Tech Response in a World in Crisis:

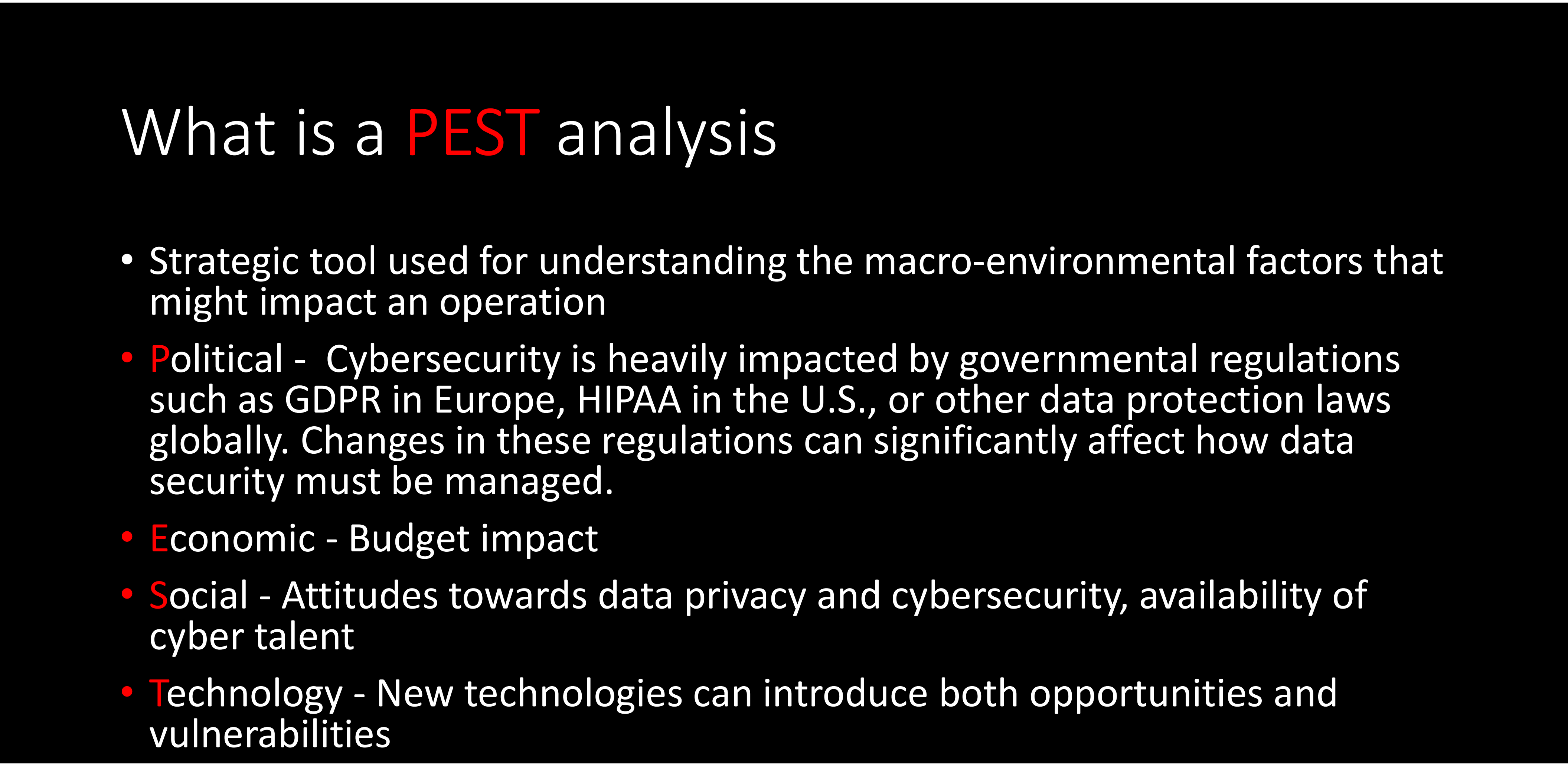
Cybersecurity and Auditing in the Age of Disruption

Who am I?

- Security Evangelist
- ISACA emerging trends working group & VP at ISACA GWDC
- 25 years in cyber including 10 years as a CISO
- CISSP,CCAK,CCSK,CRISC,CISA,CISM, CDPSE, GIAC

Agenda

- Understanding the Global Landscape through PEST Analysis
- Cybersecurity in a World at War and economic tension
- Learning from the Past and looking into the future



What is a PEST analysis

- Strategic tool used for understanding the macro-environmental factors that might impact an operation
- Political - Cybersecurity is heavily impacted by governmental regulations such as GDPR in Europe, HIPAA in the U.S., or other data protection laws globally. Changes in these regulations can significantly affect how data security must be managed.
- Economic - Budget impact
- Social - Attitudes towards data privacy and cybersecurity, availability of cyber talent
- Technology - New technologies can introduce both opportunities and vulnerabilities

PEST analysis in cybersecurity helps organizations anticipate external challenges and opportunities, aligning their security measures with broader environmental conditions. This proactive approach can enhance an organization's resilience against external disruptions and threats.

Take a moment to fill this out

Political	**E**conomic
Social	**T**echnological

How will this impact your strategy?

Example - PEST- Political, Economical, Social, Technology

POLITICAL

- War
- Increased political polarization
- Digital Sovereignty
- Lack of global cooperation around legal action against hackers
- Attacks on critical infrastructure

ECONOMICAL

- Tariffs
- Inflation
- Increased labor costs
- Increased fines for breaches
- Cost of increased security

SOCIAL

- Social Media is being used as a source of truth
- Increased polarization
- Increased cybersecurity attacks
- Demand for more security
- Increased focus on sustainability

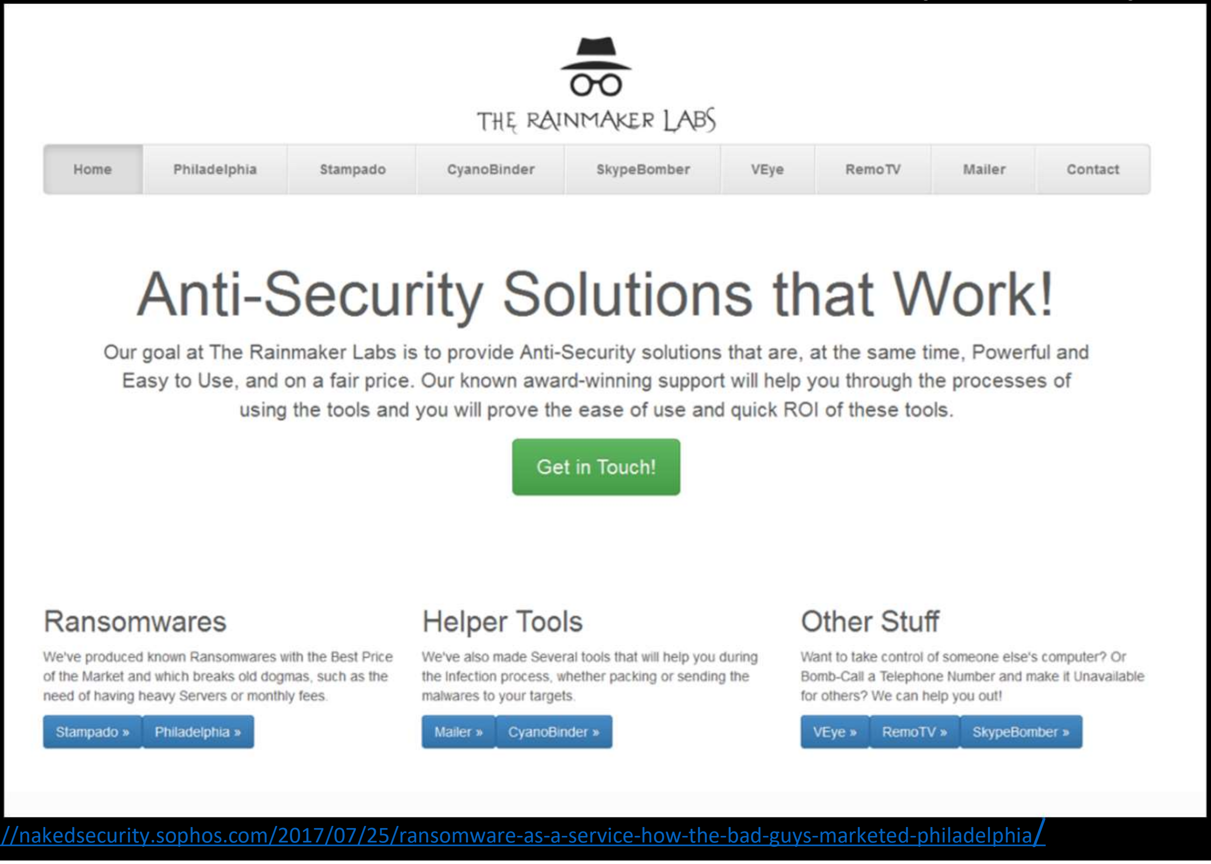
TECHNOLOGY

- AI
- Quantum
- Increased reliance on digitization and automation
- Need for leveraging cloud solutions
- Move towards Zero Trust
- Increased connectivity between OT and IT environments
- Increased need for resilience

The changing world

The Changing Face of Crime

Ransomware as a Service (RaaS)



THE RAINMAKER LABS

Anti-Security Solutions that Work!

Our goal at The Rainmaker Labs is to provide Anti-Security solutions that are, at the same time, Powerful and Easy to Use, and on a fair price. Our known award-winning support will help you through the processes of using the tools and you will prove the ease of use and quick ROI of these tools.

Ransomwares

We've produced known Ransomwares with the Best Price of the Market and which breaks old dogmas, such as the need of having heavy Servers or monthly fees.

Helper Tools

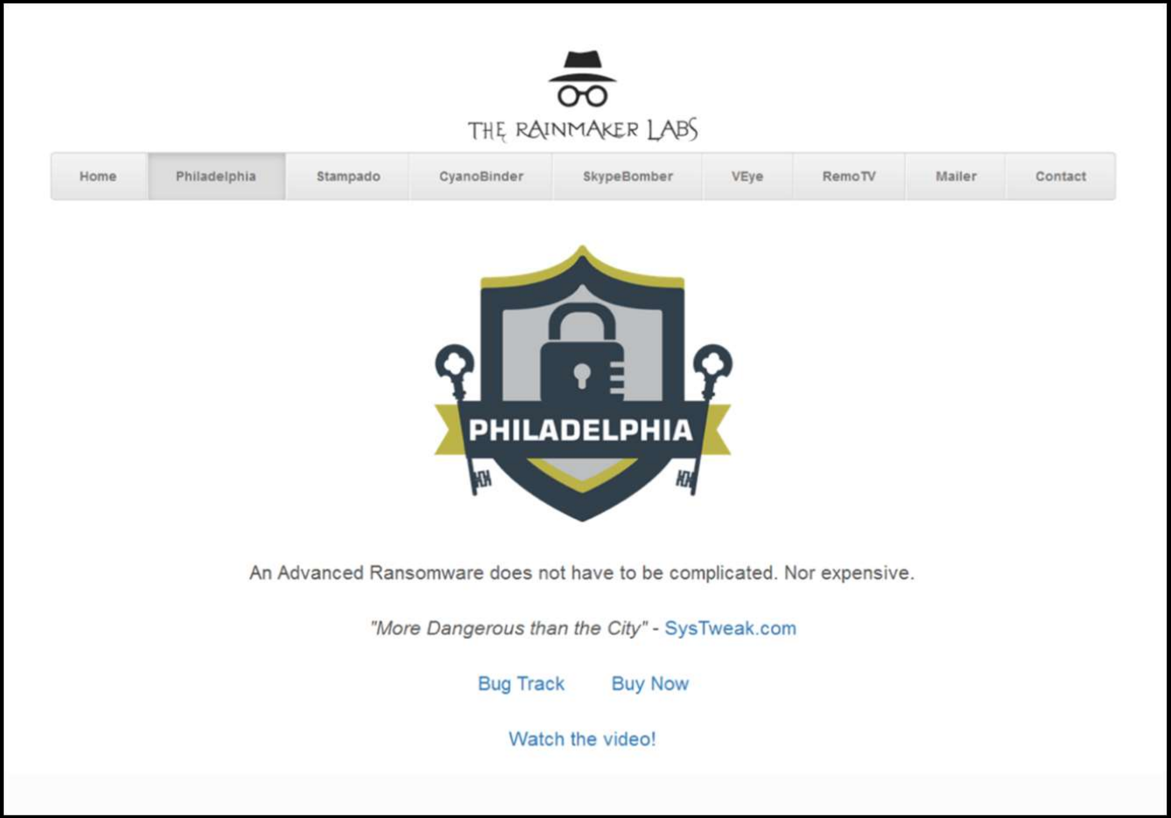
We've also made Several tools that will help you during the Infection process, whether packing or sending the malwares to your targets.

Other Stuff

Want to take control of someone else's computer? Or Bomb-Call a Telephone Number and make it Unavailable for others? We can help you out!

https://nakedsecurity.sophos.com/2017/07/25/ransomware-as-a-service-how-the-bad-guys-marketed-philadelphia/

It does not have to be complex!



An Advanced Ransomware does not have to be complicated. Nor expensive.

"More Dangerous than the City" - SysTweak.com

Bug Track Buy Now

Watch the video!

Capability to track campaigns

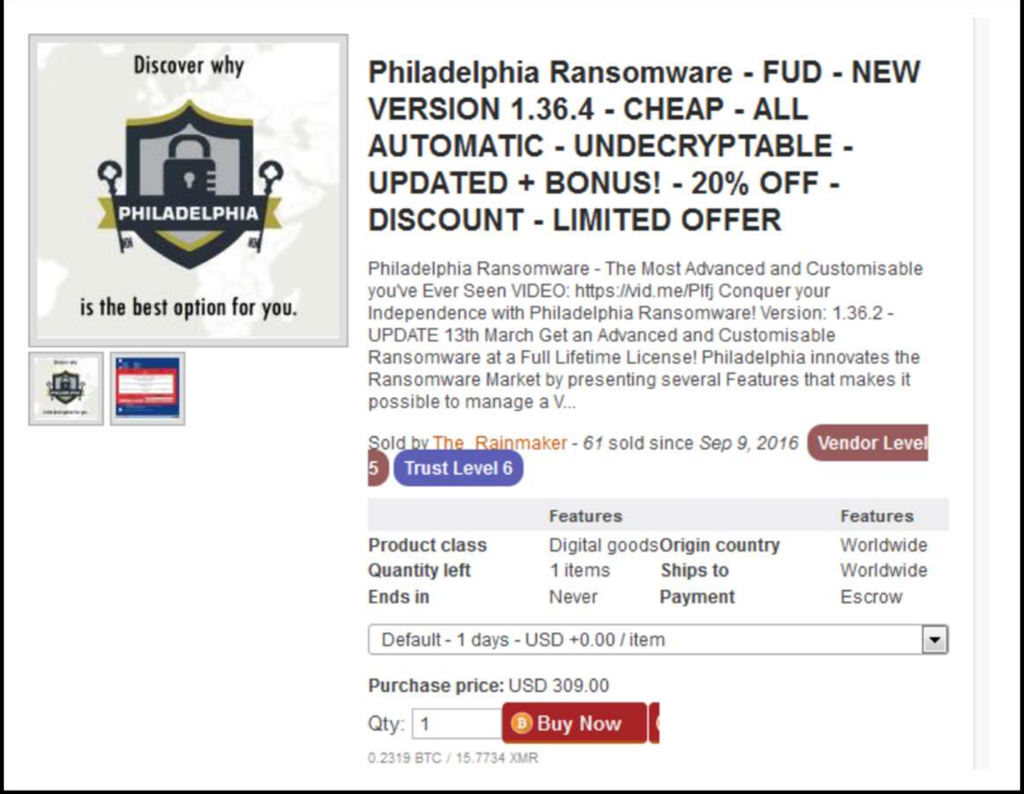
Check the transactions

Query all info about a victim

Victims can be plotted on Google maps

https://nakedsecurity.sophos.com/2017/07/25/ransomware-as-a-service-how-the-bad-guys-marketed-philadelphia/

Special offer on AlphaBay



Philadelphia Ransomware - FUD - NEW VERSION 1.36.4 - CHEAP - ALL AUTOMATIC - UNDECRYPTABLE - UPDATED + BONUS! - 20% OFF - DISCOUNT - LIMITED OFFER

Philadelphia Ransomware - The Most Advanced and Customisable you've Ever Seen VIDEO: https://vid.me/Plfj Conquer your Independence with Philadelphia Ransomware! Version: 1.36.2 - UPDATE 13th March Get an Advanced and Customisable Ransomware at a Full Lifetime License! Philadelphia innovates the Ransomware Market by presenting several Features that makes it possible to manage a V...

Sold by The_Rainmaker - *61* sold since *Sep 9, 2016* **Vendor Level 5** **Trust Level 6**

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	1 items	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Default - 1 days - USD +0.00 / item

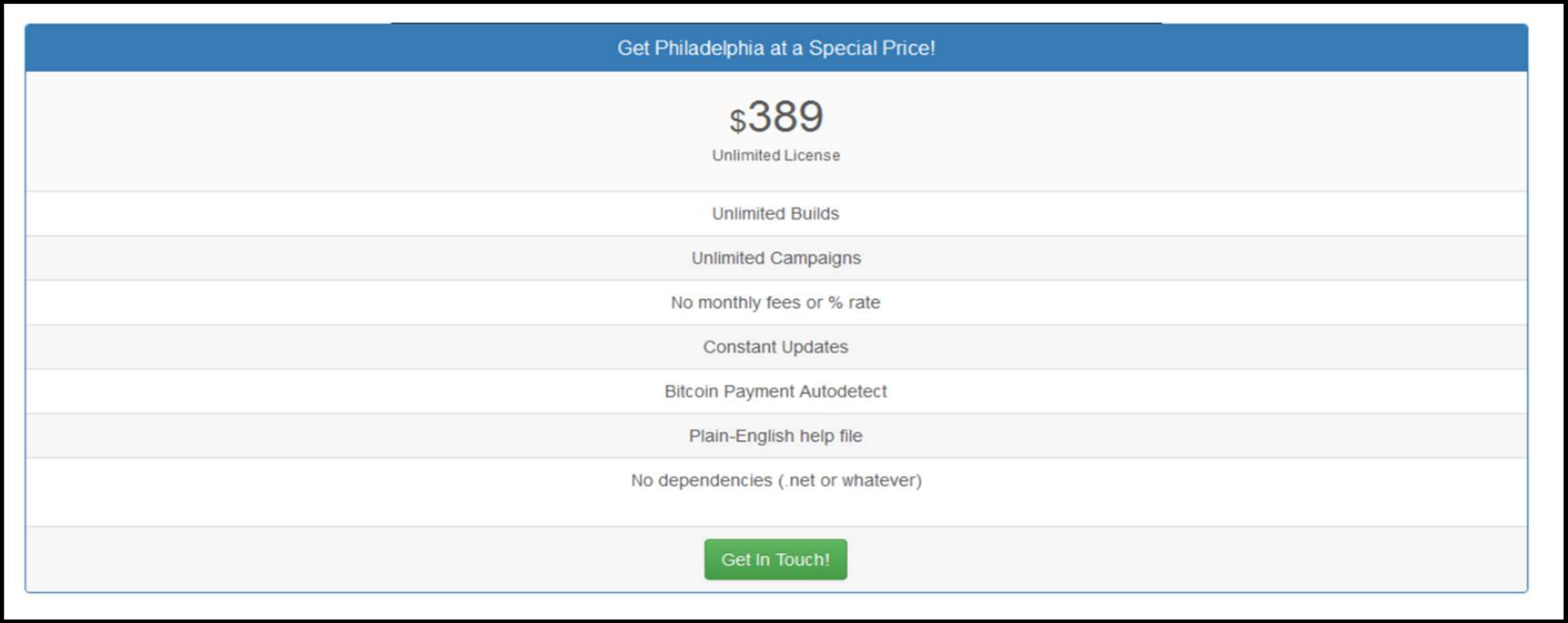
Purchase price: USD 309.00

Qty: 1 **Buy Now**

0.2319 BTC / 15.7734 XMR

https://nakedsecurity.sophos.com/2017/07/25/ransomware-as-a-service-how-the-bad-guys-marketed-philadelphia/

What you get for your money!



Get Philadelphia at a Special Price!

$389

Unlimited License

Unlimited Builds

Unlimited Campaigns

No monthly fees or % rate

Constant Updates

Bitcoin Payment Autodetect

Plain-English help file

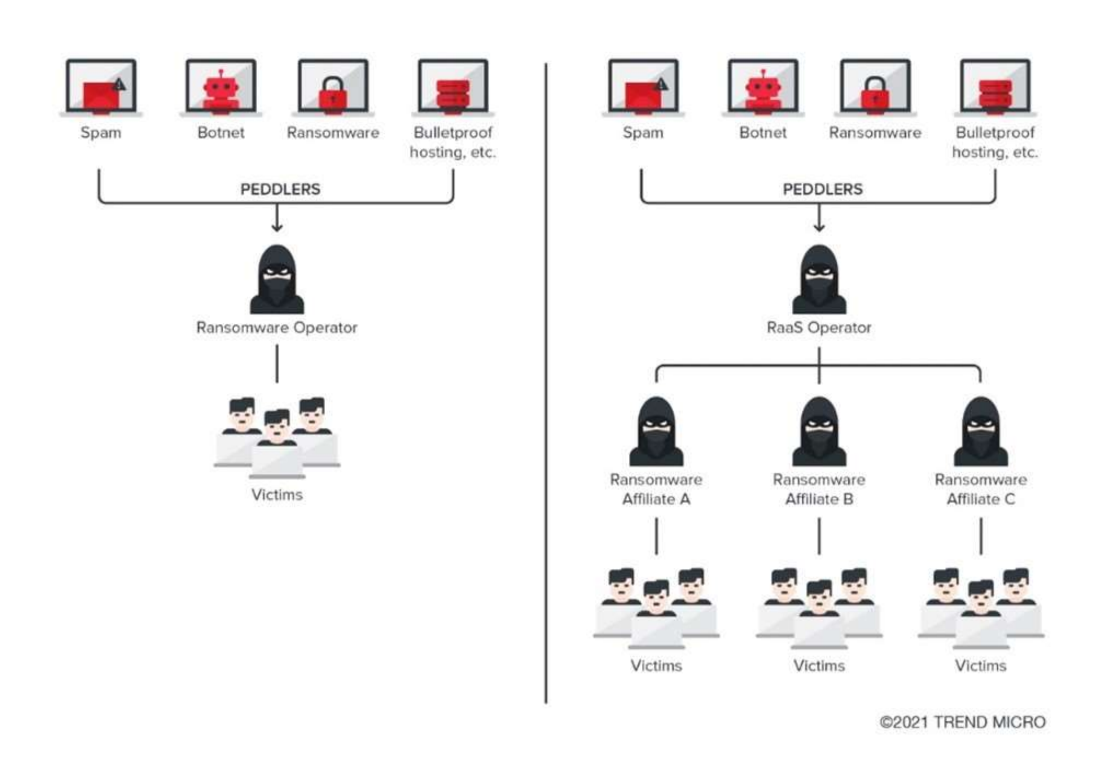
No dependencies (.net or whatever)

The price of RaaS kits ranges from **$40 per month to several thousand dollars**

The average ransom demand in 2021 was $6 million

https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/#:~:text=The%20price%20of%20RaaS%20kits,in%20order%20to%20become%20rich

Ransomware Business Model

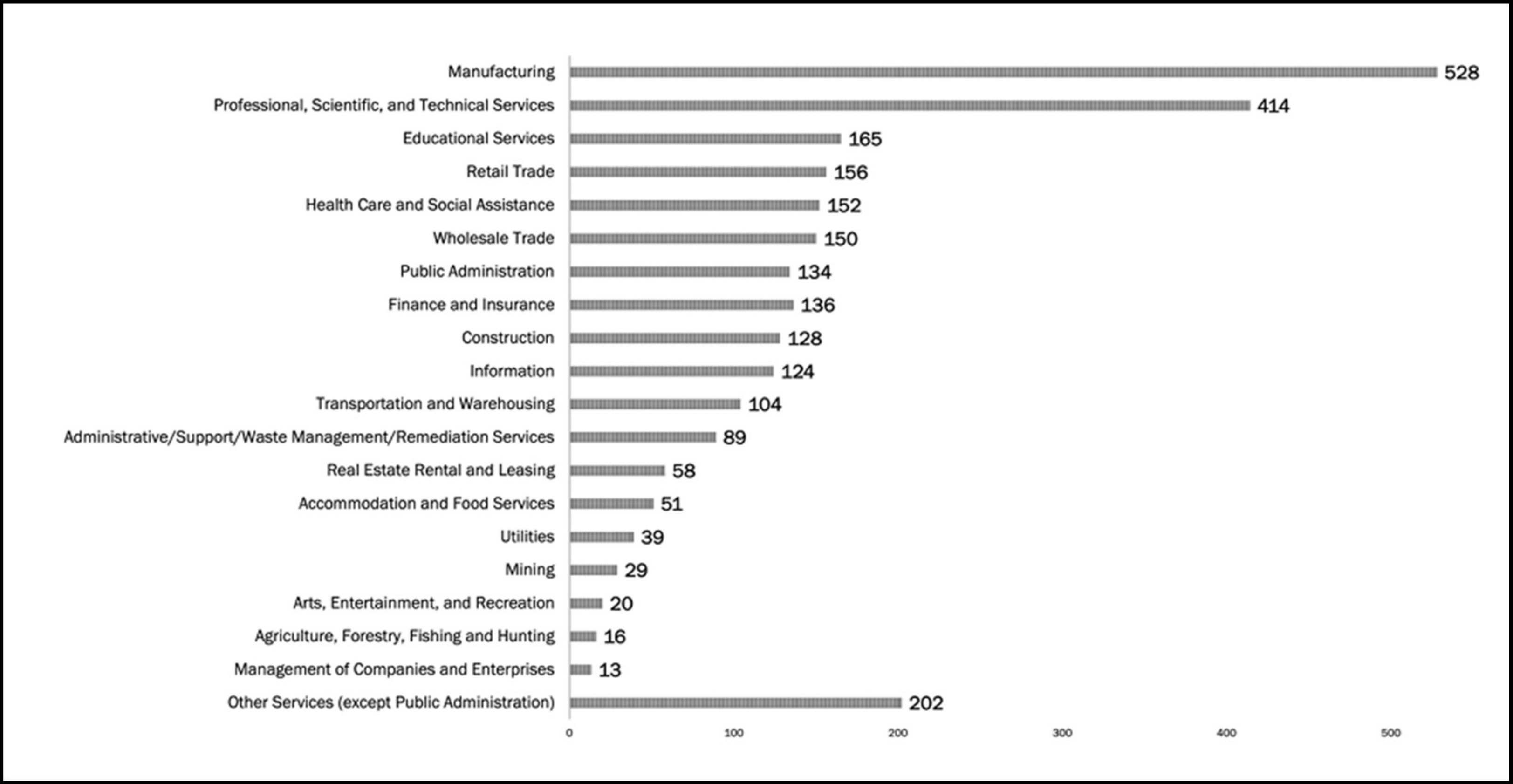


The state of Ransomware

- Top targeted industries were Manufacturing (19.5%), Professional, Scientific, and Technical Services (15.3%), and Educational Services (6.1%).
- The United States was the top targeted country, accounting for 43% of victim organizations, followed by the UK (5.7%) and Germany (4.4%).
- Ransomware groups tended to target companies with annual revenues of around $50M to $60M, with third-party vendors often being targeted for client information extortion.
- Encryption-less ransomware is on the rise, underscoring the importance of data protection and regulatory compliance in addition to addressing business interruption risks posed by traditional encryption-based attacks.
- Common ransomware indicators among victims included poor email configuration, recent credential leaks, public remote access ports, out-of date systems, and IP addresses with botnet activity
- The ransomware landscape experienced a notable uptick in February and March of 2023

2023_Ransomware_Report_Black_Kite.pdf (blackkite.com)

Ranmsomware attacks 2023 by vertical sector



2023_Ransomware_Report_Black_Kite.pdf (blackkite.com)

Who is Who

Ransomware groups often frame their activities in ways that might appear to justify their illegal actions, using arguments that position them as "ethical hackers" or claiming that they provide a form of unsolicited "public service" through their attacks.

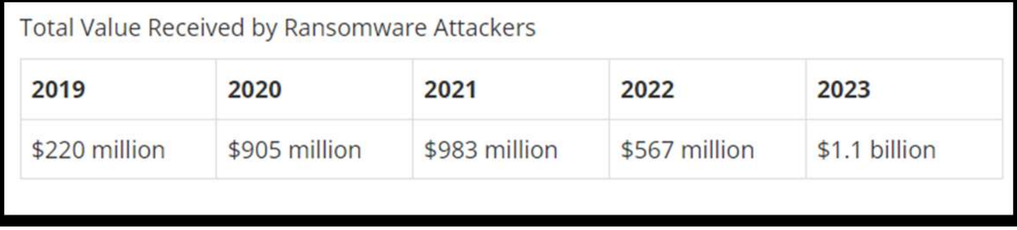
1. DarkSide Ransomware Group Claim of Ethical Guidelines: DarkSide, the group behind the disruptive Colonial Pipeline attack in 2021, has claimed to operate under a code of conduct that avoids attacks on hospitals, schools, non-profits, and government targets. They have positioned themselves as "ethical hackers," stating that their goal is not to create problems for society but rather to make money. They even issued an apology for the social consequences of the Colonial Pipeline attack.

2. REvil, a notorious ransomware group, has argued that their targets are carefully chosen based on their ability to pay the ransom, suggesting they avoid entities that would be unduly burdened by their attacks. They've positioned their actions as a business rather than mere criminal activity, implying some form of twisted corporate social responsibility.

3. NetWalkerCOVID-19 Exploitation:During the COVID-19 pandemic, NetWalker specifically targeted healthcare providers and educational institutions, justifying their actions by suggesting that these institutions have funds to pay ransoms due to increased government funding during the pandemic. They rationalized that their attacks were a form of pressure to make these organizations take their cybersecurity seriously.

4. Maze Ransomware Group Data Leak Websites: Maze was one of the first ransomware groups to use double extortion tactics, threatening to leak stolen data if their demands were not met. They justified their leaks as a demonstration of the vulnerabilities in their victims’ cybersecurity practices, suggesting that they were providing a "service" by exposing these weaknesses.

5. Phobos Claims of Security Auditing: Phobos ransomware operators have at times claimed that they are helping businesses identify security flaws. They argue that their ransom demands are akin to a fee for security auditing services, although this is merely a facade to mask their criminal intentions.



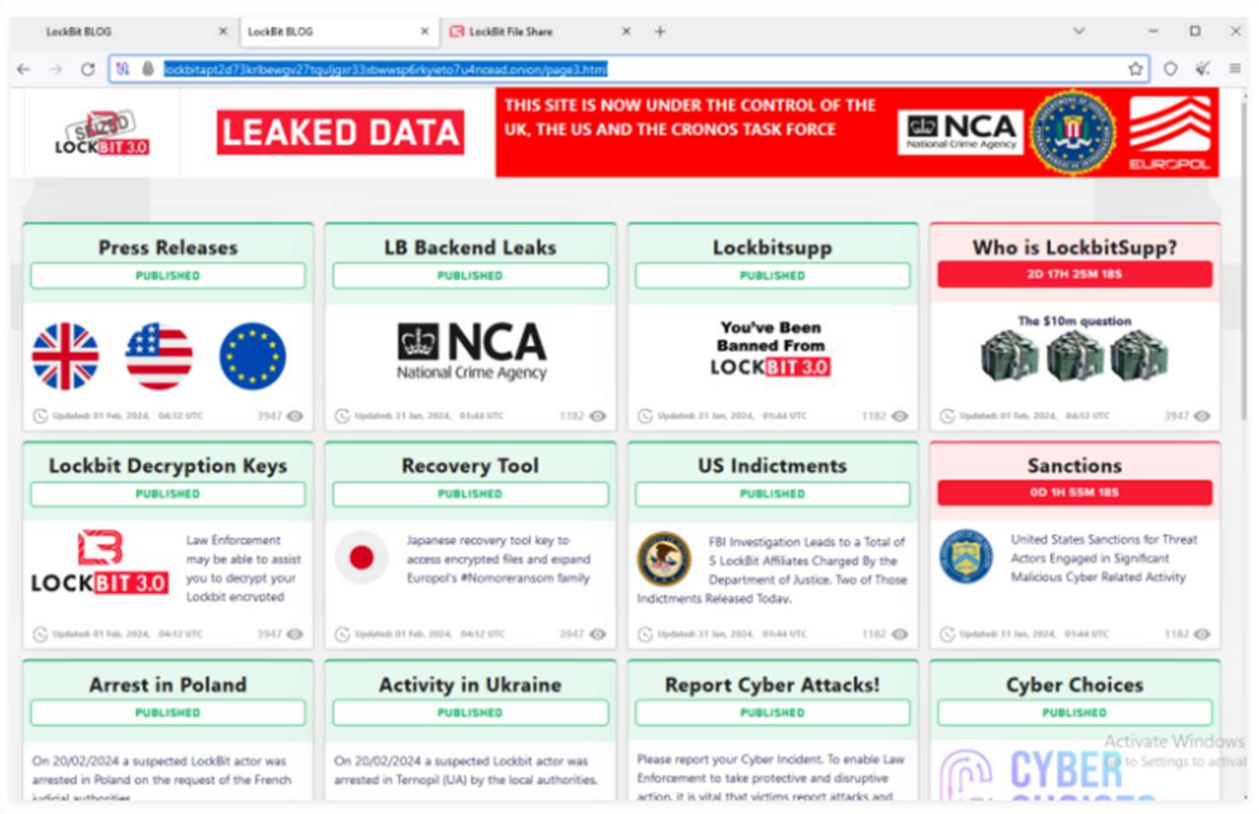
Total Value Received by Ransomware Attackers

2019	2020	2021	2022	2023
$220 million	$905 million	$983 million	$567 million	$1.1 billion

Lockbit

U.S. and U.K. authorities have seized the darknet websites run by LockBit, a prolific and destructive ransomware group that has claimed more than 2,000 victims worldwide and extorted over $120 million in payments.

Instead of listing data stolen from ransomware victims who didn't pay, LockBit's victim shaming website now offers free recovery tools, as well as news about arrests and criminal charges involving LockBit affiliates


LockBit BLOG
LockBit BLOG
LockBit File Share
lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion/page3.html
SEIZED
LOCKBIT 3.0
LEAKED DATA
NCA National Crime Agency
EUROPOL
NCA National Crime Agency
You've Been Banned From LOCKBIT 3.0
The $10m question
LOCKBIT 3.0
CYBER
Activate Windows
Go to Settings to activat

THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

Press Releases — PUBLISHED — Updated: 01 Feb, 2024, 04:12 UTC — 3947

LB Backend Leaks — PUBLISHED — Updated: 31 Jan, 2024, 01:44 UTC — 1182

Lockbitsupp — PUBLISHED — Updated: 31 Jan, 2024, 01:44 UTC — 1182

Who is LockbitSupp? — 2D 17H 25M 18S — Updated: 01 Feb, 2024, 04:12 UTC — 3947

Lockbit Decryption Keys — PUBLISHED — Law Enforcement may be able to assist you to decrypt your Lockbit encrypted — Updated: 01 Feb, 2024, 04:12 UTC — 3947

Recovery Tool — PUBLISHED — Japanese recovery tool key to access encrypted files and expand Europol's #Nomoreransom family — Updated: 01 Feb, 2024, 04:12 UTC — 3947

US Indictments — PUBLISHED — FBI Investigation Leads to a Total of 5 LockBit Affiliates Charged By the Department of Justice. Two of Those Indictments Released Today. — Updated: 31 Jan, 2024, 01:44 UTC — 1182

Sanctions — 0D 1H 55M 18S — United States Sanctions for Threat Actors Engaged in Significant Malicious Cyber Related Activity — Updated: 31 Jan, 2024, 01:44 UTC — 1182

Arrest in Poland — PUBLISHED — On 20/02/2024 a suspected LockBit actor was arrested in Poland on the request of the French judicial authorities

Activity in Ukraine — PUBLISHED — On 20/02/2024 a suspected Lockbit actor was arrested in Ternopil (UA) by the local authorities.

Report Cyber Attacks! — PUBLISHED — Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive action, it is vital that victims report attacks and

Cyber Choices — PUBLISHED

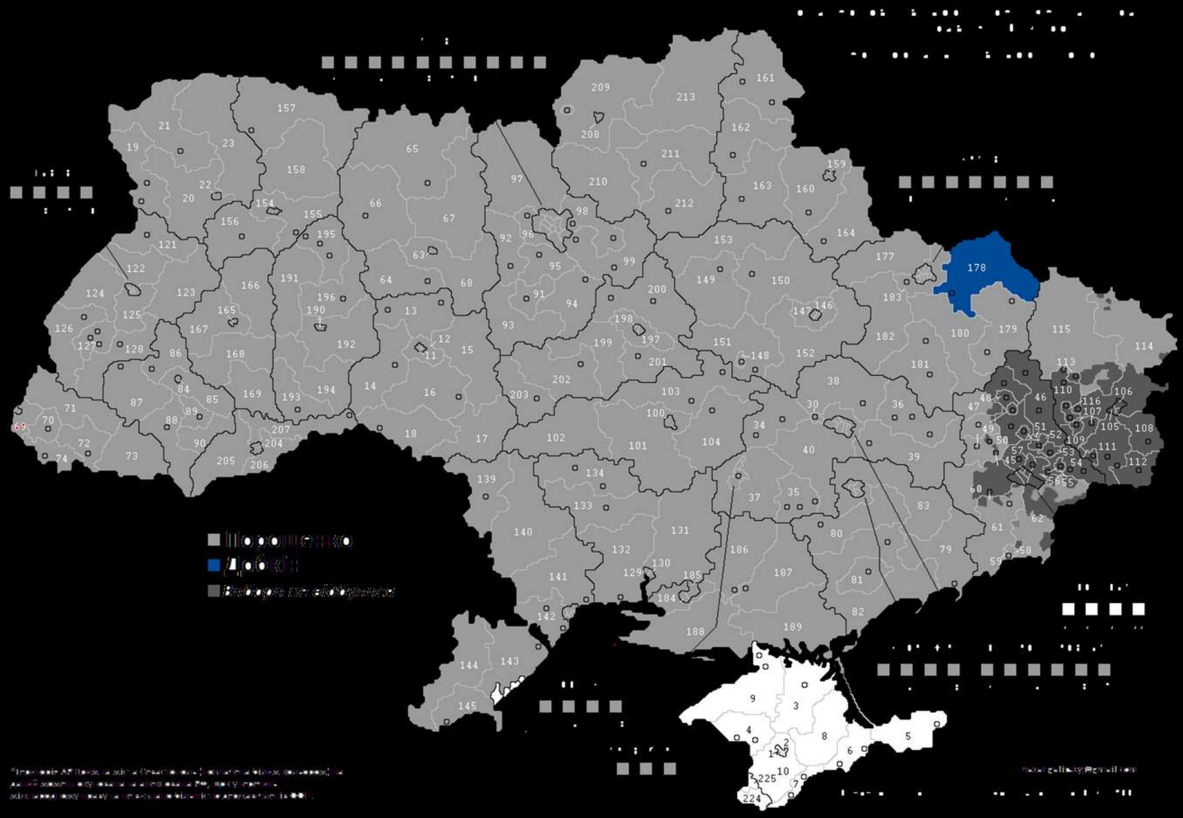
Source https://krebsonsecurity.com/2024/02/feds-seize-lockbit-ransomware-websites-offer-decryption-tools-troll-affiliates/

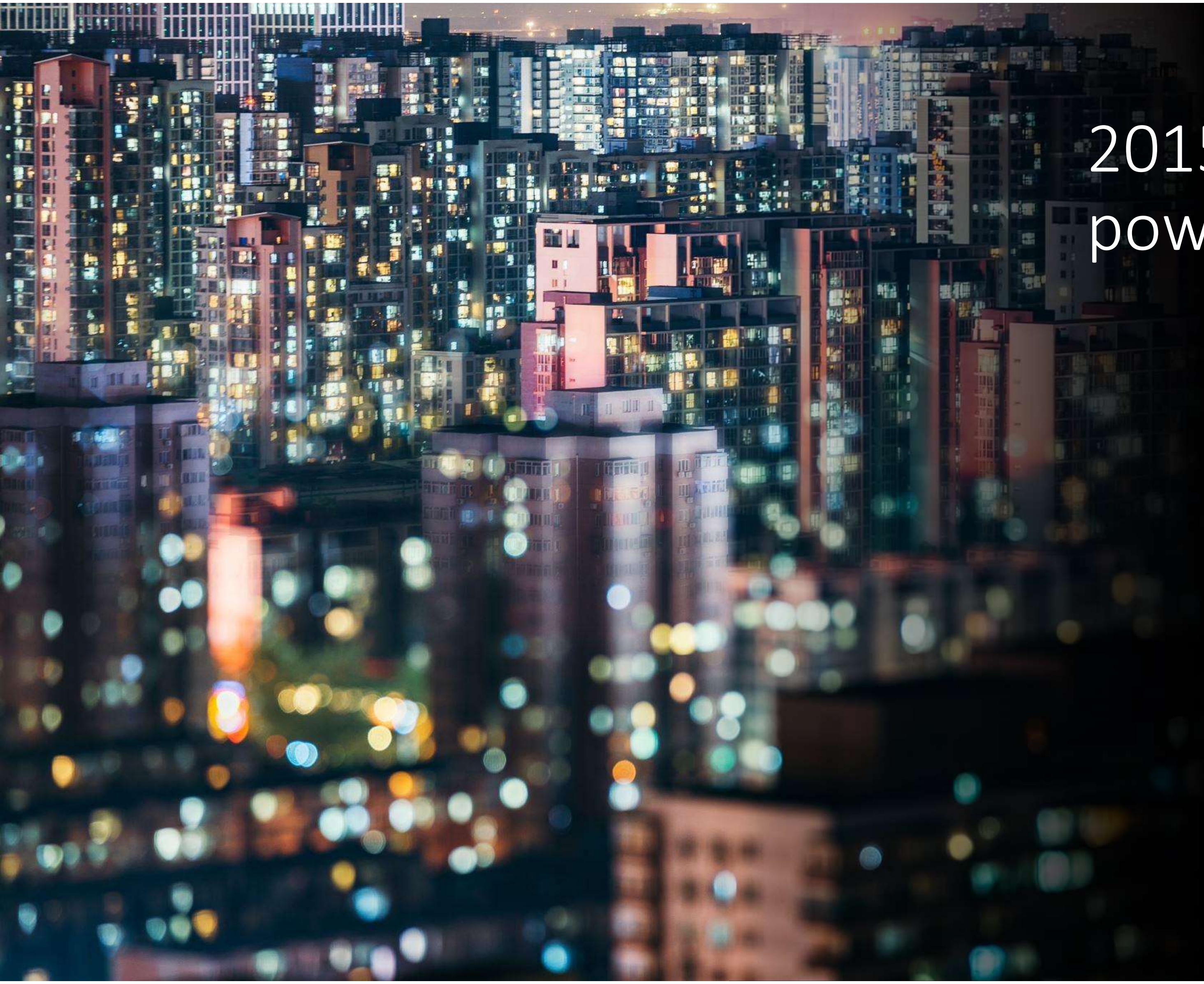
Companies are 2.5X times more likely to pay the Ransomware in cases where data has been exfiltrated in addition to being encrypted

3 trends set to drive cyberattacks and ransomware in 2024 | World Economic Forum (weforum.org)

Studying cyber attacks in the Ukraine

- 2014 Ukrainian Central election commission hacked





2015 Ukraine power grid attack

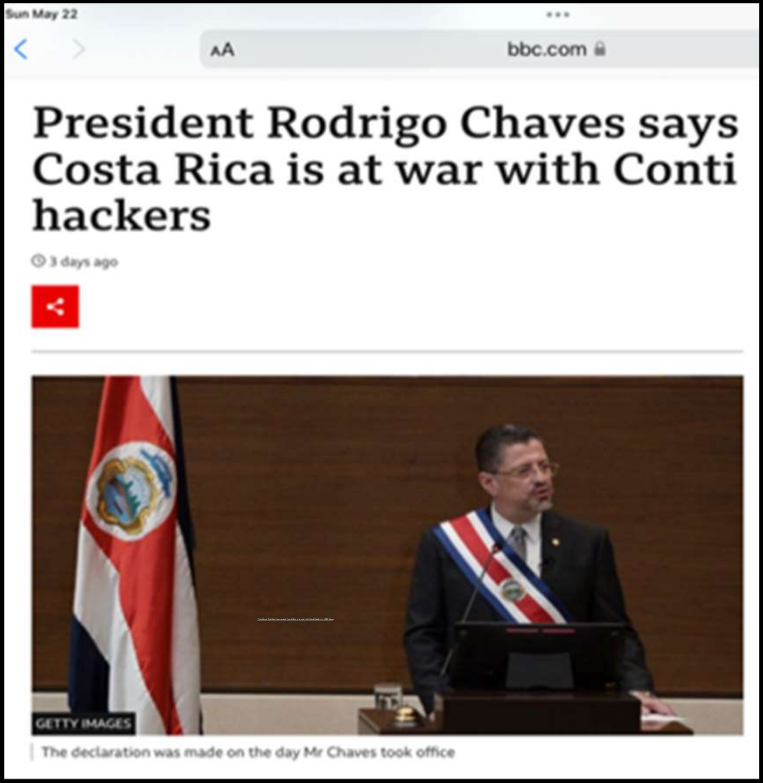
2017 Wannacry

2017 NotPetya

The intersection of crime and war

Criminals declare war on small nations

2022 Conti ransomware gang allegedly disrupted Costa Rica’s systems for collecting taxes, paying pensions, overseeing exports and paying government employees

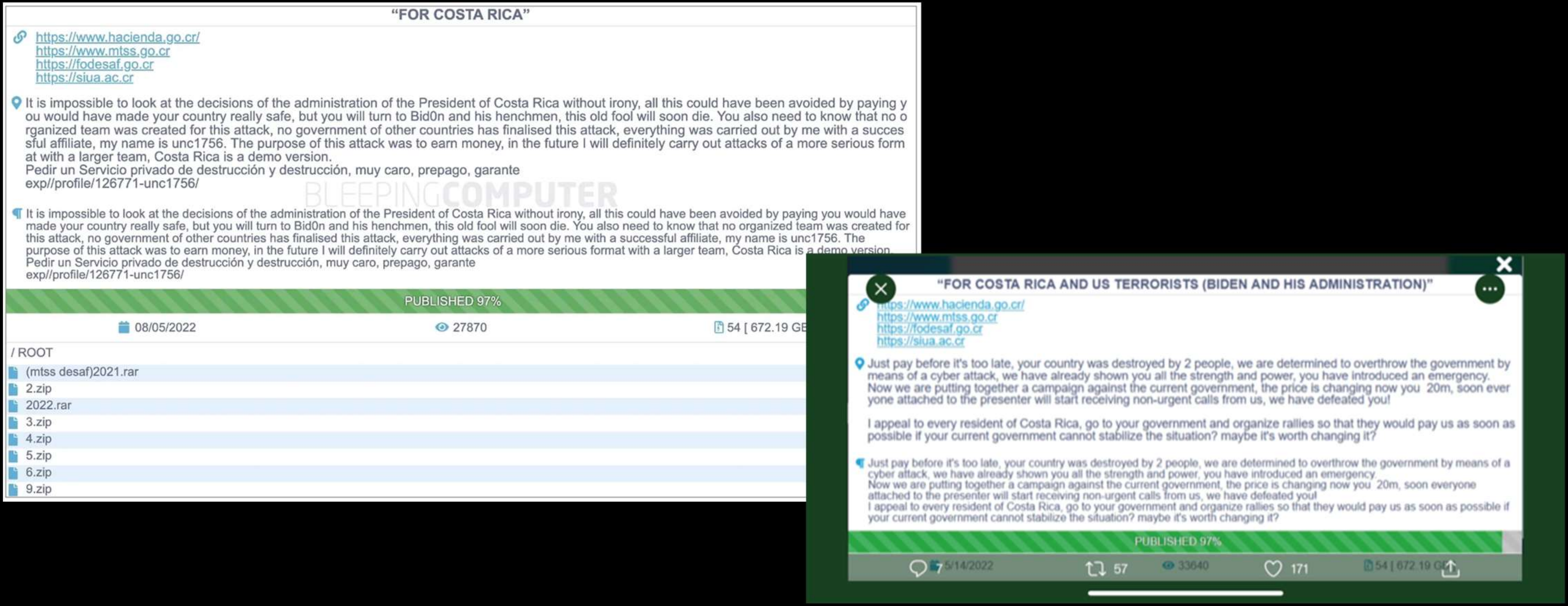


President Rodrigo Chaves says Costa Rica is at war with Conti hackers

3 days ago

The declaration was made on the day Mr Chaves took office

Costa Rica declares a National Emergency



“FOR COSTA RICA”

https://www.hacienda.go.cr/
https://www.mtss.go.cr
https://fodesaf.go.cr
https://siua.ac.cr

It is impossible to look at the decisions of the administration of the President of Costa Rica without irony, all this could have been avoided by paying you would have made your country really safe, but you will turn to Bid0n and his henchmen, this old fool will soon die. You also need to know that no organized team was created for this attack, no government of other countries has finalised this attack, everything was carried out by me with a successful affiliate, my name is unc1756. The purpose of this attack was to earn money, in the future I will definitely carry out attacks of a more serious format with a larger team, Costa Rica is a demo version.
Pedir un Servicio privado de destrucción y destrucción, muy caro, prepago, garante
exp//profile/126771-unc1756/

It is impossible to look at the decisions of the administration of the President of Costa Rica without irony, all this could have been avoided by paying you would have made your country really safe, but you will turn to Bid0n and his henchmen, this old fool will soon die. You also need to know that no organized team was created for this attack, no government of other countries has finalised this attack, everything was carried out by me with a successful affiliate, my name is unc1756. The purpose of this attack was to earn money, in the future I will definitely carry out attacks of a more serious format with a larger team, Costa Rica is a demo version.
Pedir un Servicio privado de destrucción y destrucción, muy caro, prepago, garante
exp//profile/126771-unc1756/

PUBLISHED 97%

08/05/2022 | 27870 | 54 [672.19 GE

/ ROOT

- (mtss desaf)2021.rar
- 2.zip
- 2022.rar
- 3.zip
- 4.zip
- 5.zip
- 6.zip
- 9.zip

“FOR COSTA RICA AND US TERRORISTS (BIDEN AND HIS ADMINISTRATION)”

ttps://www.hacienda.go.cr/
https://www.mtss.go.cr
https://fodesaf.go.cr
https://siua.ac.cr

Just pay before it's too late, your country was destroyed by 2 people, we are determined to overthrow the government by means of a cyber attack, we have already shown you all the strength and power, you have introduced an emergency.
Now we are putting together a campaign against the current government, the price is changing now you 20m, soon everyone attached to the presenter will start receiving non-urgent calls from us, we have defeated you!

I appeal to every resident of Costa Rica, go to your government and organize rallies so that they would pay us as soon as possible if your current government cannot stabilize the situation? maybe it's worth changing it?

Just pay before it's too late, your country was destroyed by 2 people, we are determined to overthrow the government by means of a cyber attack, we have already shown you all the strength and power, you have introduced an emergency.
Now we are putting together a campaign against the current government, the price is changing now you 20m, soon everyone attached to the presenter will start receiving non-urgent calls from us, we have defeated you!
I appeal to every resident of Costa Rica, go to your government and organize rallies so that they would pay us as soon as possible if your current government cannot stabilize the situation? maybe it's worth changing it?

PUBLISHED 97%

The Resilience Strategy

Integrate security from the design stage
MFA, IAM (RBAC), PAM, secrets management
Threat hunting
Continuous monitoring
Micro-segmentation
Endpoint detection, remediation systems
Test your defenses
Audit Administrators

Psychological warfare

disappearance that sparked all this took place Jan. 11, when a 13-year-old girl from a Russian immigrant family in Berlin went missing from her family on the way to school.

The girl – identified only as “Lisa F” in media reports – finally returned 30 hours later. She later told police she had been kidnapped and raped by a group of men who appeared to be Middle Eastern migrants.

Advance Persistent Manipulator (APM)

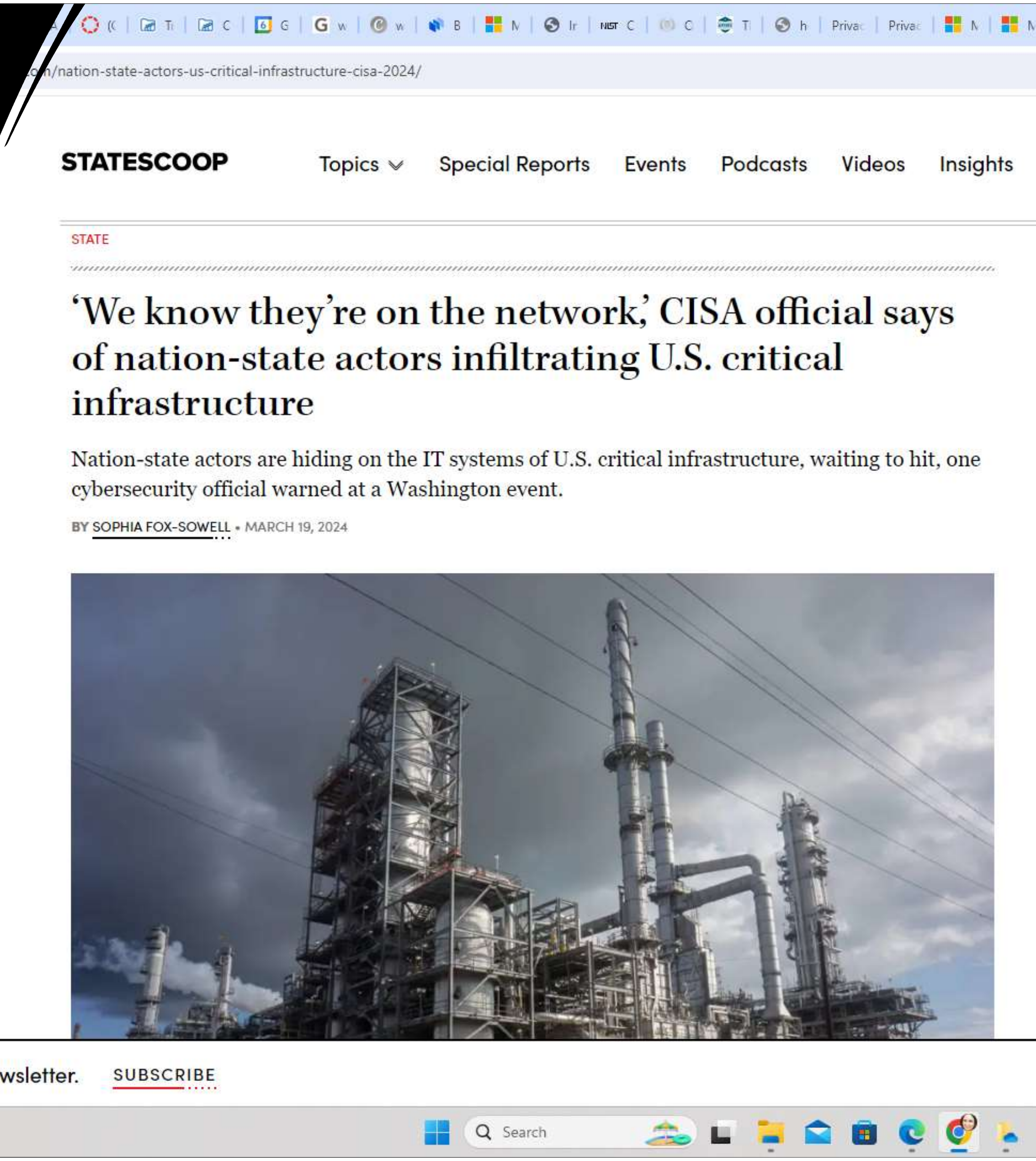
Positioning false narratives in ways that are similar to the pre-positioning of malware and other software code.

Launching broad-based and simultaneous “reporting” of these narratives from government-managed and influenced websites and amplifying their narratives through technology tools designed to exploit social media services.

Recent examples include narratives around biolabs in Ukraine and multiple efforts to obfuscate military attacks against Ukrainian civilian targets.

What Next?

They have the access that they need, and if the order was given, they could disrupt some services in this country right now

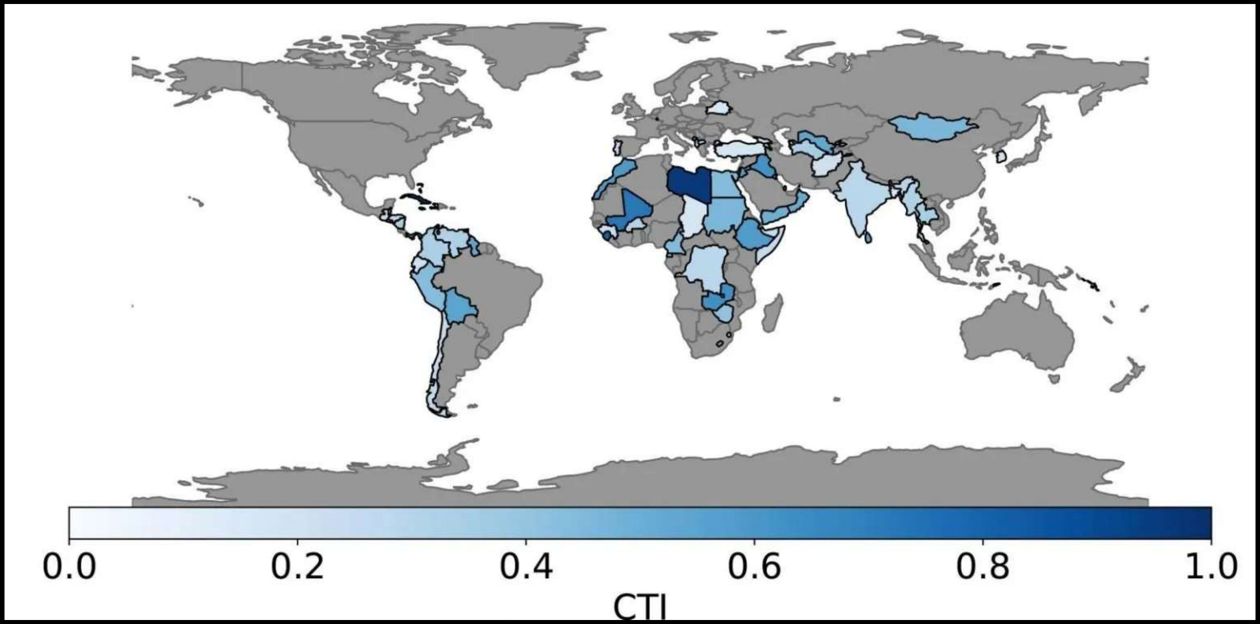


‘We know they’re on the network,’ CISA official says of nation-state actors infiltrating U.S. critical infrastructure

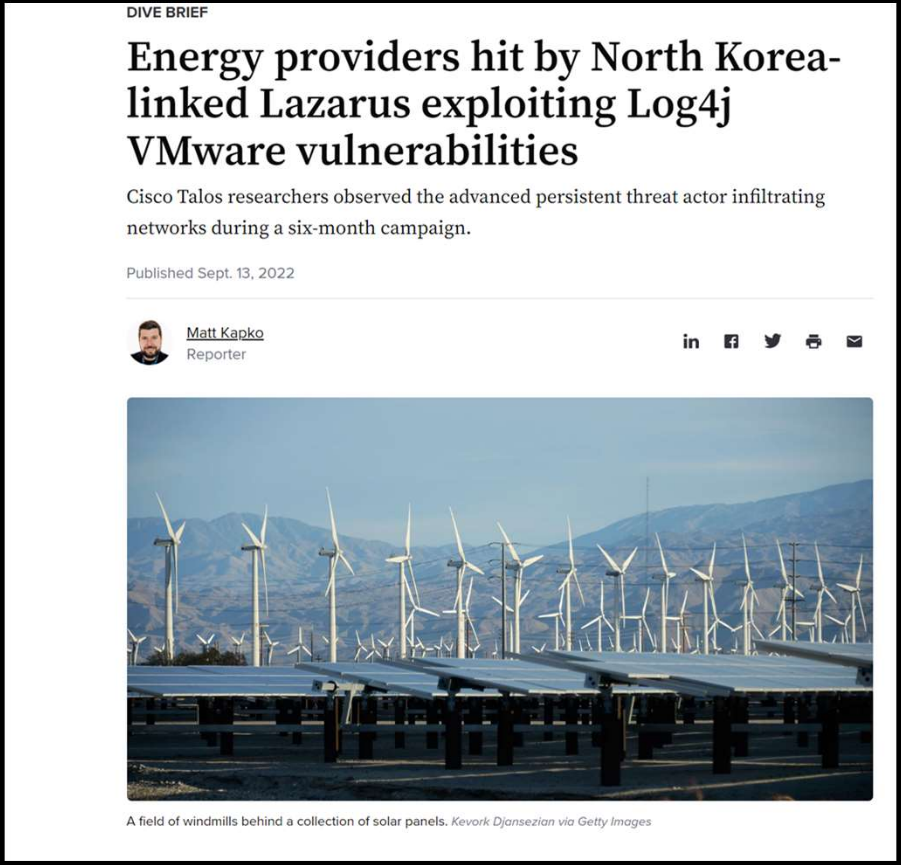
Nation-state actors are hiding on the IT systems of U.S. critical infrastructure, waiting to hit, one cybersecurity official warned at a Washington event.

BY SOPHIA FOX-SOWELL • MARCH 19, 2024

25% of the World's Internet Users Rely on Infrastructure That Is Susceptible to Attacks



Sustainability



DIVE BRIEF

Energy providers hit by North Korea-linked Lazarus exploiting Log4j VMware vulnerabilities

Cisco Talos researchers observed the advanced persistent threat actor infiltrating networks during a six-month campaign.

Published Sept. 13, 2022

Matt Kapko
Reporter

A field of windmills behind a collection of solar panels. *Kevork Djansezian via Getty Images*

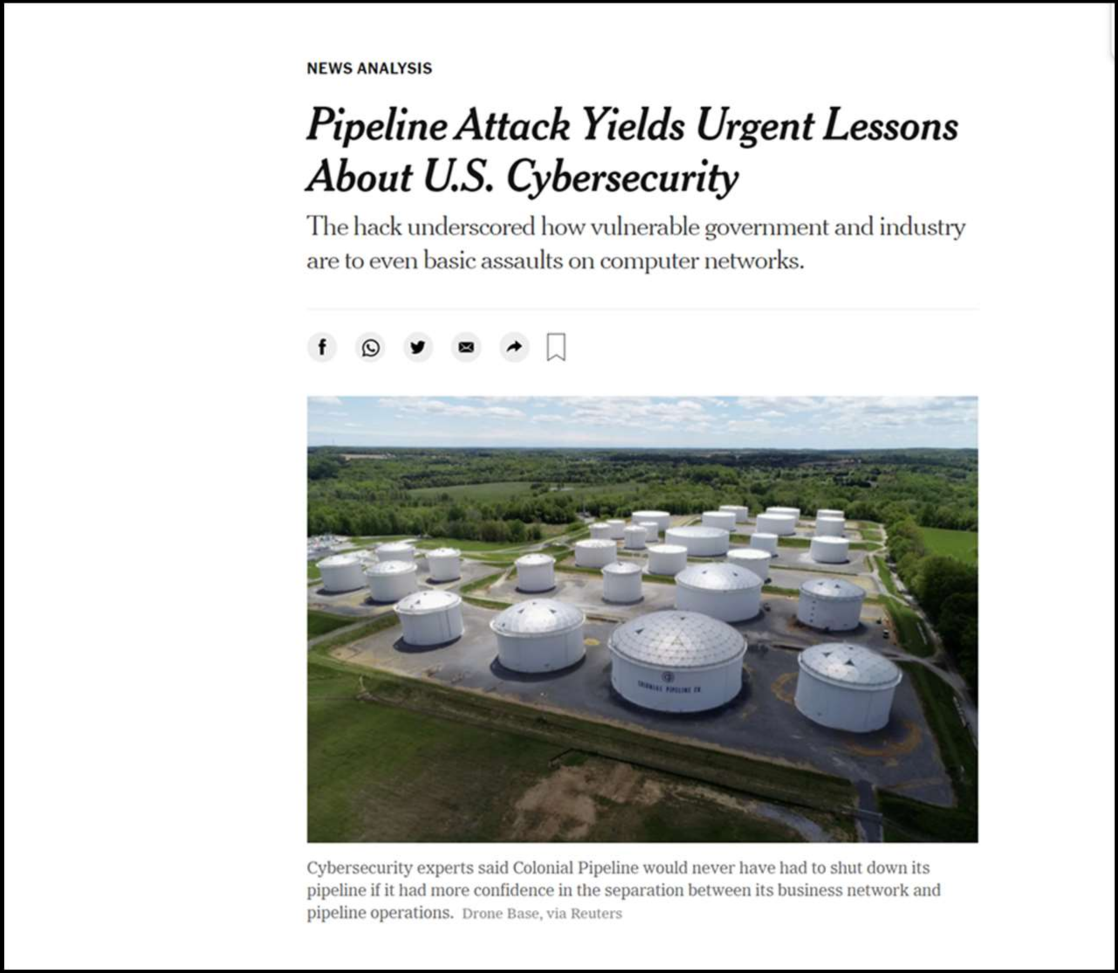
Infrastructure needed to enable our sustainable future requires far greater levels of cybersecurity than previously managed. Introducing new technology to power and manage the grid has prompted new cybersecurity challenges for energy companies, from utilities to electric vehicle operators.

As we continue to reduce our reliance on fossil fuels, we risk
becoming *more* vulnerable if we don't start associating climate resiliency with cyber resiliency.

Energy providers hit by North Korea-linked Lazarus exploiting Log4j VMware vulnerabilities | Cybersecurity Dive

Risk of Critical Infrastructure attacks

- The risk increases with one provider
- Multiple providers enable the capability to architect for resilience
- The pipeline is a textbook example of the risks



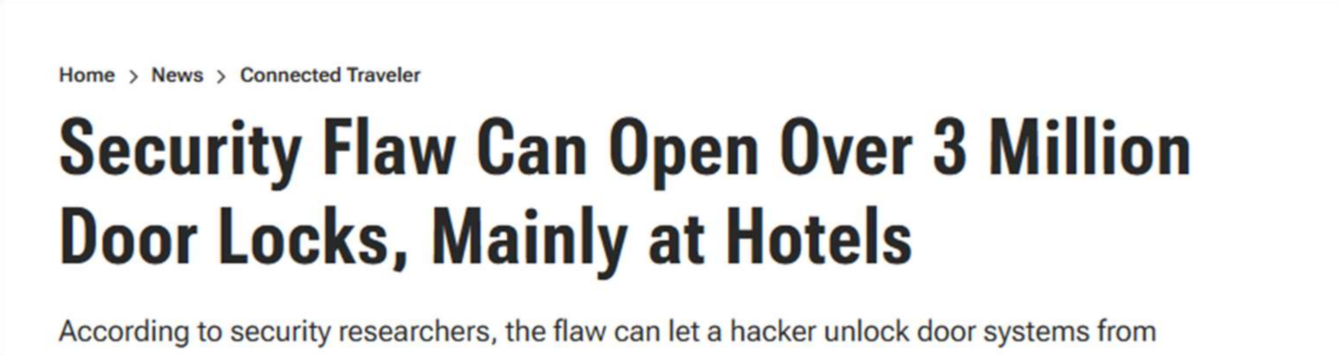
NEWS ANALYSIS

Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity

The hack underscored how vulnerable government and industry are to even basic assaults on computer networks.

Cybersecurity experts said Colonial Pipeline would never have had to shut down its pipeline if it had more confidence in the separation between its business network and pipeline operations. Drone Base, via Reuters

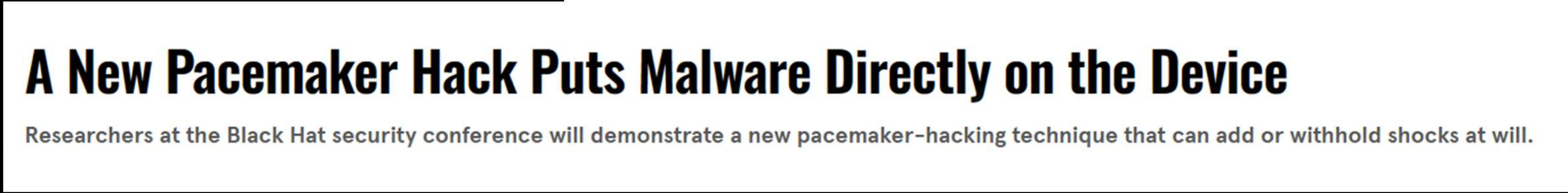
Smart Tech raises risk



Home > News > Connected Traveler

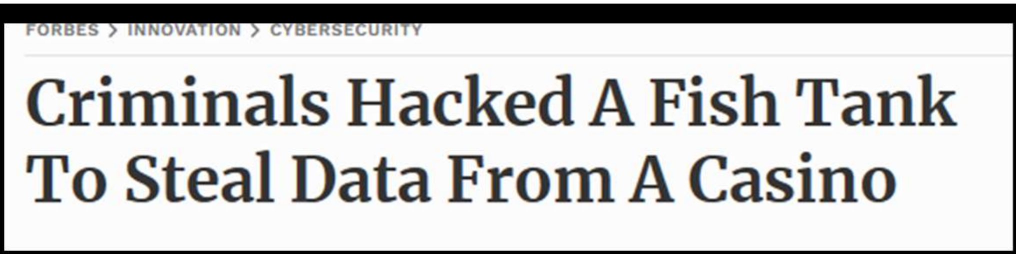
Security Flaw Can Open Over 3 Million Door Locks, Mainly at Hotels

According to security researchers, the flaw can let a hacker unlock door systems from



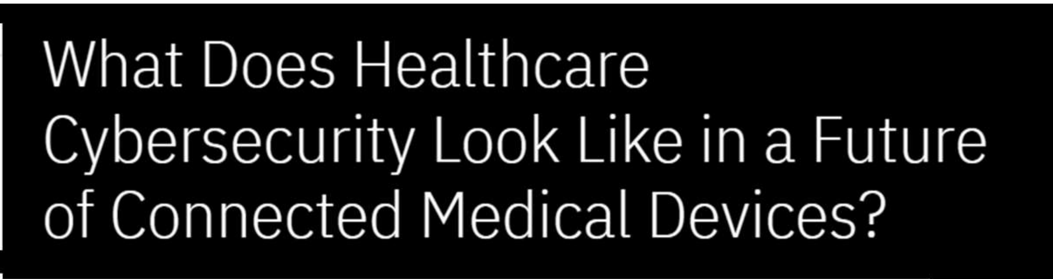
A New Pacemaker Hack Puts Malware Directly on the Device

Researchers at the Black Hat security conference will demonstrate a new pacemaker-hacking technique that can add or withhold shocks at will.

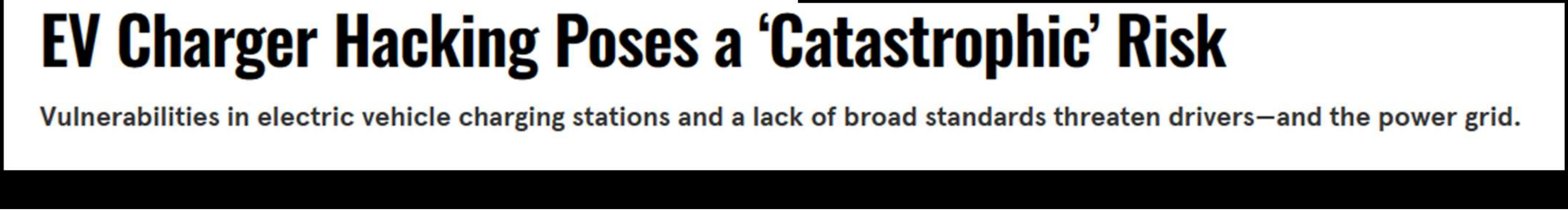


FORBES > INNOVATION > CYBERSECURITY

Criminals Hacked A Fish Tank To Steal Data From A Casino



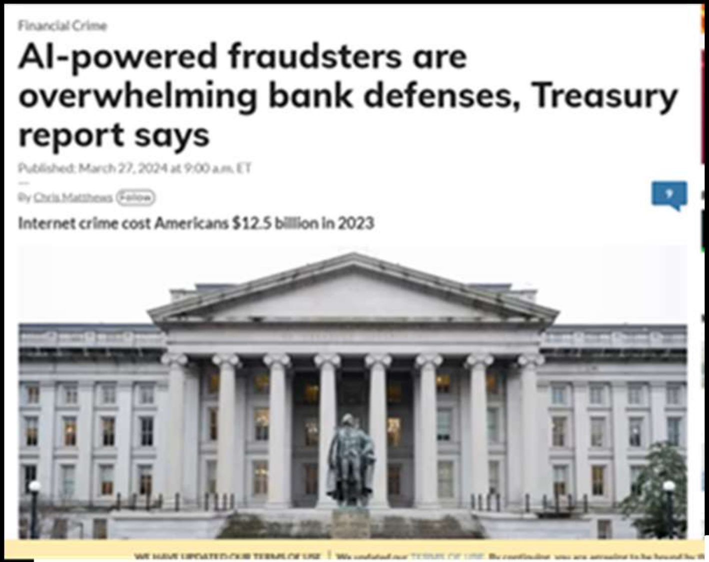
What Does Healthcare Cybersecurity Look Like in a Future of Connected Medical Devices?



EV Charger Hacking Poses a ‘Catastrophic’ Risk

Vulnerabilities in electric vehicle charging stations and a lack of broad standards threaten drivers—and the power grid.

Deep Fakes



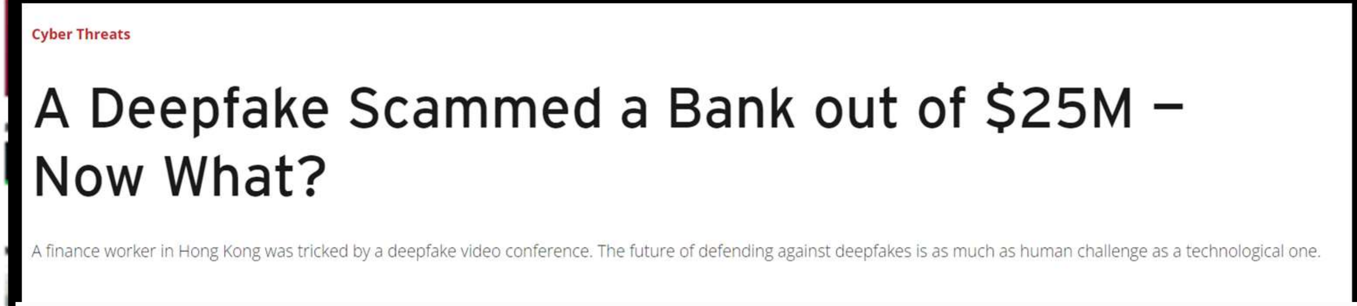
Financial Crime

AI-powered fraudsters are overwhelming bank defenses, Treasury report says

Published: March 27, 2024 at 9:00 a.m. ET

By Chris Matthews

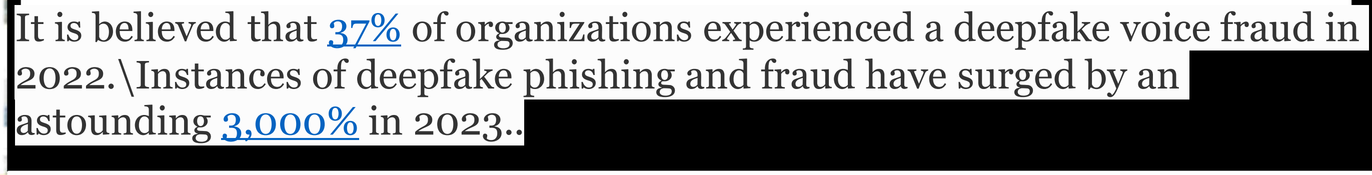
Internet crime cost Americans $12.5 billion in 2023



Cyber Threats

A Deepfake Scammed a Bank out of $25M – Now What?

A finance worker in Hong Kong was tricked by a deepfake video conference. The future of defending against deepfakes is as much as human challenge as a technological one.



It is believed that 37% of organizations experienced a deepfake voice fraud in 2022.\Instances of deepfake phishing and fraud have surged by an astounding 3,000% in 2023..

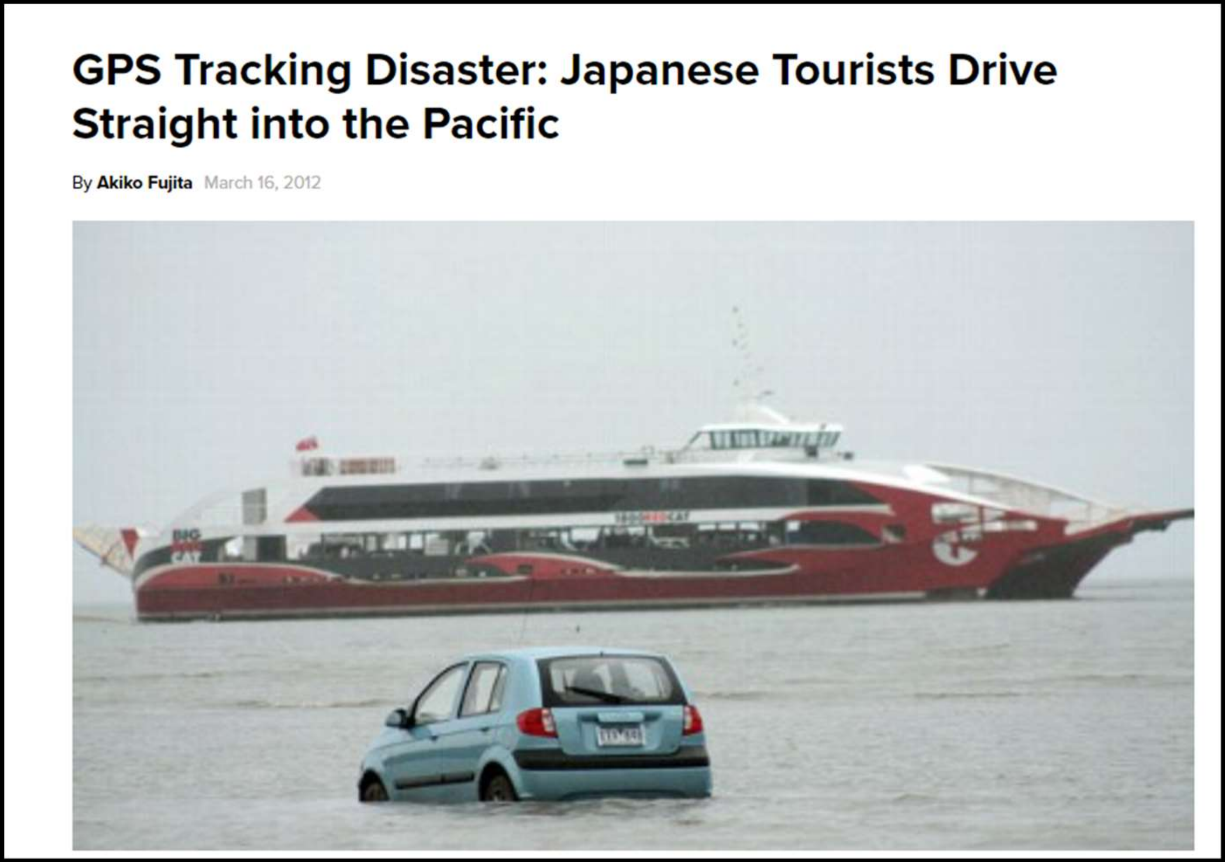
February 19, 2024

Fed finds CEO engaged in crypto “pig butchering” scam which led to bank failure

Difference between Gen AI

- "GenAI" typically refers to "Generative AI," which is a class of artificial intelligence focused on generating new content, whether that be text, images, music, code, or other forms of media. It is an application of AI where the system learns from a vast amount of data and uses it to **create new, original content** that mimics the input data in style, structure, or information
- Today, we have many security tools that use Narrow AI. Narrow AI is highly specialized and effective within its designated role. These AI capabilities are crucial for managing and mitigating the increasing complexity and volume of cybersecurity threats faced by organizations today. Heavily based on statistical methods

Are we ready for GenAI?



GPS Tracking Disaster: Japanese Tourists Drive Straight into the Pacific

By **Akiko Fujita** March 16, 2012

Resources

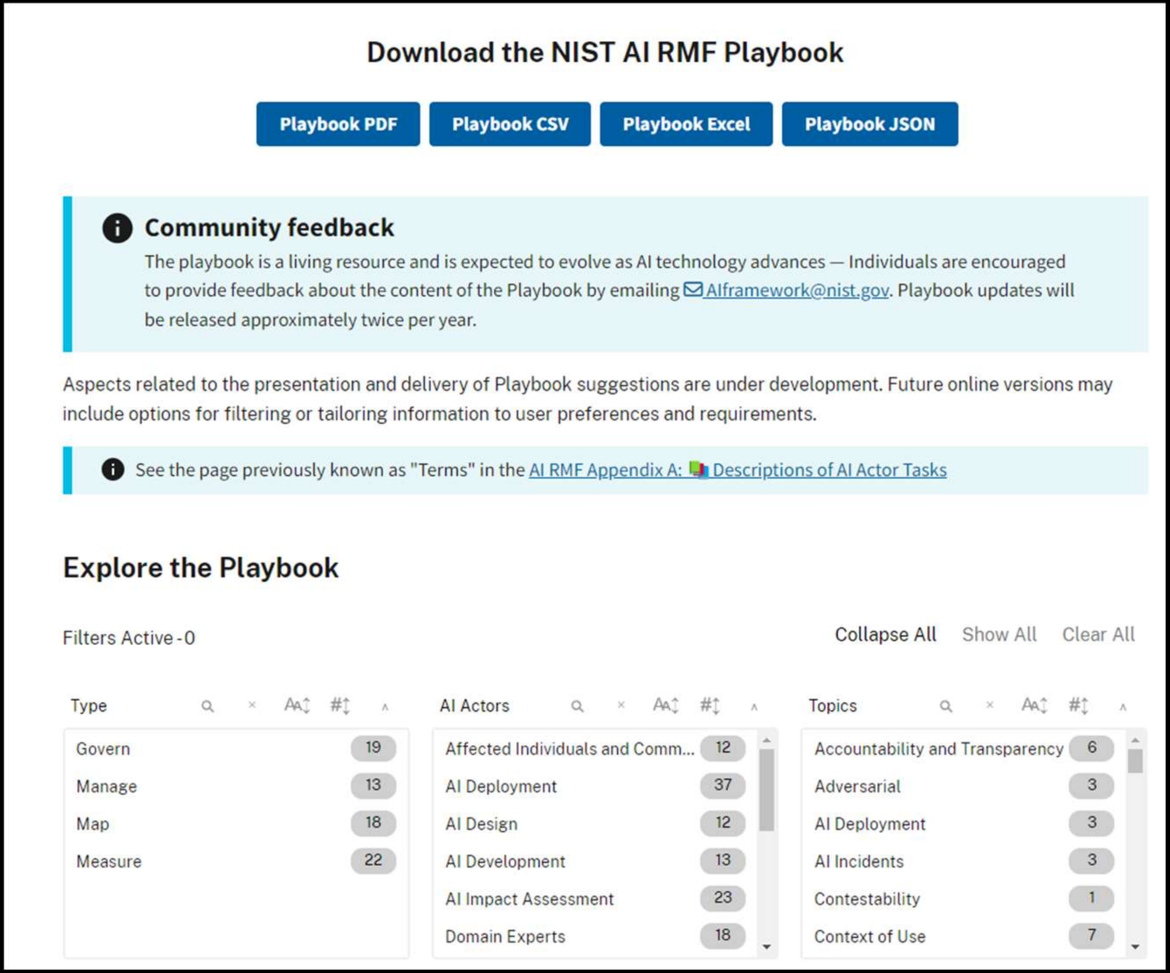
How do we assess the risk?

FS-ISAC White Papers

Vendor assessment Spreadsheet

NIST AI RMF Playbook

AI risk management Framework



Download the NIST AI RMF Playbook

Community feedback

The playbook is a living resource and is expected to evolve as AI technology advances — Individuals are encouraged to provide feedback about the content of the Playbook by emailing AIframework@nist.gov. Playbook updates will be released approximately twice per year.

Aspects related to the presentation and delivery of Playbook suggestions are under development. Future online versions may include options for filtering or tailoring information to user preferences and requirements.

See the page previously known as "Terms" in the AI RMF Appendix A: 📚 Descriptions of AI Actor Tasks

Explore the Playbook

Filters Active - 0

Type	
Govern	19
Manage	13
Map	18
Measure	22

AI Actors	
Affected Individuals and Comm...	12
AI Deployment	37
AI Design	12
AI Development	13
AI Impact Assessment	23
Domain Experts	18

Topics	
Accountability and Transparency	6
Adversarial	3
AI Deployment	3
AI Incidents	3
Contestability	1
Context of Use	7

The problem with IoT

- IoT security: the risk of hacking and cybercrime
- Lack of effective and informed government regulations
- Device compatibility: the need for interoperability and standardization
- Use of outdated software/firmware

MIRAI Attack

- The primary motive behind developing the Mirai botnet was to gain a competitive advantage in the Minecraft ecosystem
- Jha and his co-conspirators used the botnet to target competing Minecraft servers with DDoS attacks, aiming to extort them or reduce their quality of service, making Jha's own server hosting services more attractive by comparison.
- Mirai’s first major public appearance was in September 2016 when it was used to launch a massive DDoS attack on journalist Brian Krebs' website

- Mirai’s first major public appearance was in September 2016 when it was used to launch a massive DDoS attack on journalist Brian Krebs' website

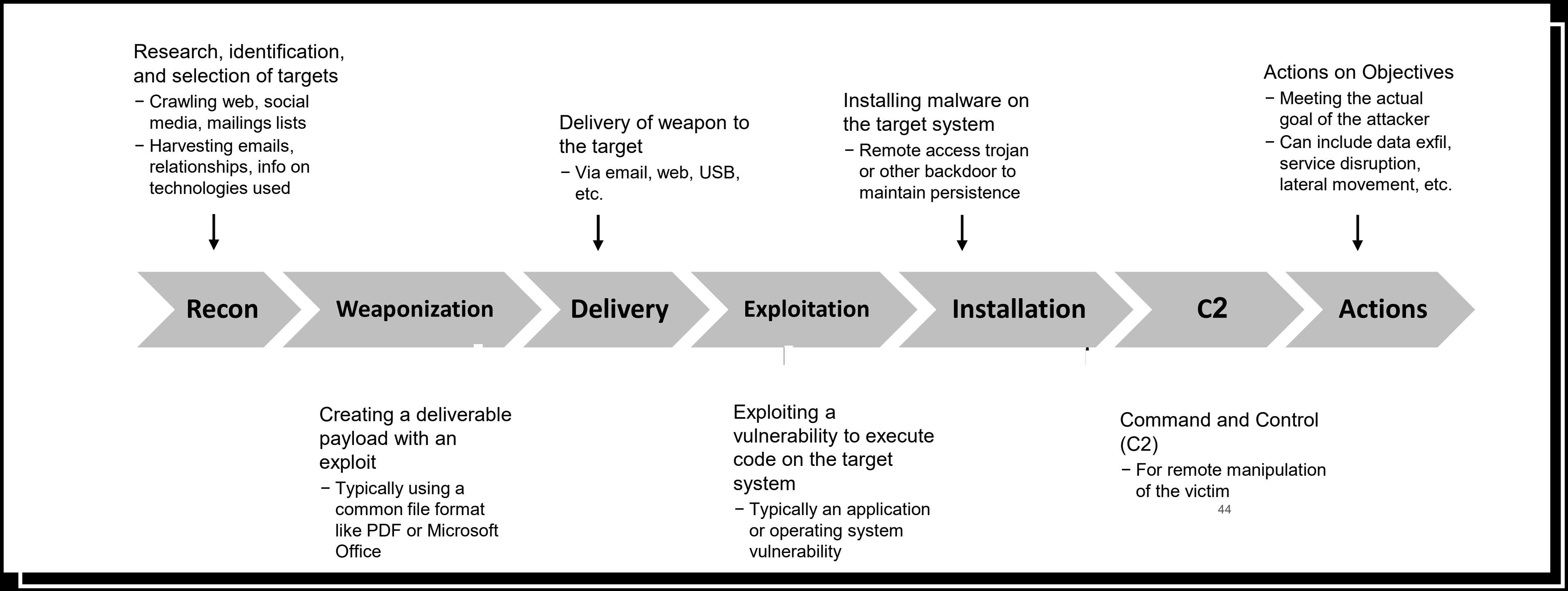
- The botnet was used to launch a massive attack on Dyn, a major DNS provider. This last attack disrupted major websites like Twitter, Netflix, Reddit, and CNN, underscoring the potential havoc IoT-based botnets could wreak.

Would you change your PEST?

Political	**E**conomic
Social	**T**echnological

Big Breaches

Kill Chain



Research, identification, and selection of targets

- Crawling web, social media, mailings lists
- Harvesting emails, relationships, info on technologies used

Creating a deliverable payload with an exploit

- Typically using a common file format like PDF or Microsoft Office

Delivery of weapon to the target

- Via email, web, USB, etc.

Exploiting a vulnerability to execute code on the target system

- Typically an application or operating system vulnerability

Installing malware on the target system

- Remote access trojan or other backdoor to maintain persistence

Command and Control (C2)

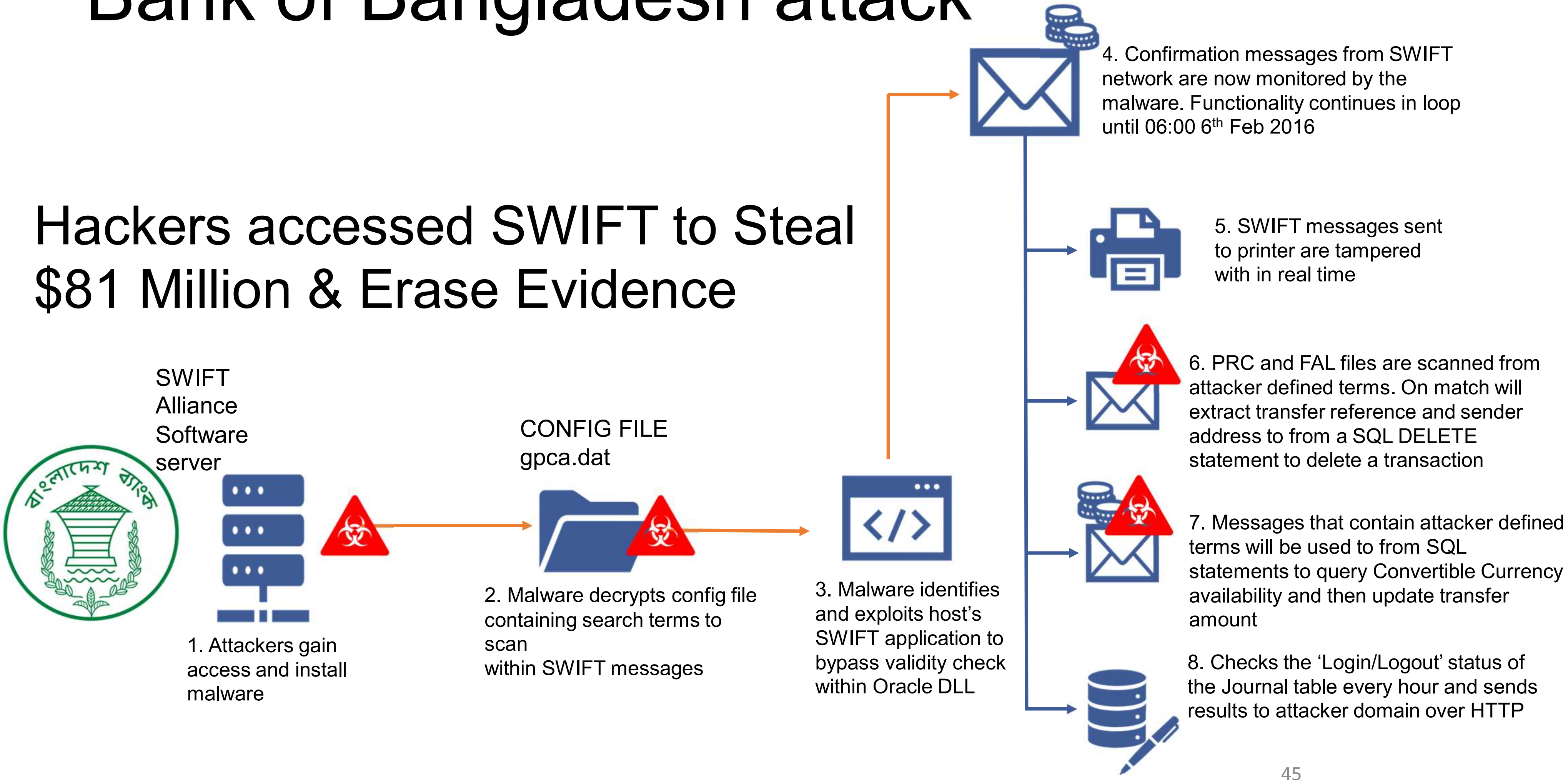
- For remote manipulation of the victim

Actions on Objectives

- Meeting the actual goal of the attacker
- Can include data exfil, service disruption, lateral movement, etc.

Bank of Bangladesh attack

Hackers accessed SWIFT to Steal $81 Million & Erase Evidence



SWIFT Alliance Software server

1. Attackers gain access and install malware

CONFIG FILE
gpca.dat

2. Malware decrypts config file containing search terms to scan
within SWIFT messages

3. Malware identifies and exploits host’s SWIFT application to bypass validity check within Oracle DLL

4. Confirmation messages from SWIFT network are now monitored by the malware. Functionality continues in loop until 06:00 6th Feb 2016

5. SWIFT messages sent to printer are tampered with in real time

6. PRC and FAL files are scanned from attacker defined terms. On match will extract transfer reference and sender address to from a SQL DELETE statement to delete a transaction

7. Messages that contain attacker defined terms will be used to from SQL statements to query Convertible Currency availability and then update transfer amount

8. Checks the ‘Login/Logout’ status of the Journal table every hour and sends results to attacker domain over HTTP

Summarizing the Attack

Setting the Stage: In February 2016, hackers attempted to steal nearly $1 billion from the central bank of Bangladesh. They managed to illegally transfer $81 million to accounts in the Philippines. This incident is one of the largest bank heists in history and serves as a crucial learning point for cybersecurity.

The Heist Details: The attackers infiltrated the bank’s systems and issued fraudulent money transfer requests via the SWIFT network, which is a global system used by banks to communicate securely about financial transactions.

The Attack Sequence

- Initial Breach: The breach began with the hackers gaining access to the bank's network. This was likely achieved through phishing emails, which allowed malware to be installed on the bank’s systems. This malware was specifically designed to interact with the SWIFT software.
- Exploitation: Using the malware, the hackers were able to spy on bank operations to learn how transactions were processed. The malware allowed the hackers to delete outgoing transfer requests from the bank's view, manipulate account balances, and hide their tracks by deleting incoming messages confirming the fraudulent transfers.
- Execution: The fraudulent requests were sent during a weekend, starting on a Friday. This timing was strategic, aimed to exploit slower response times. The hackers targeted the Federal Reserve Bank of New York, asking it to transfer money to various entities in the Philippines and Sri Lanka.

What did we learn?

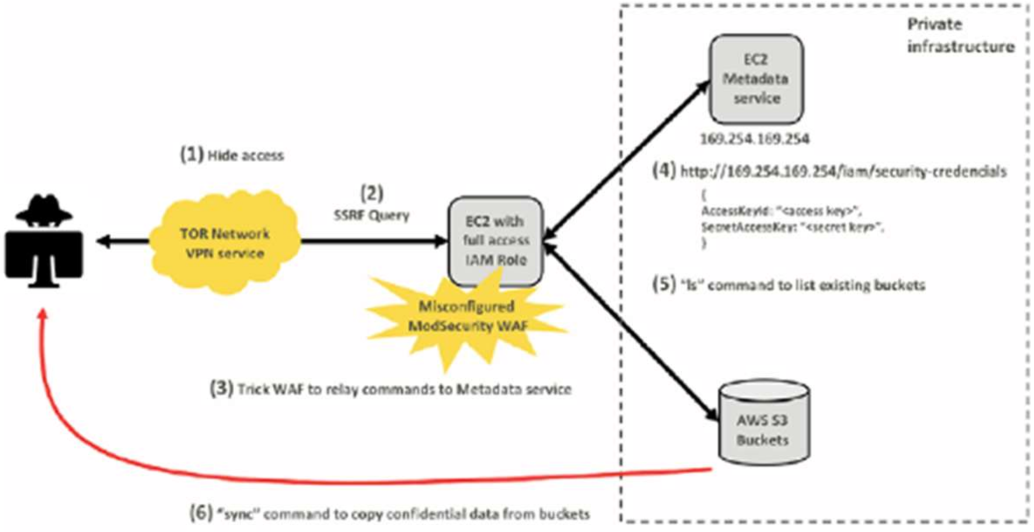
Mitigations

- Importance of Endpoint Security: The malware used in the attack was reportedly delivered via malicious email attachments, highlighting the need for robust endpoint security solutions and email filtering.
- Global Interconnectivity and Shared Vulnerability: The attack underscored the interconnected nature of global financial institutions and the shared vulnerabilities within these networks. It stressed the need for collaborative security measures across entities.
- Regulatory Compliance and Oversight: This incident led to a reevaluation of compliance and regulatory requirements, emphasizing the need for financial institutions to adhere strictly to security standards and best practices, especially in handling international transfers.
- SWIFT Customer Security Programme (CSP): Post-attack, SWIFT launched the Customer Security Programme, aimed at improving the security of the entire SWIFT ecosystem. This initiative emphasizes the importance of security controls and information sharing among member banks.
- Crisis Management and Communication: The delayed detection and response highlighted gaps in crisis management and communication. A more structured approach to crisis handling and stakeholder communication is crucial in managing the aftermath of a security breach effectively.

Capital One

Capital One Attacker Exploited Misconfigured AWS Databases

After bragging in underground forums, the woman who stole 100 million credit applications from Capital One has been found guilty.


(1) Hide access
TOR Network VPN service
(2) SSRF Query
EC2 with full access IAM Role
Misconfigured ModSecurity WAF
(3) Trick WAF to relay commands to Metadata service
Private infrastructure
EC2 Metadata service
169.254.169.254
(4) http://169.254.169.254/iam/security-credencials
{
AccessKeyId: "<access key>",
SecretAccessKey: "<secret key>",
}
(5) "ls" command to list existing buckets
AWS S3 Buckets
(6) "sync" command to copy confidential data from buckets

Summarizing the Attack

- **Setting the Stage:** In March 2019, Capital One experienced a massive data breach that exposed the personal information of approximately 106 million credit card holders in the United States and Canada. This incident ranks among the most significant data breaches involving a major financial institution and underscores critical vulnerabilities within cloud storage services.
- **The Heist Details:** The breach targeted personal information including names, addresses, phone numbers, email addresses, dates of birth, and self-reported income, along with credit scores and transaction data. Also, about 140,000 Social Security numbers and 80,000 linked bank account numbers from credit card customers were compromised. The breach was particularly notable for involving a major cloud service provider, highlighting the risks of misconfigured cloud storage.
- **The Attack Sequence**
- **Initial Breach:** The intrusion was orchestrated by a former software engineer who previously worked at Amazon Web Services, the cloud hosting provider for Capital One. Utilizing knowledge of common misconfigurations in cloud environments, the attacker exploited a specific misconfigured web application firewall to gain unauthorized access.
- **Exploitation:** After gaining access, the attacker exploited the misconfiguration to execute a series of commands that allowed them to access the folders or buckets where Capital One stored its data. The attacker then exfiltrated the sensitive data from Capital One’s storage space hosted on the cloud.
- **Execution:** The data exfiltration was executed over a few months, starting in March 2019. Notably, the breach was discovered not from internal monitoring but from an external tip. In July 2019, an anonymous email alerted Capital One to the possibility that its data was posted on GitHub, a platform for sharing and collaborating on code.

What did we learn?

Mitigations for the Capital One Attack

- Enhanced Configuration and Access Management: Proper Configuration of Security Tools: Ensure that all security tools, especially those related to web application firewalls (WAF) and other boundary protection mechanisms, are correctly configured. This involves regular audits to identify and rectify misconfigurations.
- Least Privilege Access: Implement and enforce the principle of least privilege on all systems and services. Users and applications should only have the minimum level of access necessary to perform their functions.
- Routine Security Assessments and Penetration Testing: Conduct regular security assessments and penetration tests to identify and address vulnerabilities, particularly in cloud environments. This includes testing for improper permission settings and other common misconfigurations that could allow unauthorized access.
- Advanced Monitoring and Anomaly Detection: Deploy sophisticated monitoring tools that can detect unusual access patterns or unauthorized data exfiltration activities. Implementing machine learning algorithms can help in identifying anomalies that deviate from normal operational baselines.
- Employee Training and Security Awareness: Regular training programs for all employees on the latest security practices and threat awareness, particularly focusing on the nuances of cloud security and the potential internal threats.
- Incident Response and Breach Notification Planning: Develop and regularly update an incident response plan that includes procedures for breach containment, eradication, recovery, and notification. Rapid response can significantly mitigate the damage caused by a breach.

JP Morgan Chase

In 2014, JPMorgan Chase, one of the largest financial institutions in the United States, suffered a significant cybersecurity breach

The attackers targeted a website hosting a charitable event sponsored by JPMorgan Chase

After obtaining the necessary usernames and passwords, the attackers identified a server within JPMorgan Chase's network that lacked two-factor authentication.

This oversight allowed the attackers to use the stolen credentials without needing to bypass any additional security measures like hardware tokens or SMS-based codes.

What did we learn?

Mitigations

- Need for Multi-Factor Authentication: The attackers gained access to the bank's network because a server lacked two-factor authentication. This breach underscored the importance of implementing strong multi-factor authentication systems across all access points, especially those handling sensitive or critical data.
- Enhanced Monitoring and Anomaly Detection: The duration over which the attackers had access to JP Morgan's network without detection highlighted the need for improved monitoring and anomaly detection. Financial institutions should invest in advanced threat detection systems that can identify unusual behavior patterns and potential breaches more quickly. The breach was not detected by the bank's own systems but was discovered only after the hackers had siphoned off the data and deleted logs to cover their tracks.
- Staff Training and Awareness: The incident stressed the importance of regular and rigorous training for all employees. Staff should be educated about the dangers of reusing passwords and social engineering attacks, and how to recognize them.
- Rapid Response and Incident Management: The ability to respond quickly and effectively to a breach can significantly mitigate damage. JP Morgan's response involved moving quickly to contain the breach once discovered, but earlier detection could have minimized the exposure. Establishing a well-prepared incident response team and a clear plan can enhance resilience against cyber attacks.
- Vendor and Third-Party Risk Management: Given the vast ecosystem of vendors and third parties that large institutions like JP Morgan interact with, the attack highlighted the importance of extending cybersecurity practices through the supply chain. Regular audits, security requirements, and monitoring of third parties are crucial to ensure they meet the necessary security standards.
- Regulatory Compliance and Transparency: Following the breach, there was significant scrutiny from regulators. This situation emphasized the importance of compliance with financial industry regulations and standards, and the need for transparency with regulators and customers about risk and incident management.
- Investment in Cybersecurity Infrastructure: This breach drove home the point that cybersecurity is an essential area of investment for financial institutions. Post-breach, JP Morgan pledged to double its cybersecurity spending. This reflects a broader industry acknowledgment that investing in comprehensive cybersecurity measures is not just necessary for protection but also beneficial for maintaining customer trust and institutional stability.

United Healthcare

- UnitedHealth Group experienced a significant ransomware attack on its subsidiary, Change Healthcare
- The attackers gained initial access using stolen credentials for a system that allowed remote access to Change Healthcare's network

What did we learn?

Mitigations

- Importance of Data Encryption: Data breaches in healthcare often reveal that sensitive data was not encrypted or improperly encrypted. Encrypting data both at rest and in transit is critical to safeguarding patient information against unauthorized access.
- Enhanced Access Controls: These breaches frequently expose weak access controls that allow unauthorized users to access sensitive information. Implementing strong access control mechanisms, including role-based access controls, can limit access to sensitive data to only those who need it to perform their job functions.
- Regular Security Audits and Risk Assessments: Healthcare organizations must conduct regular security audits and comprehensive risk assessments to identify and mitigate vulnerabilities. This proactive approach helps in recognizing potential security weaknesses before they can be exploited.
- Employee Training and Awareness: Human error often plays a significant role in data breaches. Regular training on security best practices, recognizing phishing attempts, and safely handling patient data can reduce the risk of breaches caused by employee mistakes.
- Advanced Threat Detection Systems: Implementing advanced monitoring and threat detection systems can help in early detection of unusual activities that could indicate a breach. Quick detection is crucial in minimizing the impact of a breach.
- Vendor Risk Management: Third-party vendors often have access to healthcare data and can be a weak link in data security. Rigorous vetting, contractual stipulations on data security, and regular audits of vendor security practices are necessary to secure the data chain.
- Incident Response Planning: Having a robust incident response plan in place is essential for quickly addressing security breaches. This plan should include steps for containment, investigation, remediation, and communication with affected individuals and regulatory bodies.
- Use of Multi-Factor Authentication (MFA): MFA can significantly enhance security by adding an additional layer of protection beyond username and password. Its adoption in healthcare, where data sensitivity is high, is particularly important.
- Regular Updates and Patch Management: Ensuring that all systems are up-to-date with the latest security patches is a fundamental security measure that can prevent breaches exploiting known vulnerabilities.
- Business Continuity Planning and Backups: Ensuring your data is backed up to immutable backups.

Best Sources of Breach Information

1. Industry Reports and Research

- Verizon Data Breach Investigations Report (DBIR): An annual report that provides analysis of data breaches and incidents, trends, and advice on how to mitigate future risks.

2. Cybersecurity News Websites

- Krebs on Security: Run by journalist Brian Krebs, this blog offers in-depth coverage of cybersecurity issues, including detailed analyses of breaches and security threats.
- Dark Reading: Covers a wide range of cybersecurity topics, from vulnerabilities and threats to protection and compliance.

3. Professional Associations and Networks

- ISACA: Offers resources, networking, and learning opportunities for cybersecurity professionals, including publications and professional development courses.
- SANS Institute: Offers training, certification, and research in cybersecurity. Their reading room includes white papers and articles on the latest security techniques and threats.

4. Podcasts and Webinars

- Cybersecurity Today: Offers frequent updates and briefings on the latest cybersecurity news, breaches, and preventive tactics.
- Darknet Diaries: Features true stories from the dark side of the Internet, including hacks, data breaches, and cybersecurity.

5. Social Media and Forums

- Twitter or X: Follow cybersecurity influencers, experts, and companies for real-time updates.
- LinkedIn Groups: Join groups related to cybersecurity to engage with other professionals and stay informed about industry trends.

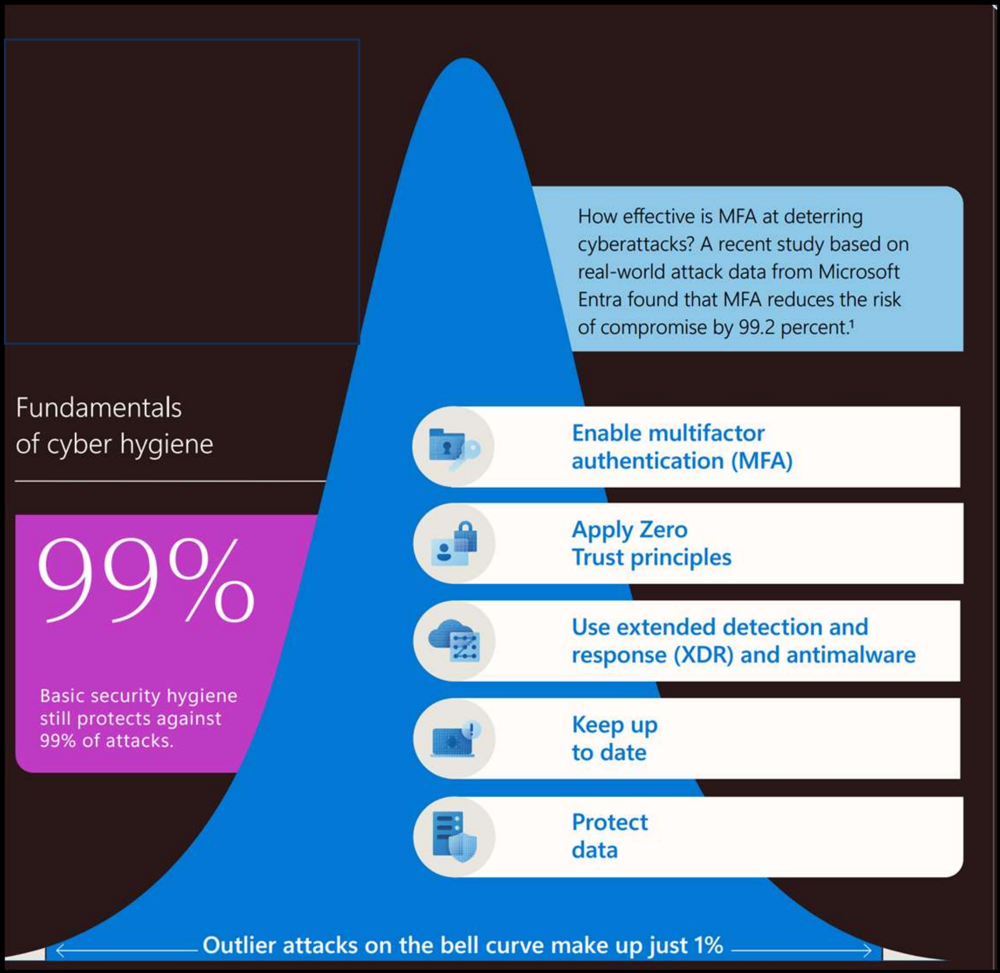
Mitigations

Cat and Mouse

Remember!

Get the basics right

CIS Critical Controls
NIST CSF



How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.[1]

Fundamentals of cyber hygiene

99%

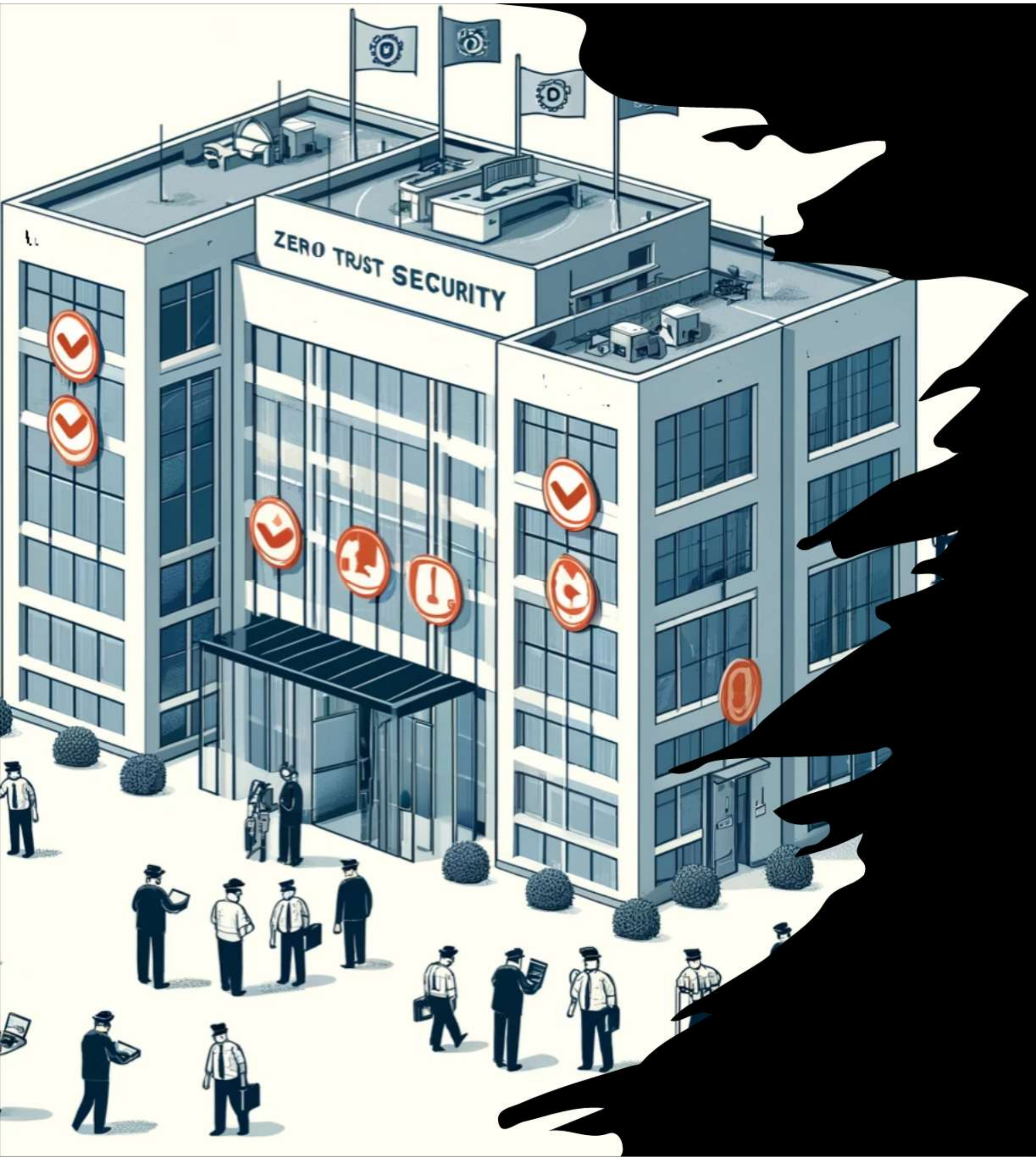
Basic security hygiene still protects against 99% of attacks.

- Enable multifactor authentication (MFA)
- Apply Zero Trust principles
- Use extended detection and response (XDR) and antimalware
- Keep up to date
- Protect data

Outlier attacks on the bell curve make up just 1%

MITRE Attack Chain

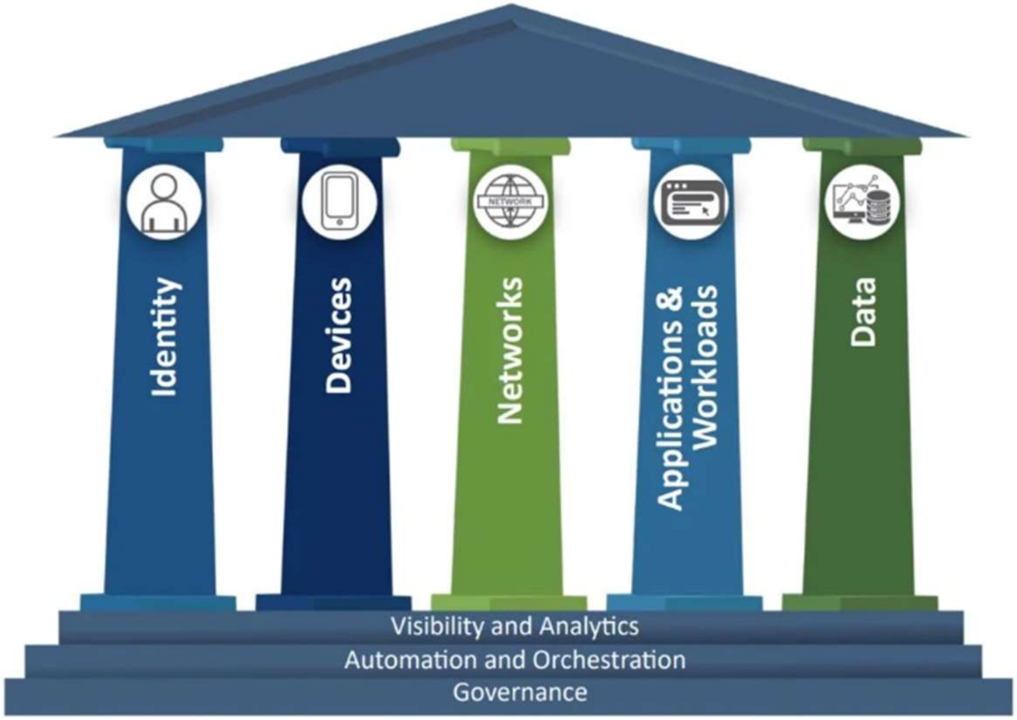
Tactics	Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Techniques									
Mitigations	WAF Update Software Vulnerability Scanning	Privileged Account Management Update Software	Password Policies Privileged Account Management	Restrict Permissions User Account Management	AD Config Audit Password Policies User Training	Disable Program NIPS Network Segmentation	Application Isolation Exploit Protection Network Segmentation	Restrict File and Directory Permissions	Filter Network Traffic DLP, NIPS Network Segmentation



Zero Trust is a cybersecurity philosophy based on the principle that organizations should not automatically trust anything inside or outside their perimeters and instead must verify everything trying to connect to their systems before granting access.

- Never Trust, Always Verify: Zero Trust is like having a bouncer at every door and window of your house, checking the ID of anyone who wants to come in, every single time, no matter if they live there or are just visiting.
- Verify and then Trust: Think of Zero Trust as the digital equivalent of double-checking that someone has the right key before letting them into a locked room, even if you've seen them use the key before.
- Security Everywhere: It's like putting a lock on every single door in a building, not just the front door. Everyone needs the right key and the right permissions to move from room to room.
- Least Privilege Access: This part of Zero Trust is like giving janitors keys that only open doors to the floors they need to clean, ensuring no one has more access than they need for their specific tasks.
- Continuous Verification: Imagine a security system that continuously checks if the people inside a building should still be there, not just at the moment they enter.

Zero Trust



Source: CISA

Zero Trust

Request Context:

Identity	Unusual behavior? Risky user's activity? Unusual location? Multi-factor Auth?
Device	Registered device? Resource privileged? Device compromised?
Application	Known application? Is it sanctioned? Password on web?
Network	Risk of the source? Internal Request? Configured to policy? Is it privileged?
Infrastructure	What is the IP? Compliant policy? Managed proxy?
Data	Data location? Data encrypted? Data sensitivity?

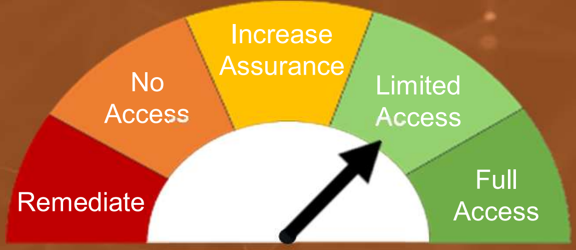
Under a Zero Trust policy, greater context and comprehensive verification means more control and tighter security

Zero Trust Verification

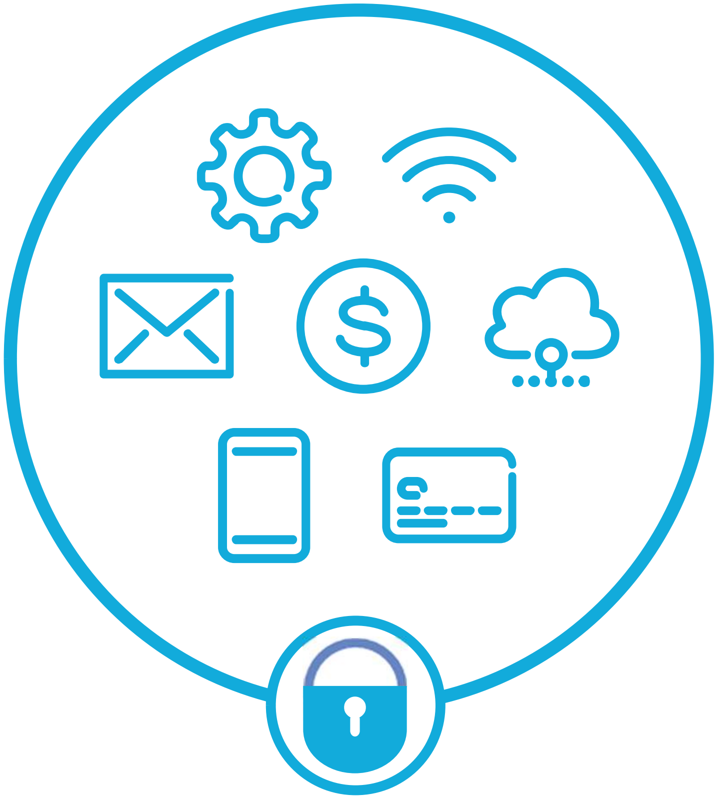
Known **Trusted**

Allowed

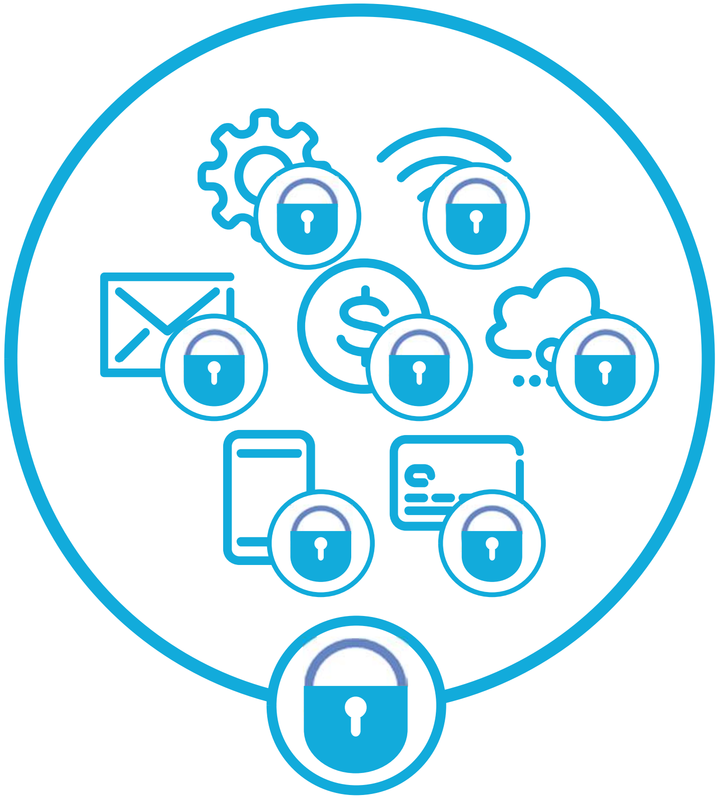
Level of Assurance Required



Traditional Model



Zero Trust Model

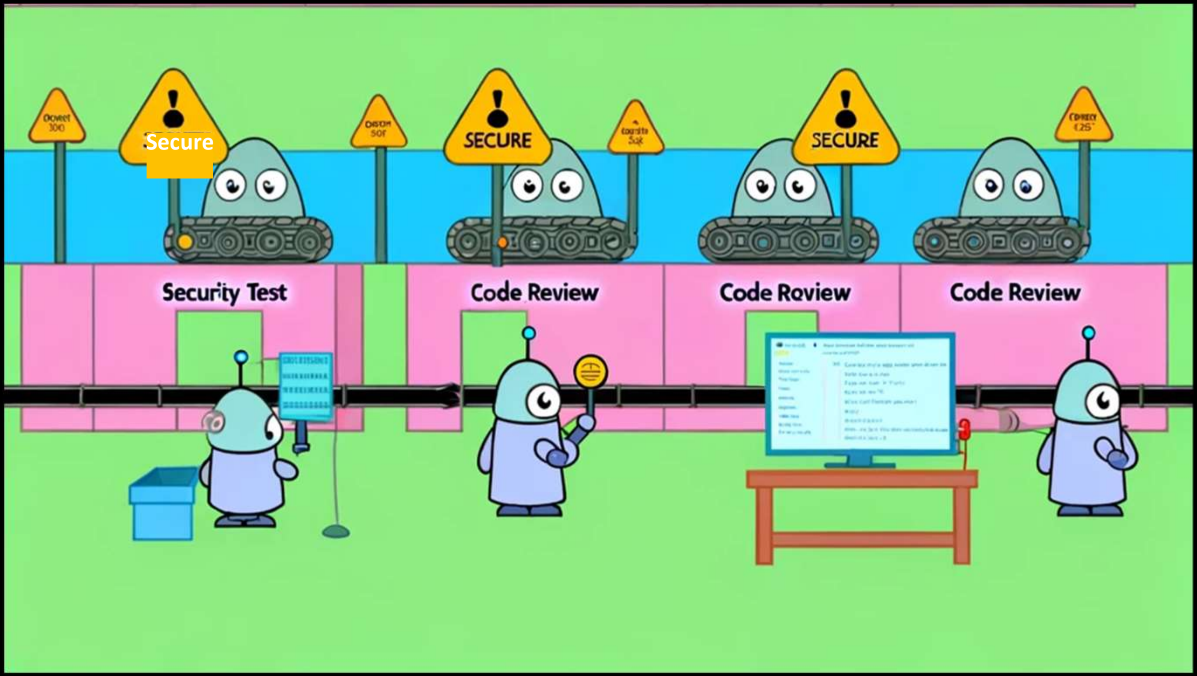


Abandon the concepts of network-based connectivity and instead connect users to applications

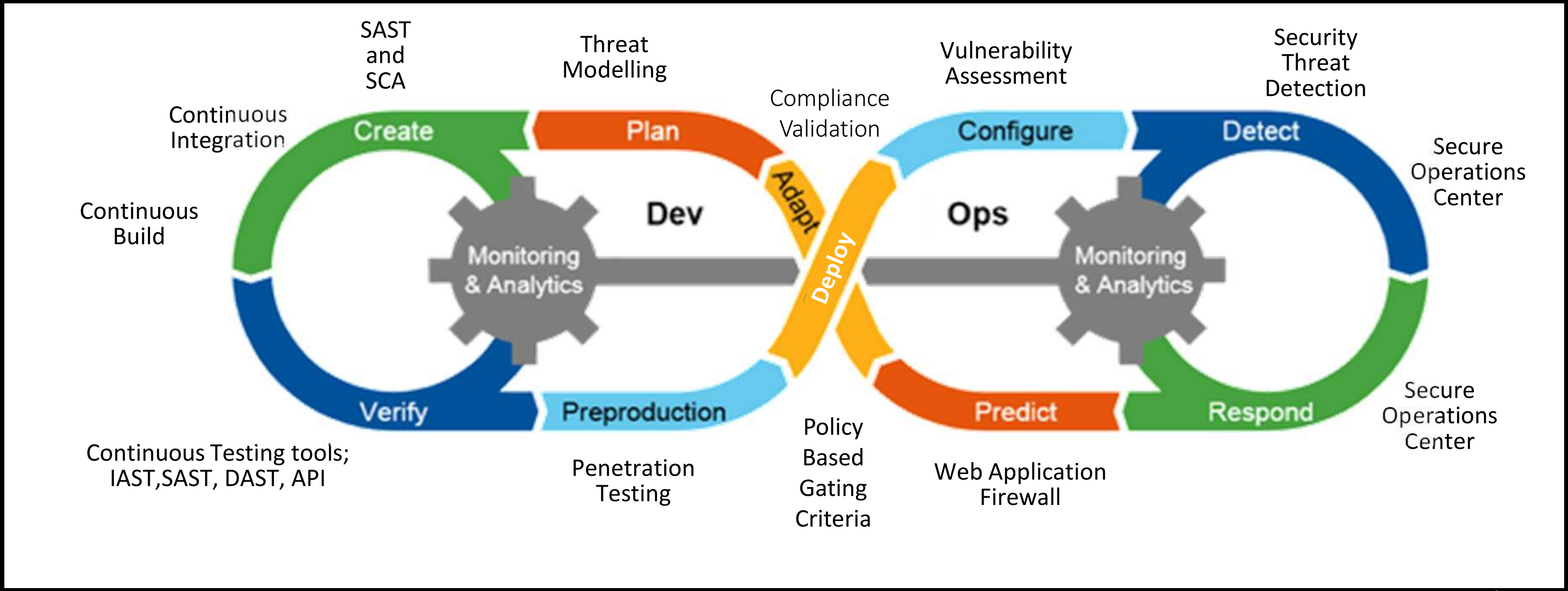
A word on Secure Code

Building Secure Code

- Producing Secure code is like a factory with security checks along the way
- The cost is lower the earlier you find the issue
- A flaw could create a open door
- Shift left is the mantra and what you measure



Security Aspect in Context of the Continuous Delivery Pipeline



Core security activities

- Threat modeling
- Secure code reviews
- Vulnerability scans & assessments
- Penetration tests
- Applies to custom & COTS
- Managed WAF

Collaboration

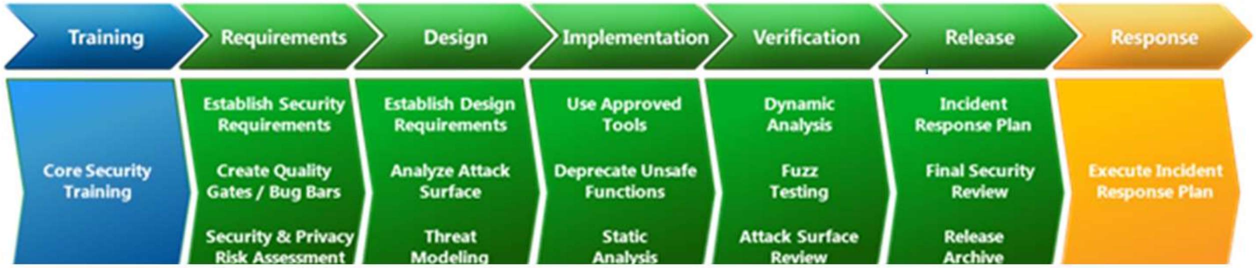
- Educating developers on secure coding
- Practices with workshops, talks, lesson learned
- Secure coding standards
- Secure code library & other reference materials

Experts review

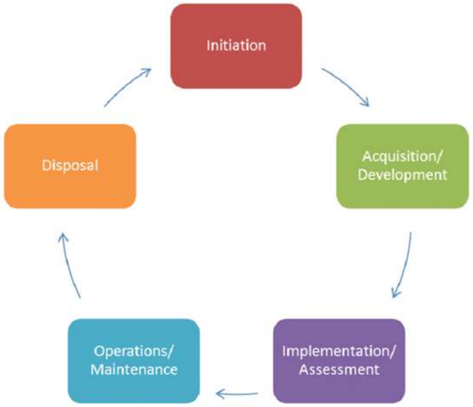
- Bug bounty programs
- Red Team exercises

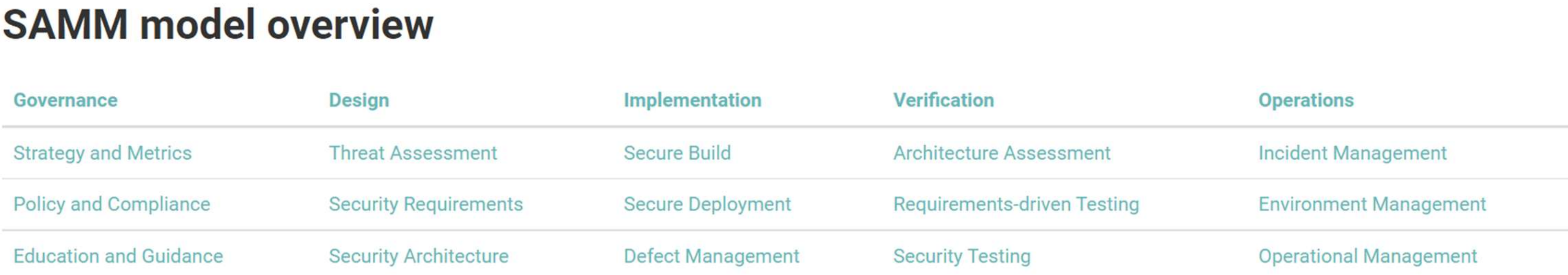
Application Security Guidelines and Frameworks

Microsoft SDLC



Training	Requirements	Design	Implementation	Verification	Release	Response
Core Security Training	Establish Security Requirements Create Quality Gates / Bug Bars Security & Privacy Risk Assessment	Establish Design Requirements Analyze Attack Surface Threat Modeling	Use Approved Tools Deprecate Unsafe Functions Static Analysis	Dynamic Analysis Fuzz Testing Attack Surface Review	Incident Response Plan Final Security Review Release Archive	Execute Incident Response Plan





SAMM model overview

Governance	Design	Implementation	Verification	Operations
Strategy and Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Policy and Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Education and Guidance	Security Architecture	Defect Management	Security Testing	Operational Management

Gartner recommends that the oversight of the application security program itself — which includes any published documents — live with a dedicated application security team.

Summary

- Understanding the Global Landscape through PEST Analysis
- Cybersecurity in a World at War and economic tension
- Learning from the Past and looking into the future

Thank you

- Any questions???
- Contact nairsushi@gmail.com
- Follow me on LinkedIn https://www.linkedin.com/in/sushilanair/
- Twitter @sushila_nair

Community builds our skills and network