

Threats and Opportunities

Oregon Joint Legislative Committee on Information Management & Technology

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

Current and Emerging Threats

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

The New York Times **Hackers Are Holding Baltimore Hostage:
How They Struck and What's Next**

May, 19 2019

*The Atlanta
Journal-Constitution*

**Cost of City of Atlanta's cyber
attack: \$2.7 million — and rising**

April 12, 2018

**The
Guardian**

**Colonial Pipeline confirms it paid \$4.4M
ransom to hacker gang after attack**

May 20, 2021

n p r

**Meat Supplier JBS Is The Latest
Company Hit With Ransomware**

Jun 2, 2021

ZDNet

**Acer reportedly targeted with \$50
million ransomware attack**

March 22, 2021

CNN

**Ransomware attack hits Virginia
Legislature.**

December 13, 2021

SECURITY

Bose victim of ransomware attack

May 26, 2021

ZDNet

**Singtel hit by third-party vendor's
security breach**

Feb 11, 2021

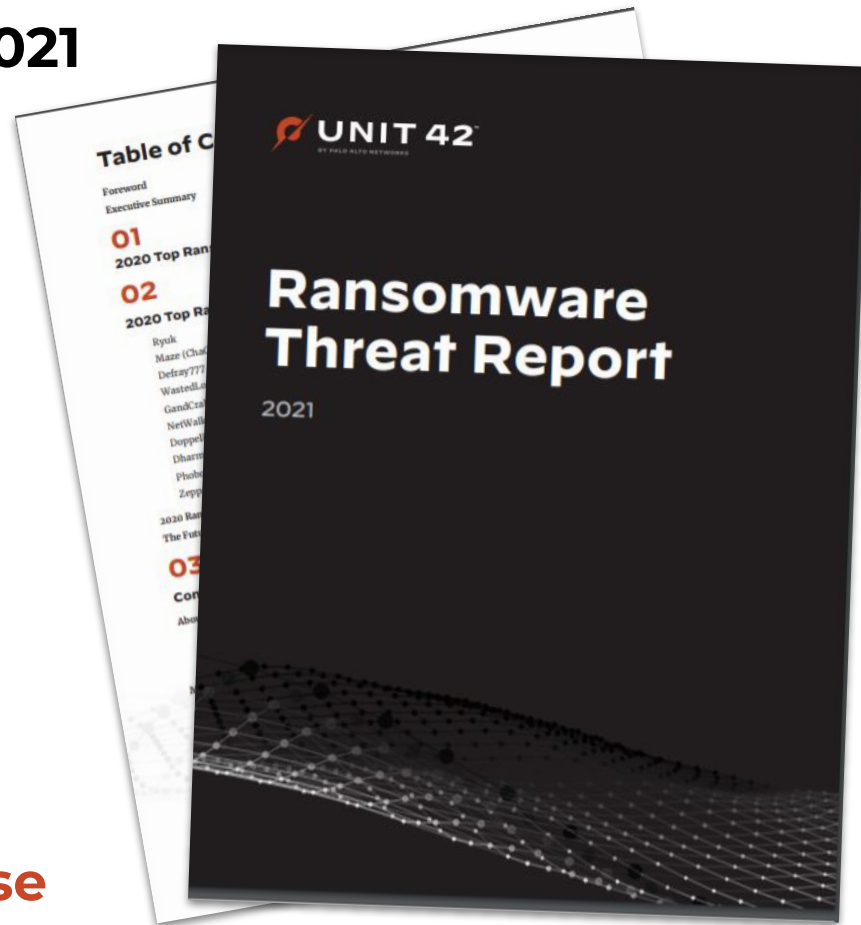
Ransomware: Key Trends in 2021

\$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

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

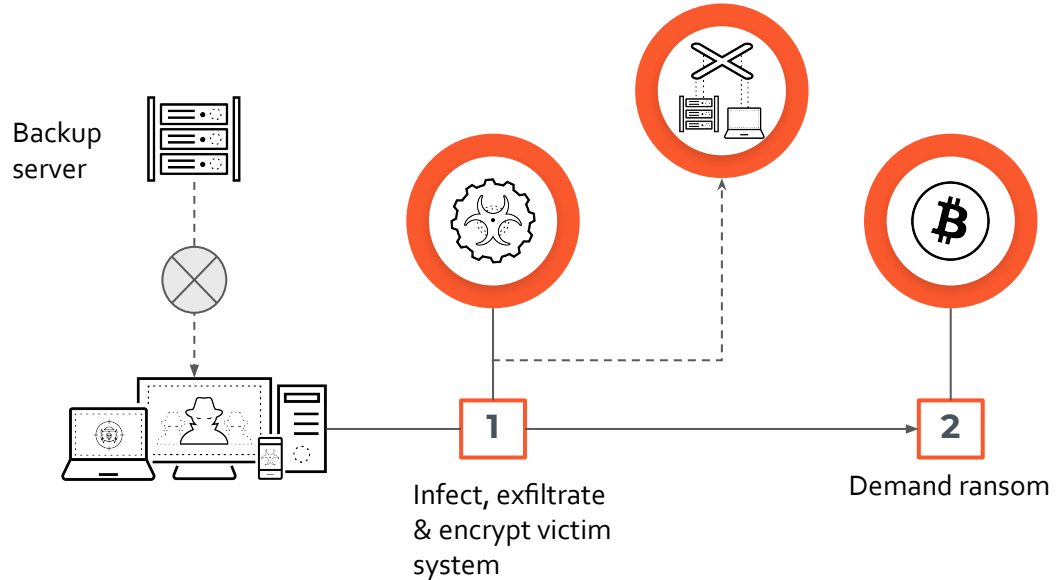
Extortion Payments Hit New Records as Ransomware Crisis Intensifies

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



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.

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

cisa.gov/uscert

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	Fuel CMS SQL Injection Vulnerability	December 10, 2021	FUEL CMS 1.4.7 allows SQL Injection via the col parameter to /pages/items, /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 uses the "toJSON" 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 3.6.5 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 contains an improper privilege management vulnerability which allows local users to obtain root access.	Apply updates per vendor instructions.	June 10, 2022	
CVE-2019-1871	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 attackers 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. Exploitation allows for remote code execution.	Apply updates per vendor instructions.	June 10, 2022	
CVE-2020-8816	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 lease.	Apply updates per vendor instructions.	June 10, 2022	

Unknown Vulnerability Exploitation: Apache Log4j

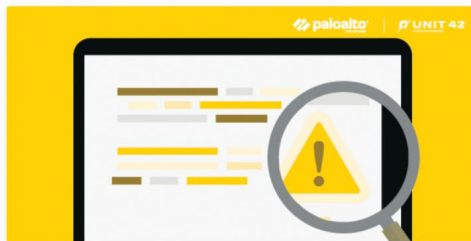
[Tools](#) [ATOMs](#) [Security Consulting](#) [About Us](#) [Under Attack?](#)

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

196,142 people reacted 380 15 min. read

SHARE

By Tao Yan, Qi Deng, Haozhe Zhang, Yu Fu, Josh Grunzweig, Mike Harbison and Robert Falcone
December 10, 2021 at 1:00 PM
Category: [Unit 42](#)
Tags: [Apache Log4j](#), [CVE-2017-5645](#), [CVE-2019-17571](#), [CVE-2021-44228](#), [CVE-2021-44832](#), [CVE-2021-45046](#), [CVE-2021-45105](#), [denial of service](#), [exploit](#), [log4j](#), [log4j 2](#), [RCE](#), [vulnerability](#)



This post is also available in: [日本語 \(Japanese\)](#)

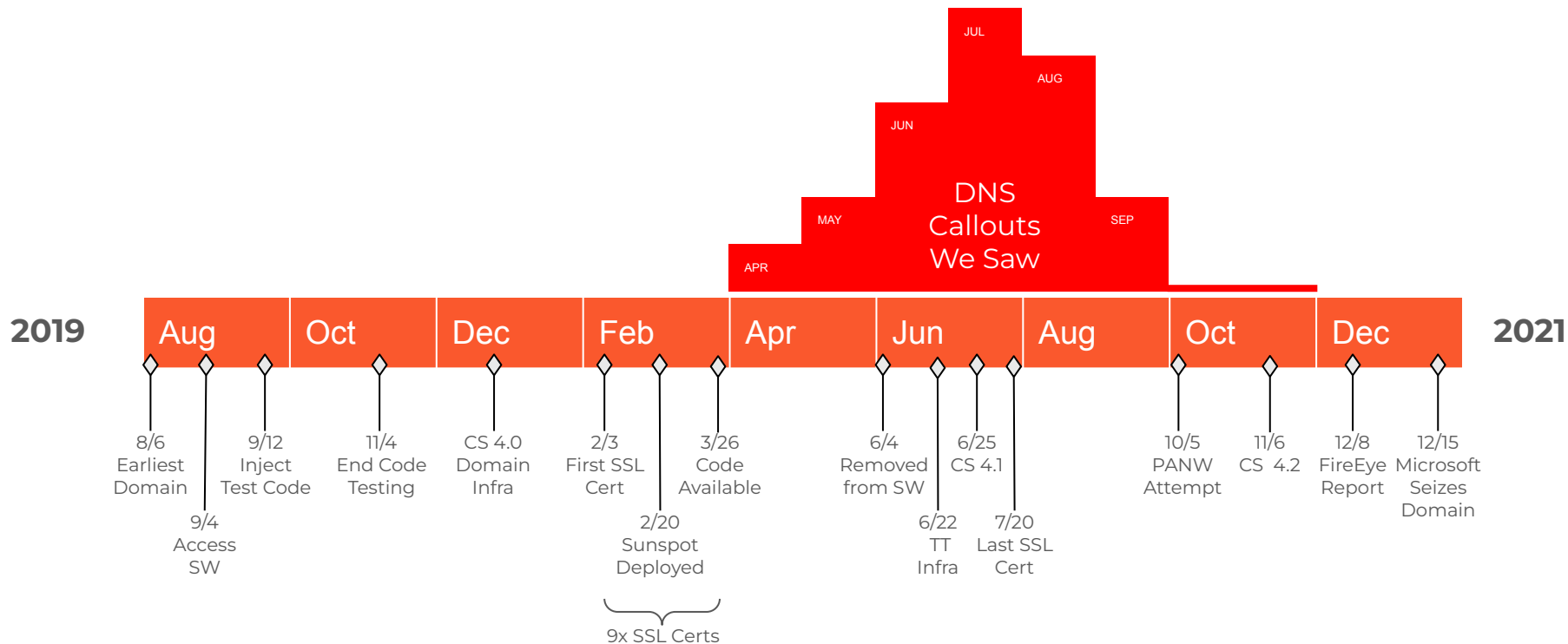
Executive Summary

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 malicious payload. Due to the discovery of this exploit being so recent, there are still many servers, both on-

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



The right tools and solutions can counter threats.

- Need visibility and security enforcement across key areas including cloud, network, and endpoint.
- Capabilities should be automated and integrated across tools and environments (cloud, network, endpoint).

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