Trending Cybersecurity Threats for Businesses

Presented By: Chad Knutson, CISSP, CISA, CRISC, CDPSE
SBS CyberSecurity, LLC

Welcome!

AUDIO

- If you are experiencing audio issues using your computer's speaker, you can call in via a phone by calling:

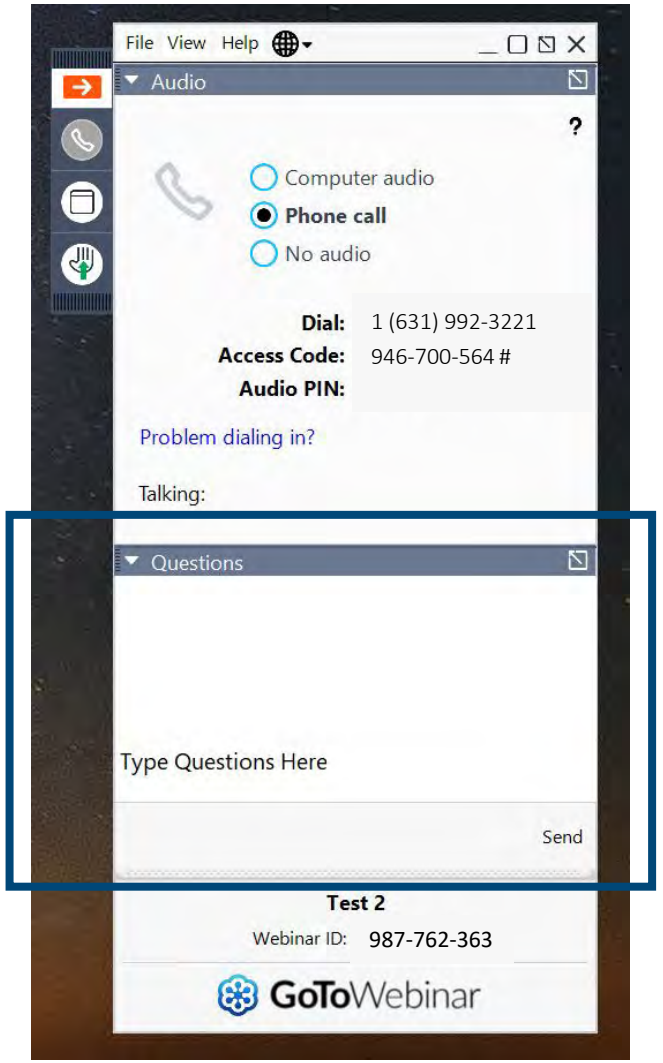
  (631) 992-3221 Access Code: 946-700-564

QUESTIONS

- Use the "Questions" panel to submit any questions throughout the webinar.

RECORDING

- This webinar is being recorded. A link to the recording will be emailed to you following the webinar, as well as posted on the Bank First website.



Contact Information

Follow us on Social:

Chad Knutson

- President, CISO, Partner
- CISA, CRISC, CISSP
- Master's of Information Assurance
- Phone: 605-480-3366
- chad@sbscyber.com
- www.sbscyber.com

SBS Institute

- sbsinstitute@sbscyber.com
- 605-269-0909

Agenda

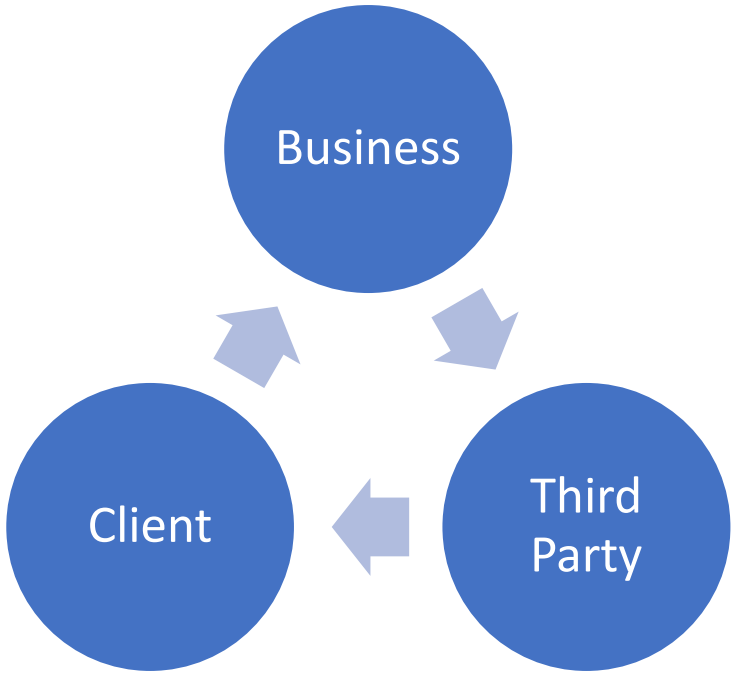
- CYBERSECURITY
  - What are the biggest threats today?
- POTENTIAL IMPACTS
  - How is your business at risk?
- TAKEAWAYS
  - How to mitigate cybersecurity risk (systems, training, etc.)
  - Insurance
  - Resources to partner with

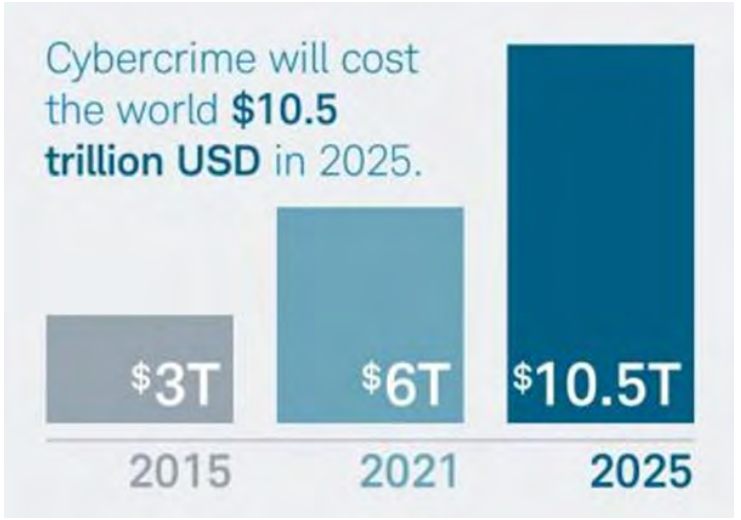
SBS INSTITUTE

CYBERSECURITY

Why?

- Evolving Threat Landscape
- CyberSecurity trends and evolving risks and threats





Source

Summary

This industry, like many others, is beset by Social Engineering attacks. Manufacturing also saw a marked rise in Ransomware related breaches.

Frequency	585 incidents, 270 with confirmed data disclosure
Top Patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 82% of breaches
Threat Actors	External (82%), Internal (19%), Multiple (1%) (breaches)
Actor Motives	Financial (92%), Espionage (6%), Convenience (1%), Grudge (1%), Secondary (1%) (breaches)
Data Compromised	Personal (66%), Credentials (42%), Other (36%), Payment (19%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (14), Access Control Management (6), Secure Configuration of Enterprise Assets and Software (4)

Summary

The combination of the System Intrusion and Social Engineering patterns account for the majority of cases in this sector. The Use of stolen credentials is widespread and employees have a definite tendency to fall for Social tactics.

Frequency	1,892 Incidents, 630 with confirmed data disclosure
Top Patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 81% of breaches
Threat Actors	External (74%), Internal (26%) (breaches)
Actor Motives	Financial (97%), Espionage (2%), Grudge (1%) (breaches)
Data Compromised	Credentials (63%), Personal (49%), Other (21%), Bank (9%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (14), Access Control Management (6), Secure Configuration of Enterprise Assets and Software (4)

Source

Incidents vs Breaches

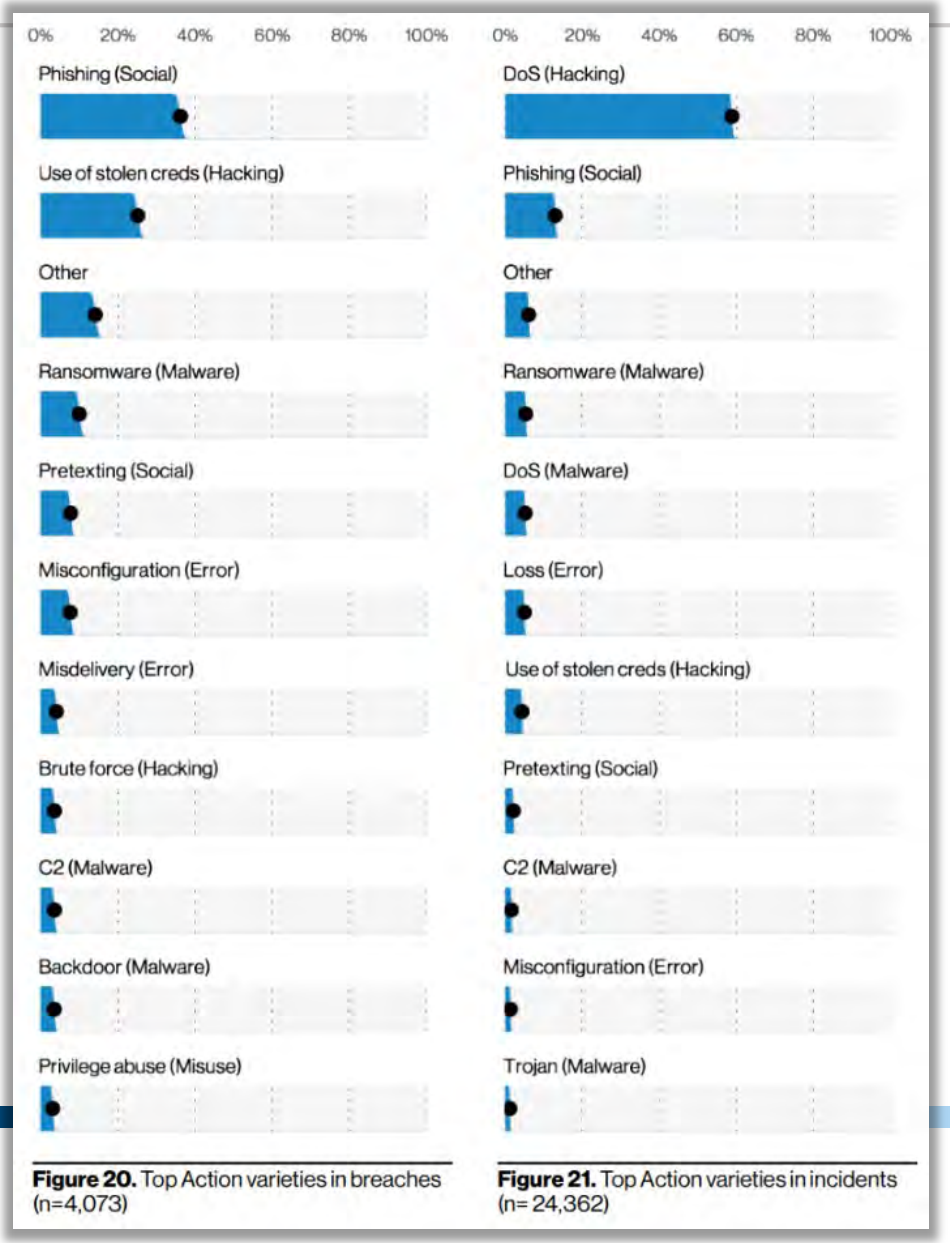
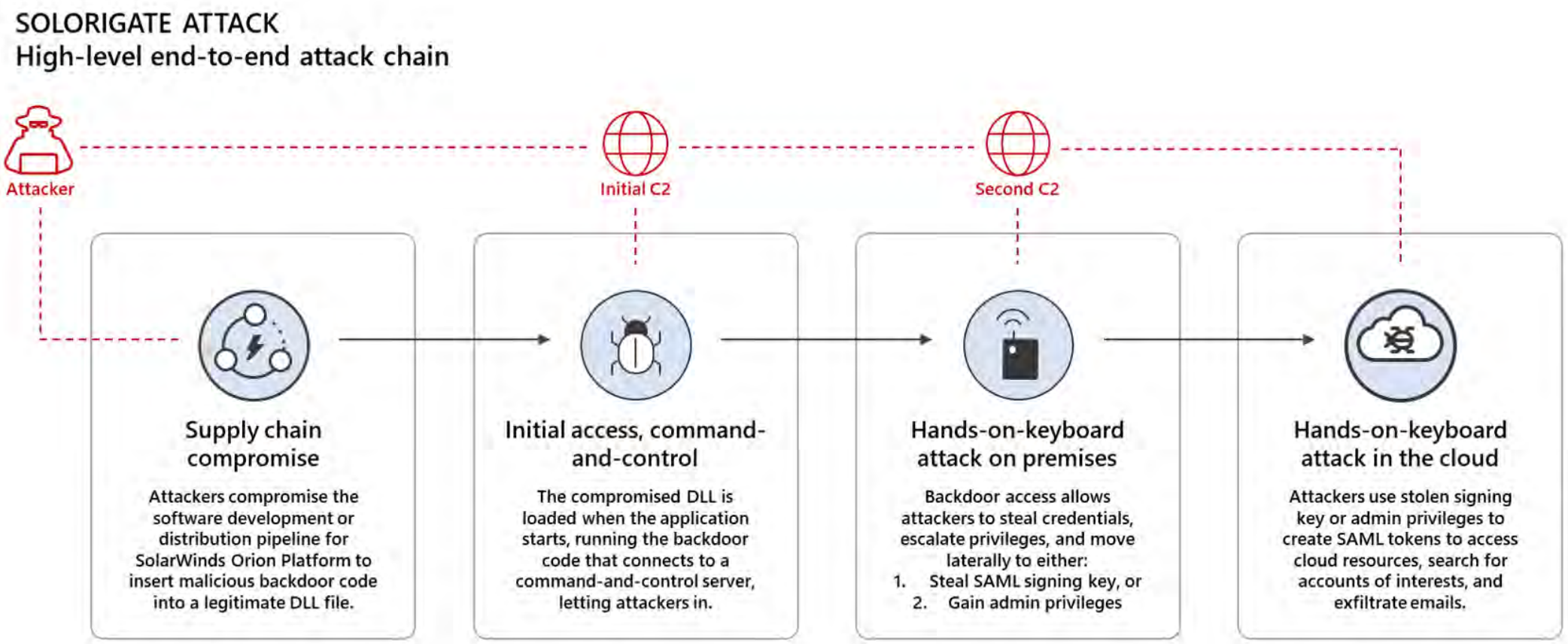


Figure 20. Top Action varieties in breaches (n=4,073)

Figure 21. Top Action varieties in incidents (n= 24,362)

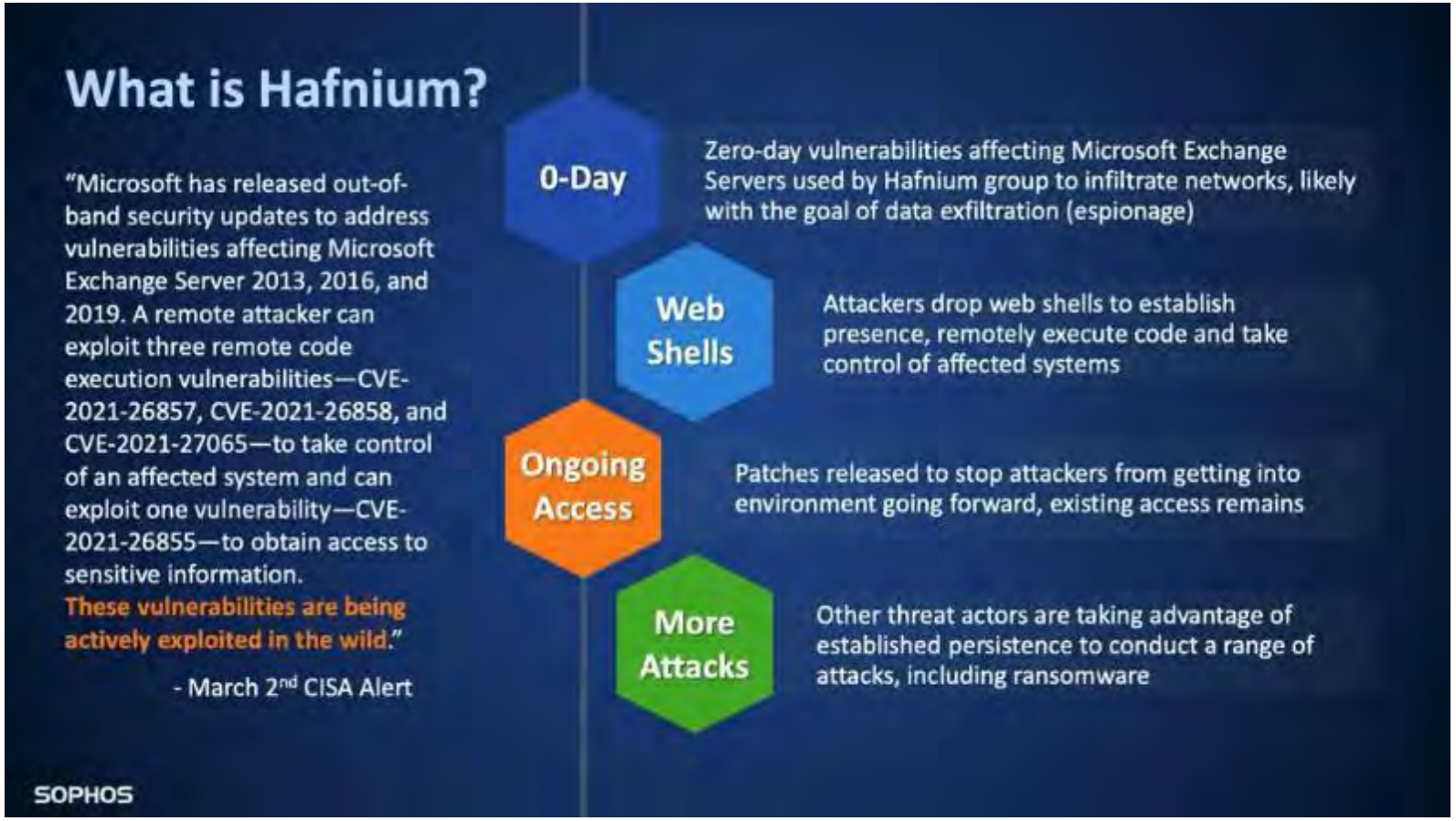
[Source]

SolarWinds Attack



Source

Microsoft Exchange Vulnerability



Source

Colonial Pipeline

- Largest fuel pipeline in the U.S
- $4.4 million in Bitcoins paid to “DarkSide”
- Stole nearly 100 gigabytes of data
- Cause: single compromised password
- April 29 through a VPN account (no longer used account)
- Ransom May 7th, controller's shutdown pipeline (first in 57 years)
- May 12th, resumed service.

Source

Alert (AA22-011A)

More Alerts

Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

Original release date: January 11, 2022 | Last revised: March 01, 2022

Summary

Note: *this advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 10. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.*

This joint Cybersecurity Advisory (CSA)—authored by the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA)—is part of our continuing cybersecurity mission to warn organizations of cyber threats and help the cybersecurity community reduce the risk presented by these threats. This CSA provides an overview of Russian state-sponsored cyber operations; commonly observed tactics, techniques, and procedures (TTPs); detection actions; incident response guidance; and mitigations. This overview is intended to help the cybersecurity community reduce the risk presented by these threats.

CISA, the FBI, and NSA encourage the cybersecurity community—especially critical infrastructure network defenders—to

Actions Critical Infrastructure Organizations Should Implement to Immediately Strengthen Their Cyber Posture.

- *Patch all systems. Prioritize patching known exploited vulnerabilities.*
- Implement multi-factor authentication.
- *Use antivirus software.*

CISA Alerts


National Cyber Awareness System > Alerts > Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector

Alert (AA22-083A)

More Alerts

Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector

Original release date: March 24, 2022

Print | Tweet | Send | Share

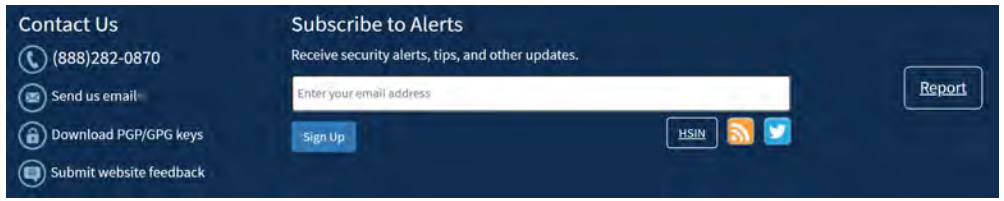
Summary

This joint Cybersecurity Advisory (CSA)—coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Energy (DOE)—provides information on multiple intrusion campaigns conducted by state-sponsored Russian cyber actors from 2011 to 2018 and targeted U.S. and international Energy Sector organizations. CISA, the FBI, and DOE responded to these campaigns with appropriate action in and around the time that they occurred. CISA, the FBI, and DOE are sharing this information in order to highlight historical tactics, techniques, and procedures (TTPs) used by adversaries to target U.S. and international Energy Sector organizations.

On March 24, 2022, the U.S. Department of Justice unsealed indictments of three Russian Federal Security Service (FSB) officers and a Russian Federation Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM) employee for their involvement in the following intrusion campaigns against U.S. and international oil refineries, nuclear facilities, and energy companies.[1]

Actions to Take Today to Protect Energy Sector Networks:
- Implement and ensure robust network segmentation between IT and ICS networks.
- Enforce MFA to authenticate to a system.
- Manage the creation of, modification of, use of—and permissions

[Sign Up](#)


Contact Us

(888)282-0870

Send us email

Download PGP/GPG keys

Submit website feedback

Subscribe to Alerts

Receive security alerts, tips, and other updates.

Enter your email address

Sign Up

HSIN

Report


AA22-083A : Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector

AA22-076A : Strengthening Cybersecurity of SATCOM Network Providers and Customers

AA22-074A : Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability

AA22-057A : Destructive Malware Targeting Organizations in Ukraine

AA22-055A : Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks

AA22-054A : New Sandworm Malware Cyclops Blink Replaces VPNFilter

AA22-047A : Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology

AA22-040A : 2021 Trends Show Increased Globalized Threat of Ransomware

AA22-011A : Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

Critical Infrastructure

cisa.gov

Russia Cybersecurity Concerns

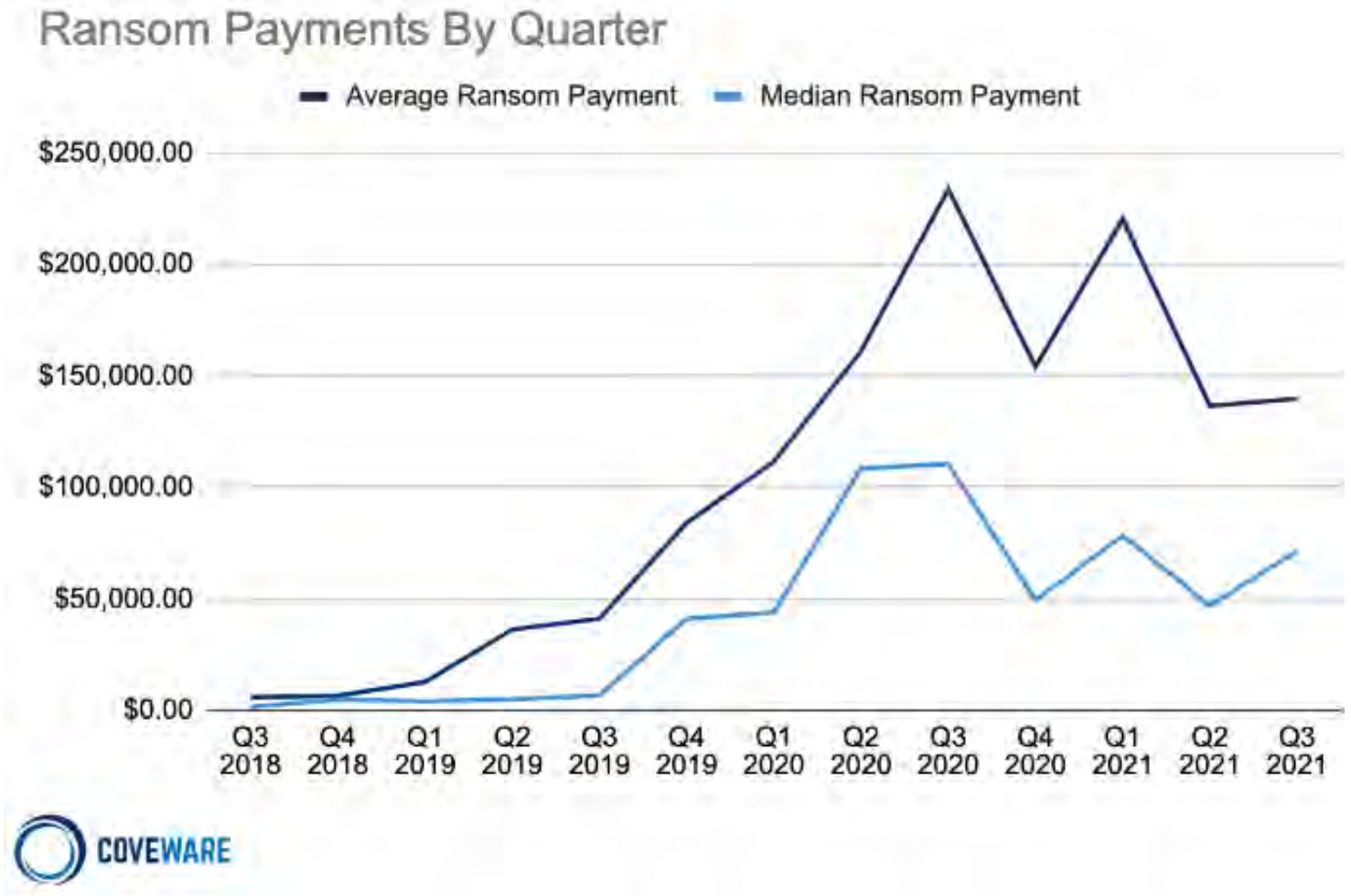
1. Direct attacks against critical infrastructure sector
2. Indirect collateral damage from attacks
3. Unaffiliated cybercriminals leveraging opportunity

SBS INSTITUTE

POTENTIAL IMPACTS

Ransomware Trends

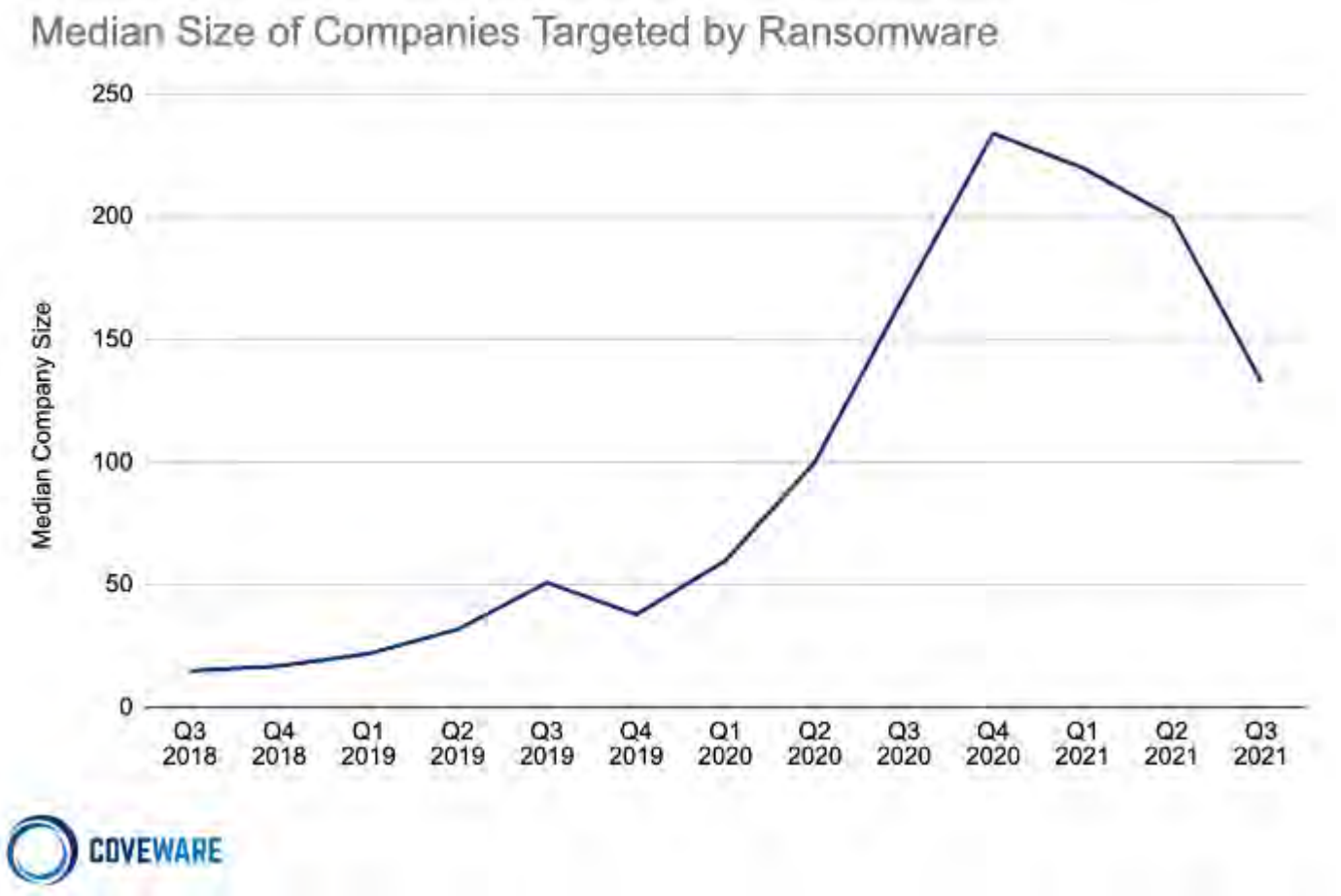
$139,739 in Q3 2021 - a 2.3% increase from Q2



Average downtime decreased to 22 days (-5%)

https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts

Ransomware Trends

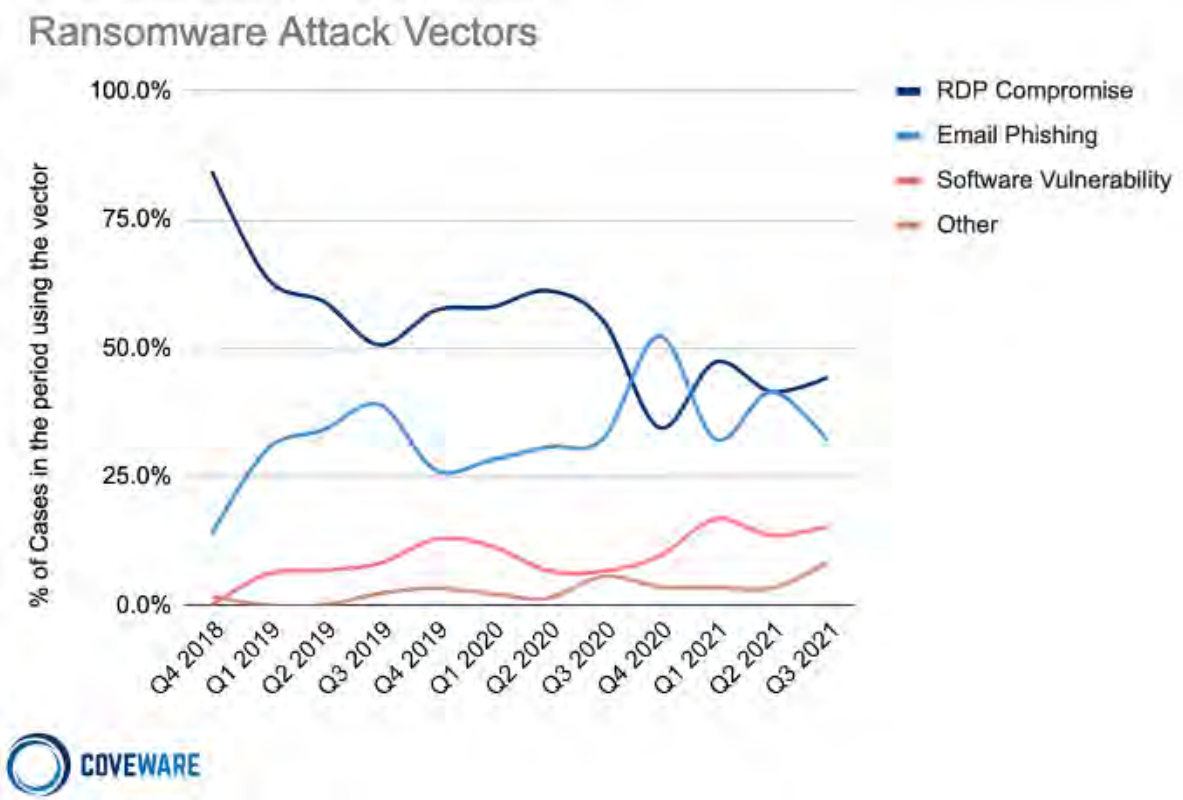


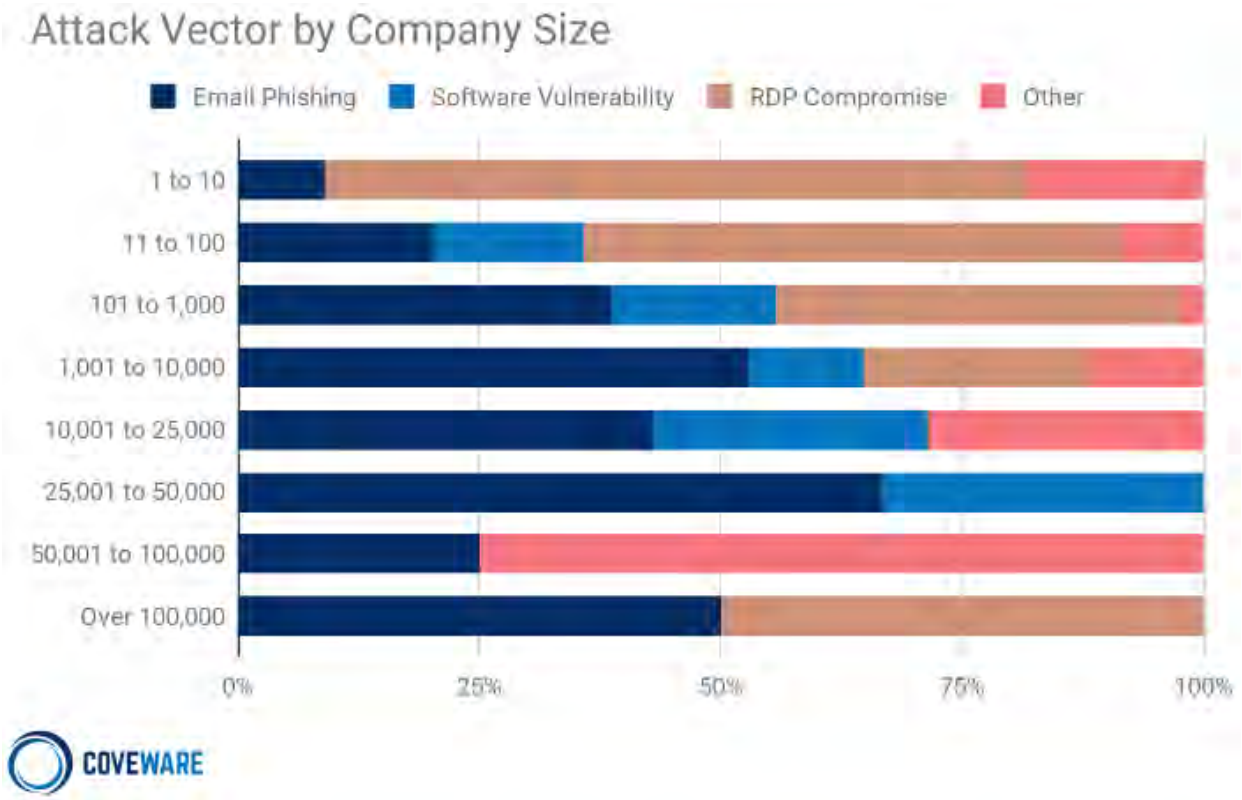
83.36% of Ransomware attacks in Q3 involved data exfiltration

200 = Median # of Employees of Ransomware victims (84% - >1000 people)

https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts

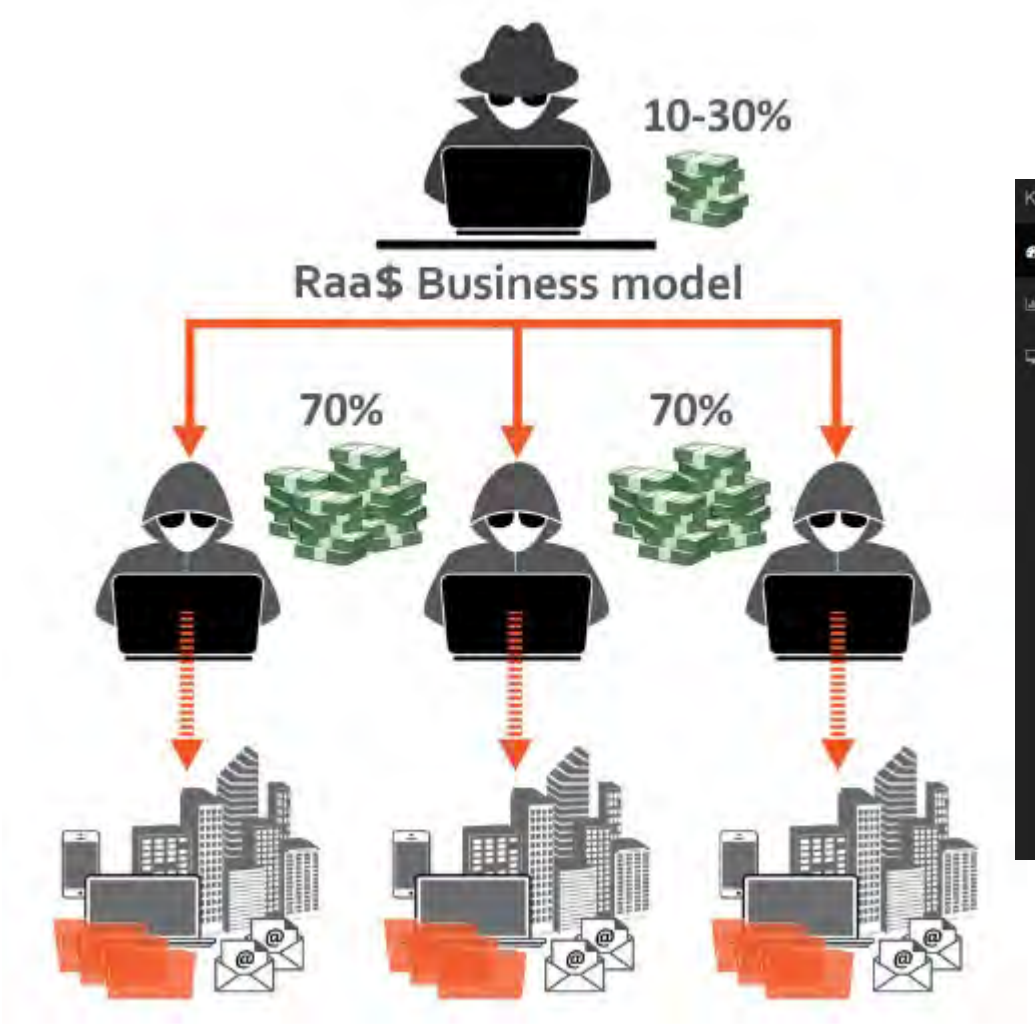
Ransomware Trends

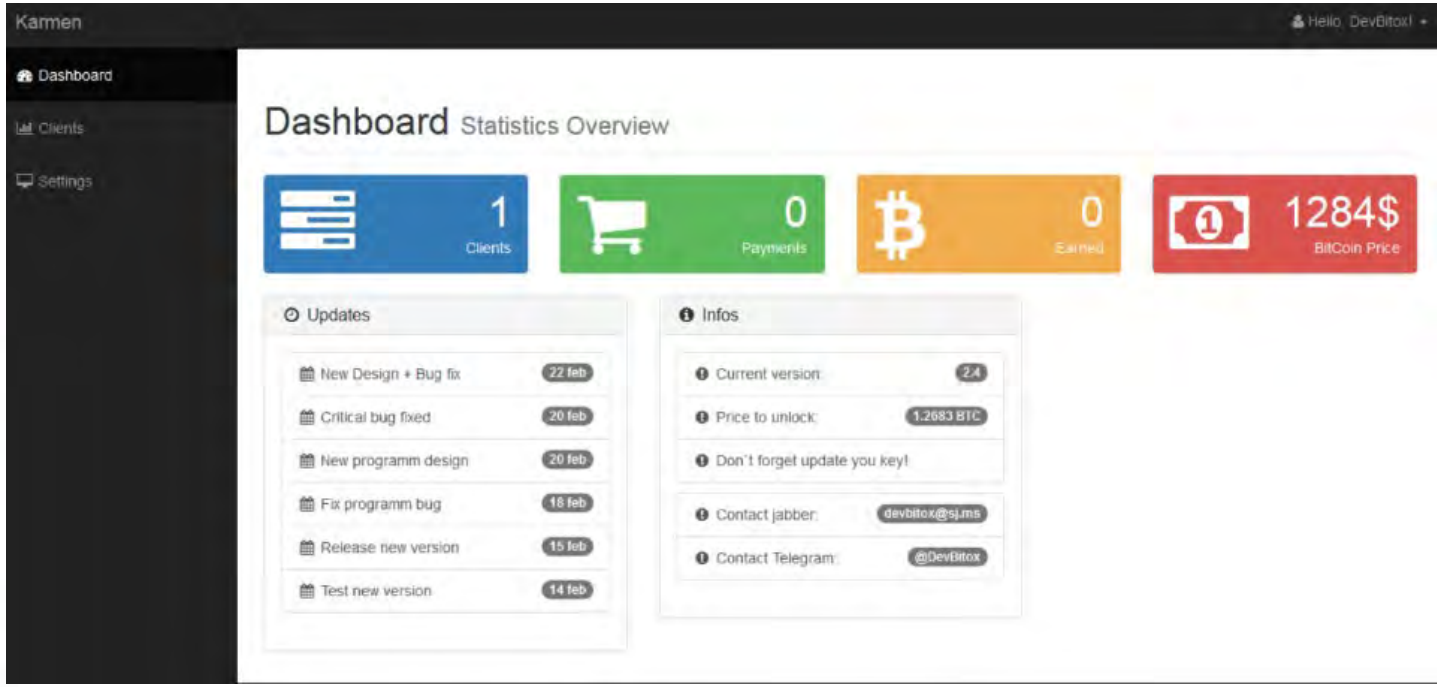




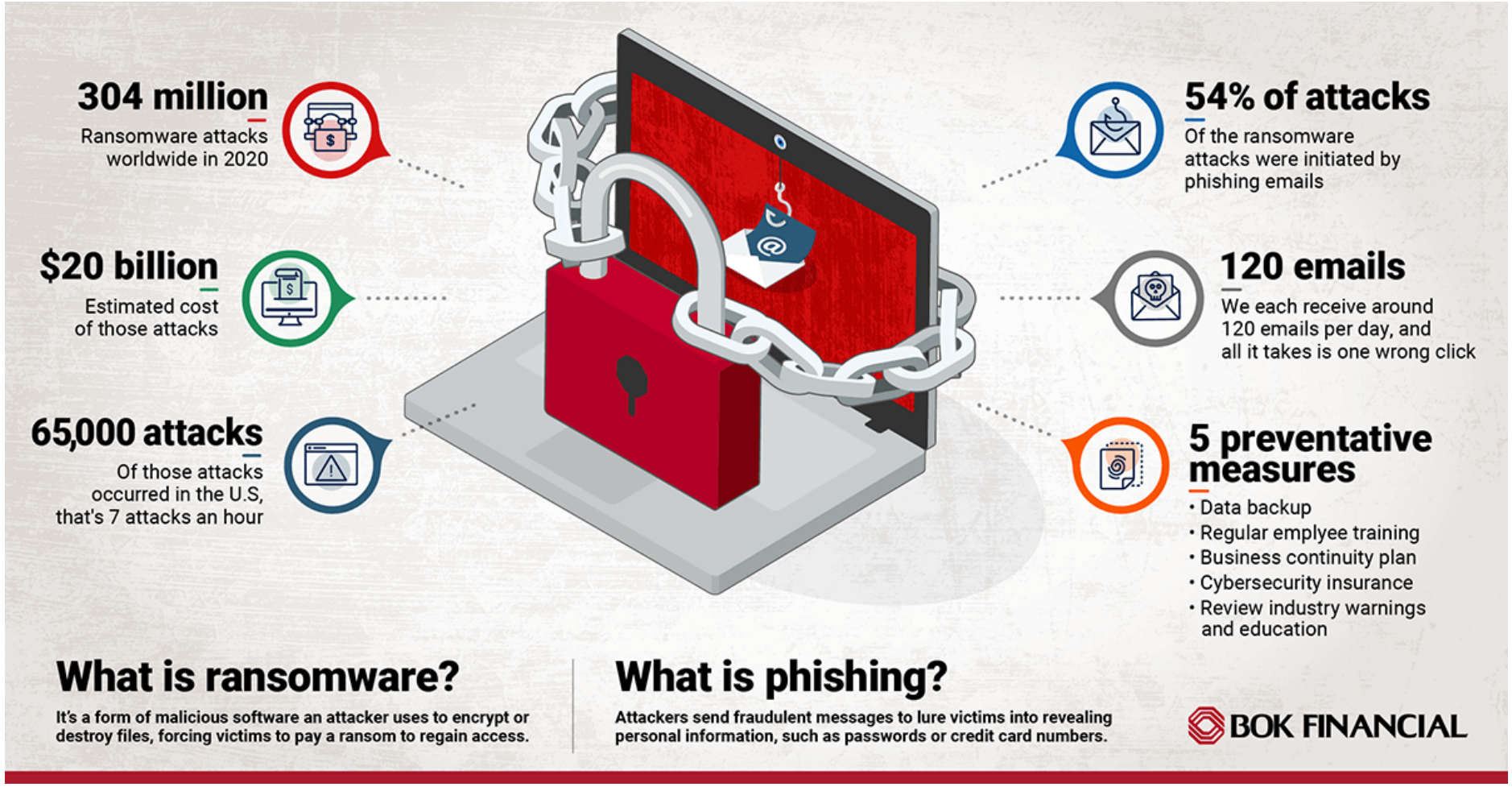
https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts

Ransomware Raas





Ransomware Stats



Ransomware Best Practices

- Eliminate or Secure RDP
- Offline Backups
- MFA
- Patch Management

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA22-040A

February 9, 2022

ACSC Australian Cyber Security Centre

National Cyber Security Centre
a part of GCHQ

2021 Trends Show Increased Globalized Threat of Ransomware

SUMMARY

In 2021, cybersecurity authorities in the United States,[1][2][3] Australia,[4] and the United Kingdom[5] observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally. The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors, including the Defense Industrial Base, Emergency Services, Food and Agriculture, Government Facilities, and Information Technology Sectors. The Australian Cyber Security Centre (ACSC) observed continued ransomware

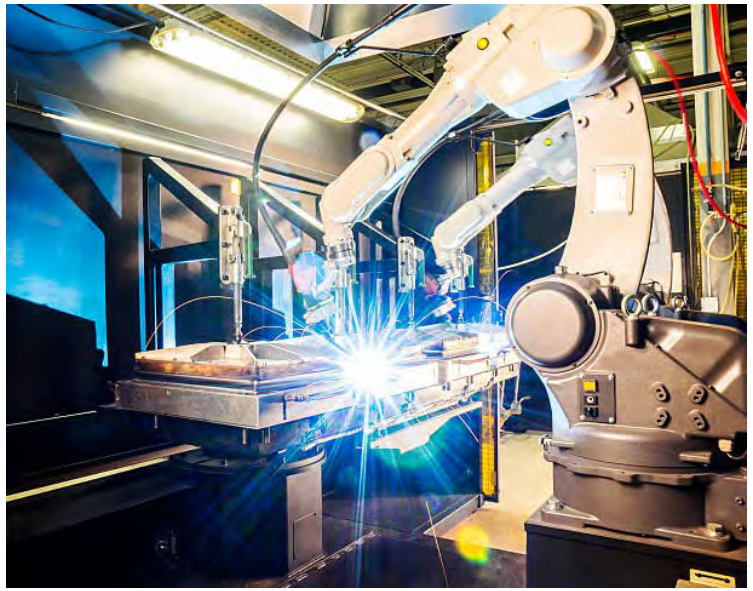
Immediate Actions You Can Take Now to Protect Against Ransomware:

- Update your operating system and software.
- Implement user training and phishing exercises to raise awareness about the risks of suspicious links and attachments.
- If you use Remote Desktop Protocol (RDP), secure and monitor it.
- Make an offline backup of your data.
- Use multifactor authentication (MFA).

Source

Aerospace Manufacturing

- Phishing email UPS shipment
- Ransomware Infection
- Took manufacturing systems offline
- Couldn’t print and sign a contract
- Costing $500K per day in loss revenue
- Took 7 days to regain partial operations
- Additional 7 days to restore fully
- Paid $400K in ransom, decryption too slow



SBS INSTITUTE

TAKEAWAYS

CIS Top 18 Cyber Controls

SBS INSTITUTE

CIS Controls™

Version 7: a prioritized set of actions to protect your organization and data from known cyber attack vectors.

CIS Controls V7 separates the controls into three distinct categories:

Basic:
Key controls which should be implemented in every organization for essential cyber defense readiness.

Foundational:
Technical best practices provide clear security benefits and are a smart move for any organization to implement.

Organizational:
These controls are more focused on people and processes involved in cybersecurity.

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

> "Start by taking care of the basics: build a solid cybersecurity foundation by implementing the [CIS Controls], especially application white-listing, standard secure configurations, reduction of administrative privileges and a quick patching process."

Zurich Insurance Group
Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures
Switzerland

NIST Cybersecurity Framework

SBS INSTITUTE

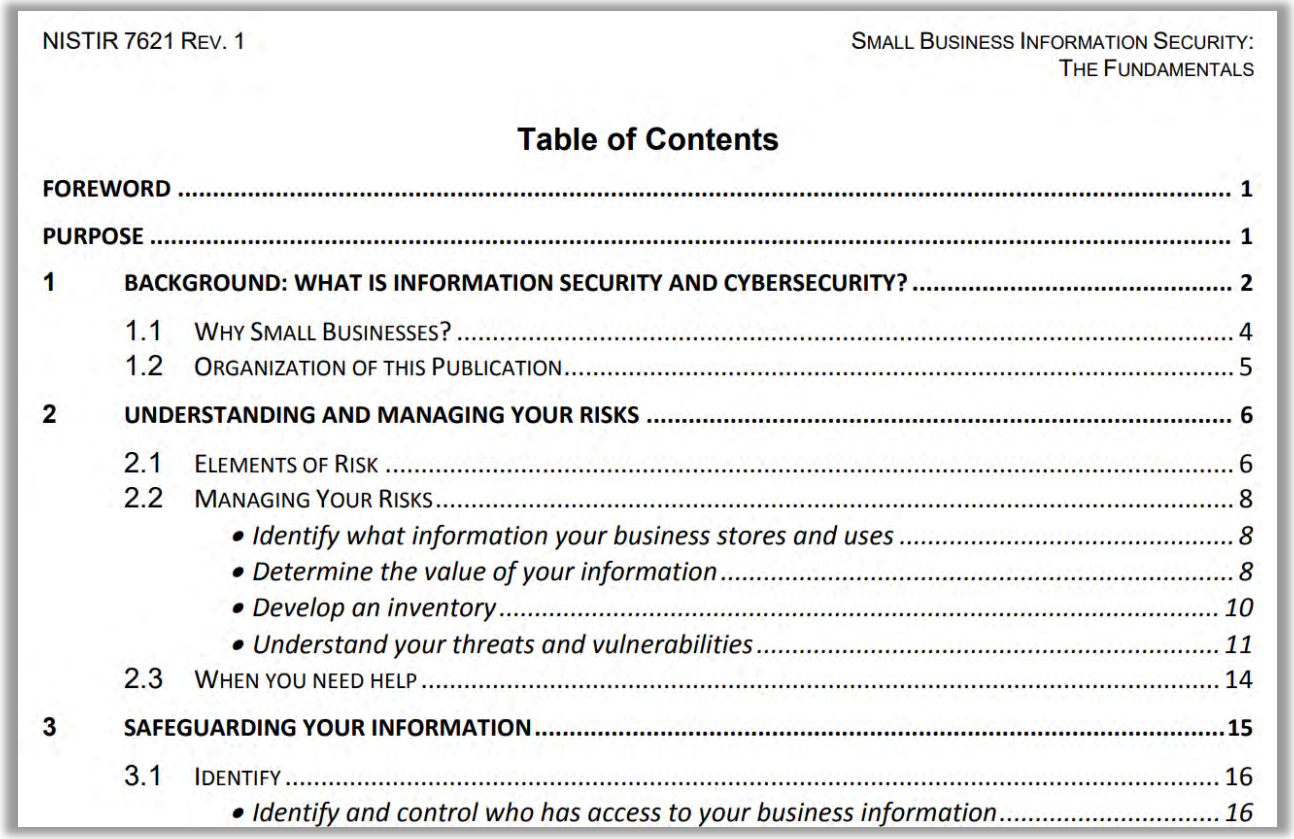
Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Source

NIST 7621

- Descriptive information
- Fundamentals of security
- Worksheets and examples



NISTIR 7621 REV. 1 — SMALL BUSINESS INFORMATION SECURITY: THE FUNDAMENTALS

Table of Contents

[Small Business Information Security: the Fundamentals (nist.gov)]

NIST 7621

- Require individual user accounts for each employee.
  - Hacker has access to more information
  - No accountability for user activity
  - Security compliance challenges

NIST 7621

- Limit employee access to data and information
  - The more access you give an employee, the more you risk giving to hacker
  - Use Need to Know access model
  - Data privacy concerns

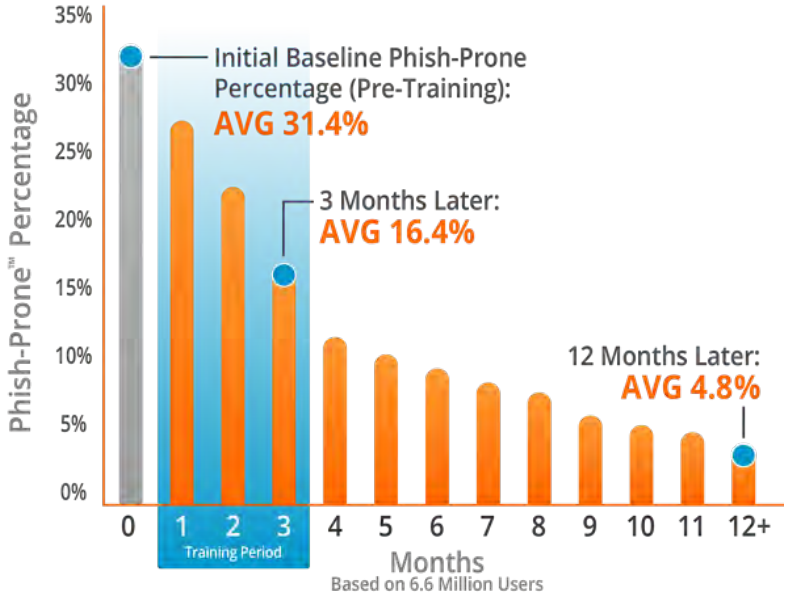
NIST 7621

- Patch your operating systems and applications
  - NOT just “Windows” but also Adobe, Office, Chrome, … **Anything**
  - System firmware
  - Don’t forget Firewalls and Networking equipment
  - At least monthly, consider **weekly**
  - Critical vulnerabilities must be patched in hours
  - Make backups before updating

NIST 7621

Train your employees

- Phishing #1 and #2 largest business risk



Source: 2021 KnowBe4 Phishing by Industry Benchmarking Report

Note: The initial Phish-Prone percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation.

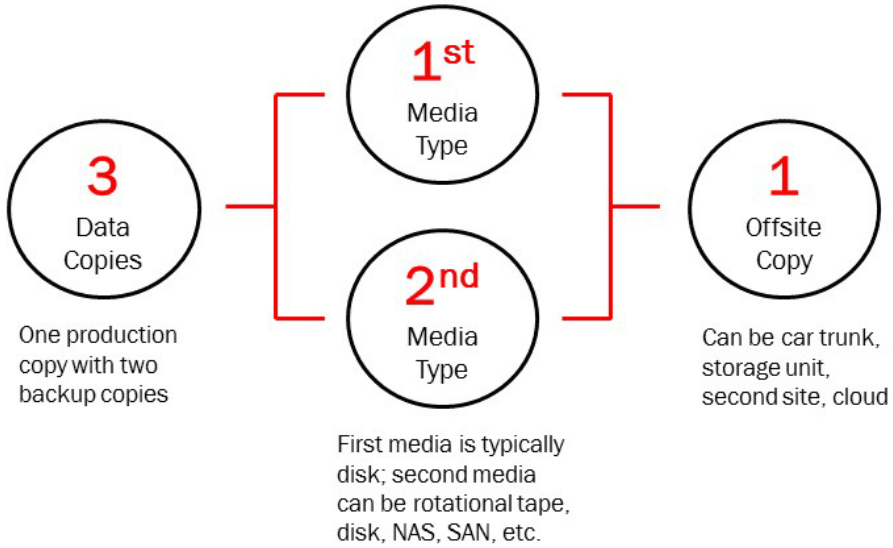
Subsequent time periods reflect Phish-Prone percentages for the subset of users who received training with the KnowBe4 console.

KnowBe4
Human error. Conquered.

NIST 7621

Make incremental backups of important business data/information

- Ensure they are complete and work. **Test.**
- Keep copies **offline** (Ransomware Proof)
- Make copies often. How much can you loose?
- Replication doesn't count.



NIST 7621

Use strong passwords

- Defaults – Change Them
- Reuse – Never Reuse
- Complexity – Make LONG

onelogin

1Password

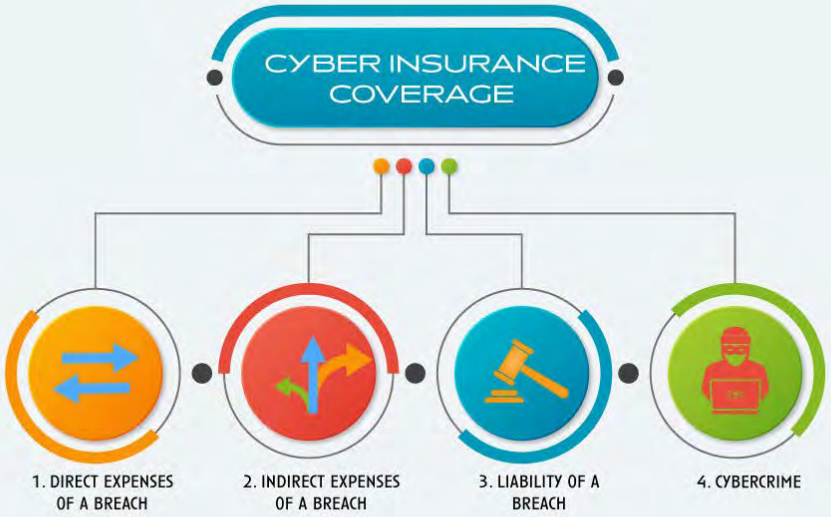
dashlane

LastPass

RoboForm

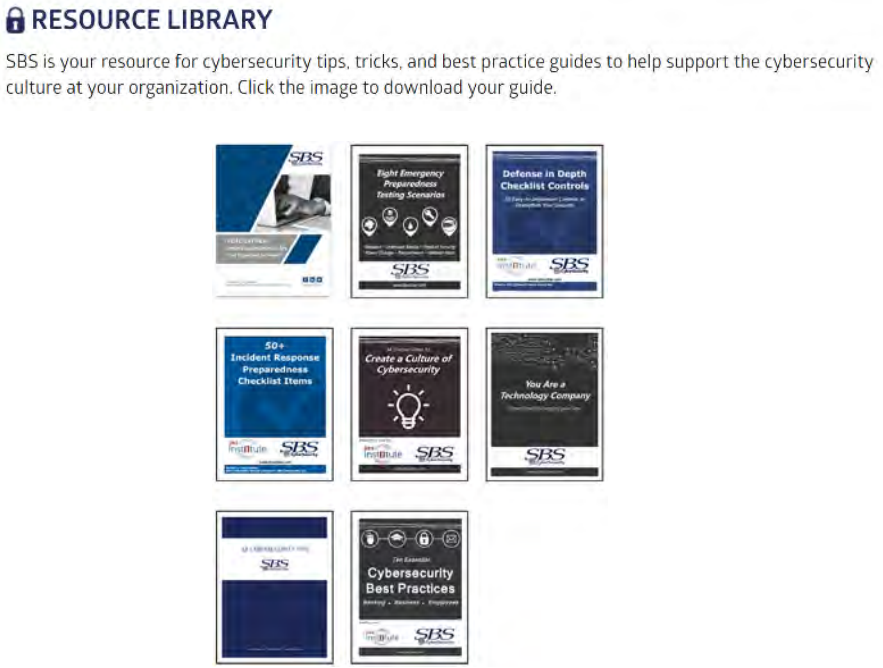
NIST 7621

Consider cyber insurance



Be Prepared – Incident Response

- Consider a tabletop test – roleplay ransomware
  - SBS Testing Example – various testing scenarios
  - Testing video - Successful Tabletop Testing Strategies
- Document a Plan
- Learn from other businesses incidents



We Want To Hear From You!

QUESTIONS?

If you have any questions following the webinar, please contact your local Bank First office. The webinar recording will be sent following the webinar.

YOU COULD WIN A $100 VISA® GIFT CARD!

Following the live webinar, all attendees will have the opportunity to complete a short survey. Those who complete it will automatically be entered to win a $100 Visa gift card! A winner will be randomly chosen from all survey responders and be contacted via email by Tuesday, April 5, 2022. The survey will be prompted at the end of the webinar and will be included in the follow-up email.

SBS CyberSecurity

www.sbscyber.com

BankFirst

www.bankfirst.com | MEMBER FDIC
EQUAL HOUSING LENDER

THANK YOU FOR JOINING US!