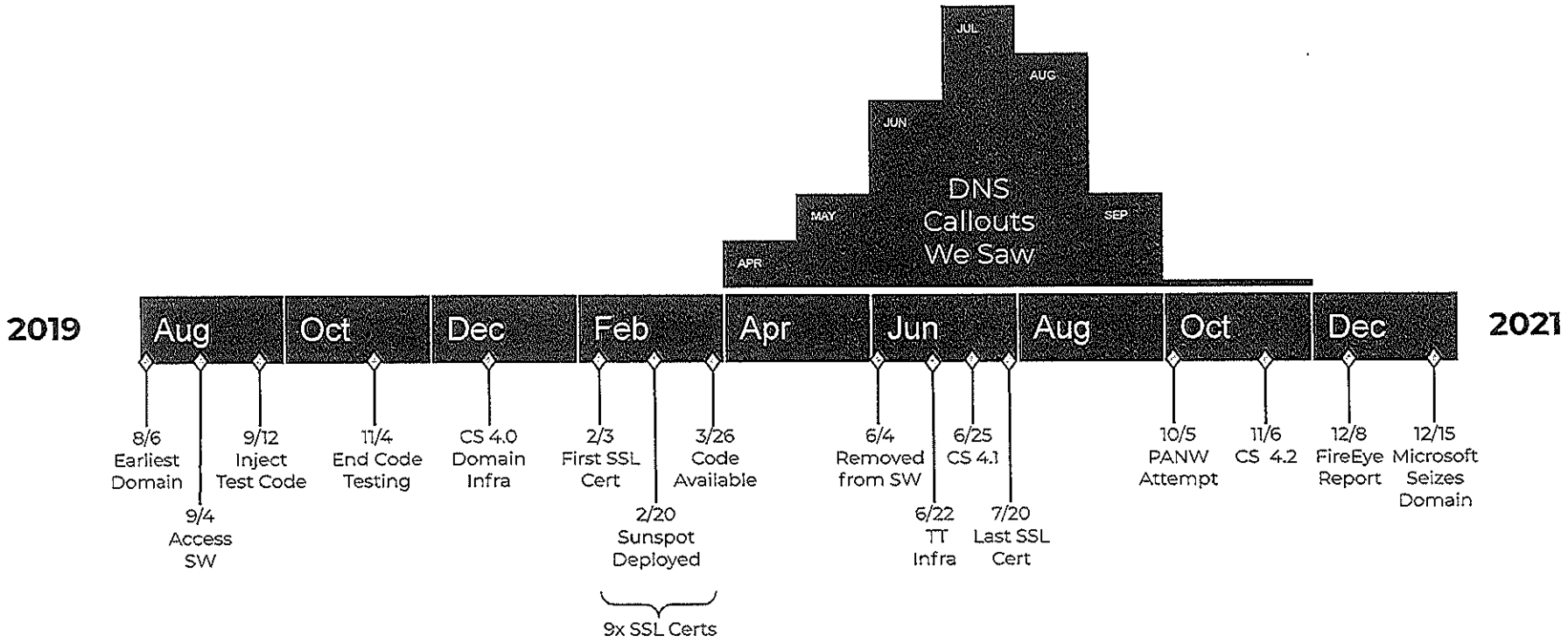
Executive Summary

On Dec. 9, 2021, a remote code execution (RCE) vulnerability in Apache Log4j 2 was identified being exploited in the wild. Public proof of concept (PoC) code was released and subsequent investigation revealed that exploitation was incredibly easy to perform. By submitting a specially crafted request to a vulnerable system, depending on how the system is configured, an attacker is able to instruct that system to download and subsequently execute a

Supply Chain Attacks

Supply chain attacks seek to damage an organization by targeting less-secure elements in the supply chain. It's a "low and slow" way for attackers to gain access to organizations' networks under the cover of a trusted source.

SolarWinds Software Supply Chain Attack - Timeline



What Can You As Policymakers Do?

- Incentivize The Adoption of Best Practices and Standards.
- Support smaller governments and municipalities.
- Mandate Reporting of Ransomware and Other Incidents.
- Understand the Threats.
- Understand What You're Spending on Cybersecurity.
- Know What Your Attackers See.
- Ensure that Cybersecurity is a Core Function of Government.

Questions and Answers