Vermont House Committee on Energy and Technology: Understanding Cybersecurity Threats and Opportunities

Thomas MacLellan
Director, Government Affairs & Strategy
Palo Alto Networks
April 1, 2022

paloalto® NETWORKS

Our vision	We envision a world where each day is safer and more secure than the one before.
Our mission	To be the cybersecurity partner of choice, protecting our digital way of life.
Our promise	We've got the next-generation of cybersecurity innovation.
Market context	Accelerated digital transformation in an environment of elevated risk
Organizational imperative for our customers	Managing risk to ensure business continuity, employee engagement, brand reputation, technological advancement and overall ROI

Palo Alto Networks Cybersecurity Academy: Training the Next Generation of Cyber Warriors

Palo Alto Networks Cybersecurity Academy works with degree-granting, nationally accredited secondary or post-secondary academic institutions interested in teaching our next-generation technology to their students. The Cybersecurity Academy works with academic institutions and instructors to prepare students for exciting careers in the rapidly growing areas of cloud, network and infrastructure security.

Palo Alto Networks Cyber Scholars: Scholarships

- **Fourteen** scholarships up to **$10,000** available
- Applications close **April 4, 2022**
- Open to students **enrolled in HBCUs** in 2022-23 school year, majoring in **STEM or Business**
- Will also be offered a **company internship** in Summer 2023 (must be enrolled in an academic program in 2023-24 school year), a Palo Alto Networks **employee mentor**, and **quarterly networking and resource events** throughout the academic year.
- Learn more about our commitment to uplifting Black youth ages 5-25 on our website.

Current and Emerging Threats

Ransomware

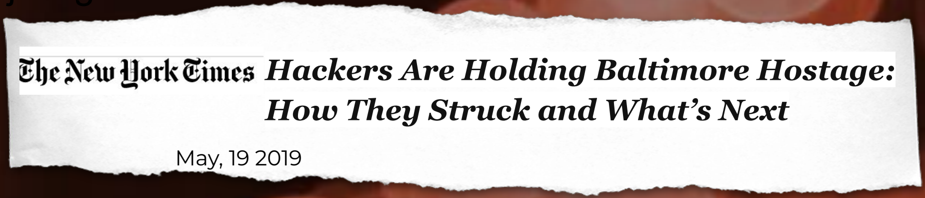
Industrial Control System Attacks

Vulnerability Exploitation

Supply Chain

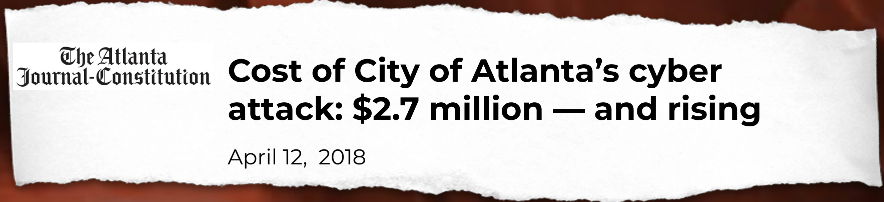
ajc logo

ajc logo



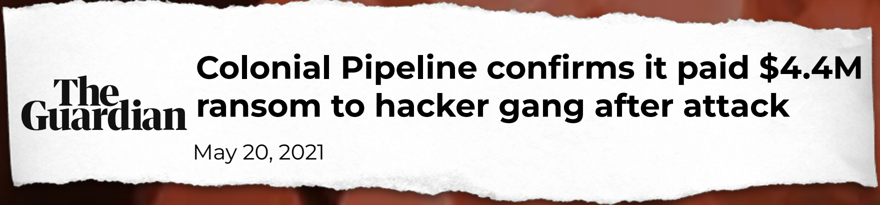
The New York Times *Hackers Are Holding Baltimore Hostage: How They Struck and What's Next*

May, 19 2019



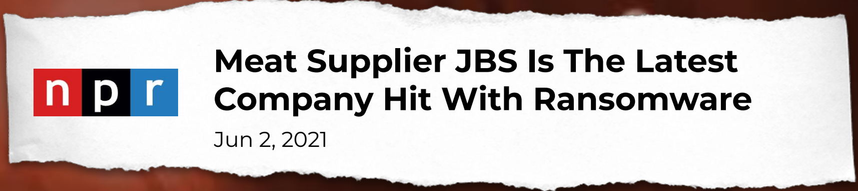
The Atlanta Journal-Constitution **Cost of City of Atlanta's cyber attack: $2.7 million — and rising**

April 12, 2018



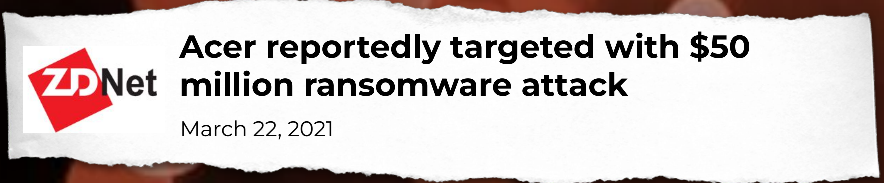
The Guardian **Colonial Pipeline confirms it paid $4.4M ransom to hacker gang after attack**

May 20, 2021



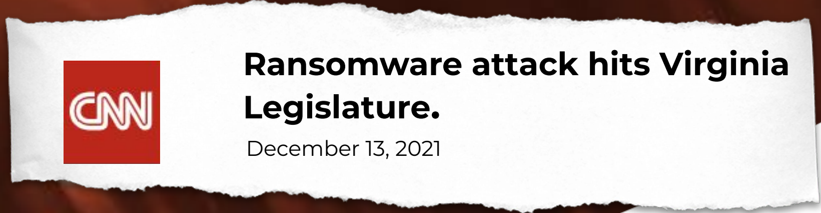
npr **Meat Supplier JBS Is The Latest Company Hit With Ransomware**

Jun 2, 2021



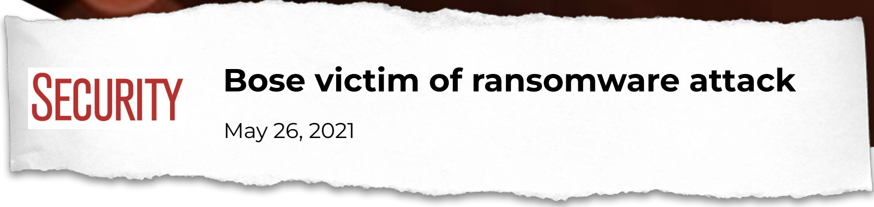
ZDNet **Acer reportedly targeted with $50 million ransomware attack**

March 22, 2021



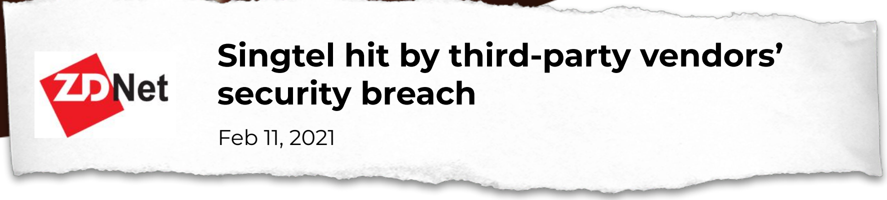
CNN **Ransomware attack hits Virginia Legislature.**

December 13, 2021



SECURITY **Bose victim of ransomware attack**

May 26, 2021



ZDNet **Singtel hit by third-party vendors' 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

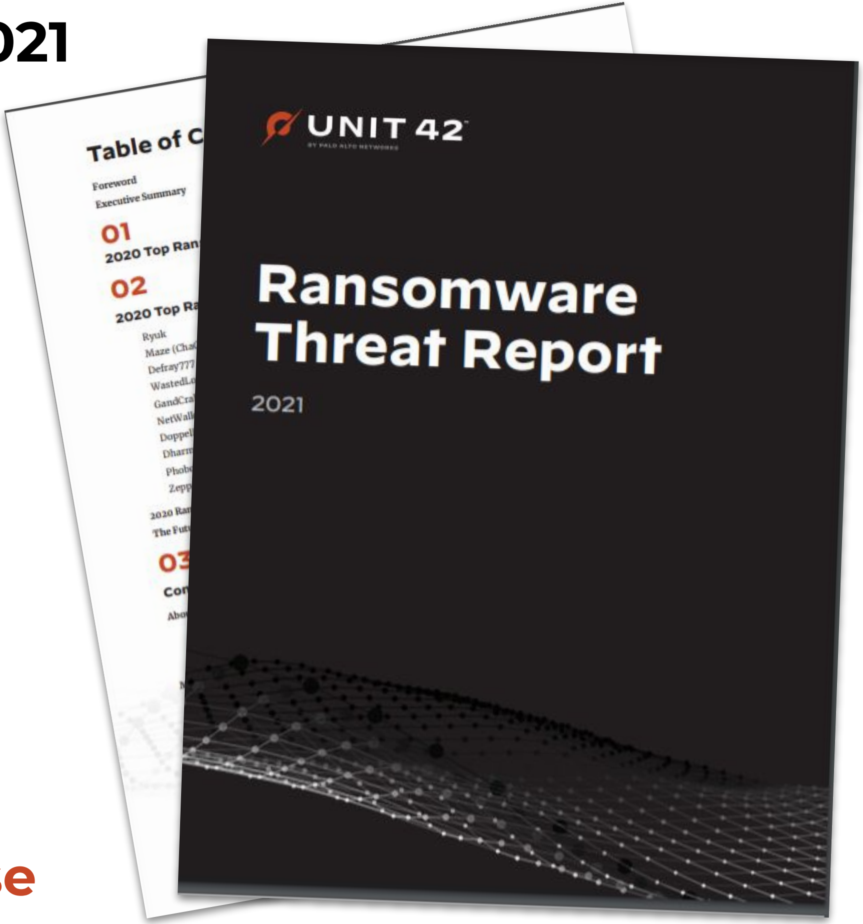


Table of C

Foreword

Executive Summary

01

2020 Top Ran

02

2020 Top Ra

Ryuk

Maze (ChaC

Defray777

WastedLo

GandCra

NetWall

Doppel

Dharm

Phobo

Zepp

2020 Ran

The Fut

03

Con

Abo

UNIT 42

BY PALO ALTO NETWORKS

Ransomware Threat Report

2021

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

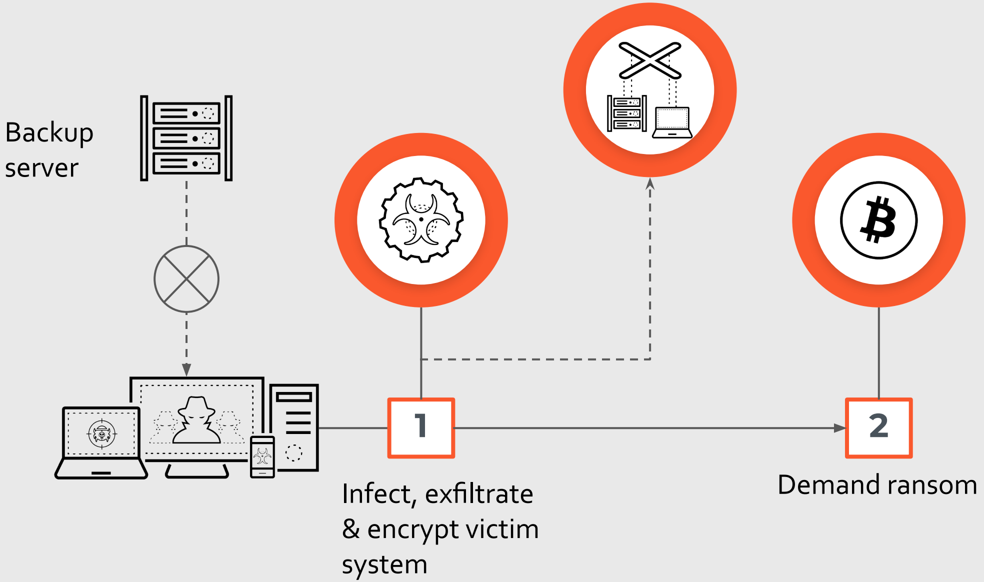
Customers, business partners, employees and media contacted

Extortion Payments Hit New Records as Ransomware Crisis Intensifies

Colonial Pipeline

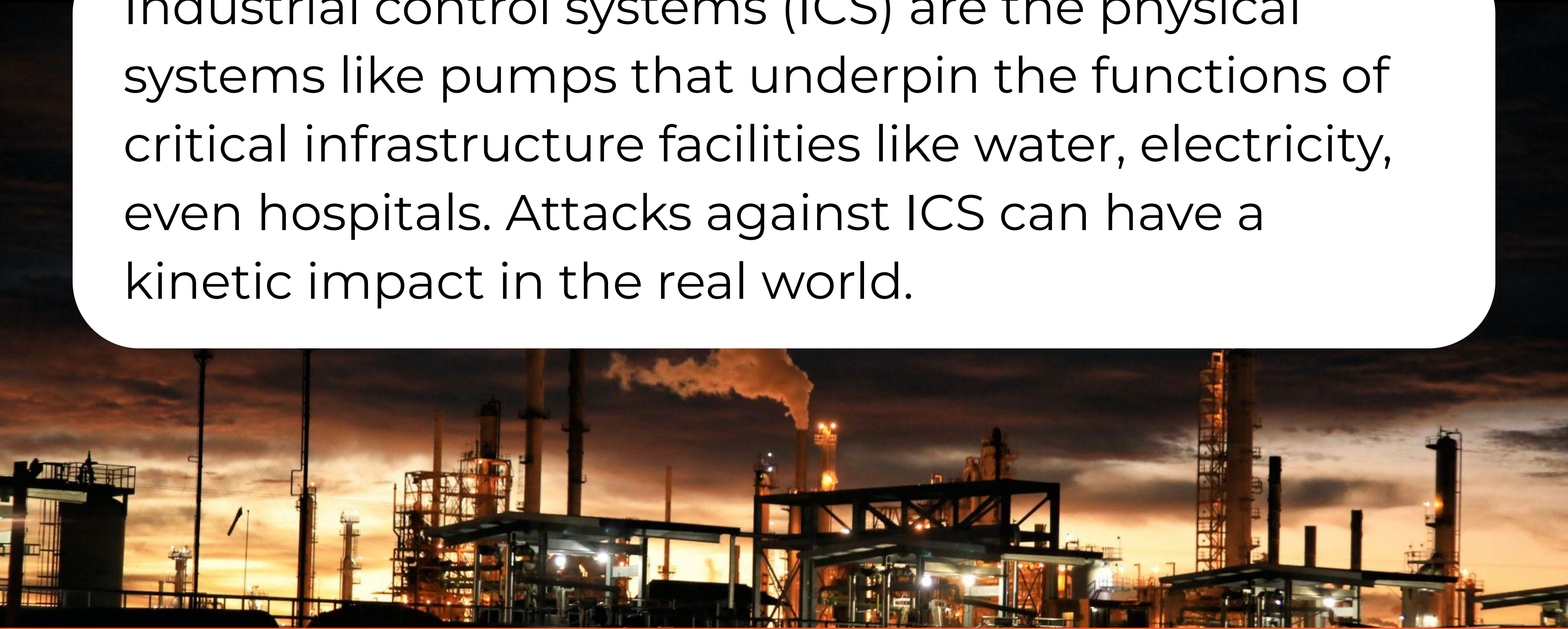
What Happened MAY 2021:

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

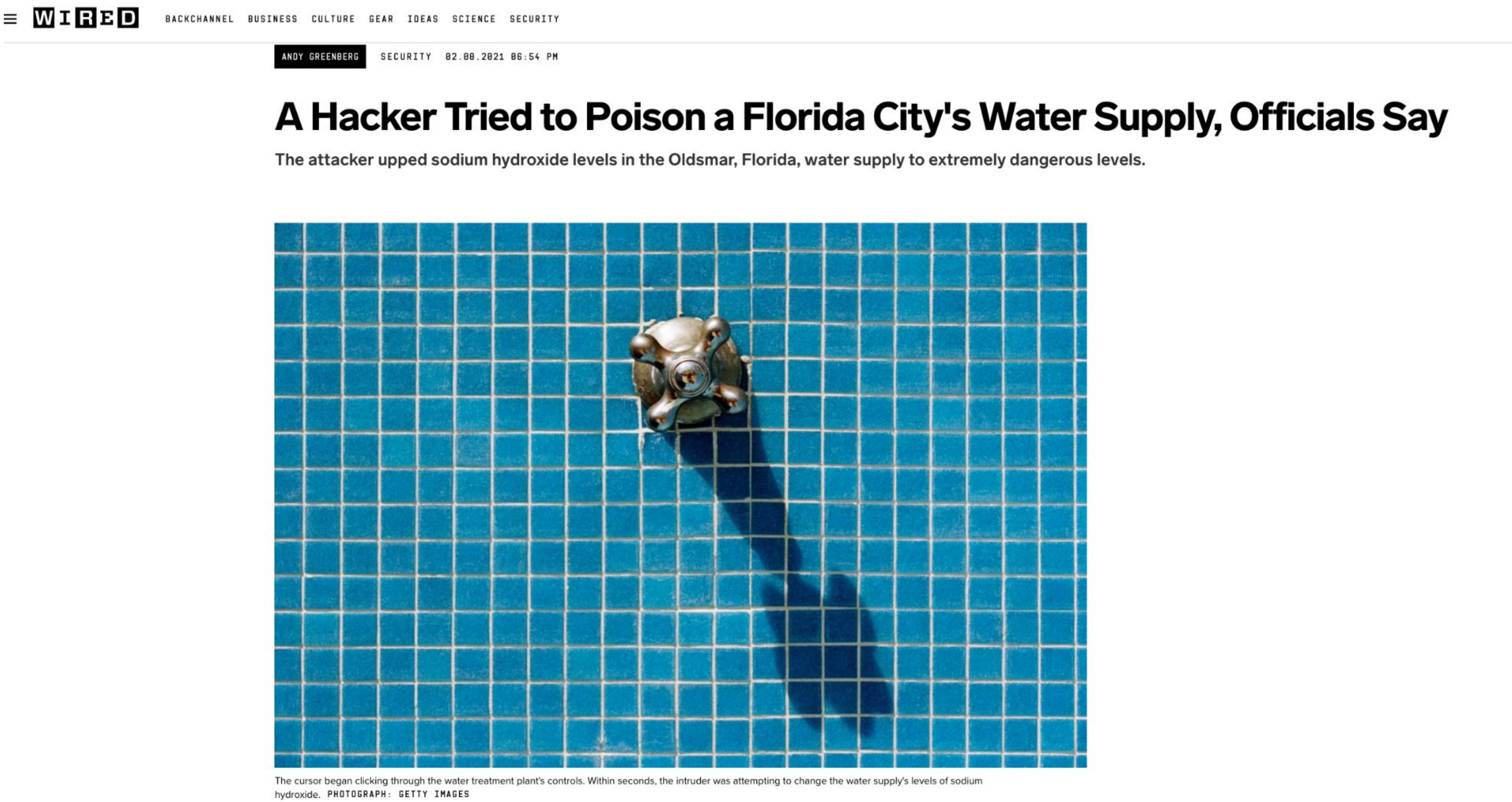


Industrial Control Systems Attacks

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



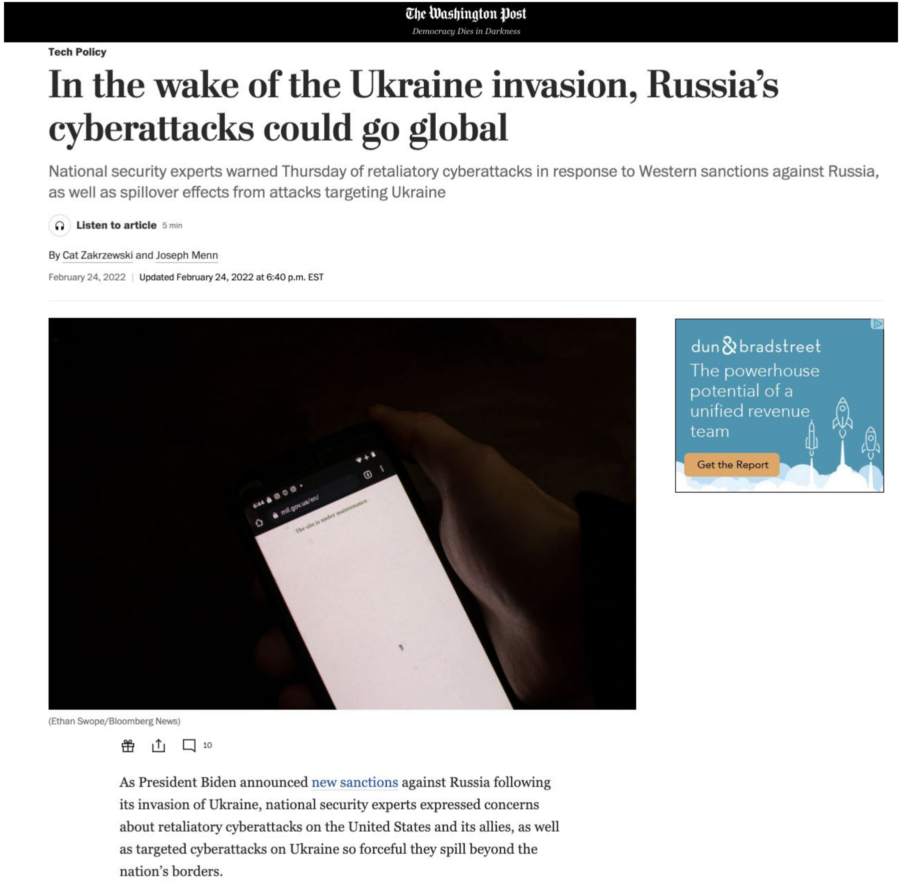
ANDY GREENBERG SECURITY 02.08.2021 06:54 PM

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

Rising Threat Against Infrastructure



The Washington Post
Democracy Dies in Darkness

Tech Policy

In the wake of the Ukraine invasion, Russia’s cyberattacks could go global

National security experts warned Thursday of retaliatory cyberattacks in response to Western sanctions against Russia, as well as spillover effects from attacks targeting Ukraine

Listen to article 5 min

By Cat Zakrzewski and Joseph Menn

February 24, 2022 | Updated February 24, 2022 at 6:40 p.m. EST

(Ethan Swope/Bloomberg News)

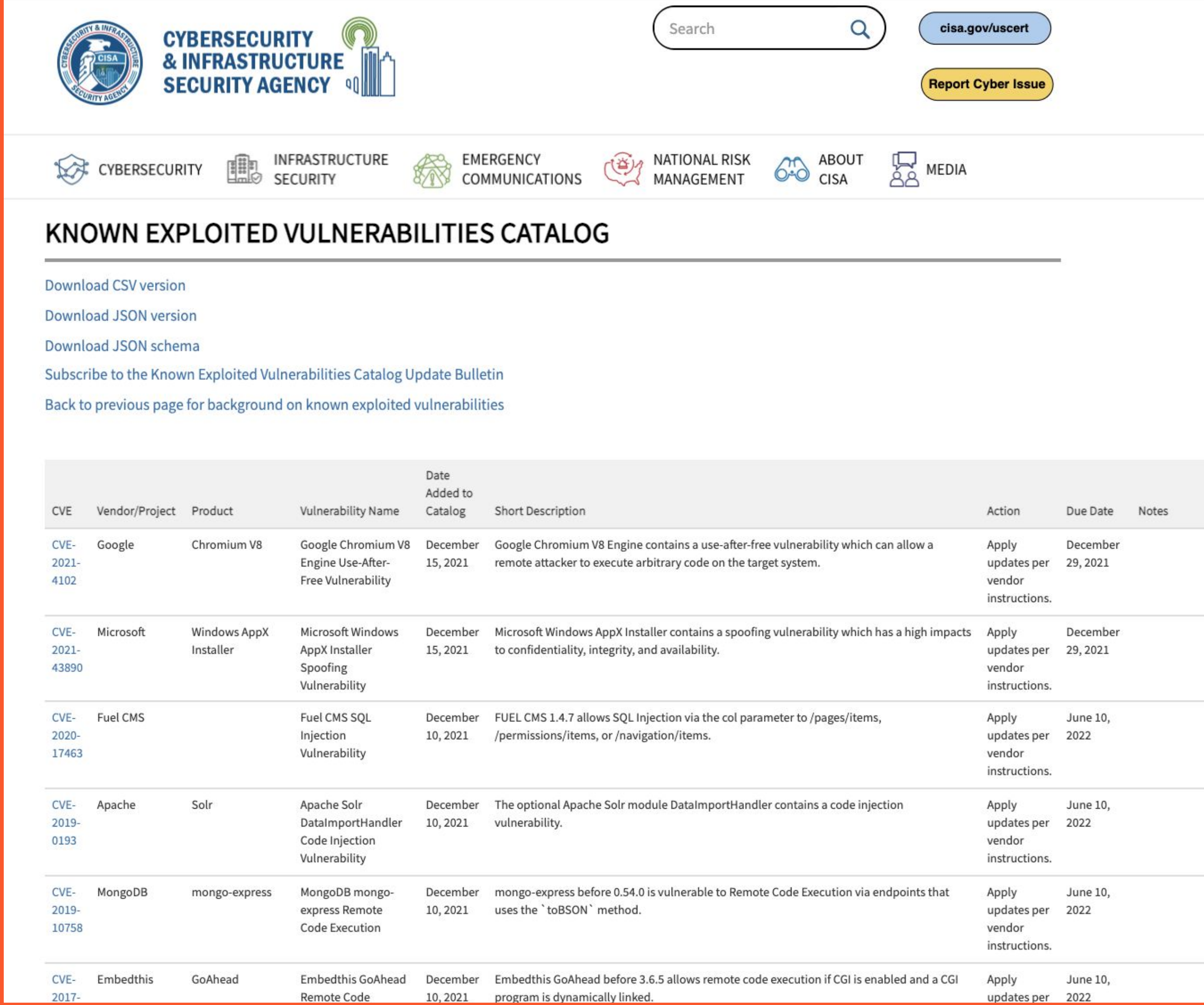
10

As President Biden announced new sanctions against Russia following its invasion of Ukraine, national security experts expressed concerns about retaliatory cyberattacks on the United States and its allies, as well as targeted cyberattacks on Ukraine so forceful they spill beyond the nation’s borders.

Exploitation of Known or Unknown Vulnerabilities

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



KNOWN EXPLOITED VULNERABILITIES CATALOG

Download CSV version

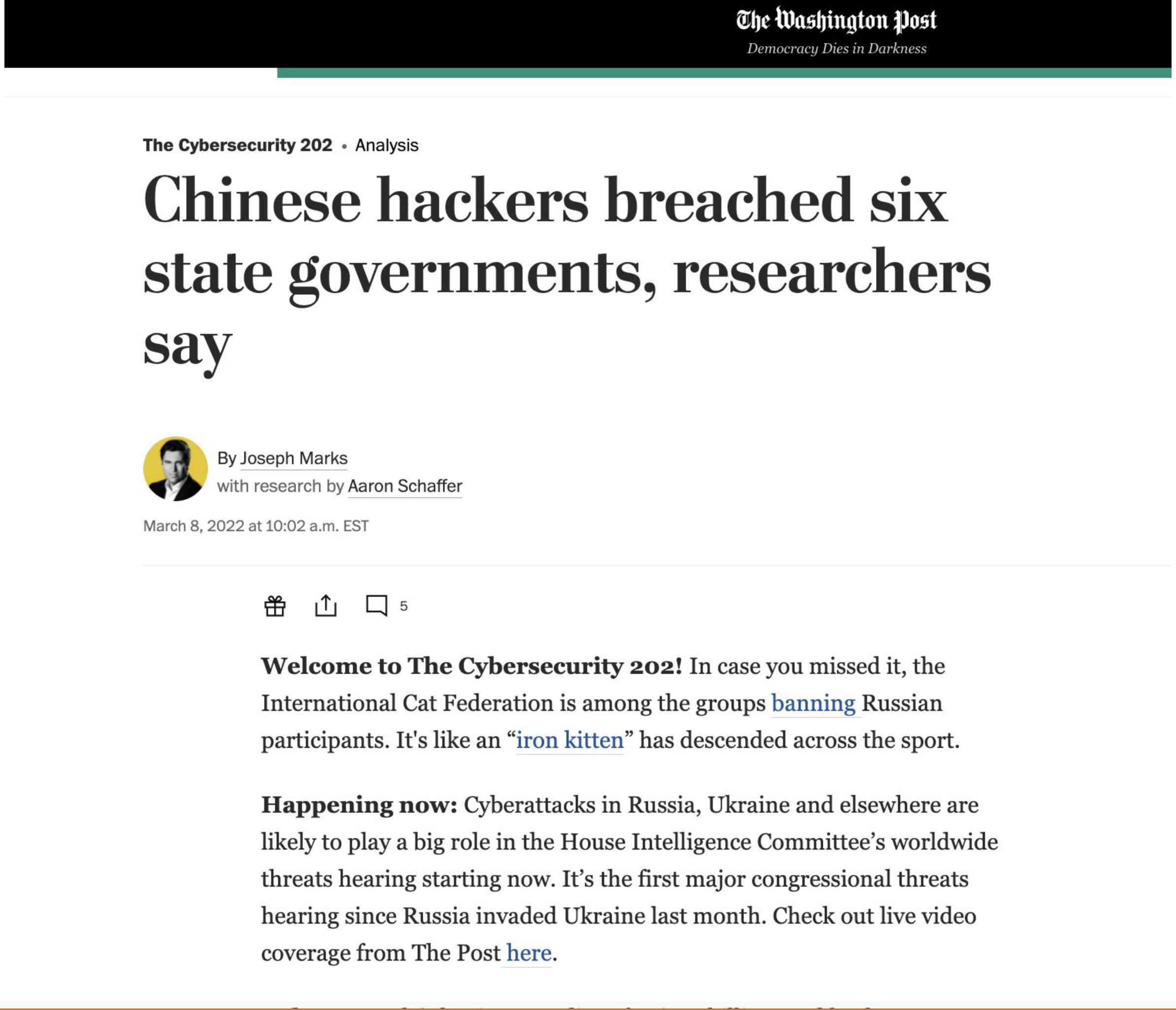
Download JSON version

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 impacts 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 /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 `toBSON` method.	Apply updates per vendor instructions.	June 10, 2022	
CVE-2017-	Embedthis	GoAhead	Embedthis GoAhead Remote Code	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	June 10, 2022	



The Washington Post
Democracy Dies in Darkness

The Cybersecurity 202 • Analysis

Chinese hackers breached six state governments, researchers say

By Joseph Marks
with research by Aaron Schaffer

March 8, 2022 at 10:02 a.m. EST

5

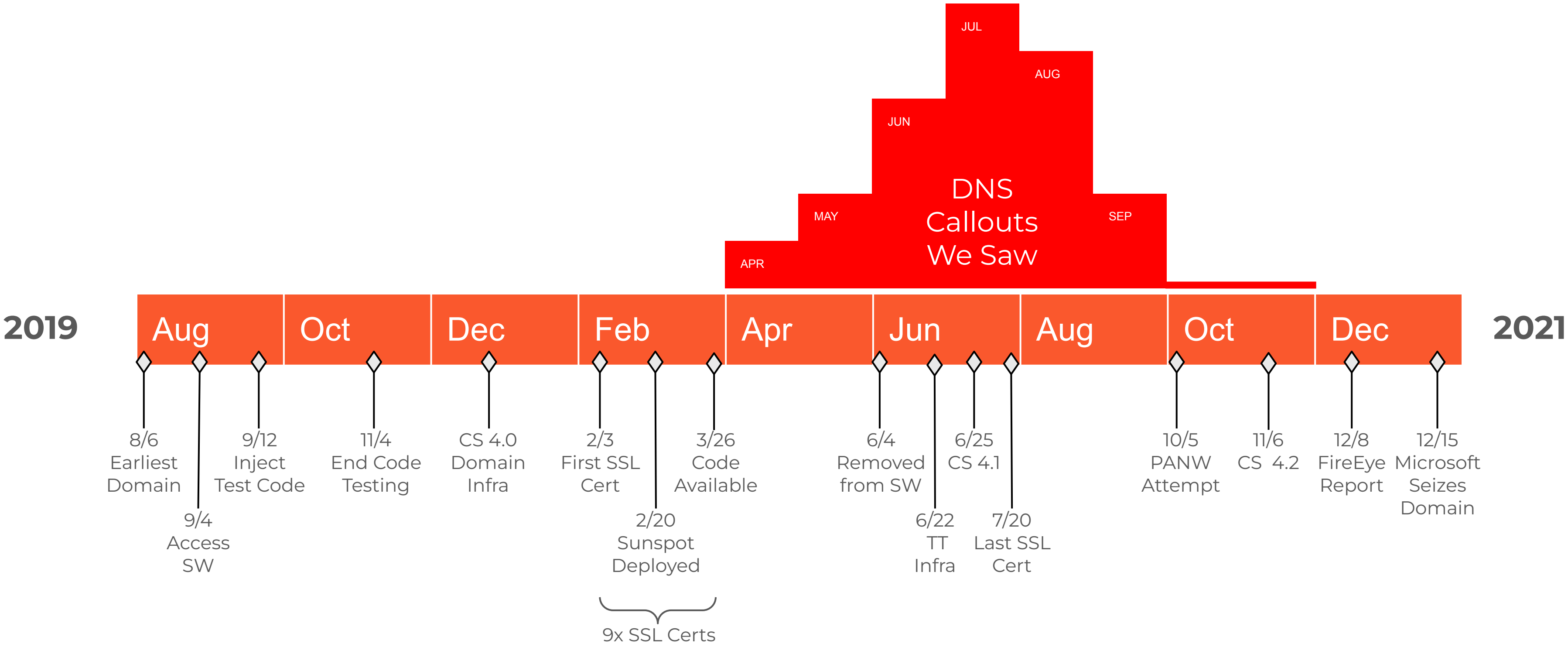
Welcome to The Cybersecurity 202! In case you missed it, the International Cat Federation is among the groups banning Russian participants. It's like an "iron kitten" has descended across the sport.

Happening now: Cyberattacks in Russia, Ukraine and elsewhere are likely to play a big role in the House Intelligence Committee's worldwide threats hearing starting now. It's the first major congressional threats hearing since Russia invaded Ukraine last month. Check out live video coverage from The Post here.

Supply Chain Attacks

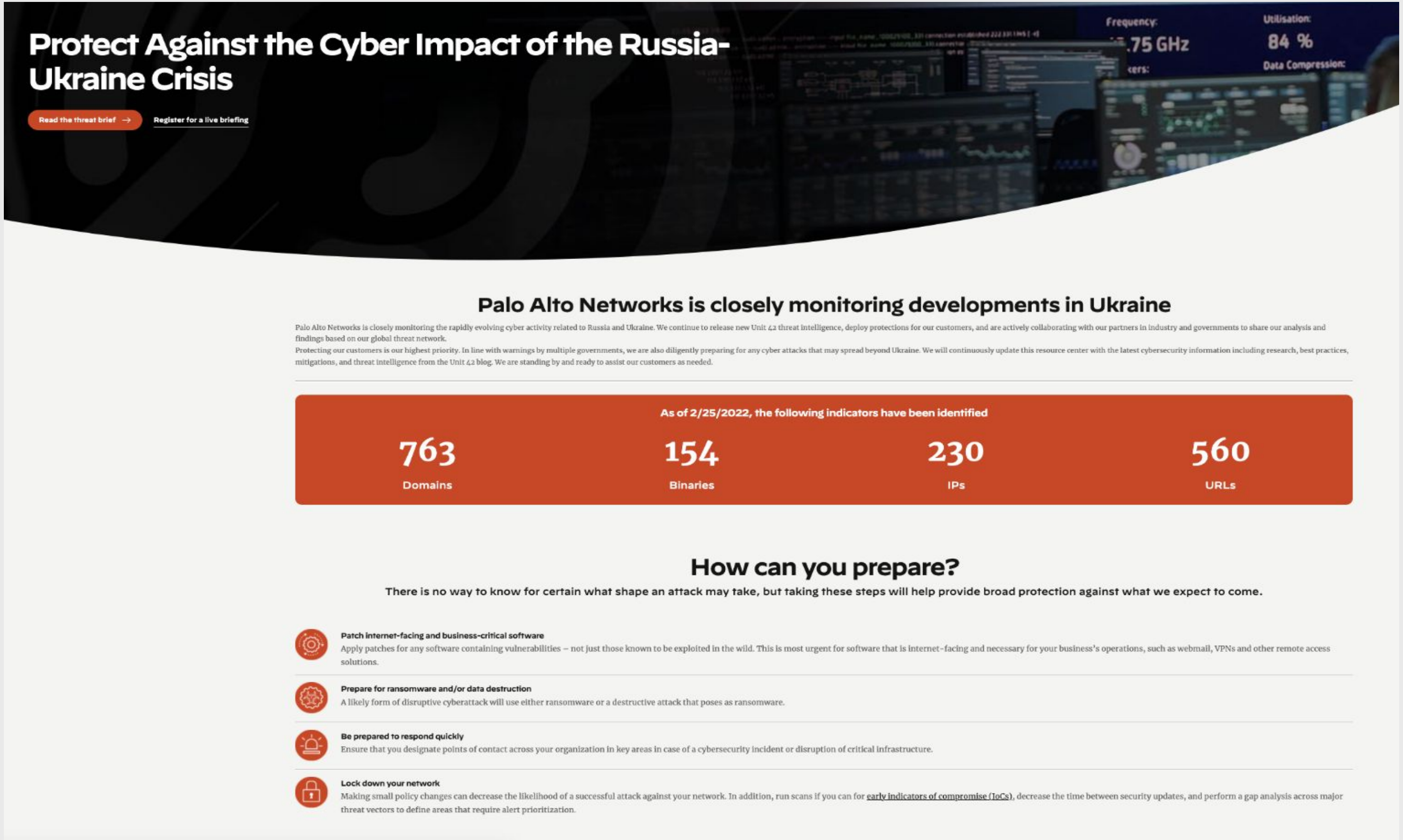
Supply chain attacks seek to damage an organization by targeting less-secure elements in the supply chain. It’s a “low and slow” way for attackers to gain access to organizations’ networks under the cover of a trusted source.

SolarWinds Software Supply Chain Attack - Timeline



Changing Threat Contexts

Growing Global Threats



Protect Against the Cyber Impact of the Russia-Ukraine Crisis

Palo Alto Networks is closely monitoring developments in Ukraine

Palo Alto Networks is closely monitoring the rapidly evolving cyber activity related to Russia and Ukraine. We continue to release new Unit 42 threat intelligence, deploy protections for our customers, and are actively collaborating with our partners in industry and governments to share our analysis and findings based on our global threat network.

Protecting our customers is our highest priority. In line with warnings by multiple governments, we are also diligently preparing for any cyber attacks that may spread beyond Ukraine. We will continuously update this resource center with the latest cybersecurity information including research, best practices, mitigations, and threat intelligence from the Unit 42 blog. We are standing by and ready to assist our customers as needed.

As of 2/25/2022, the following indicators have been identified

763	154	230	560
Domains	Binaries	IPs	URLs

How can you prepare?

There is no way to know for certain what shape an attack may take, but taking these steps will help provide broad protection against what we expect to come.

Patch internet-facing and business-critical software
Apply patches for any software containing vulnerabilities – not just those known to be exploited in the wild. This is most urgent for software that is internet-facing and necessary for your business's operations, such as webmail, VPNs and other remote access solutions.

Prepare for ransomware and/or data destruction
A likely form of disruptive cyberattack will use either ransomware or a destructive attack that poses as ransomware.

Be prepared to respond quickly
Ensure that you designate points of contact across your organization in key areas in case of a cybersecurity incident or disruption of critical infrastructure.

Lock down your network
Making small policy changes can decrease the likelihood of a successful attack against your network. In addition, run scans if you can for early indicators of compromise (IoCs), decrease the time between security updates, and perform a gap analysis across major threat vectors to define areas that require alert prioritization.

Hybrid Workforce Here to Stay

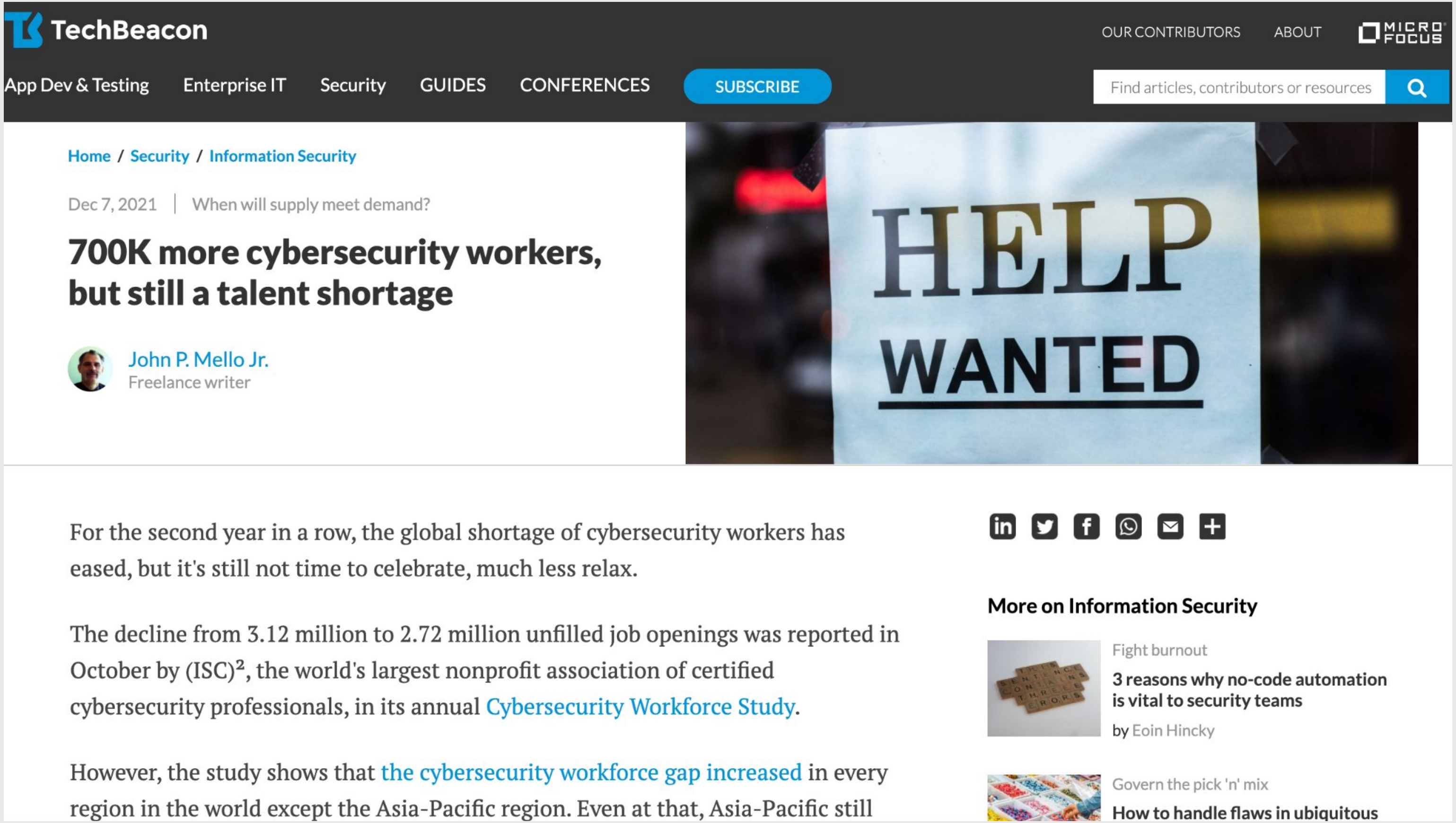
McKinsey & Company

McKinsey Global Institute

The future of work after COVID-19

February 18, 2021 | Report

Cybersecurity Workforce Constraints



Home / Security / Information Security

Dec 7, 2021 | When will supply meet demand?

700K more cybersecurity workers, but still a talent shortage

John P. Mello Jr.
Freelance writer

For the second year in a row, the global shortage of cybersecurity workers has eased, but it's still not time to celebrate, much less relax.

The decline from 3.12 million to 2.72 million unfilled job openings was reported in October by (ISC)², the world's largest nonprofit association of certified cybersecurity professionals, in its annual Cybersecurity Workforce Study.

However, the study shows that the cybersecurity workforce gap increased in every region in the world except the Asia-Pacific region. Even at that, Asia-Pacific still

More on Information Security

Fight burnout
3 reasons why no-code automation is vital to security teams
by Eoin Hincky

Govern the pick 'n' mix
How to handle flaws in ubiquitous

The right tools and solutions can counter threats and maximize your scarce human resources: Opportunities to Drive Innovation

- **Comprehensive Visibility**
- **Relentless Automation**
- **Actionable Security**

As you modernize so are the attackers.

Roadmap for the Future: Secure Access Service Edge (SASE)

“Digitalization, work from anywhere and cloud-based computing have accelerated cloud-delivered SASE offerings to enable anywhere, anytime access from any device. Security and risk management leaders should build a migration plan from legacy perimeter and hardware-based offerings to a SASE model.” You can’t just flip a switch to adopt SASE and enable anywhere, anytime access from any device.

“The vast majority of enterprise SASE adoption will occur over several years, prioritizing areas of greatest opportunity in terms of cost savings, eliminating complexity and redundant vendors, and risk reduction through adoption of a zero-trust secure posture.” (Gartner, 2021)

A Unique Opportunity to Develop Unity of Effort: State & Local Cybersecurity Grant Program

Cybersecurity and Infrastructure Security Agency

Questions and Answers