HillSouth

iT solutions.

Security Event

A REAL TIME DISCUSSION

About Us

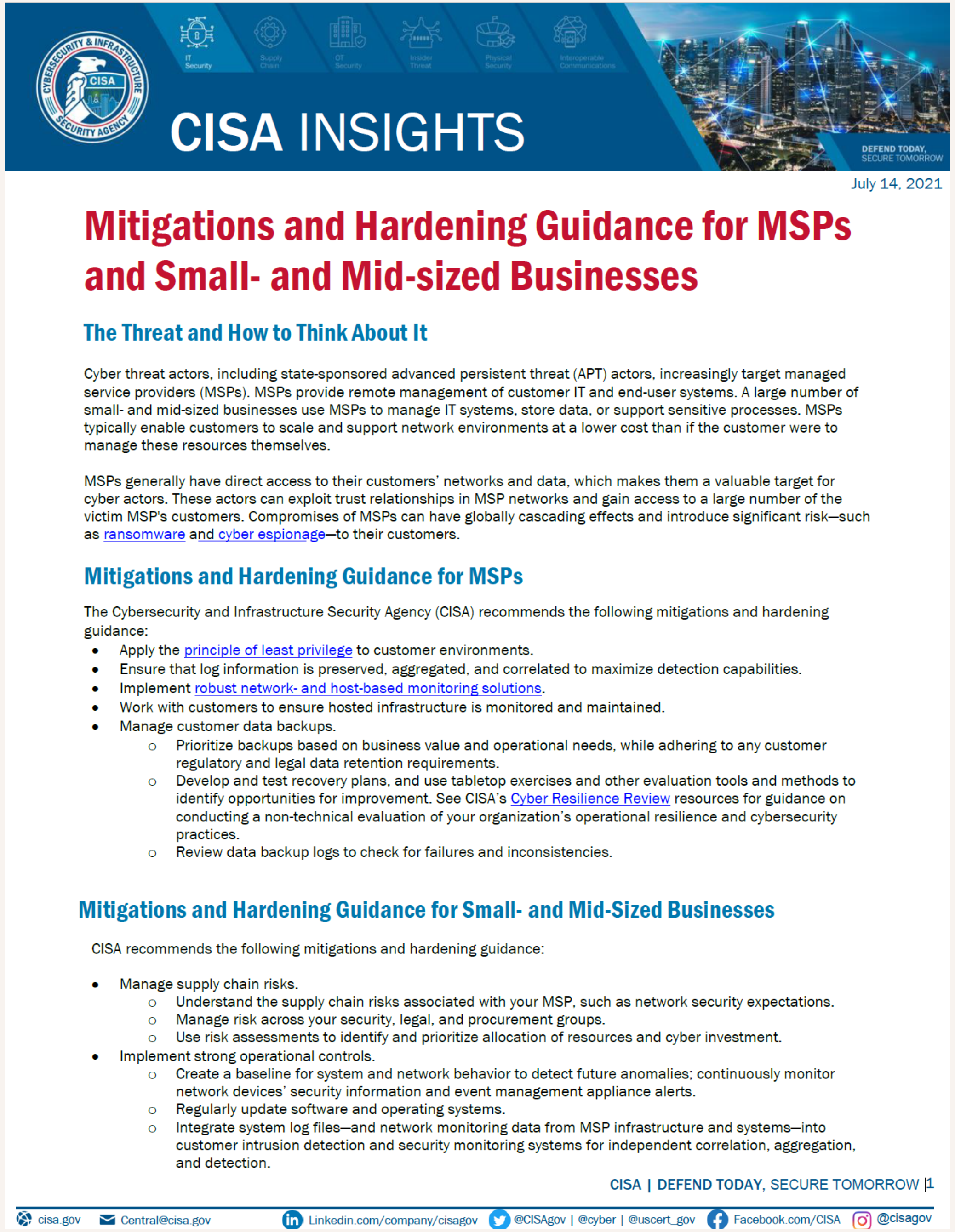
IT professionals working in the IT Managed Services Provider (MSP) space to deliver value to clients

Infamous Quote

There are two types of companies in this world: those that have been hacked and those that will be.

-SC Governor Nikki Haley
Discussing SC DOR breach of 3.8 million identities

POWER LUNCH
GLOBAL RANSOMWARE ATTACK
1,500 COMPANIES INVOLVED



CISA INSIGHTS

DEFEND TODAY, SECURE TOMORROW

July 14, 2021

Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses

The Threat and How to Think About It

Cyber threat actors, including state-sponsored advanced persistent threat (APT) actors, increasingly target managed service providers (MSPs). MSPs provide remote management of customer IT and end-user systems. A large number of small- and mid-sized businesses use MSPs to manage IT systems, store data, or support sensitive processes. MSPs typically enable customers to scale and support network environments at a lower cost than if the customer were to manage these resources themselves.

MSPs generally have direct access to their customers' networks and data, which makes them a valuable target for cyber actors. These actors can exploit trust relationships in MSP networks and gain access to a large number of the victim MSP's customers. Compromises of MSPs can have globally cascading effects and introduce significant risk—such as ransomware and cyber espionage—to their customers.

Mitigations and Hardening Guidance for MSPs

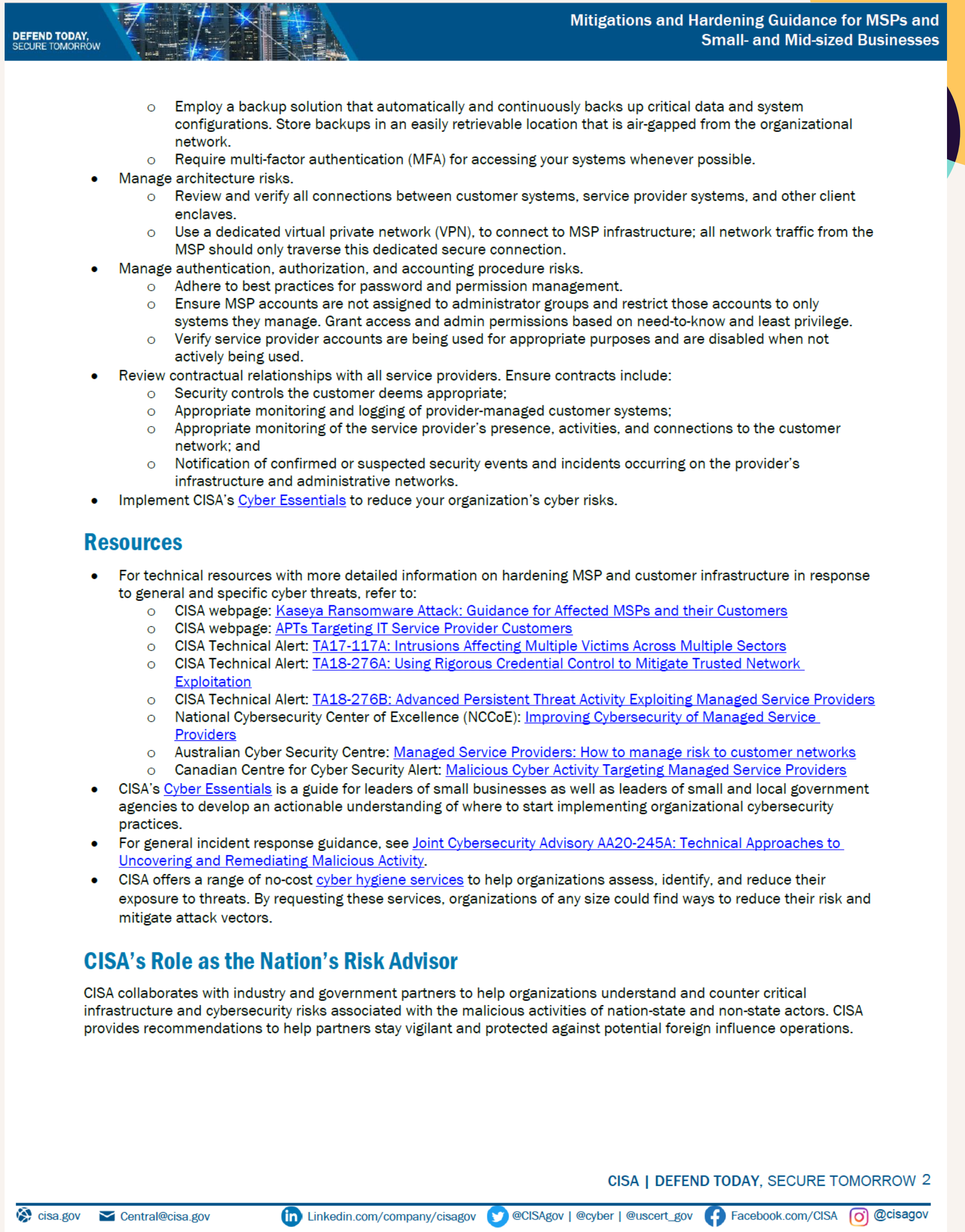
The Cybersecurity and Infrastructure Security Agency (CISA) recommends the following mitigations and hardening guidance:

- Apply the principle of least privilege to customer environments.
- Ensure that log information is preserved, aggregated, and correlated to maximize detection capabilities.
- Implement robust network- and host-based monitoring solutions.
- Work with customers to ensure hosted infrastructure is monitored and maintained.
- Manage customer data backups.
  - Prioritize backups based on business value and operational needs, while adhering to any customer regulatory and legal data retention requirements.
  - Develop and test recovery plans, and use tabletop exercises and other evaluation tools and methods to identify opportunities for improvement. See CISA's Cyber Resilience Review resources for guidance on conducting a non-technical evaluation of your organization's operational resilience and cybersecurity practices.
  - Review data backup logs to check for failures and inconsistencies.

Mitigations and Hardening Guidance for Small- and Mid-Sized Businesses

CISA recommends the following mitigations and hardening guidance:

- Manage supply chain risks.
  - Understand the supply chain risks associated with your MSP, such as network security expectations.
  - Manage risk across your security, legal, and procurement groups.
  - Use risk assessments to identify and prioritize allocation of resources and cyber investment.
- Implement strong operational controls.
  - Create a baseline for system and network behavior to detect future anomalies; continuously monitor network devices' security information and event management appliance alerts.
  - Regularly update software and operating systems.
  - Integrate system log files—and network monitoring data from MSP infrastructure and systems—into customer intrusion detection and security monitoring systems for independent correlation, aggregation, and detection.



  - Employ a backup solution that automatically and continuously backs up critical data and system configurations. Store backups in an easily retrievable location that is air-gapped from the organizational network.
  - Require multi-factor authentication (MFA) for accessing your systems whenever possible.
- Manage architecture risks.
  - Review and verify all connections between customer systems, service provider systems, and other client enclaves.
  - Use a dedicated virtual private network (VPN), to connect to MSP infrastructure; all network traffic from the MSP should only traverse this dedicated secure connection.
- Manage authentication, authorization, and accounting procedure risks.
  - Adhere to best practices for password and permission management.
  - Ensure MSP accounts are not assigned to administrator groups and restrict those accounts to only systems they manage. Grant access and admin permissions based on need-to-know and least privilege.
  - Verify service provider accounts are being used for appropriate purposes and are disabled when not actively being used.
- Review contractual relationships with all service providers. Ensure contracts include:
  - Security controls the customer deems appropriate;
  - Appropriate monitoring and logging of provider-managed customer systems;
  - Appropriate monitoring of the service provider's presence, activities, and connections to the customer network; and
  - Notification of confirmed or suspected security events and incidents occurring on the provider's infrastructure and administrative networks.
- Implement CISA's Cyber Essentials to reduce your organization's cyber risks.

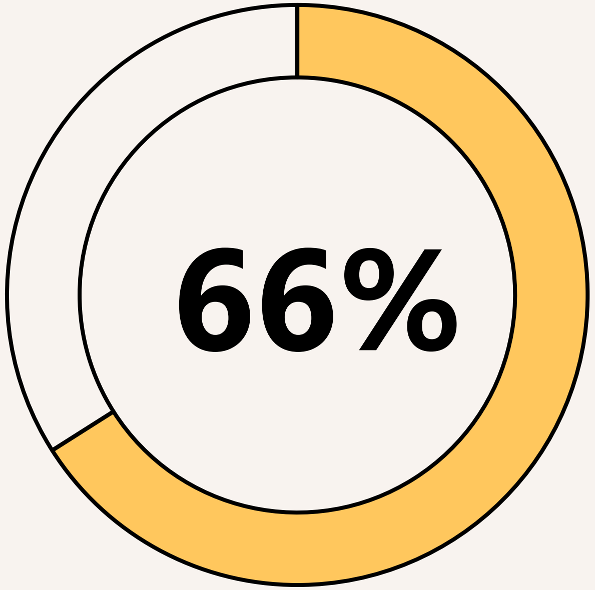
Resources

- For technical resources with more detailed information on hardening MSP and customer infrastructure in response to general and specific cyber threats, refer to:
  - CISA webpage: Kaseya Ransomware Attack: Guidance for Affected MSPs and their Customers
  - CISA webpage: APTs Targeting IT Service Provider Customers
  - CISA Technical Alert: TA17-117A: Intrusions Affecting Multiple Victims Across Multiple Sectors
  - CISA Technical Alert: TA18-276A: Using Rigorous Credential Control to Mitigate Trusted Network Exploitation
  - CISA Technical Alert: TA18-276B: Advanced Persistent Threat Activity Exploiting Managed Service Providers
  - National Cybersecurity Center of Excellence (NCCoE): Improving Cybersecurity of Managed Service Providers
  - Australian Cyber Security Centre: Managed Service Providers: How to manage risk to customer networks
  - Canadian Centre for Cyber Security Alert: Malicious Cyber Activity Targeting Managed Service Providers
- CISA's Cyber Essentials is a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices.
- For general incident response guidance, see Joint Cybersecurity Advisory AA20-245A: Technical Approaches to Uncovering and Remediating Malicious Activity.
- CISA offers a range of no-cost cyber hygiene services to help organizations assess, identify, and reduce their exposure to threats. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

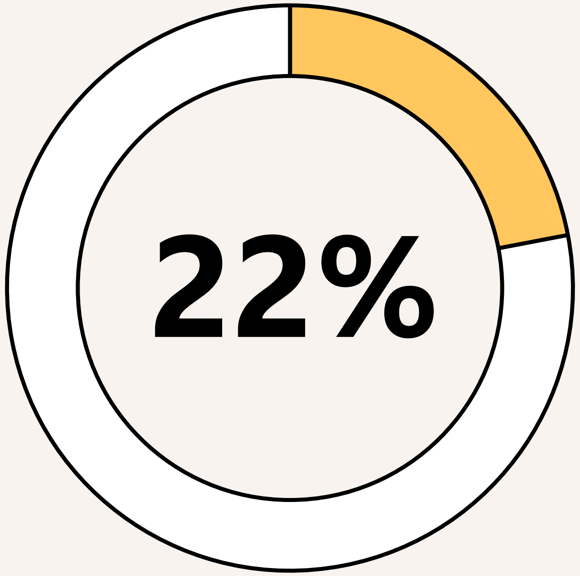
CISA's Role as the Nation's Risk Advisor

CISA collaborates with industry and government partners to help organizations understand and counter critical infrastructure and cybersecurity risks associated with the malicious activities of nation-state and non-state actors. CISA provides recommendations to help partners stay vigilant and protected against potential foreign influence operations.

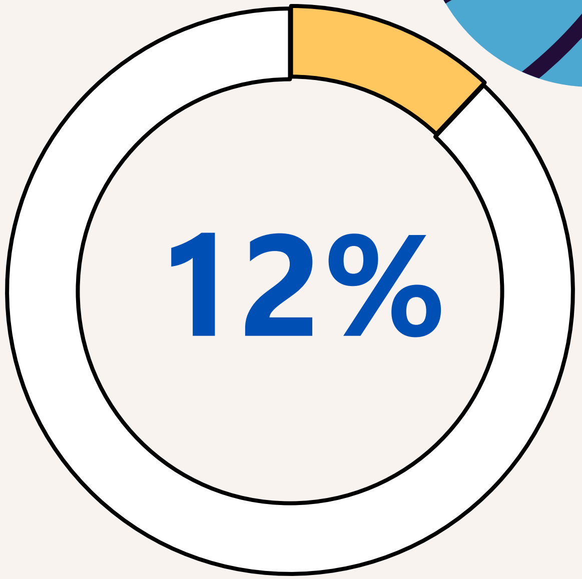
Ransomware in Government



Hit by ransomware in the last year

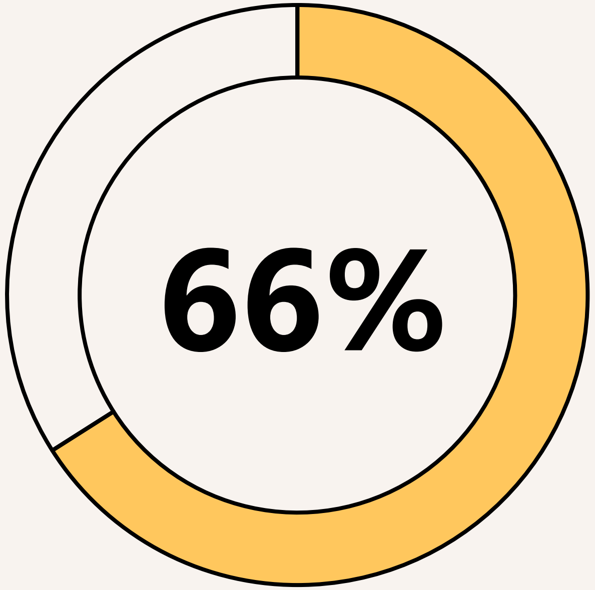


Not hit by ransomware in the last year, but expect to be hit in the future

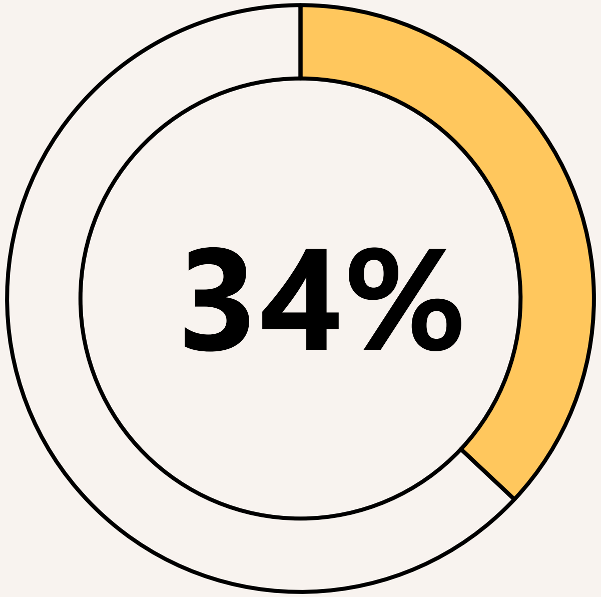


Not hit by ransomware in the last year, and don’t expect to be hit in the future

Ransomware in Government



2021



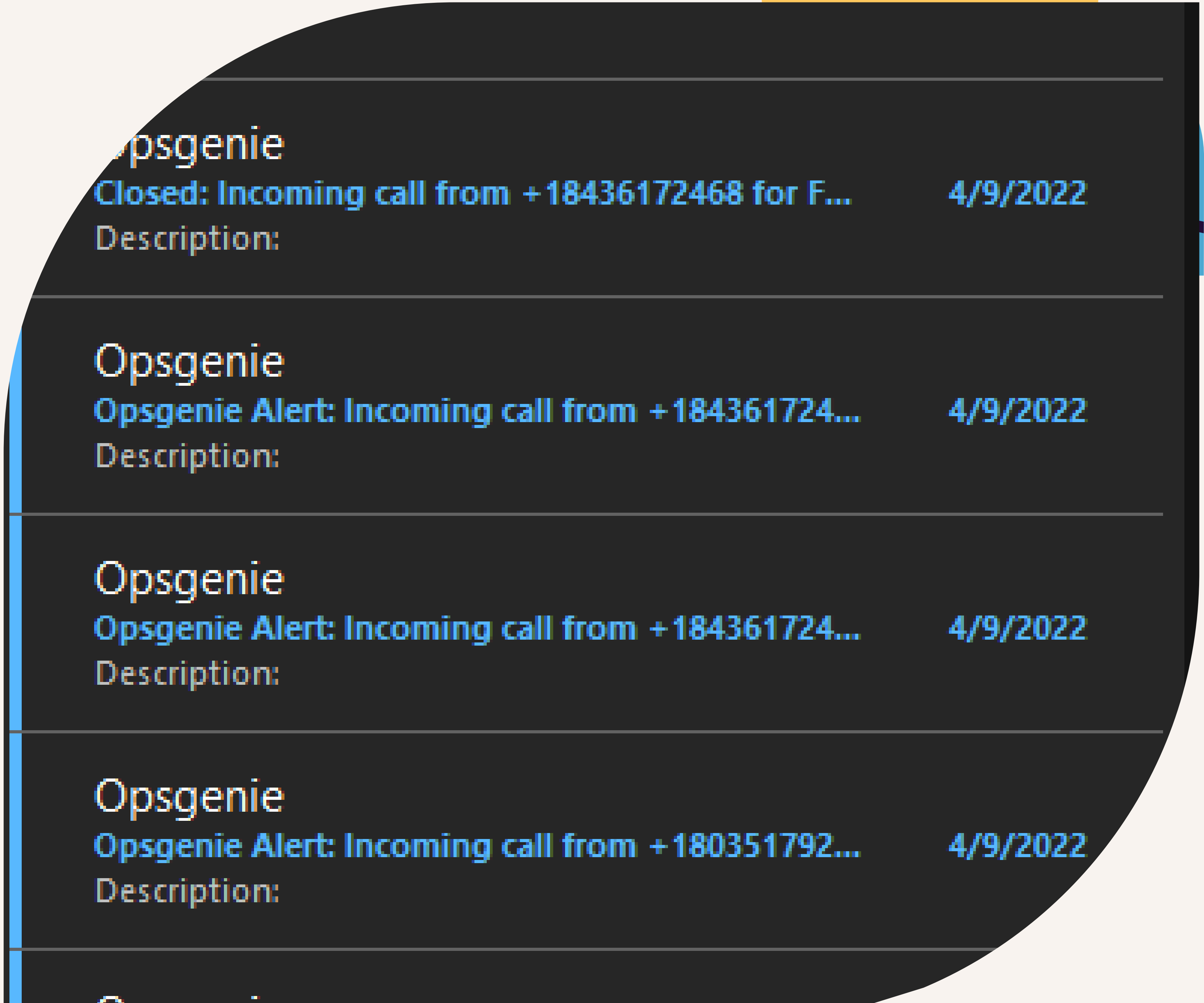
2020

01

HillSouth Event

A timeline of events

Saturday, April 9, 2022



psgenie
Closed: Incoming call from +18436172468 for F... 4/9/2022
Description:

Opsgenie
Opsgenie Alert: Incoming call from +184361724... 4/9/2022
Description:

Opsgenie
Opsgenie Alert: Incoming call from +184361724... 4/9/2022
Description:

Opsgenie
Opsgenie Alert: Incoming call from +180351792... 4/9/2022
Description:

What Happened?

Important files on your network was ENCRYPTED and now they have "4daaffb" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your network was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, bank statements.
- Manufacturing documents including: datagrams, schemas, drawings in solidworks format
- And more...

Samples are available on your personal web page linked below.

>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> What should I do next?

1) Download and install Tor Browser from: https://torproject.org/

Weekend Priorities

Restoration

Repair as remotely as possible

Restore servers from backups

Secure Systems

Stay ahead of the hackers

Remove ransomware software

Determine what other tools have been deployed

Communications

Contact customers proactively & reactively respond

Scripting against our attackers

ScreenConnect Client (2d26cc88d1fa81eb)
ScreenConnect Client (461c93936157c3a2)
ScreenConnect Client (3d9ea22063498b54)
ScreenConnect Client (461c93936157c3a2)
ScreenConnect Client (2d26cc88d1fa81eb)
ScreenConnect Client (461c93936157c3a2)
ScreenConnect Client (3d9ea22063498b54)
ScreenConnect Client (3302dd200fcf6a0e)
ScreenConnect Client (6ef3ee57ab8b50a6)
ScreenConnect Client (14131755237f3ae1)
ScreenConnect Client (1dce768ee06e8f0d)
ScreenConnect Client (adf02e34cba839d2)
tsd-setup.exe

Sunday, April 11, 2022

Vectors

- Scripts

Restoration

Report to IC3

Initial Vendor Response

Quick Stats

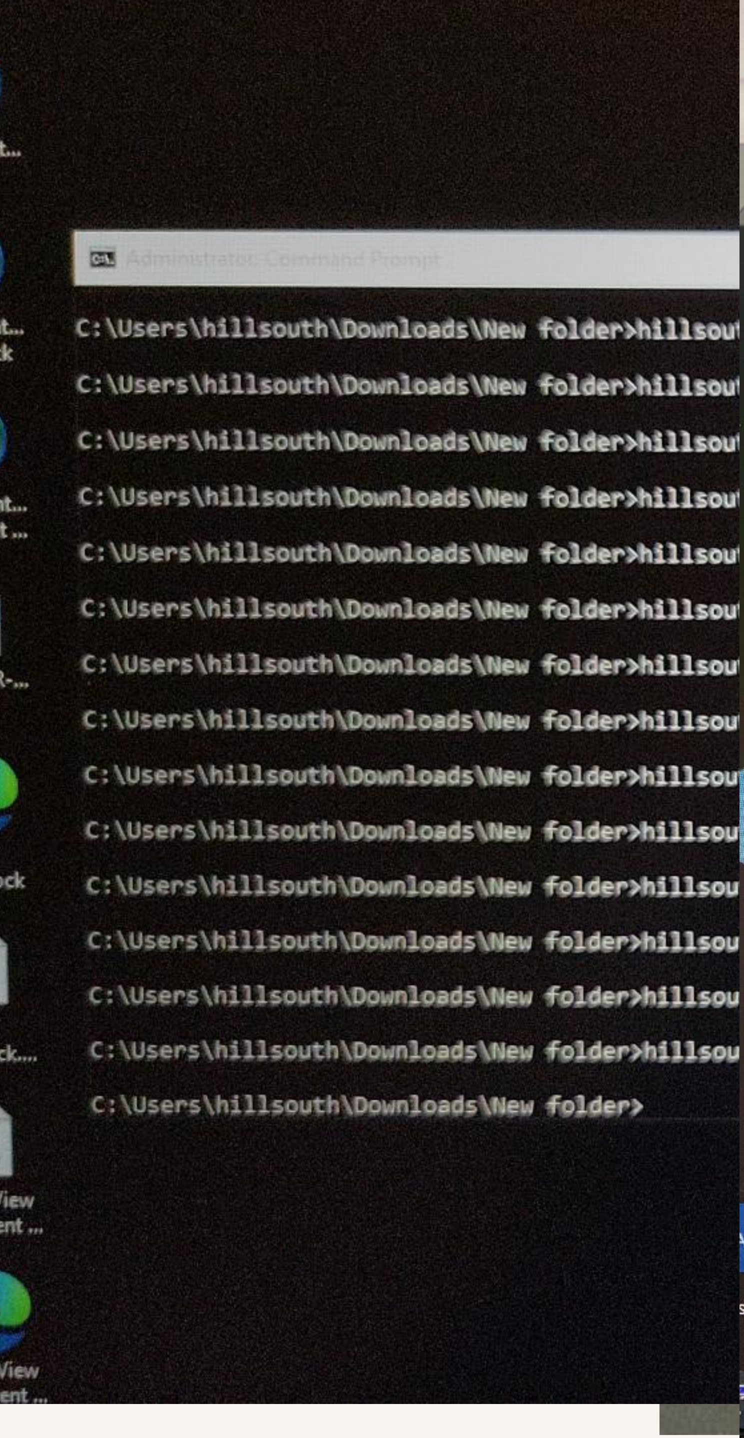
1700

Workstations connected and managed

180 servers

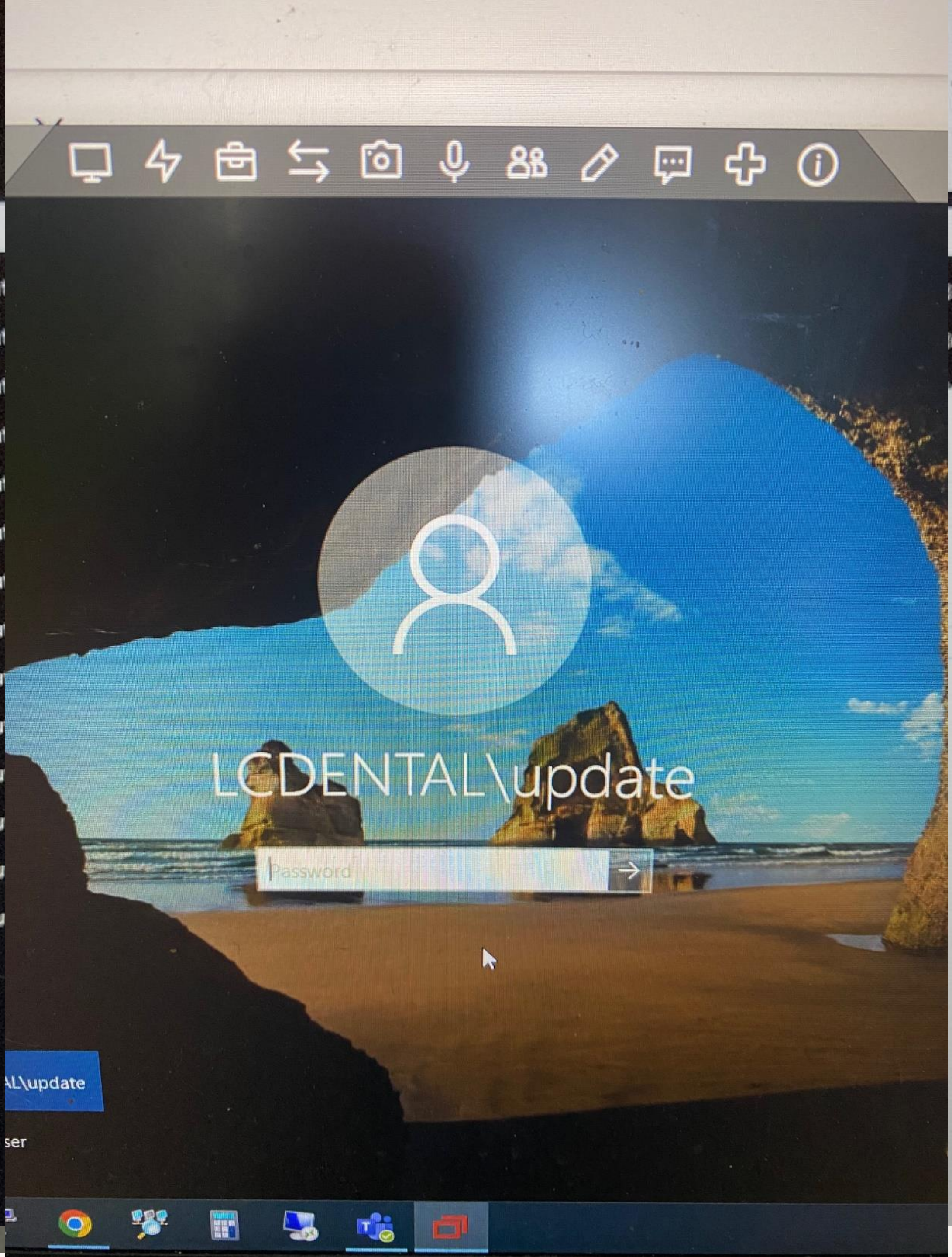
75%

Inside HillSouth's datacenter



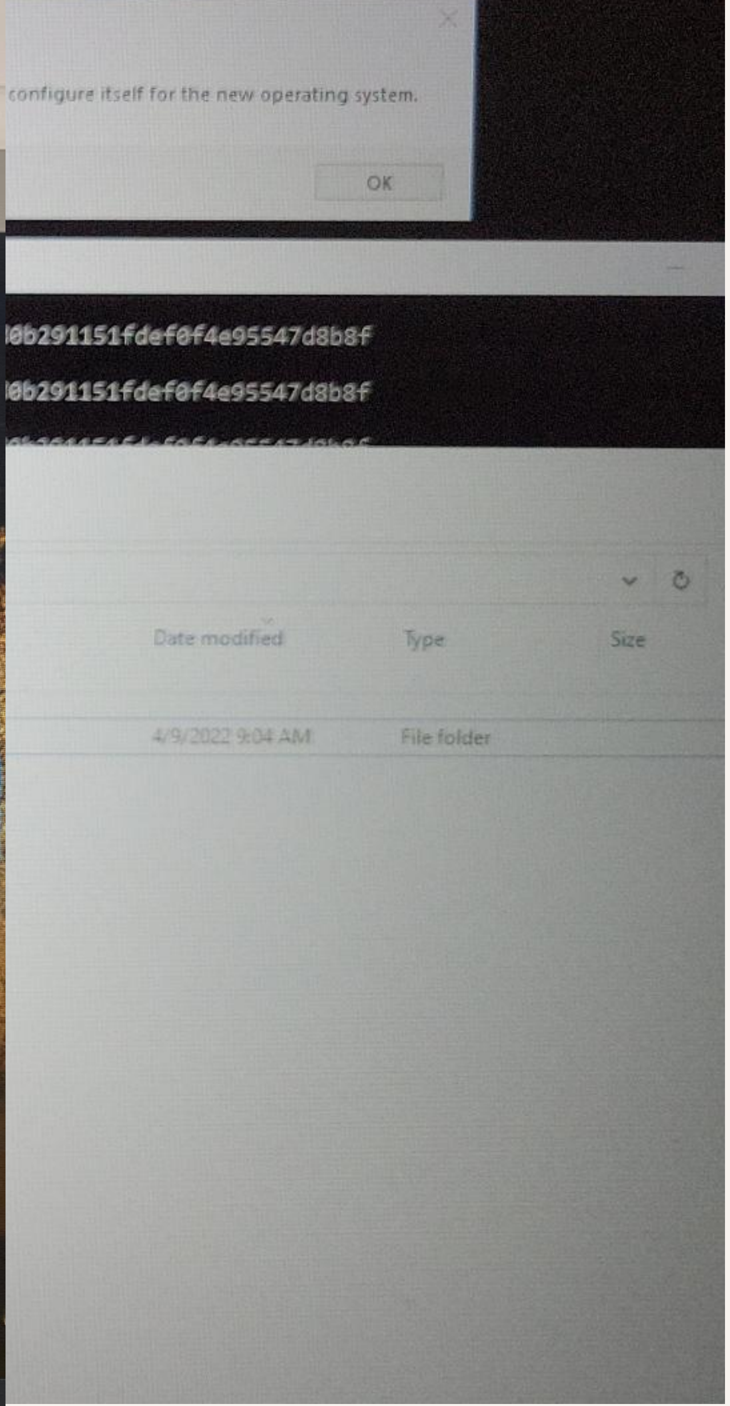
Administrator: Command Prompt

```
C:\Users\hillsouth\Downloads\New folder>hillsou
C:\Users\hillsouth\Downloads\New folder>hillsou
C:\Users\hillsouth\Downloads\New folder>hillsou
C:\Users\hillsouth\Downloads\New folder>hillsou
C:\Users\hillsouth\Downloads\New folder>hillsou
C:\Users\hillsouth\Downloads\New folder>hillsou
C:\Users\hillsouth\Downloads\New folder>hillsou
C:\Users\hillsouth\Downloads\New folder>hillsou
C:\Users\hillsouth\Downloads\New folder>hillsou
C:\Users\hillsouth\Downloads\New folder>hillsou
C:\Users\hillsouth\Downloads\New folder>hillsou
C:\Users\hillsouth\Downloads\New folder>hillsou
C:\Users\hillsouth\Downloads\New folder>hillsou
C:\Users\hillsouth\Downloads\New folder>hillsou
C:\Users\hillsouth\Downloads\New folder>
```



LCDENTAL\update

Password

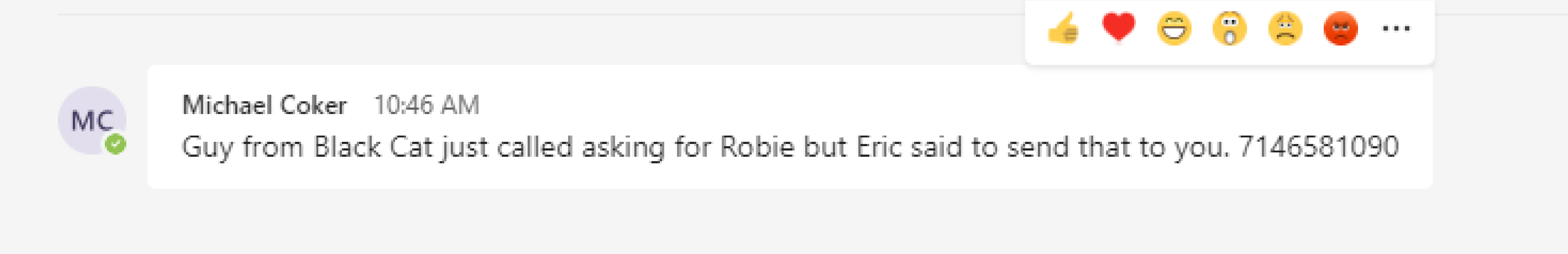


configure itself for the new operating system.

```
0b291151fdef0f4e95547d8b8f
0b291151fdef0f4e95547d8b8f
```

	Date modified	Type	Size
	4/9/2022 9:04 AM	File folder	

Tuesday, April 12, 2022



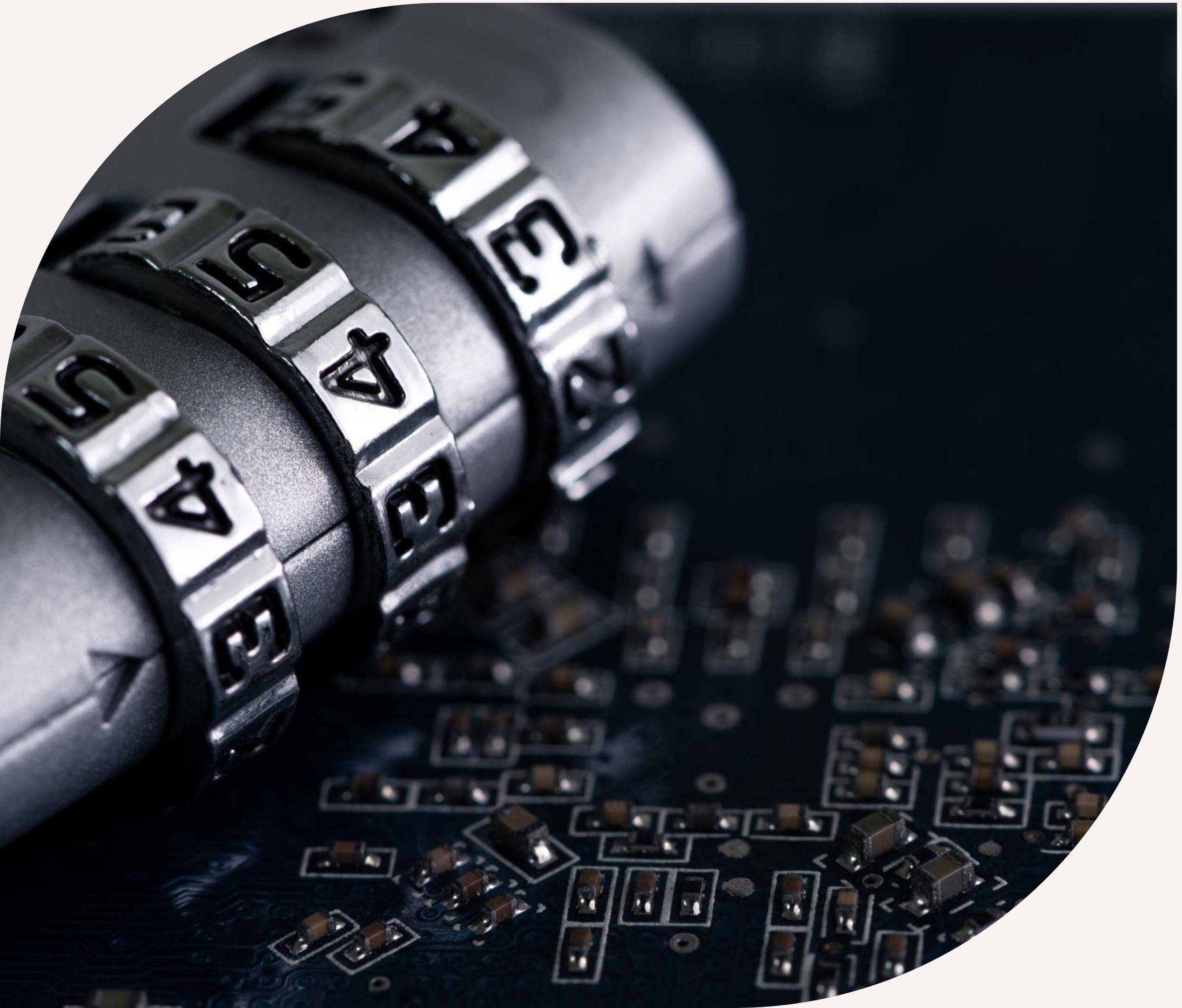
Michael Coker 10:46 AM

Guy from Black Cat just called asking for Robie but Eric said to send that to you. 7146581090

Friday, April 15, 2022

DDoS

Monday, April 18, 2022



Client E-Mail MFA

02 Response to Event

Who, what, when

The Cyber Response Team

MC
Mullen Coughlin
KROLL
COVEWARE
South Carolina SLED Law Enforcement Division 1947
Department of Justice Federal Bureau of Investigation

Mullen Coughlin

Cyber privacy attorneys
Project managers

Kroll

Cyber forensic auditors

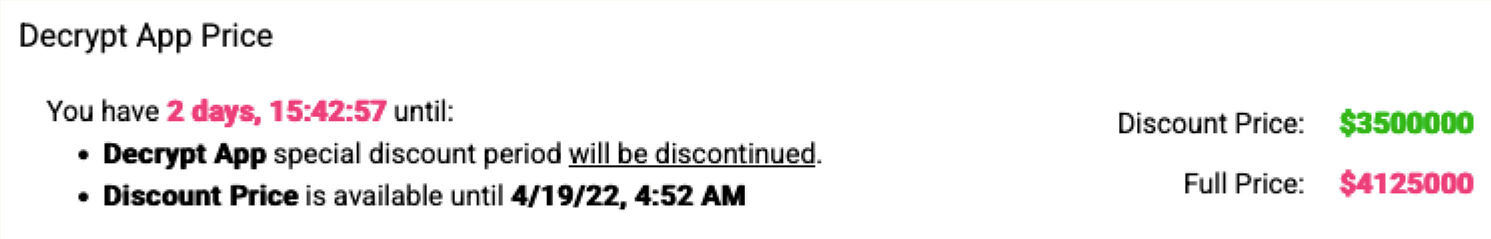
CoveWare

Cyber ransom negotiation experts

Law Enforcement

State & Federal interest exists in all levels of cybercrime

COVEWARE



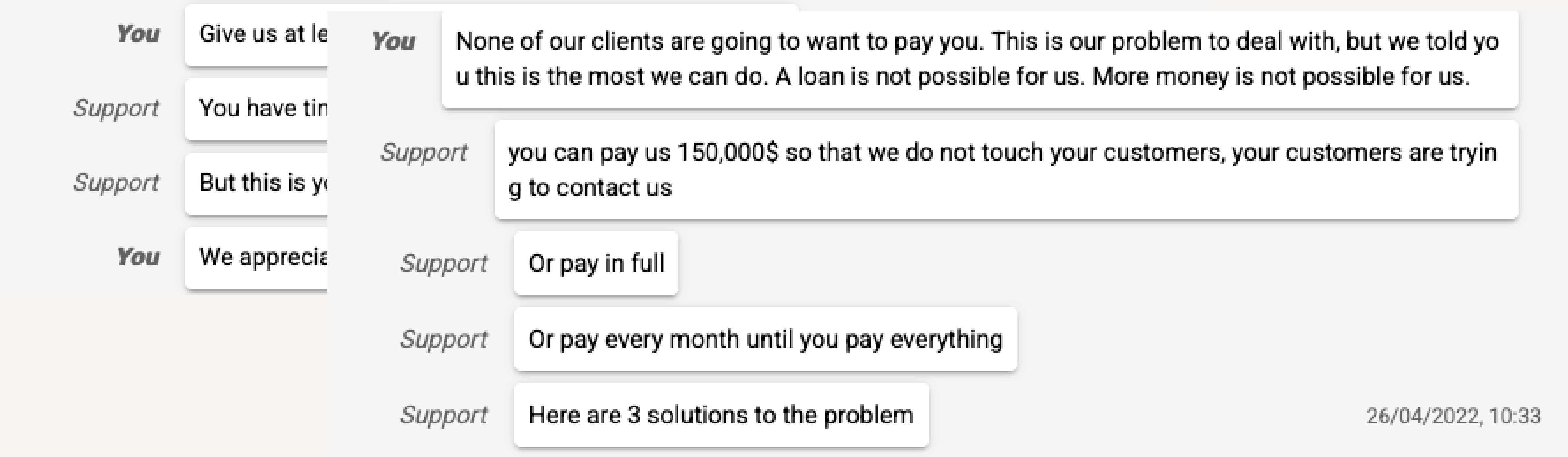
Decrypt App Price

You have 2 days, 15:42:57 until:

- **Decrypt App** special discount period will be discontinued.
- **Discount Price** is available until **4/19/22, 4:52 AM**

Discount Price: $3500000

Full Price: $4125000



You Give us at le

Support You have tin

Support But this is y

You We apprecia

You None of our clients are going to want to pay you. This is our problem to deal with, but we told yo u this is the most we can do. A loan is not possible for us. More money is not possible for us.

Support you can pay us 150,000$ so that we do not touch your customers, your customers are tryin g to contact us

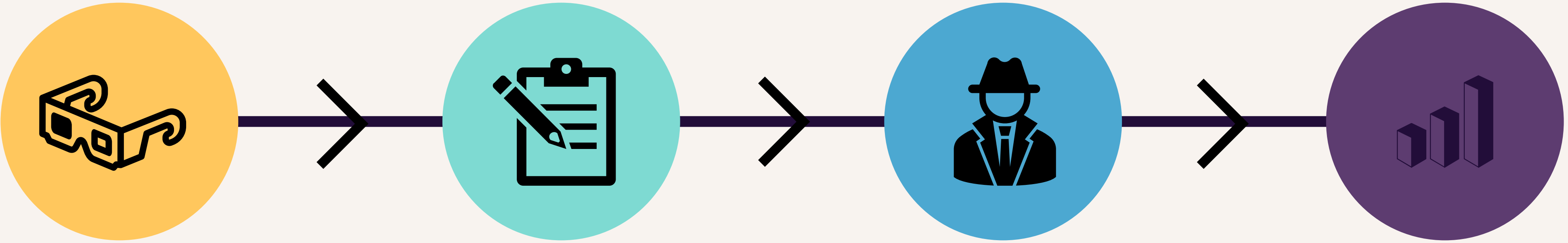
Support Or pay in full

Support Or pay every month until you pay everything

Support Here are 3 solutions to the problem

26/04/2022, 10:33

KROLL



Additional Eyes

We deployed Kroll’s utilities across our enterprise & clients’

Alerts

We triaged alerts together looking for suspicious activity

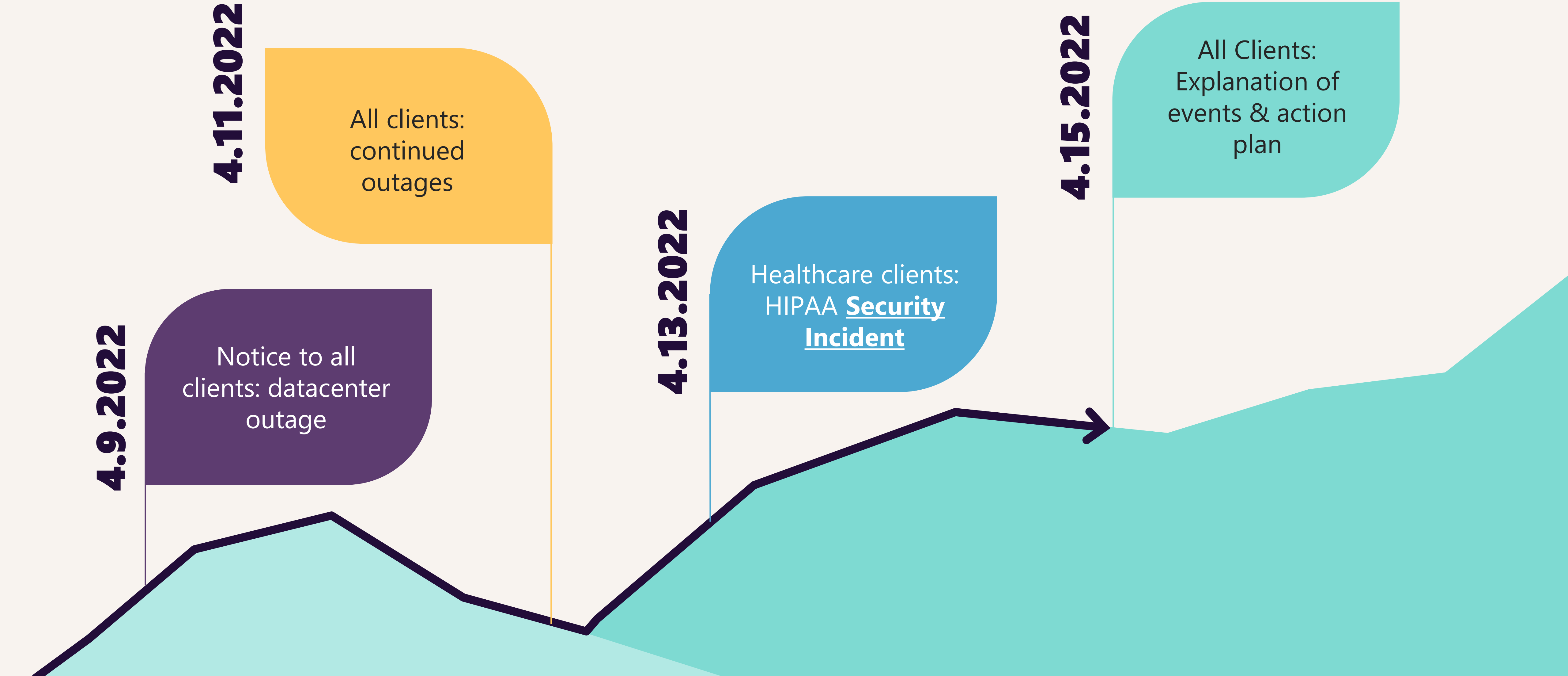
Intelligence

Massive amounts of data were transmitted

Analysis

Final report sent to our interested clients

Initial Timeline of Notifications



4.9.2022

Notice to all clients: datacenter outage

4.11.2022

All clients: continued outages

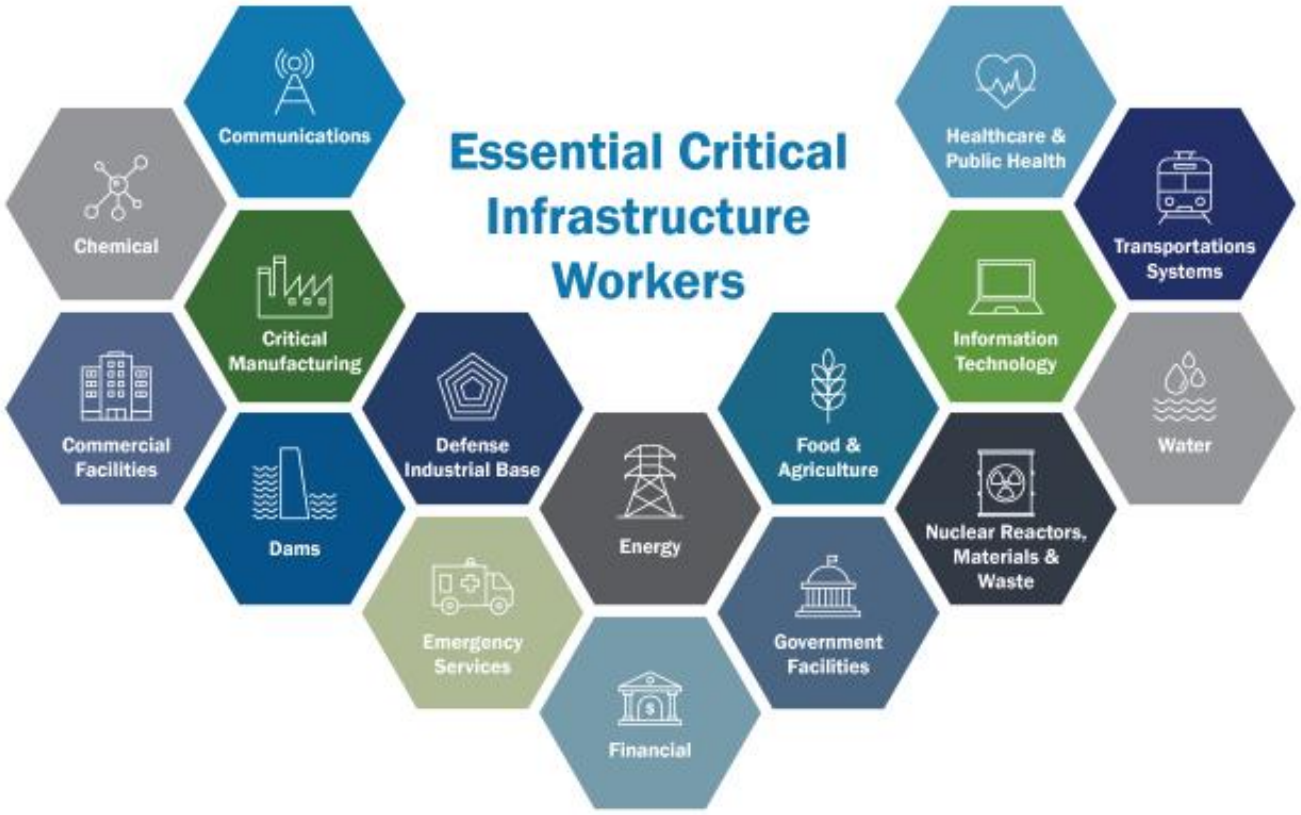
4.13.2022

Healthcare clients: HIPAA **Security Incident**

4.15.2022

All Clients: Explanation of events & action plan

Cyber Crime & Law Enforcement

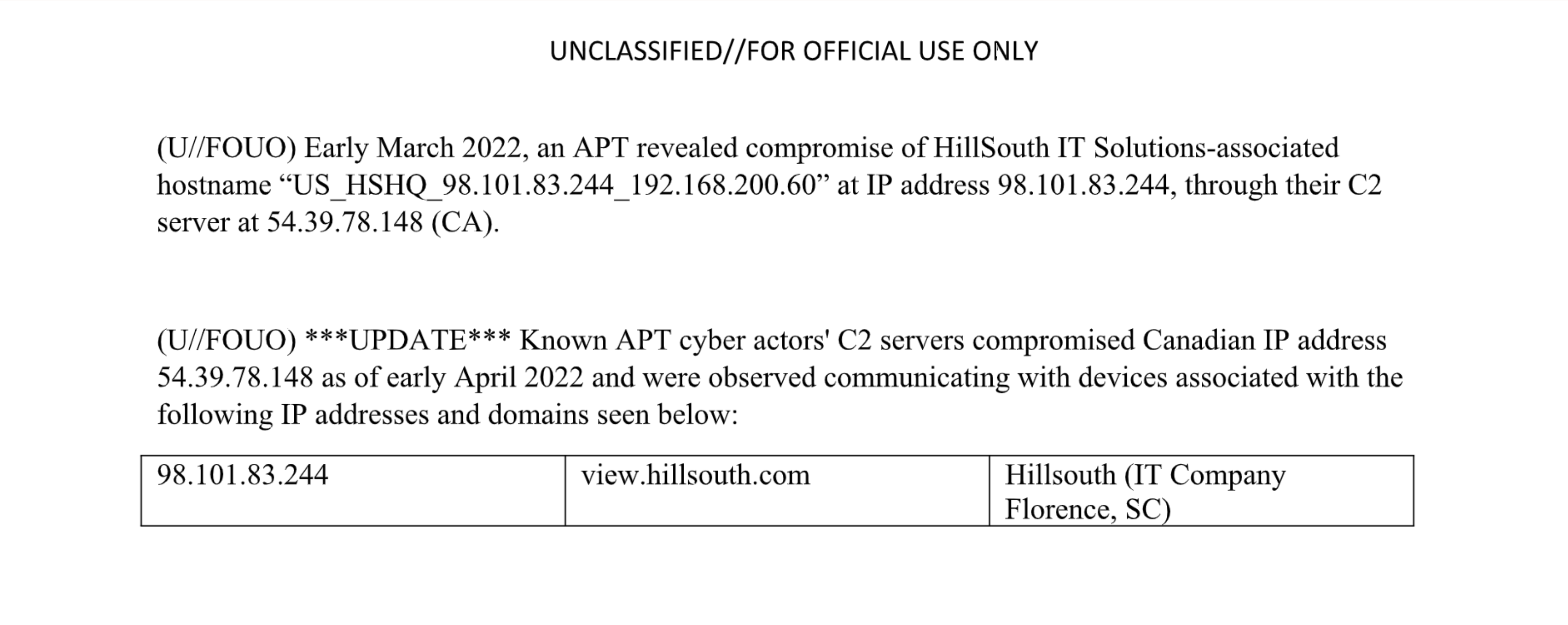


Essential Critical Infrastructure Workers

cisa.gov

5.20.2022

CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY



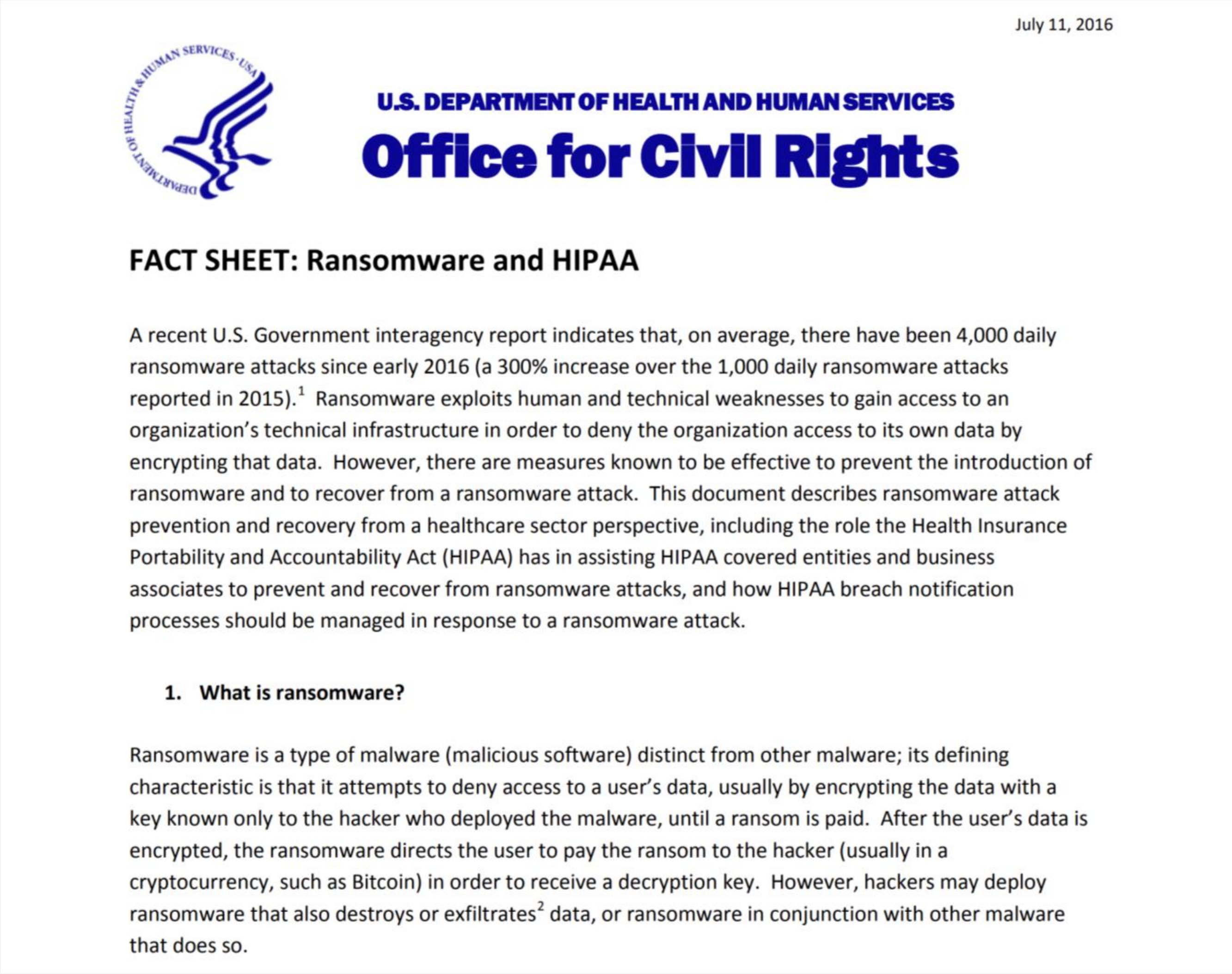
UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U//FOUO) Early March 2022, an APT revealed compromise of HillSouth IT Solutions-associated hostname "US_HSHQ_98.101.83.244_192.168.200.60" at IP address 98.101.83.244, through their C2 server at 54.39.78.148 (CA).

(U//FOUO) ***UPDATE*** Known APT cyber actors' C2 servers compromised Canadian IP address 54.39.78.148 as of early April 2022 and were observed communicating with devices associated with the following IP addresses and domains seen below:

98.101.83.244	view.hillsouth.com	Hillsouth (IT Company Florence, SC)

HIPAA Considerations



July 11, 2016

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office for Civil Rights

FACT SHEET: Ransomware and HIPAA

A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015).[1] Ransomware exploits human and technical weaknesses to gain access to an organization's technical infrastructure in order to deny the organization access to its own data by encrypting that data. However, there are measures known to be effective to prevent the introduction of ransomware and to recover from a ransomware attack. This document describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack.

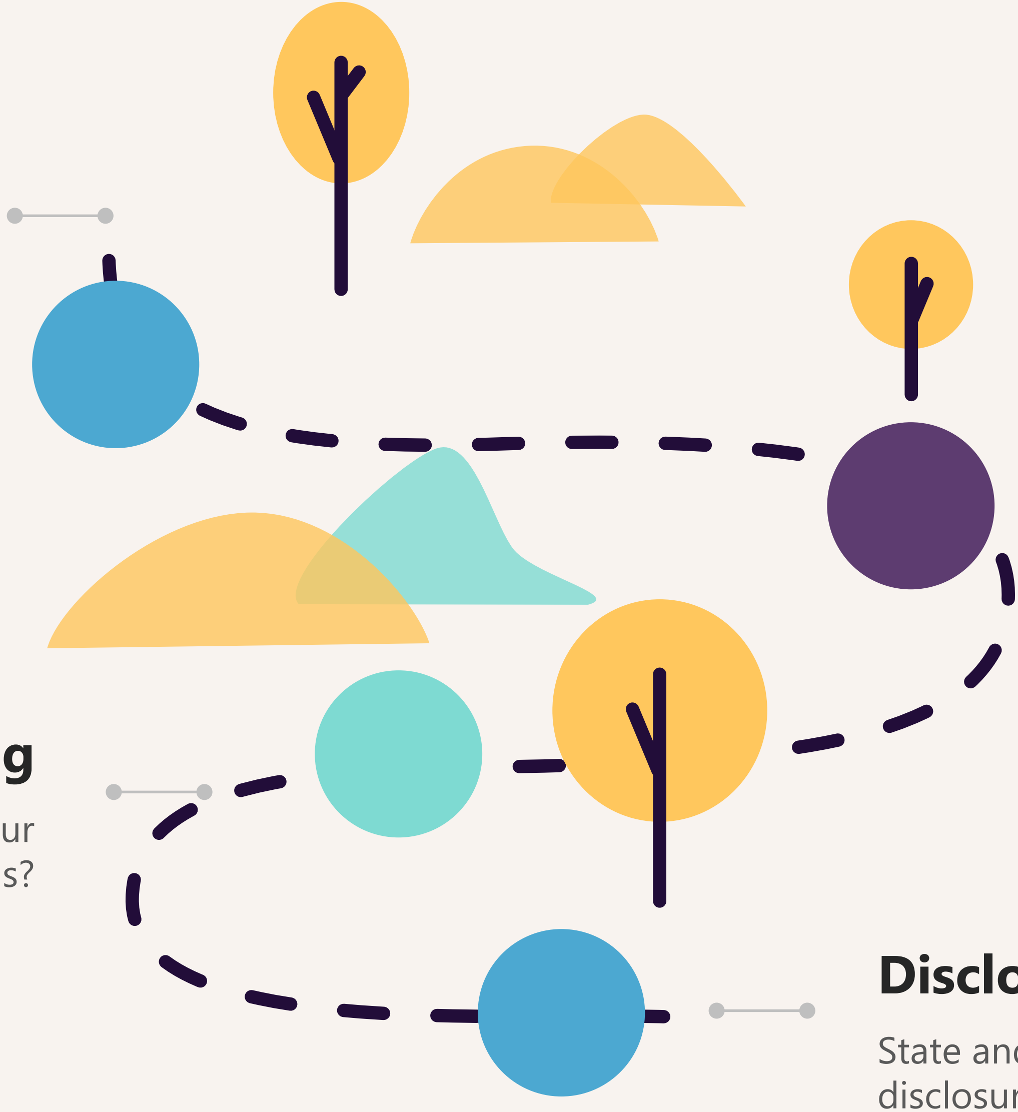
1. What is ransomware?

Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy ransomware that also destroys or exfiltrates[2] data, or ransomware in conjunction with other malware that does so.

Incident: … an attempt (successful or not) to gain access to … data

Breach: a loss of data

Disclosure Roadmap



Assessment

Follow the HIPAA Ransomware guide

Data Analysis

Is there evidence of data loss or access inside our system?

Decisioning

How sure are we about our analysis?

Disclosure

State and or federal disclosure

South Carolina Breach Notice

S.C. Code § 39-1-90

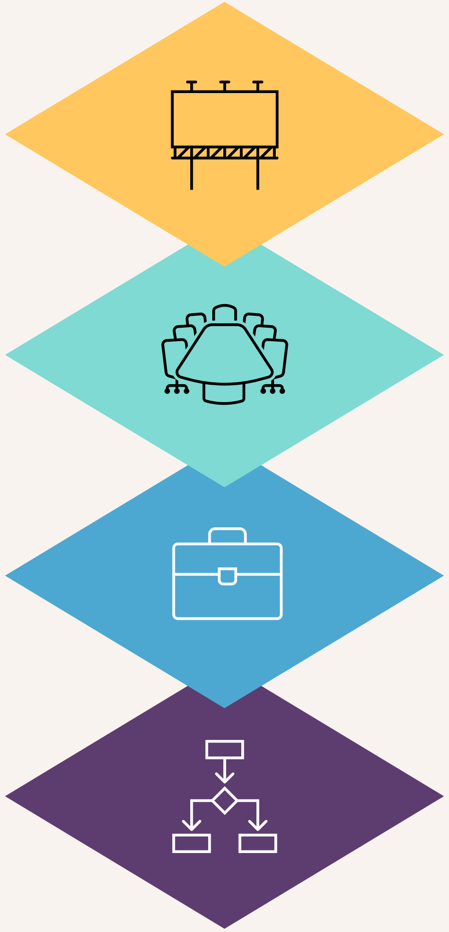
- Employee records
- Financial records
- Anything identifiable that is bankable

03 Lessons Applied

HillSouth's Changes

- MFA – clients & vendors
- Overhaul Endpoint Security
- Reset all passwords
- Rollout desktop protection suite
- Vendor overhauls

Workstation Protection System



Logon monitoring

Detect & log local administrator logons

PC Isolate

Isolate the PC from network if compromised

Early Warning Isolate

Unusual file copy, delete, or overwrite locks the system down until confirmed

Event Log & App Data Monitor

Suspicious clearing of log files and new hidden apps

Insurance Questions

Ransom Payment

Ultimate get out of jail?

Exclusions

These are growing

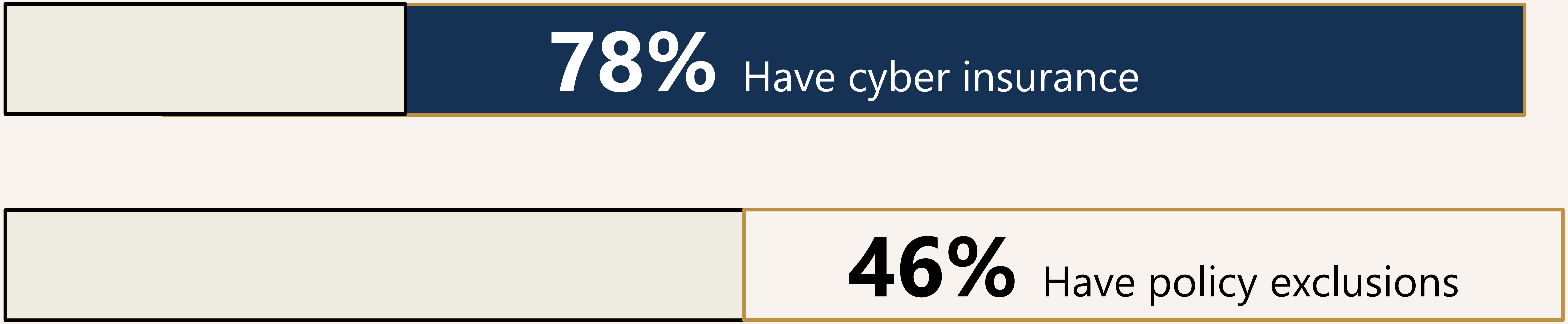
Lost Revenue

How long Will the Business suffer?

Notification Costs

How much is enough for state/federal laws?

Cyberinsurance in Healthcare



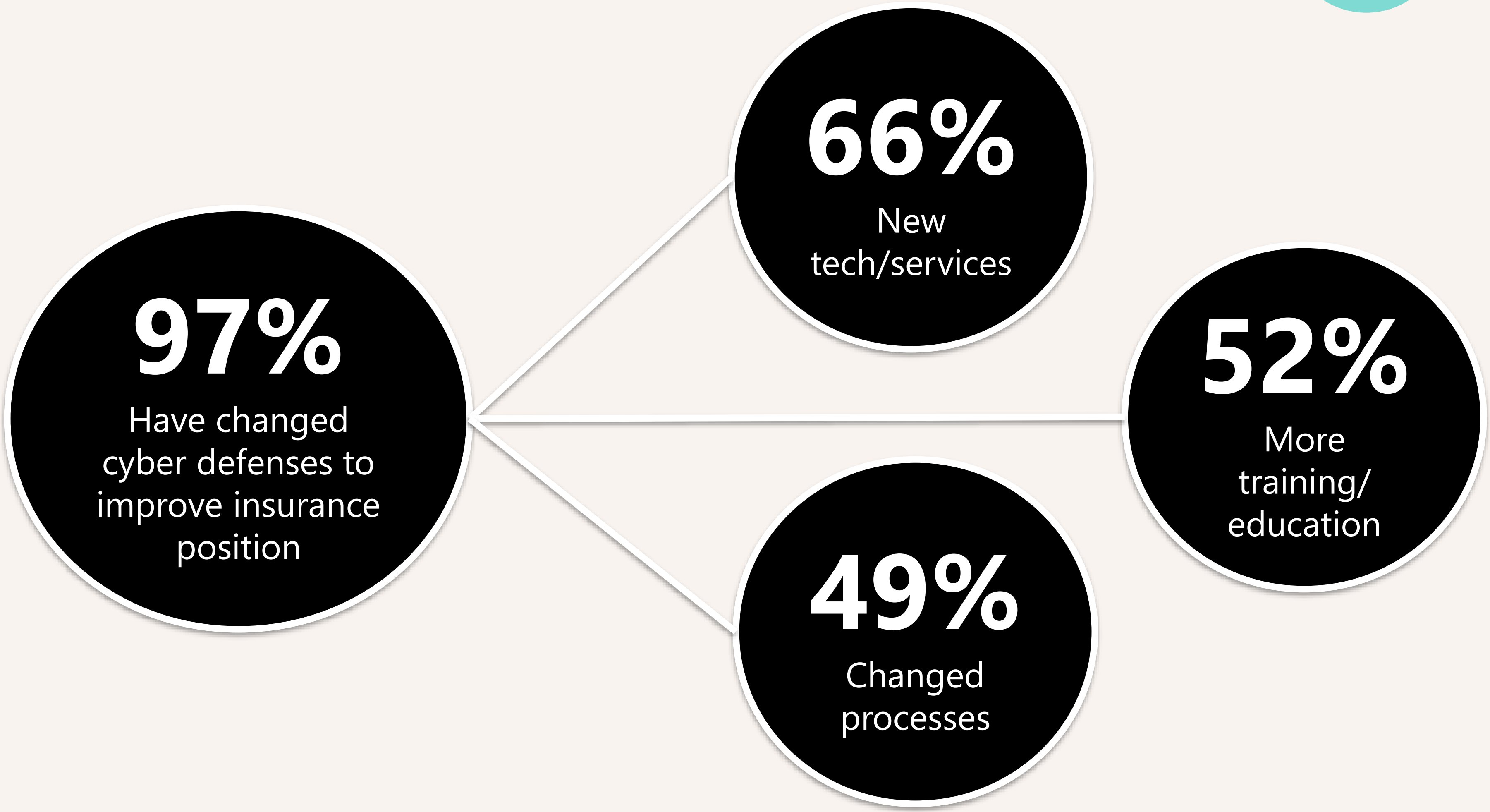
78% Have cyber insurance

46% Have policy exclusions

Cyberinsurance Challenges

51%	Higher level of cybersecurity needed
45%	Policies are more complex
48%	Fewer companies now offer cyber insurance
46%	The process takes longer
34%	It’s more expensive

Cyberinsurance Effecting Change



97%
Have changed cyber defenses to improve insurance position

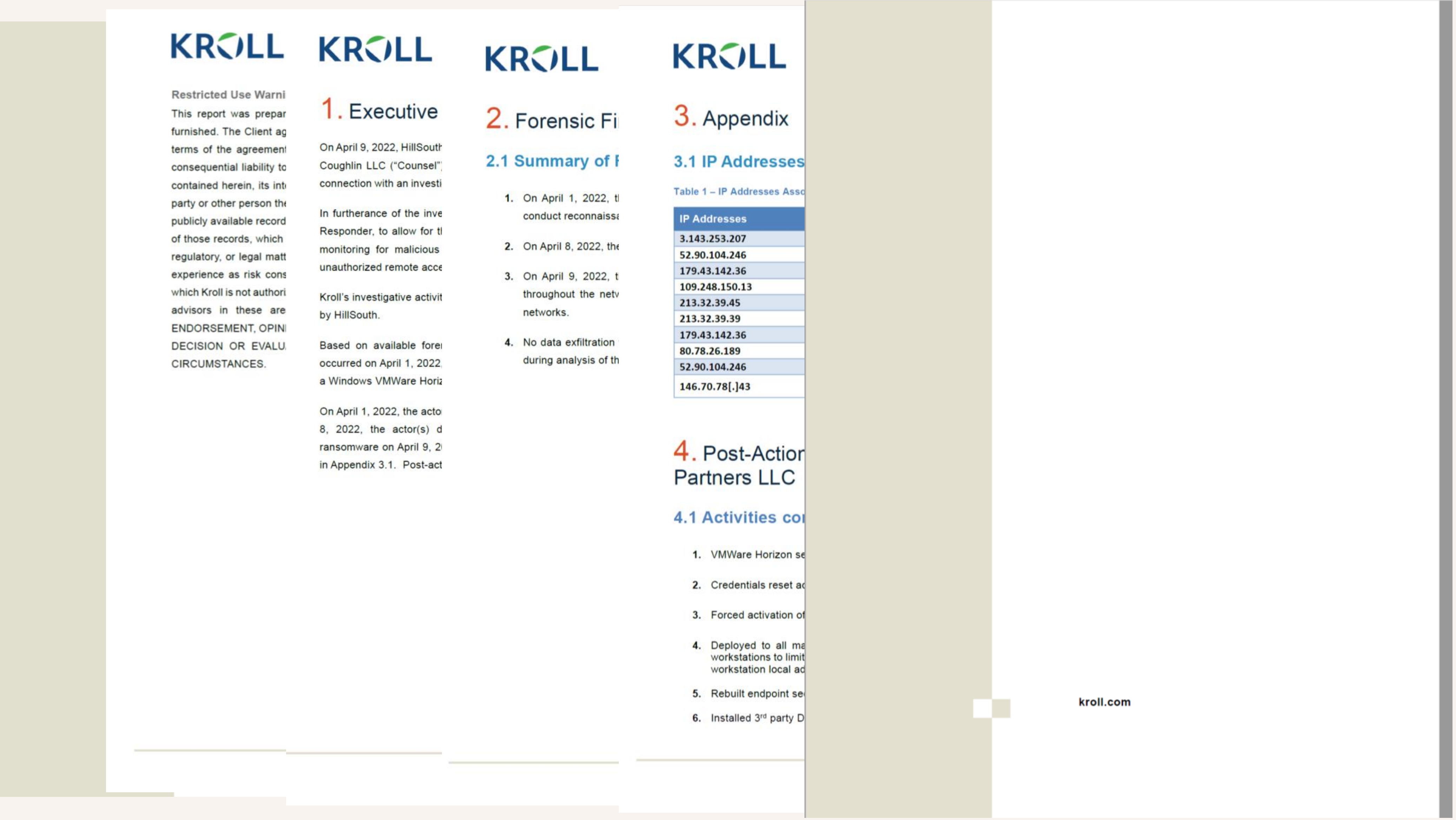
66%
New tech/services

52%
More training/ education

49%
Changed processes

04

Conclusions



KROLL

Restricted Use Warni

This report was prepar
furnished. The Client ag
terms of the agreement
consequential liability to
contained herein, its int
party or other person the
publicly available record
of those records, which
regulatory, or legal matt
experience as risk cons
which Kroll is not authori
advisors in these are
ENDORSEMENT, OPINI
DECISION OR EVALU
CIRCUMSTANCES.

KROLL

1. Executive

On April 9, 2022, HillSouth
Coughlin LLC ("Counsel")
connection with an investi

In furtherance of the inve
Responder, to allow for t
monitoring for malicious
unauthorized remote acce

Kroll's investigative activit
by HillSouth.

Based on available fore
occurred on April 1, 2022
a Windows VMWare Horiz

On April 1, 2022, the acto
8, 2022, the actor(s) d
ransomware on April 9, 2
in Appendix 3.1. Post-act

KROLL

2. Forensic Fi

2.1 Summary of F

1. On April 1, 2022, t
conduct reconnaiss

2. On April 8, 2022, the

3. On April 9, 2022, t
throughout the netv
networks.

4. No data exfiltration
during analysis of th

KROLL

3. Appendix

3.1 IP Addresses

Table 1 – IP Addresses Asso

IP Addresses
3.143.253.207
52.90.104.246
179.43.142.36
109.248.150.13
213.32.39.45
213.32.39.39
179.43.142.36
80.78.26.189
52.90.104.246
146.70.78[.]43

4. Post-Actior
Partners LLC

4.1 Activities co

1. VMWare Horizon se

2. Credentials reset ac

3. Forced activation of

4. Deployed to all ma
workstations to limit
workstation local ad

5. Rebuilt endpoint se

6. Installed 3rd party D

kroll.com

Our Lessons Learned

01 Data exists in more places than you’re presently backing up

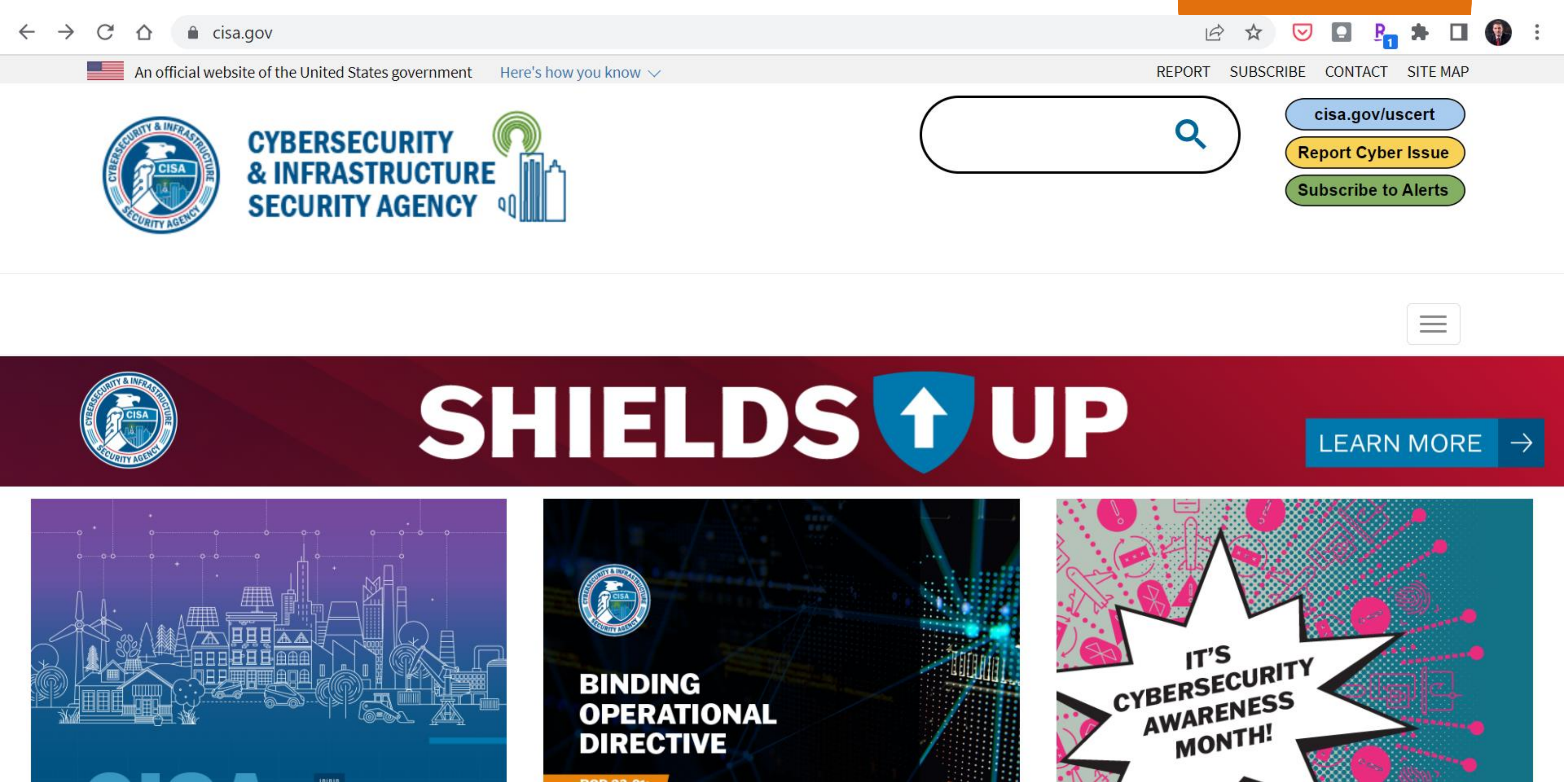
02 Cloud to cloud backups are still necessary (& cheap)

03 You need less Admins than you have today

04 Look out for command and control applications/discovery apps

05 MFA everything – with no exceptions

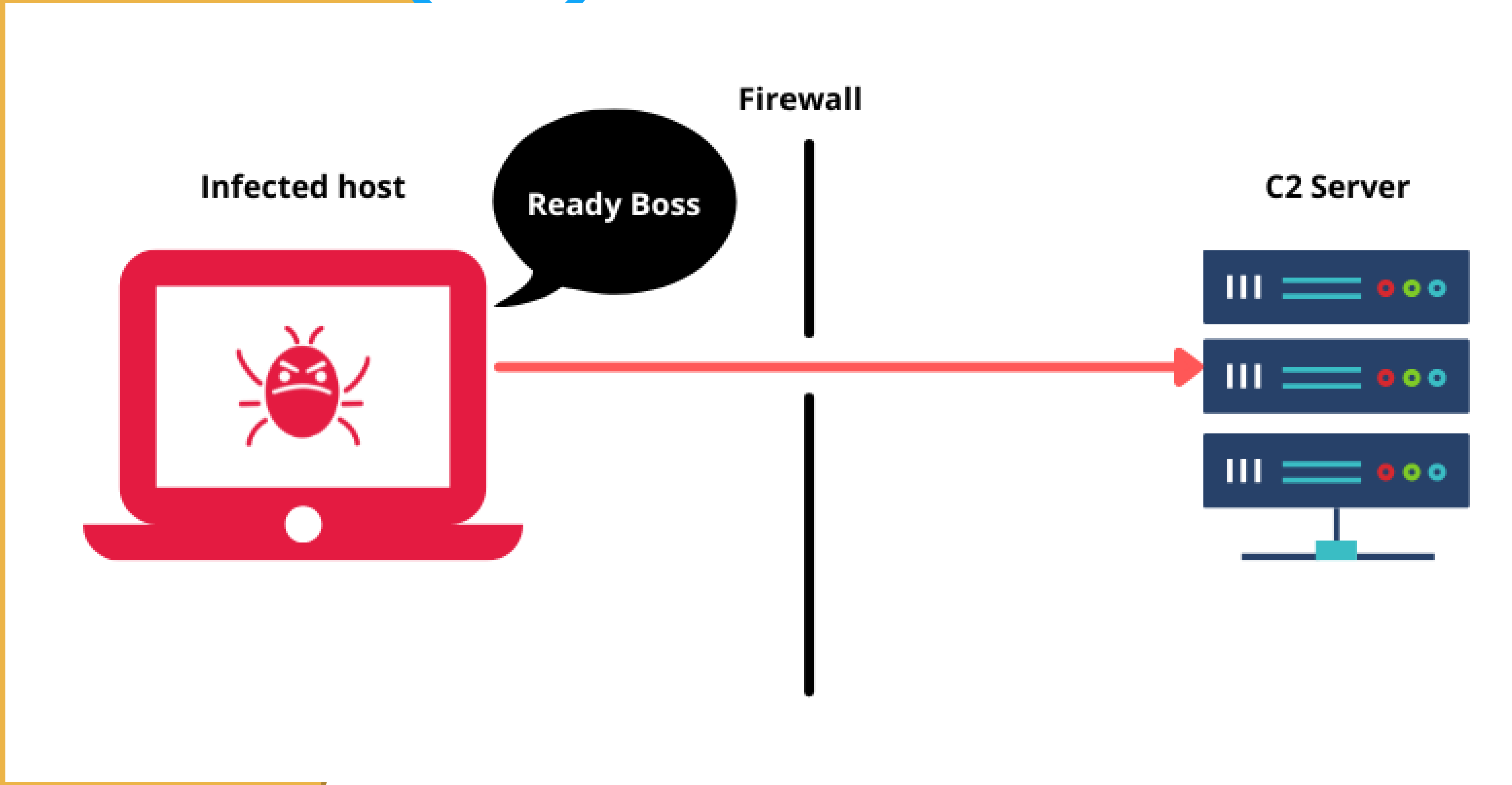
06 Plan for the worst and practice if you can


cisa.gov
An official website of the United States government
Here's how you know
REPORT
SUBSCRIBE
CONTACT
SITE MAP
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
cisa.gov/uscert
Report Cyber Issue
Subscribe to Alerts
SHIELDS UP
LEARN MORE
BINDING OPERATIONAL DIRECTIVE
IT'S CYBERSECURITY AWARENESS MONTH!

1

TA

Threat actor



4

C2

Command and Control [server]

KEY TAKEAWAY

Thank You

☎ (843) 432-4010

🌐 robby@hillsouth.com