VIRGINIA
IT AGENCY

WELCOME TO THE

APRIL 6, 2022

ISOAG MEETING

VIRGINIA IT AGENCY

AGENDA

- WELCOME/INTRODUCTION: MIKE WATSON
- ARLYN ELISE/UVA
- JOHN SINGLETON/VSP
- MELISSA GOLDATE, JON FORD & STEVE ELOVITZ/MANDIANT
- KATHY BORTLE, JIM STURDEVANT
- UPCOMING EVENTS
- ADJOURN

UNIVERSITY of VIRGINIA | SCHOOL of DATA SCIENCE

Data Science

A Discipline Without Walls

Arlyn Burgess
Associate Dean for Administration
University of Virginia, School of Data Science

April 6, 2022

Agenda

01

Defining Data Science

A model for **internal and external consistency**

02

Implementing a Sustainable Growth Plan

Identifying gaps, and meeting them with a strong public partnership

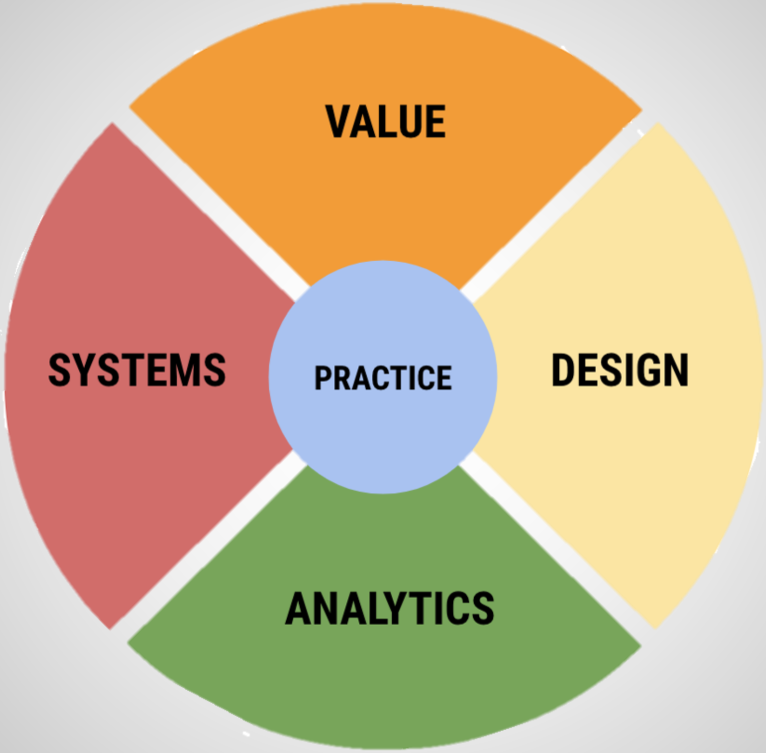
03

Building A School Without Walls

Bounded ambition in an inclusive, collaborative, vibrant, and dynamic community

Defining Data Science

Creating alignment, understanding, and consistency in growth and development



UNIVERSITY of VIRGINIA | SCHOOL of DATA SCIENCE

The Matrix of the Model

	Systems	Analytics	Design	Value
Education	Aggregating student data	Predictive models for K-12	Push campaigns	Bias and social inequalities
Finance	Cybersecurity and fraud	Adversarial models for fraud	Investment storytelling	ROI of Data Science
Digital Humanities	Sensor Network data	Text analytics on corpus	Data representation	Data creation and evaluation
Public Policy	Aggregating agency data	Predictive policing	COVID dashboards	Security and privacy

Core Values

- Excellence – What we do, we do best.
- Inclusivity – We respect people, value diversity, and are committed to equity.
- Openness – We are committed to open innovation and transparent teamwork.
- Be FAIR[1] – We support the ability Find, Access, Interoperate, and Reuse data and all other research and education products

[1] https://doi.org/10.1038/sdata.2016.18

Implementing a Sustainable Growth Plan

Partnership

Resources

Program Developme nt

Partnership

Opportunities for Engagement

- Capstone projects
  MSDS projects for solving real-world data problems (includes agency projects)
- Sustainable project alignment
  Ongoing opportunity for collaboration and mutually beneficial engagement
- Data Justice Academy
  Building bridges and creating opportunity

Resources

How we make it happen

- Philanthropy
  Transformative gifts for growth
  Sustainability giving plans
- Research
  Growth of broad-based funding
  Addressing grand challenges
- Tuition
  Competitive, but affordable
  Creating opportunities
- Partnership
  Corporate and public partnership
  Mutually beneficial opportunities

Program Development

Programs

- Master of Science in Data Science
  Residential 11-month
  Online 5 semester
  Professional Masters with experiential learning
- Undergraduate Minor
  Meets the model of data science
  Prepares for data literacy with any field
- PhD (forthcoming)
  Establishes a research strength
  Allows for integration and collaboration across fields
- Undergraduate Major (forthcoming)
  Follows the model of data science
  Create depth of understanding
  Creates a new standard for the field
  Encourages and promotes diversity

Building a School Without Walls

- **Program Development**

  Research, academic, and community program development is at the core of what we do and how we grow in size and impact.

- **Administration**

  Development of policies and procedures to determine how to grow and scale is important for growth and retention.

- **Open and Responsible**

  A commitment to openness in practice and dissemination and the practice of data science whereby all aspects of these endeavors include ethical, legal and policy factors.

- **Diversity, Equity, and Inclusion**

  Recognizing and addressing issues of diversity, equity, and inclusion in data science and academia is paramount to building community.

- **Recognition**

  The recognition of the role all people associated within and outside the School play in building a School and developing people in alignment with priorities

- **Collaboration**

  Collaboration among disciplines, institutions, and within the community while pushing the boundaries of traditional academia. Serving as R&D for state and local government.

ONWARDS!

VSP Incident Response

First Sergeant John Singleton

Date: 6 Apr.
2022

VALOR • SERVICE • PRIDE

Outline

- Rise of Cyber Crime
- Virginia Fusion Center
- High Tech Crimes Division
- Virginia Computer Crimes Act
- Reporting Cyber Incidents
- VSP Response
- Preparing for the Inevitable
- Question / Comments

VALOR • SERVICE • PRIDE

Rise of Cyber Crime

Since March 2020, the Commonwealth has experienced a significant increase in cyber related crimes, many of those specifically targeting governmental entities.

Currently averaging 1+ significant incident per month

Historic average was 3 or less per year.

Organizations of all sizes (and budgets) have been affected.

Common Incident Types

Any cyber incident can be report to VSP. Commonly reported events include:

- Business Email Compromise
- Credential Theft
- Network Intrusion
- Ransomware

This is a common pattern for the evolution of an attack.

Common Attack Vectors

A variety of exploits have been utilized but the majority are taking advantage of easily preventable vulnerabilities.

- Weak IT Passwords
- Vulnerable Operating Systems
- Improperly Configured Security
- Overly Permissive Firewall Rules
- Lack of sufficient backups

Virginia Fusion Center

Collaborative effort of state and federal agencies working in conjunction with local partners to share resources, expertise, and/or information to better identify, detect, prevent, and respond to terrorist and criminal activity utilizing an all crimes/all hazards approach.

- Multi-Jurisdictional Information Sharing Center
- Centralized Reporting
- Resource organization and coordination
- Facilitates communication between stakeholders

High Tech Crimes Division

Primarily responsible for assisting local, state, and federal partners with investigations involving electronic devices and information. Primary unit tasked with investigating computer related and child exploitation offenses defined by the Code of Virginia.

Made up of four sections:

- **High Tech Crimes Section**
- Computer Evidence Recovery
- Tactical Support
- NoVA Internet Crimes Against Children Task Force

Computer Crimes Act

Defined in Title 18.2, Chapter 5, Article 7.1. Commonly applicable sections:

- § 18.2-152.3. Computer fraud
- **§ 18.2-152.4. Computer trespass**
- § 18.2-152.5. Computer invasion of privacy
- § 18.2-152.6. Theft of computer services
- 18.2-152.7:1. Harassment by computer

Generally Class 1 Misdemeanors, can rise to Class 3 to 6 Felonies under certain circumstances.

https://law.lis.virginia.gov/vacodefull/title18.2/chapter5/article7.1/

A Crime Has Occurred

VSP is responsible for investigating computer based crimes in a manner consistent with all other crimes. Your equipment, personnel, and actions are part of that investigation (don’t panic).

While the vast majority of cyber incidents are from external threat, that is not always the case. **Transparency** is important to making an early determination of the source of the attack.

It is possible that someone in your organization or a former employee is involved in the incident.

Cyber Incidents

You are not alone.

Reporting Cyber Incidents

Contact the VSP Fusion Center

vfc@vsp.virginia.gov (monitored 24/7)

Recommended Notifications

- Chain of Command
- Legal Staff
- **Cyber Insurance Provider**
- VITA (if applicable)

Response Assessment

VSP will facilitate a virtual meeting with stakeholders and assistance providers such as FBI, MS-ISAC, VITA, CISA to determine the following:

- Contact Information
- Basic details and timeline
- Scope of the incident
- Impacted services
- Potentially exposed information
- Additional resources needed
- Next Steps

What We Do

When on-scene response is requested our goals are simple:

- Quick response
- Identify potential vulnerabilities
- Stop unauthorized access
- Identify affected devices
- Isolate affected devices
- Provide advice/consultation for safe restoration
- Identify the threat actor

We want to get you to a “safe” state as soon as possible.

How We Do It

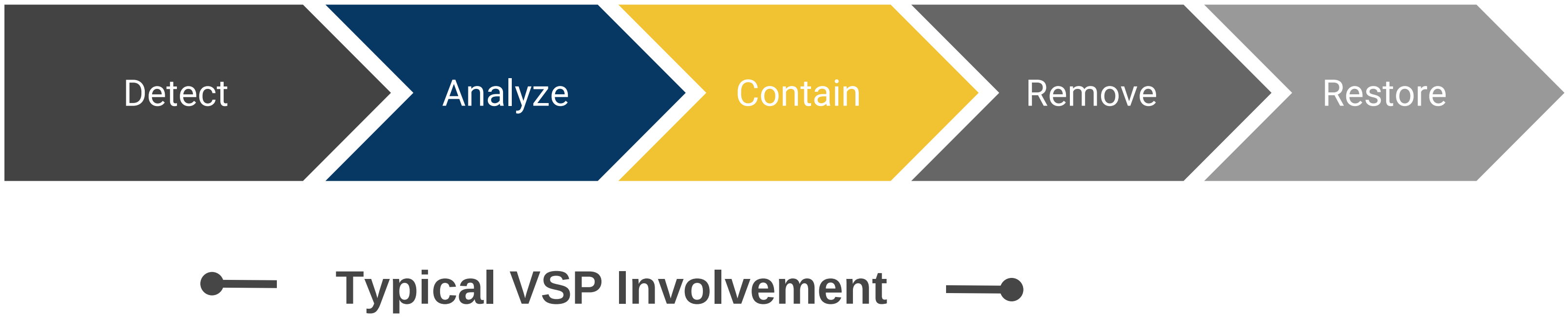
HTCS resources are often on-scene the same day the report is made. Our core services during a response are:

- Interviews
- Device triage on affected devices
- Full disk imaging for preservation and analysis
- Full Network traffic capture
- Log Analysis

Questions to Expect

- Recent employee terminations
- Current disgruntled employees
- New or varied 3rd party contractors
- Inventory of devices
- Current **Network Map**
- External access policies
- Suspicious email campaigns
- Suspicious access attempts
- Out of date software in use
- IT Password complexity, re-use, lifespan
- New software installations
- New network equipment
- Reported infections by contractors or 3rd party providers

Cyber Incident Lifecycle



Detect

Analyze

Contain

Remove

Restore

Typical VSP Involvement

What We Don’t Do

Recovering from IR events are often a complex series of tasks performed by a variety of stakeholders over a long period of time to complete the mission.

- Provide endpoint monitoring and protection
- Re-image devices
- Re-build network services
- Provide temporary hardware and software
- Analyze IT policy and procedure

Prepare for the Inevitable

Strong passwords are free, weak ones will cost you

Prepare for the Inevitable

If your organization isn’t doing the following minimum priorities, you are a ripe target for ransomware. These are relatively easy to accomplish and cost much less than a single ransomware event to complete (most cost nothing). It is never too late to start.

- Password Audit for strength, re-use, and lifespan.
- Upgrade ALL out of date Operating Systems
- Backup Audit - Test restoration and ensure some copy is offsite and offline
- Firewall Rule Audit - ensure that no unnecessary traffic is allowed externally and internally

Prepare for the Inevitable

- Use Network Segmentation
- Ensure up to date endpoint protection and definitions
- Least privilege Audit - ensure that authority is properly scoped to the minimum that is needed to accomplish any task
- External access Audit - Do you really need that VPN access? Is the user properly restricted once connected to the network?
- **Up to date Network map** - Physical and Logical - this will help you identify weak points and unnecessary traffic as well as being an asset in recovery if needed.

Advanced Preparation

- Offsite log management
- Patch / Update management
- Penetration testing
- Security awareness training
- Media destruction protocol
- Physical access controls
- Change management
- Update Software and vendor contact lists
- Inventory of sensitive info locations (PII, etc)

Surviving Ransomware

Backups - not Copies

- Having only an on-network copy of your files is not good
- Ensure that your organization has a backup policy and procedure that keeps critical data off-network
- Validate your backups
- Test your restoration procedure before you need them

Recap

- Cyber Attacks are Increasing Rapidly
- Preparation and IT are key to prevention
- Strong passwords are free
- You are not alone
- You can survive ransomware
- VSP and partners are here to help

Questions / Comments

Email Contacts

bci.htcd@vsp.virginia.gov

vfc@vsp.virginia.gov

MANDIANT

Ransomware Evolution, Challenges and Solutions

Jon Ford

Managing Director – Government Solutions

About the Presenter

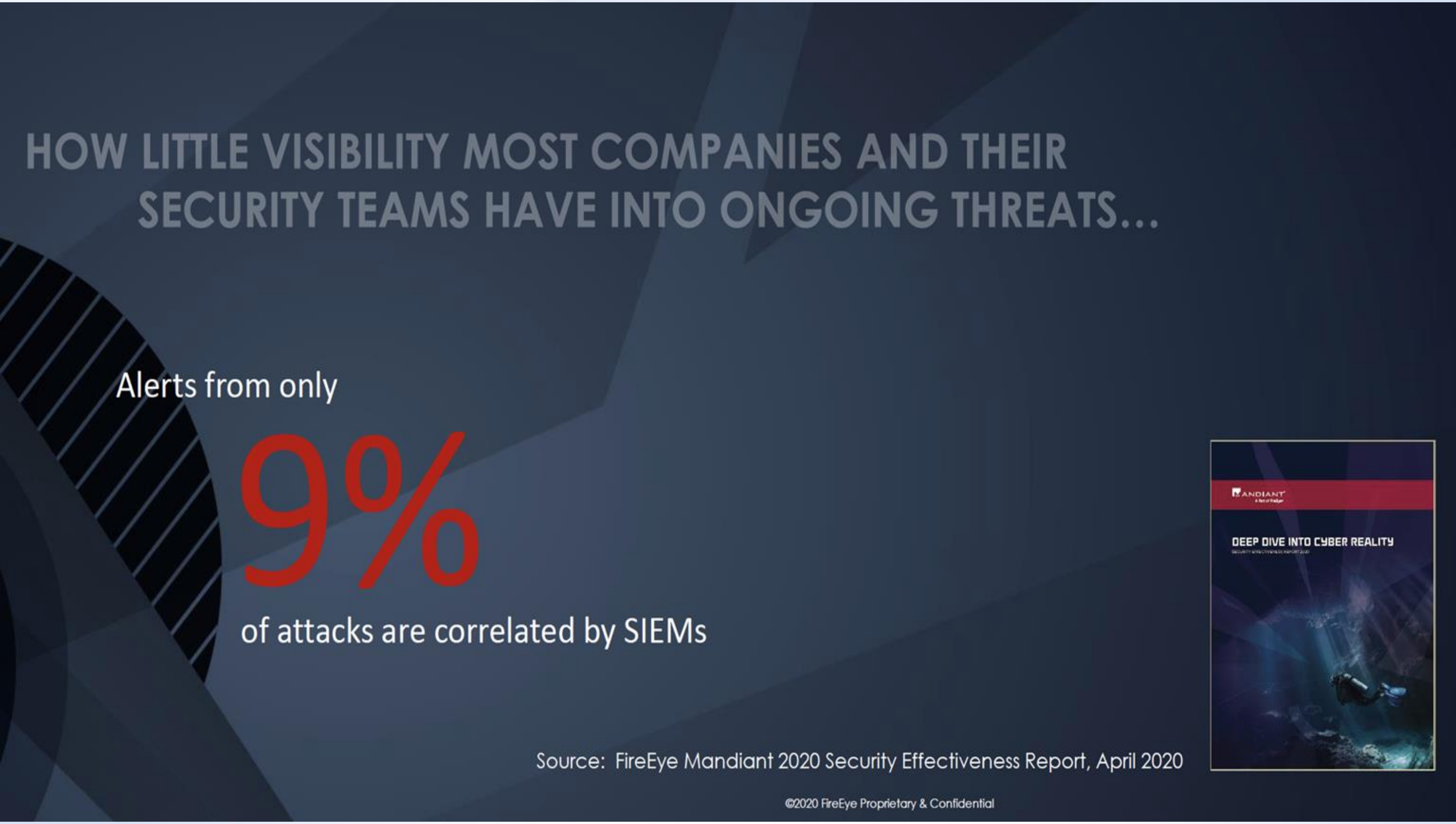
- **Jon Ford**
- Managing Director, FireEye Mandiant
- Based in San Antonio TX, USA
- Leads a team of incident responders that have responded to over a thousand incidents
- 20+ years of experience with incident response and red teaming
- Previously led the global Incident Response teams at the FBI

MANDIANT

Multi-Faceted Extortion

MANDIANT

Did You Know?



HOW LITTLE VISIBILITY MOST COMPANIES AND THEIR SECURITY TEAMS HAVE INTO ONGOING THREATS…

Alerts from only

9%

of attacks are correlated by SIEMs

MANDIANT
DEEP DIVE INTO CYBER REALITY

Source: FireEye Mandiant 2020 Security Effectiveness Report, April 2020

©2020 FireEye Proprietary & Confidential

RESEARCH DEMONSTRATES WHY BREACHES SO FREQUENTLY OCCUR

53%

Organizations are completely missing or unaware of executed attacks

Broken Processes & Misconfigured Tools…

Not preventing over

68%

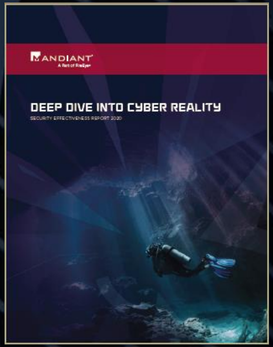
of ransomware attacks…

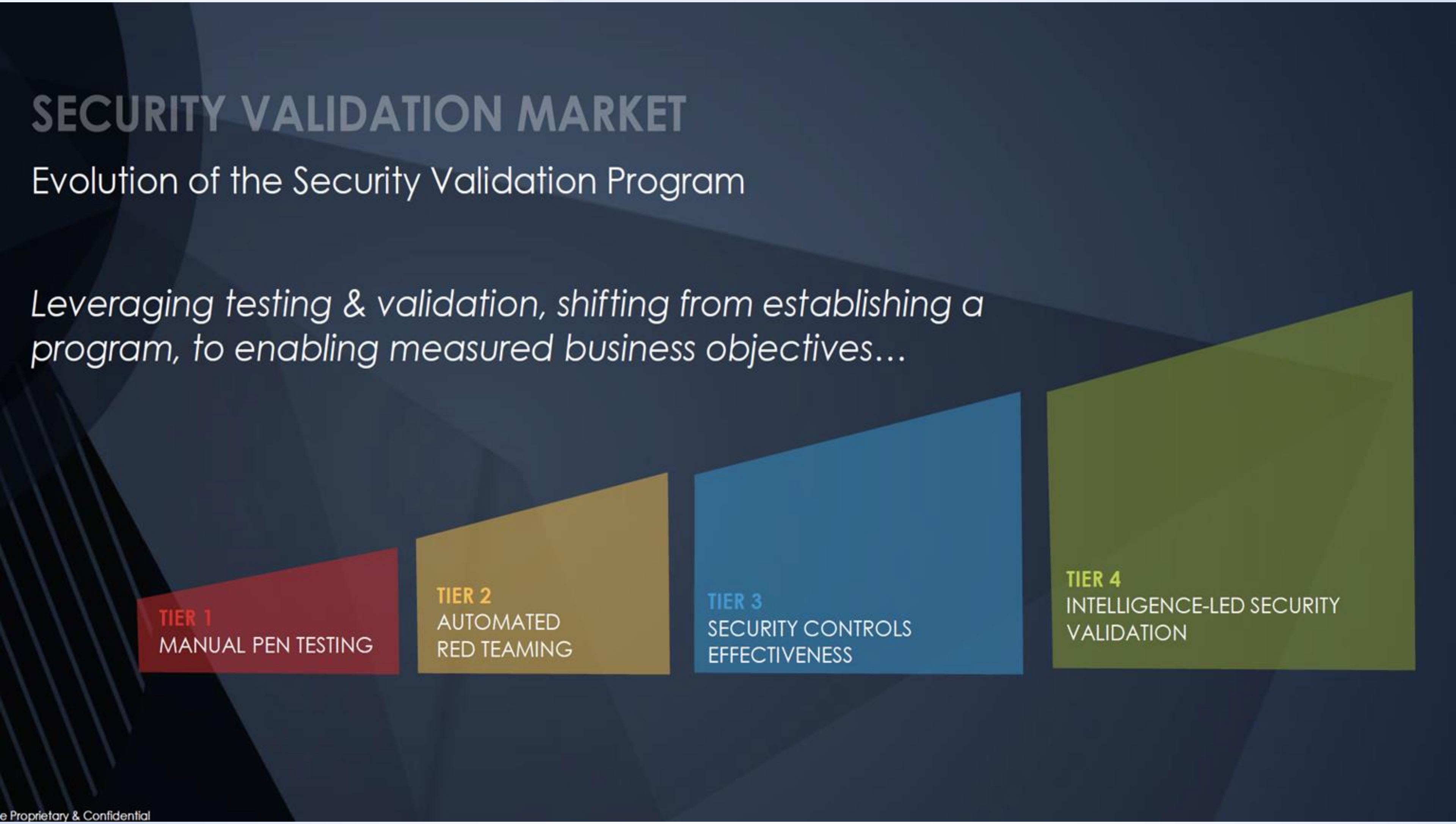
On average

91%

of attacks go undetected

Source: FireEye Mandiant 2020 Security Effectiveness Report


MANDIANT
A Part of FireEye
DEEP DIVE INTO CYBER REALITY
SECURITY EFFECTIVENESS REPORT 2020



SECURITY VALIDATION MARKET

Evolution of the Security Validation Program

Leveraging testing & validation, shifting from establishing a program, to enabling measured business objectives…

TIER 1
MANUAL PEN TESTING

TIER 2
AUTOMATED RED TEAMING

TIER 3
SECURITY CONTROLS EFFECTIVENESS

TIER 4
INTELLIGENCE-LED SECURITY VALIDATION

e Proprietary & Confidential

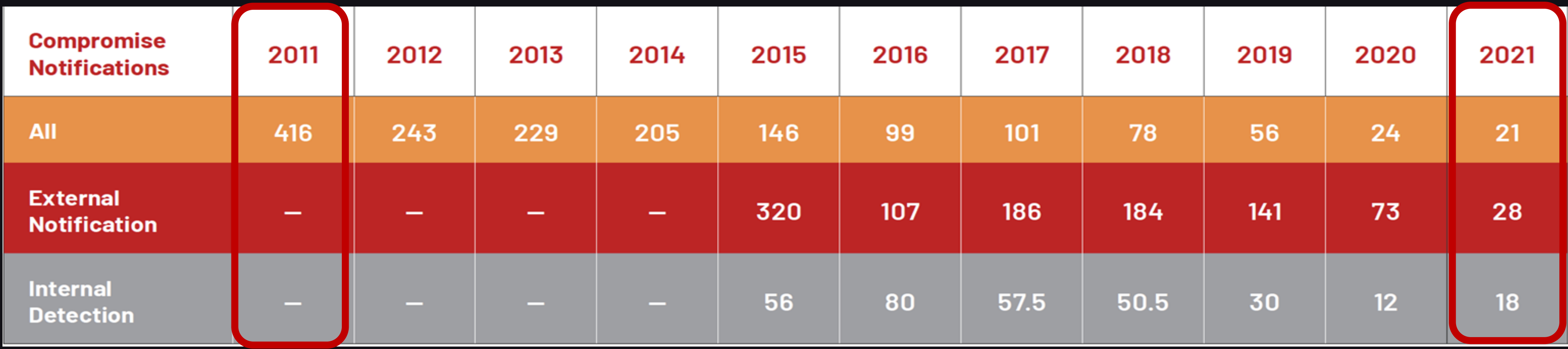
Attacker Dwell Time

Year Over Year

56
DAYS
2019 Global Median Dwell Time

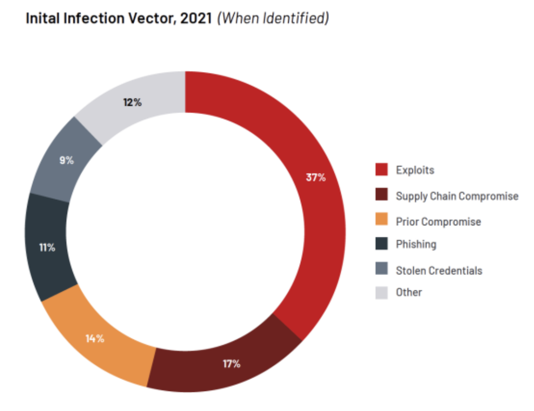
21
DAYS
2021 Global Median Dwell Time

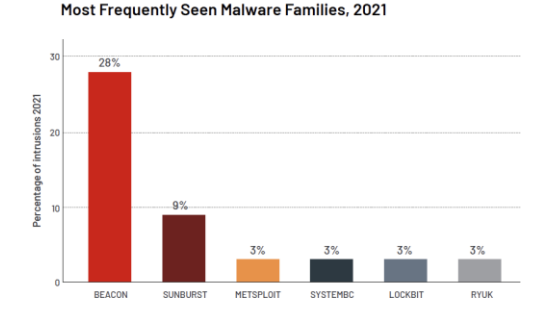
Over A Decade

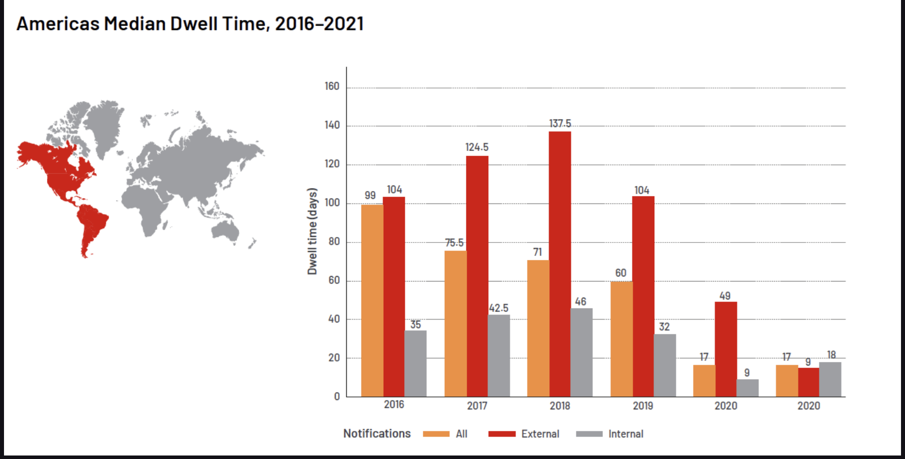


Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
All	416	243	229	205	146	99	101	78	56	24	21
External Notification	—	—	—	—	320	107	186	184	141	73	28
Internal Detection	—	—	—	—	56	80	57.5	50.5	30	12	18

2021 Trends


Inital Infection Vector, 2021 *(When Identified)*

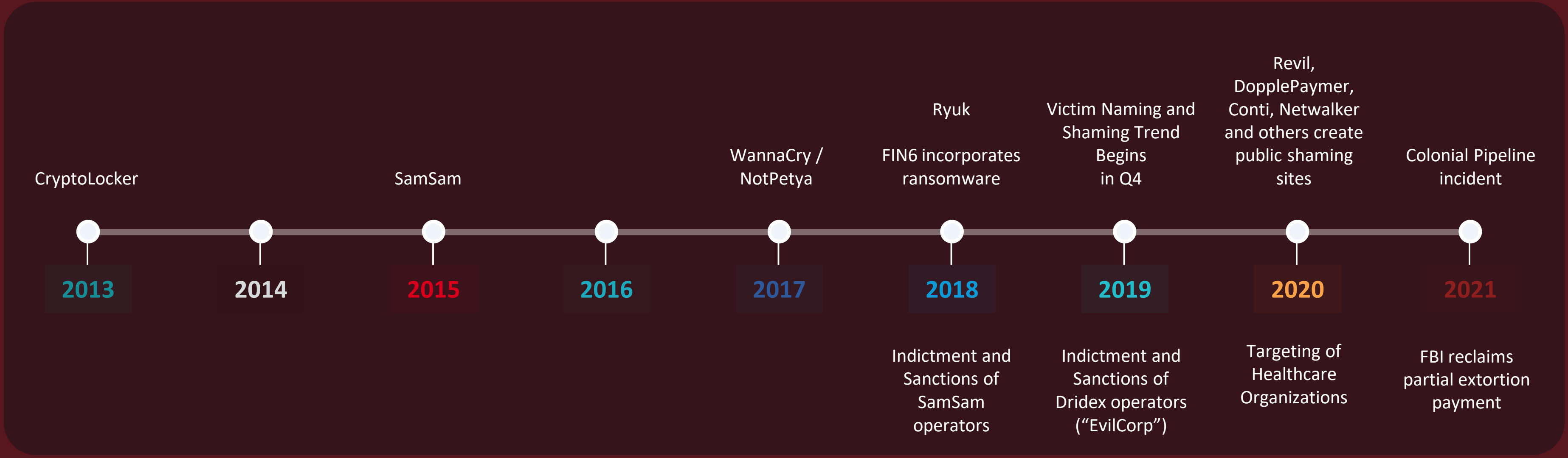

Most Frequently Seen Malware Families, 2021


Americas Median Dwell Time, 2016–2021

Multifaceted Extortion

- “Multifaceted extortion” is the act of leveraging multiple techniques to coerce victims
  - Theft of sensitive data
  - Deployment of ransomware encryptors
  - Public shaming
  - Amplification through the media
  - Distributed denial of service attacks
  - Extortion of business partners and customers
  - Personal attacks and harassment of employees
- Maze made this trend mainstream at the end of 2019
- Replicated by many other threat actors
- Surge in compromises of organizations in September and October 2020

Evolution of Ransomware



2013
CryptoLocker

2014

2015
SamSam

2016

2017
WannaCry / NotPetya

2018
Ryuk

FIN6 incorporates ransomware

Indictment and Sanctions of SamSam operators

2019
Victim Naming and Shaming Trend Begins in Q4

Indictment and Sanctions of Dridex operators (“EvilCorp”)

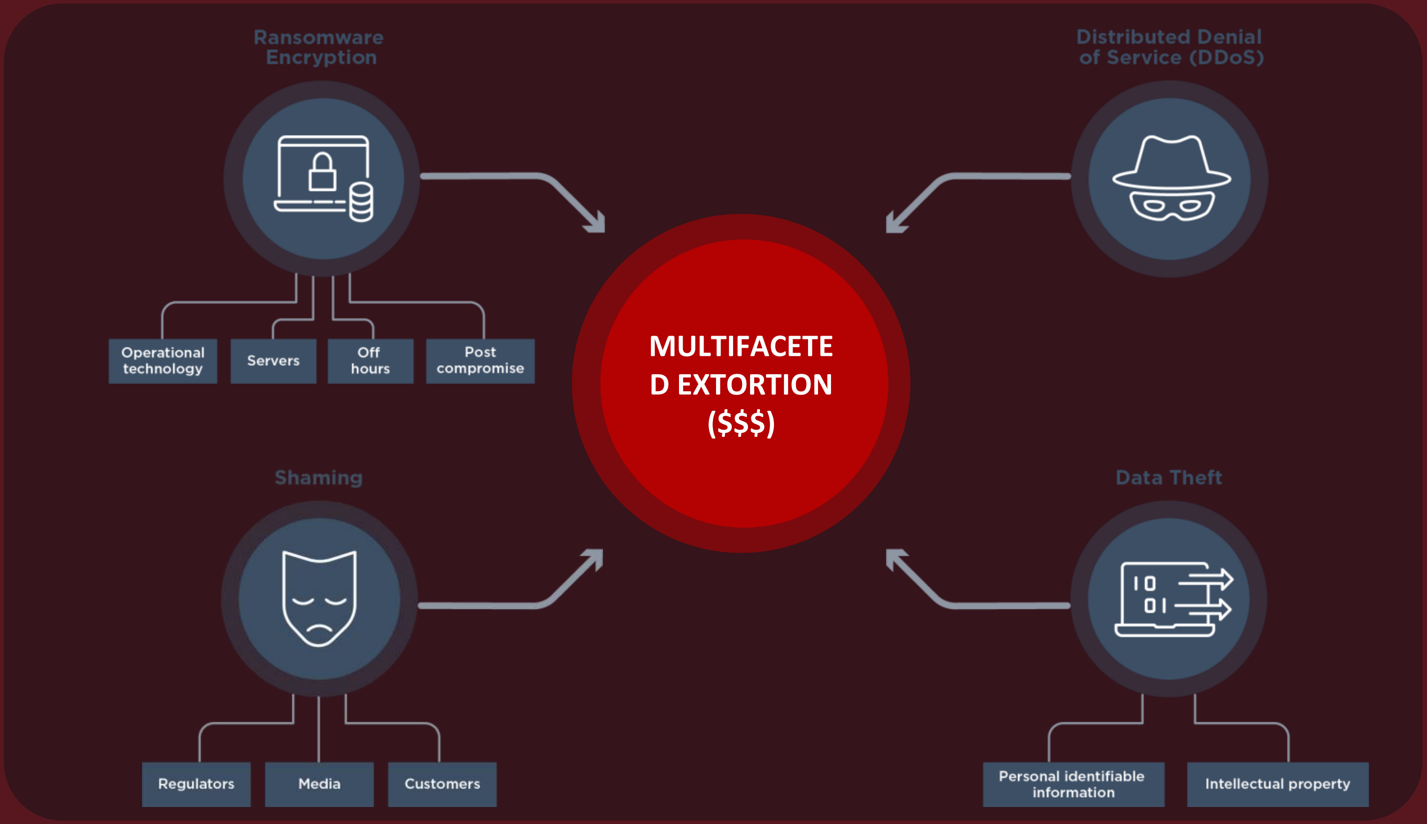
2020
Revil, DopplePaymer, Conti, Netwalker and others create public shaming sites

Targeting of Healthcare Organizations

2021
Colonial Pipeline incident

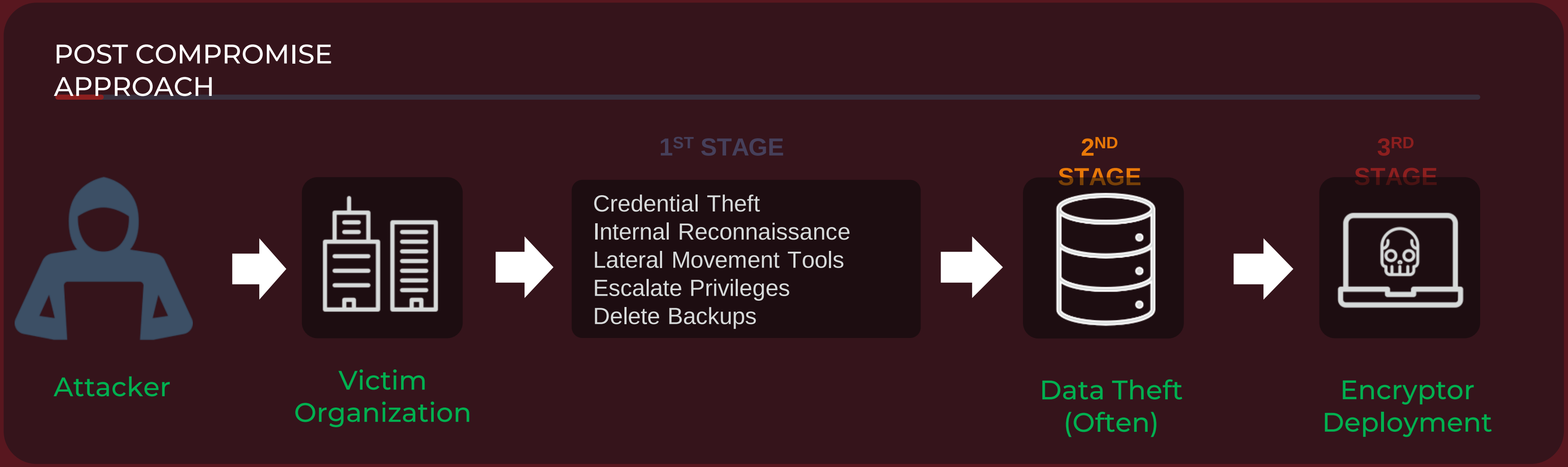
FBI reclaims partial extortion payment

Evolution of Ransomware



©2021 Mandiant

Evolution of Ransomware



POST COMPROMISE APPROACH

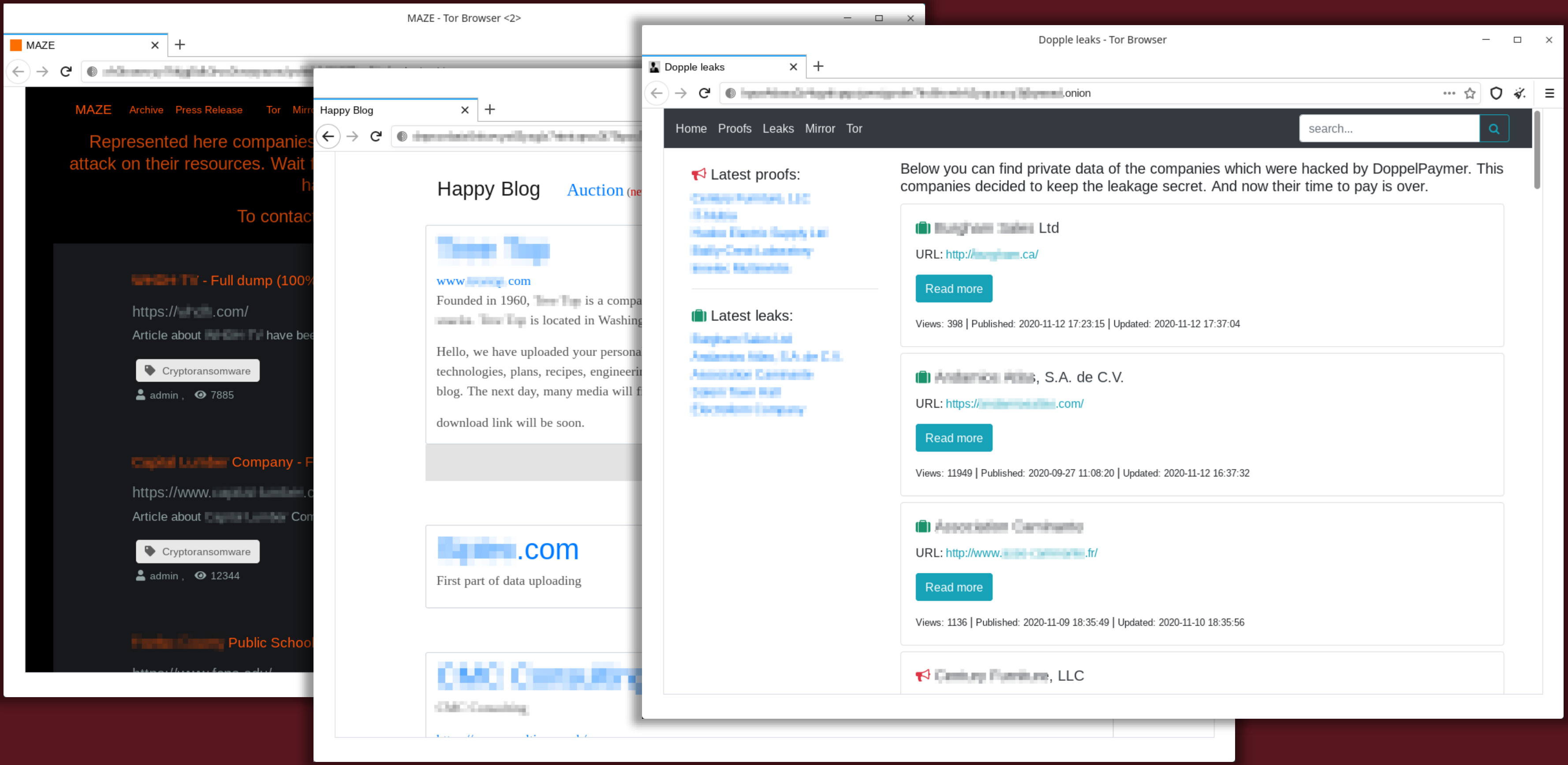
1ST STAGE

- Credential Theft
- Internal Reconnaissance
- Lateral Movement Tools
- Escalate Privileges
- Delete Backups

2ND STAGE

3RD STAGE

Victim Shaming Sites and Data Exposure



Represented here companies attack on their resources. Wait t h

To contac

[redacted] - Full dump (100%

https://[redacted].com/

Article about [redacted] have bee

Cryptoransomware

admin , 7885

[redacted] Company - F

https://www.[redacted]

Article about [redacted] Com

Cryptoransomware

admin , 12344

[redacted] Public Schoo

Happy Blog Auction (ne

[redacted]

www.[redacted].com

Founded in 1960, [redacted] is a compa [redacted] is located in Washing

Hello, we have uploaded your persona technologies, plans, recipes, engineeri blog. The next day, many media will f

download link will be soon.

[redacted].com

First part of data uploading

[redacted]

Latest proofs:

[redacted]

Latest leaks:

[redacted]

Below you can find private data of the companies which were hacked by DoppelPaymer. This companies decided to keep the leakage secret. And now their time to pay is over.

[redacted] Ltd

URL: http://[redacted].ca/

Read more

Views: 398 | Published: 2020-11-12 17:23:15 | Updated: 2020-11-12 17:37:04

[redacted], S.A. de C.V.

URL: https://[redacted].com/

Read more

Views: 11949 | Published: 2020-09-27 11:08:20 | Updated: 2020-11-12 16:37:32

[redacted]

URL: http://www.[redacted].fr/

Read more

Views: 1136 | Published: 2020-11-09 18:35:49 | Updated: 2020-11-10 18:35:56

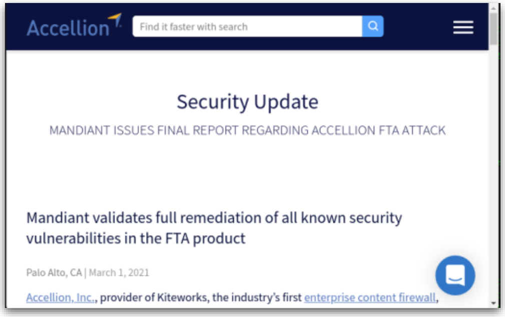
[redacted], LLC

MANDIANT

Data Theft and Extortion At Scale

Data Theft and Extortion at Scale

- A series of **security vulnerabilities in a secure file transfer solution** are identified by a threat group
- A group exploits the vulnerabilities and **steals sensitive corporate data** from dozens of organizations
- A month later, many **victims receive extortion demands** – some that don't pay have their data published on the threat actor's victim shaming site
- Vendor **engages Mandiant** to perform a security assessment of their product
- Mandiant identified **additional security vulnerabilities** and validated all known vulnerabilities are patched



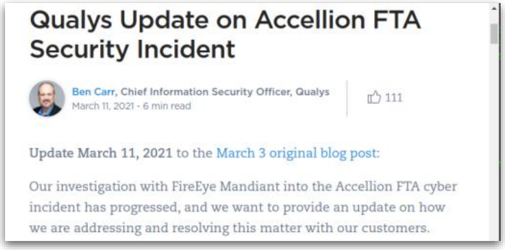
Security Update

MANDIANT ISSUES FINAL REPORT REGARDING ACCELLION FTA ATTACK

Mandiant validates full remediation of all known security vulnerabilities in the FTA product

Palo Alto, CA | March 1, 2021

Accellion, Inc., provider of Kiteworks, the industry's first enterprise content firewall,


Qualys Update on Accellion FTA Security Incident

Ben Carr, Chief Information Security Officer, Qualys
March 11, 2021 - 6 min read

Update March 11, 2021 to the March 3 original blog post:

Our investigation with FireEye Mandiant into the Accellion FTA cyber incident has progressed, and we want to provide an update on how we are addressing and resolving this matter with our customers.

Multifaceted Extortion Intrusion Root Causes

Most common techniques

1. Email-based phishing
2. Commodity malware
3. Exploitation of known and patched vulnerabilities
4. Stolen credentials and lack of multifactor authentication on remote access
5. Zero day vulnerabilities
6. Supply chain attacks (compromising service providers who have credentials or network access to other organizations)
7. Collaboration with initial access brokers (who may use any of the above techniques)

More recent trends include:

1. Telephone based social engineering
2. Use of non-privileged credentials, data theft, and extortion (no deployment of encryptors)
3. Stolen credentials and MFA push/call spamming

Ransomware Learnings and Observations

- Threat actors often disable endpoint detection and response (EDR) solutions before deploying malware
- Encryptors are often deployed through the following ways:
  - Batch scripts, PSExec, WMI, etc.
  - Group Policy Objects
  - Software deployment technology used by the victim
- Intrusion durations vary significantly:
  - Some intrusions are executed and completed within hours or days
  - Some intrusions have significant dwell time, usually due to access handover to other groups

Ransomware Learnings and Observations

- The vast majority of threat actors that deploy ransomware are financially motivated (however some governments conduct extortion as a false flag)
- Ransomware and multifaceted extortion operators are very loud – several opportunities to detect and respond to intrusions

Ransomware Recovery Challenges

- Ransomware recovery time depends on multiple variables:
  - Scope of the disruption
  - Resiliency of the backup and restoration systems and processes
  - Preservation of systems and evidence
  - Access to ransomware decryptors
  - Speed and efficacy of ransomware decryptor
- Recovery usually takes days. Can take weeks or months for full recovery for some organizations

Extortion Considerations

1 How **quickly can you recover** your systems and data on your own?

2 How **reliable** is the threat actor?

3 Did the threat actor **steal data** before they deployed their encryptors? How sensitive is the data that they stole?

4 Does the threat actor still have **active access** to your network?

5 Will **cybersecurity insurance** cover the claim?

6 **If considering payment** - Is the **threat actor sanctioned** by the U.S. Department of Treasury?

Learnings from Paying Threat Actors

1 Threat actors usually have **multiple backdoors** and can technically re-encrypt data if they wanted to

2 You don’t know who you’re paying - some threat actors are **sanctioned**

3 Many threat actors are **reliable** – their business model depends on it

4 Many threat actors **move on to the next target** when paid – they have plenty of victims to choose from

5 **No guarantees** that stolen data will be deleted (despite providing “proof” of deletion)

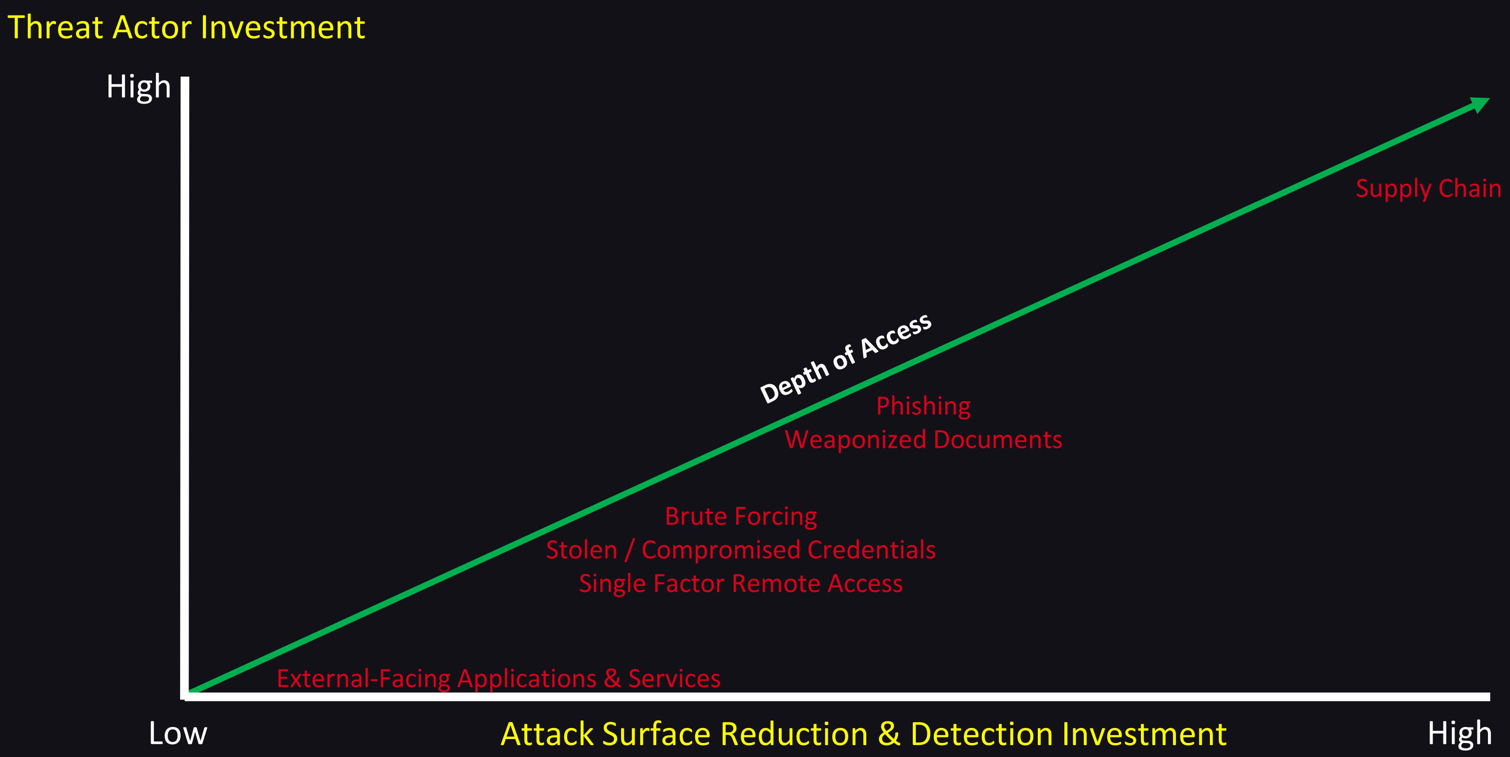
6 Prior to 2019, we observed many threat actors that publicized stolen data and **re-extorted victims** after being paid

Proactive Protection and Hardening

Incident Response Best Practices

- **Develop an incident response plan** before you need it
- Conduct a **Ransomware Assessment** to know your exposure to a ransomware attack
- Ensure everyone is **aligned** on the same goal: **detection, response, then recovery**
- **Communicate frequently** and with **full transparency**
- **Practice empathy** but **set expectations** – it’s OK not to know the answer

Common Initial Access Methods



Proactive Protection and Hardening - Access

- Identify and harden external-facing assets and pathways into an environment
  - Scan / Identity / Mitigate
- Harden access methods for external-facing assets
  - Strong authentication + MFA
- Segment external-facing systems from internal infrastructure and identities
- Use separate (non-privileged) accounts for daily usage (including when accessing email and external resources)
- Disable macros (external senders) and harden / patch MS Office
- Remove local administrative permissions for standard users

Proactive Protection and Hardening - Credentials

- Identify privileged accounts and groups – and minimize credential exposure for privileged accounts
- Leverage the Protected Users Security Group for AD-based privileged accounts
- Enforce identity tiering for privileged accounts – with logon and access restrictions enforced
- Remove the capability for local administrative accounts to be used for remote logons to other endpoints
  - Randomize the password for the built-in local administrative account on endpoints
- Harden endpoints so that clear-text passwords are not stored in memory

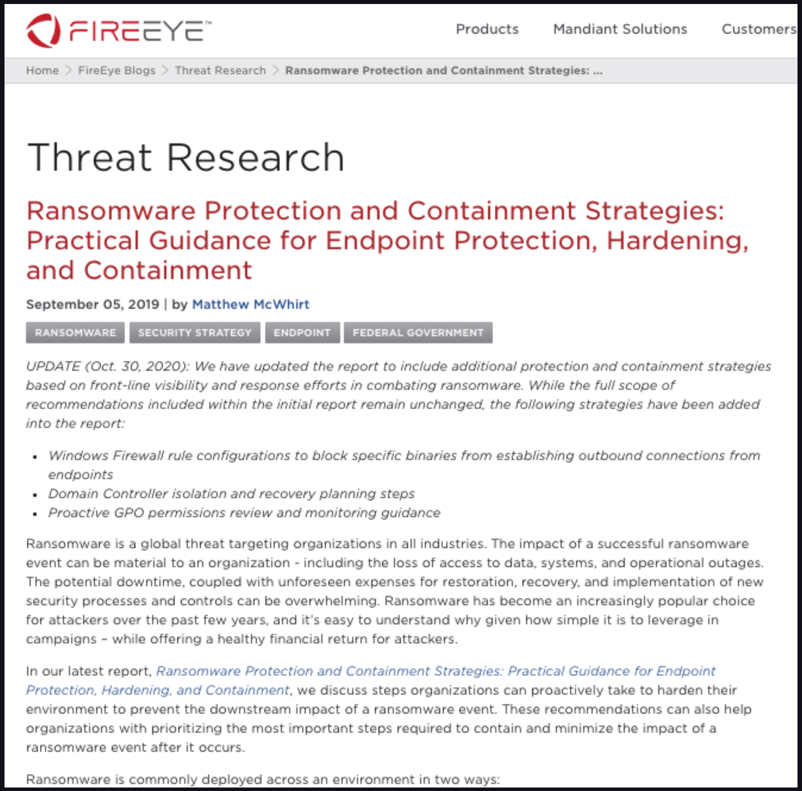
Proactive Protection and Hardening - Connectivity

- Enforce network segmentation between security and operation zones
- Restrict endpoint-to-endpoint communications
- Disable unnecessary services on endpoints
- Restrict the scope of accounts that can remotely access and interface with endpoints
  - Harden remote access methods for connecting to endpoints
- Leverage dedicated and enclaved privilege access workstations (PAWs) for performing administrative tasks
- Disable or restrict access to administrative / hidden shares on endpoints

Additional Proactive & Protective Focus Areas

- Enforce both network and identity segmentation between environments (ex: IT and OT)
- Establish and exercise backup plans for Domain Controllers / IAM stores / critical assets and data
- Enforce egress restrictions (external communication flows) for servers, core assets, and OT assets
- Enclave and isolate management interfaces for networking and security devices – including virtualization infrastructure
- Prevent external comms on SMB

Ransomware Protection and Containment Strategies



FIREEYE
Products
Mandiant Solutions
Customers
Home > FireEye Blogs > Threat Research > Ransomware Protection and Containment Strategies: ...

Threat Research

Ransomware Protection and Containment Strategies: Practical Guidance for Endpoint Protection, Hardening, and Containment

September 05, 2019 | by Matthew McWhirt

RANSOMWARE SECURITY STRATEGY ENDPOINT FEDERAL GOVERNMENT

UPDATE (Oct. 30, 2020): We have updated the report to include additional protection and containment strategies based on front-line visibility and response efforts in combating ransomware. While the full scope of recommendations included within the initial report remain unchanged, the following strategies have been added into the report:

- *Windows Firewall rule configurations to block specific binaries from establishing outbound connections from endpoints*
- *Domain Controller isolation and recovery planning steps*
- *Proactive GPO permissions review and monitoring guidance*

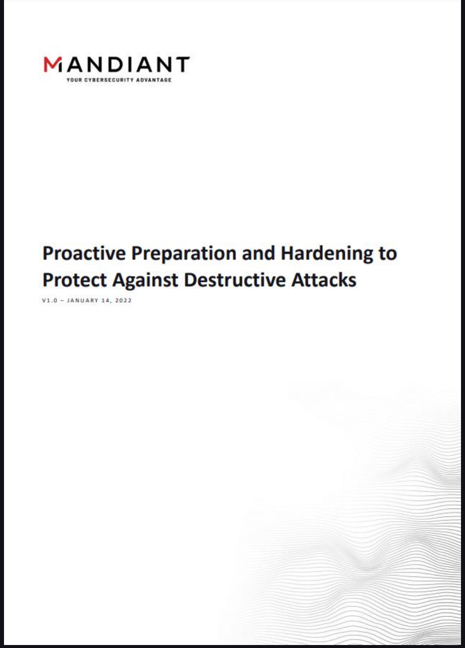
Ransomware is a global threat targeting organizations in all industries. The impact of a successful ransomware event can be material to an organization - including the loss of access to data, systems, and operational outages. The potential downtime, coupled with unforeseen expenses for restoration, recovery, and implementation of new security processes and controls can be overwhelming. Ransomware has become an increasingly popular choice for attackers over the past few years, and it's easy to understand why given how simple it is to leverage in campaigns – while offering a healthy financial return for attackers.

In our latest report, *Ransomware Protection and Containment Strategies: Practical Guidance for Endpoint Protection, Hardening, and Containment*, we discuss steps organizations can proactively take to harden their environment to prevent the downstream impact of a ransomware event. These recommendations can also help organizations with prioritizing the most important steps required to contain and minimize the impact of a ransomware event after it occurs.

Ransomware is commonly deployed across an environment in two ways:

For More Information and Intelligence

- Proactive Preparation and Hardening to Protect Against Destructive Attacks
  - Available at: https://www.mandiant.com/resources/protect-against-destructive-attacks
- Mandiant Advantage
  - Available at: mandiant.com/ti-free



MANDIANT
YOUR CYBERSECURITY ADVANTAGE

Proactive Preparation and Hardening to Protect Against Destructive Attacks

V1.0 – JANUARY 14, 2022

CHECK OUT
MANDIANT ADVANTAGE

COV-WIDE PHISHING CAMPAIGN

MARCH 2022

KATHY BORTLE & JAMES STURDEVANT, SR.

Incident Response Specialists

VITA/CSRM/THREAT MANAGEMENT TEAM

APRIL 6TH, 2022

OVERVIEW

OVERVIEW

March 2022 Phishing Campaign (Q1 2022)

VITA selected five messages that should have been relatively easy to identify to set a baseline. These messages were sent to all users with an active email address. The test for each group ran for three days after message delivery to collect the results. Any messages that bounced due to an account being disabled, were removed from the results before being sent to the ISO.

Here's what we learned…..

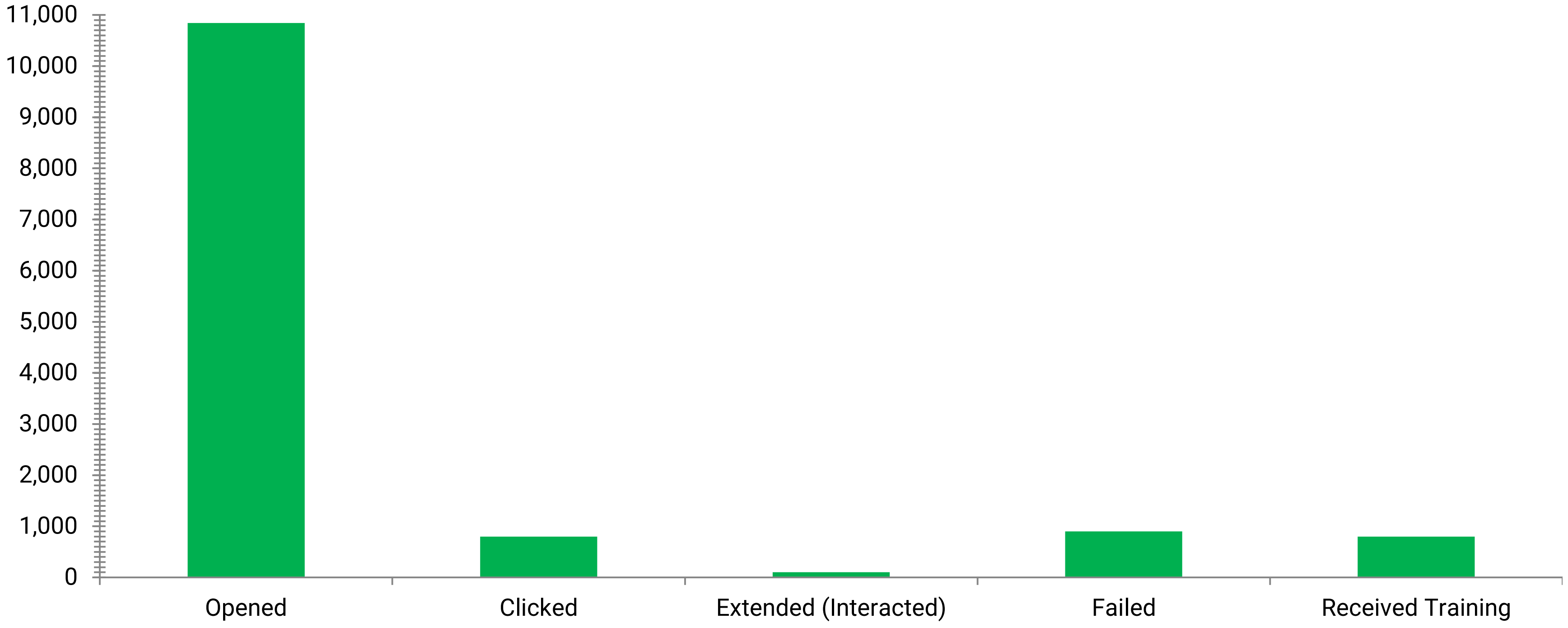
1. All domains need to be verified as whitelisted before the campaign starts.
2. All user accounts need to be verified as active before the campaign starts
3. The exhaustive report, which provides the actions a user performed, is limited to 2,500 rows not 2,500 users.
4. The .CSV file is meant to hold all results.

MARCH 2022

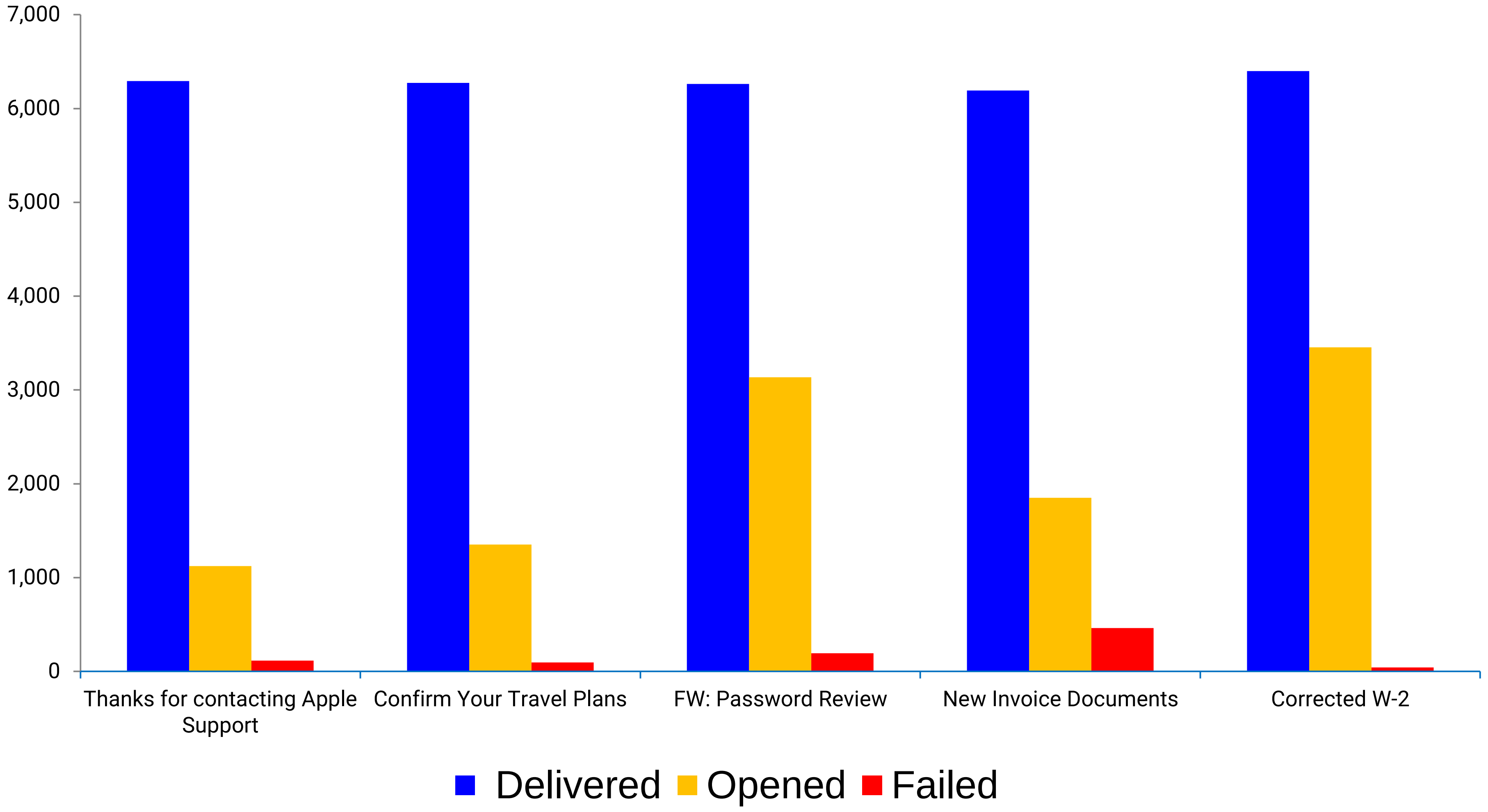
PHISHING CAMPAIGN

RESULTS

COV RESULTS BY ACTION TAKEN MARCH 2022

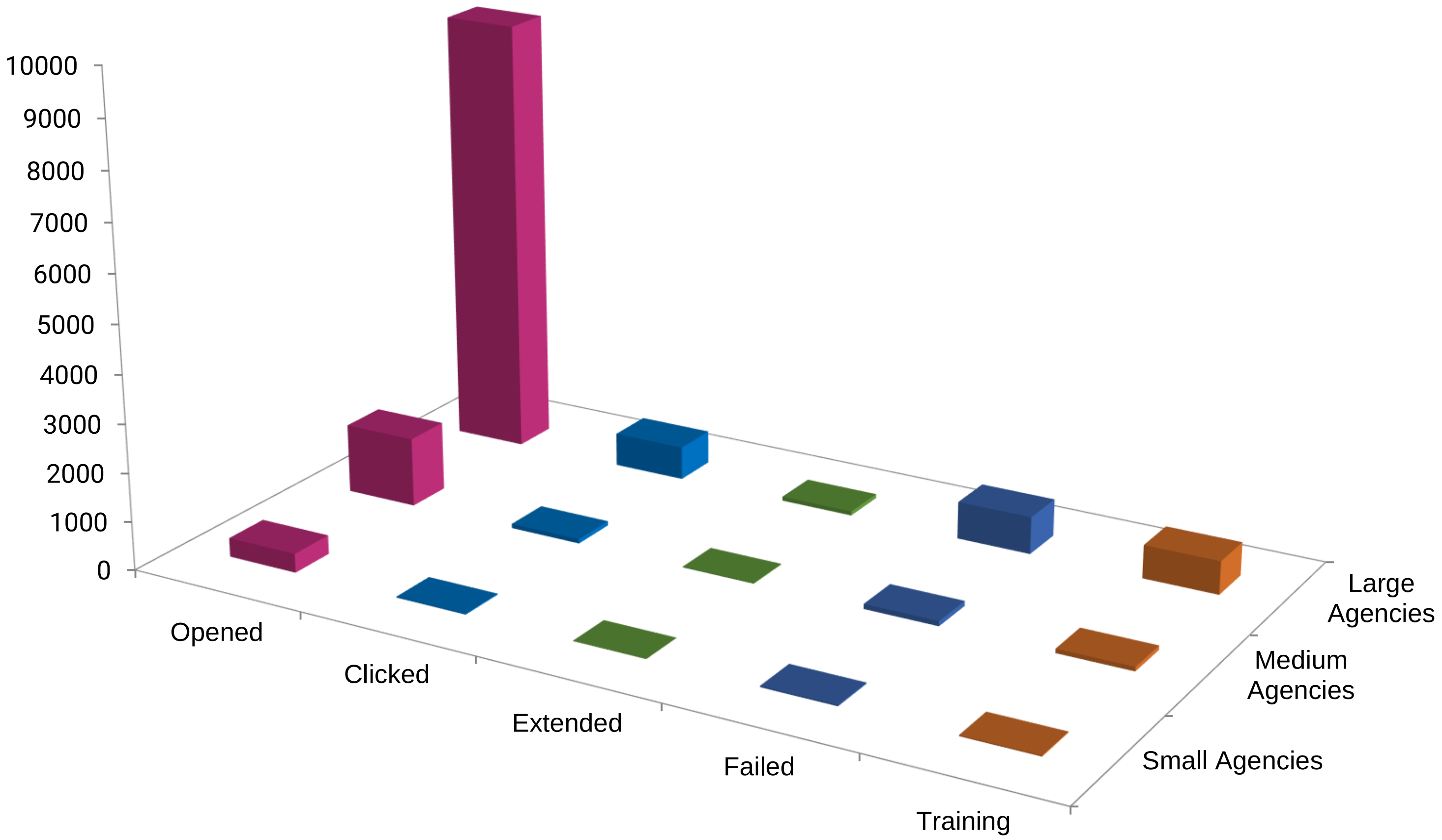


COV RESULTS BY PHISHING MESSAGE
MARCH 2022

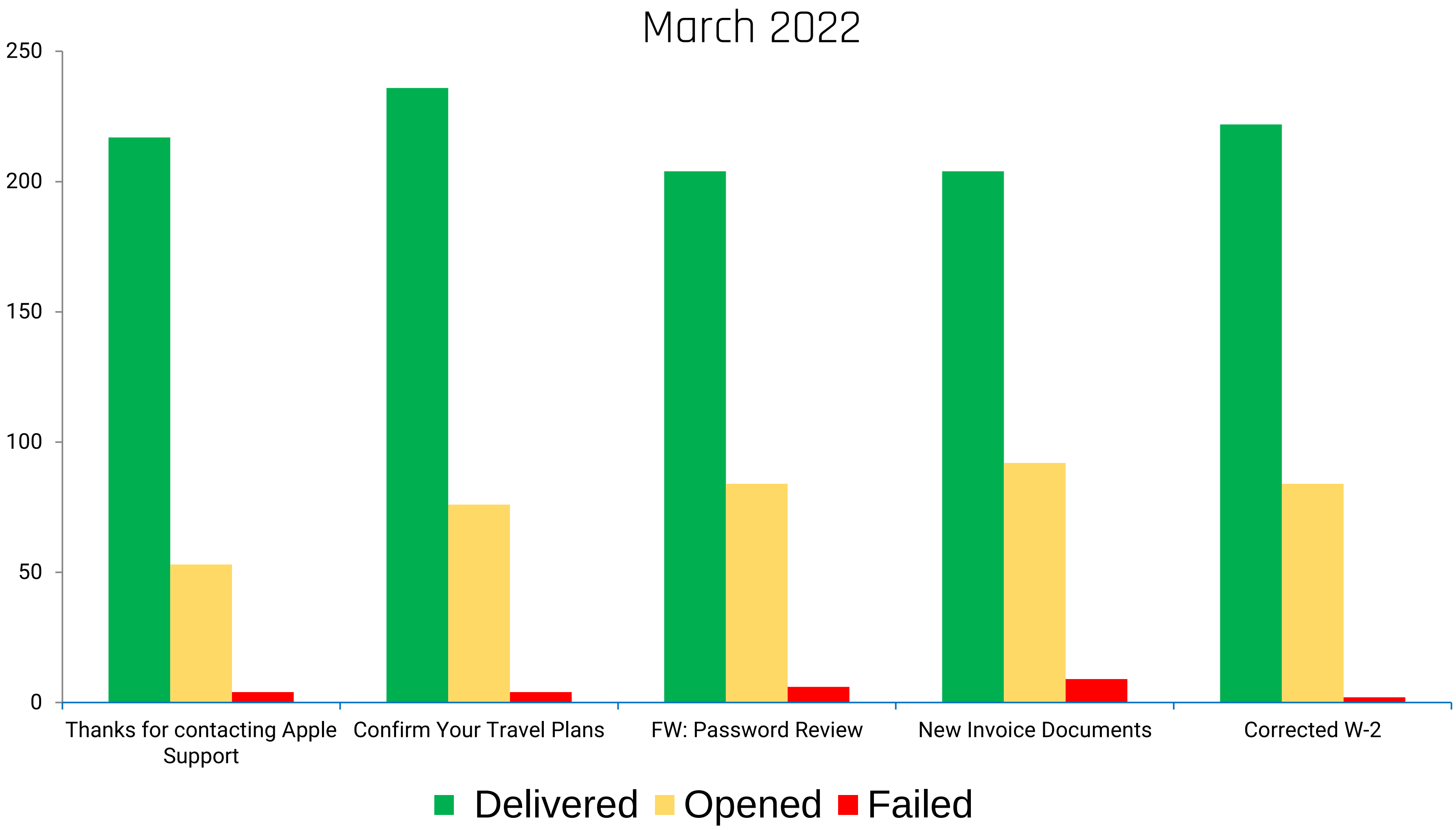


VIRGINIA IT AGENCY

AGENCY RESULTS BY ACTION TAKEN MARCH 2022

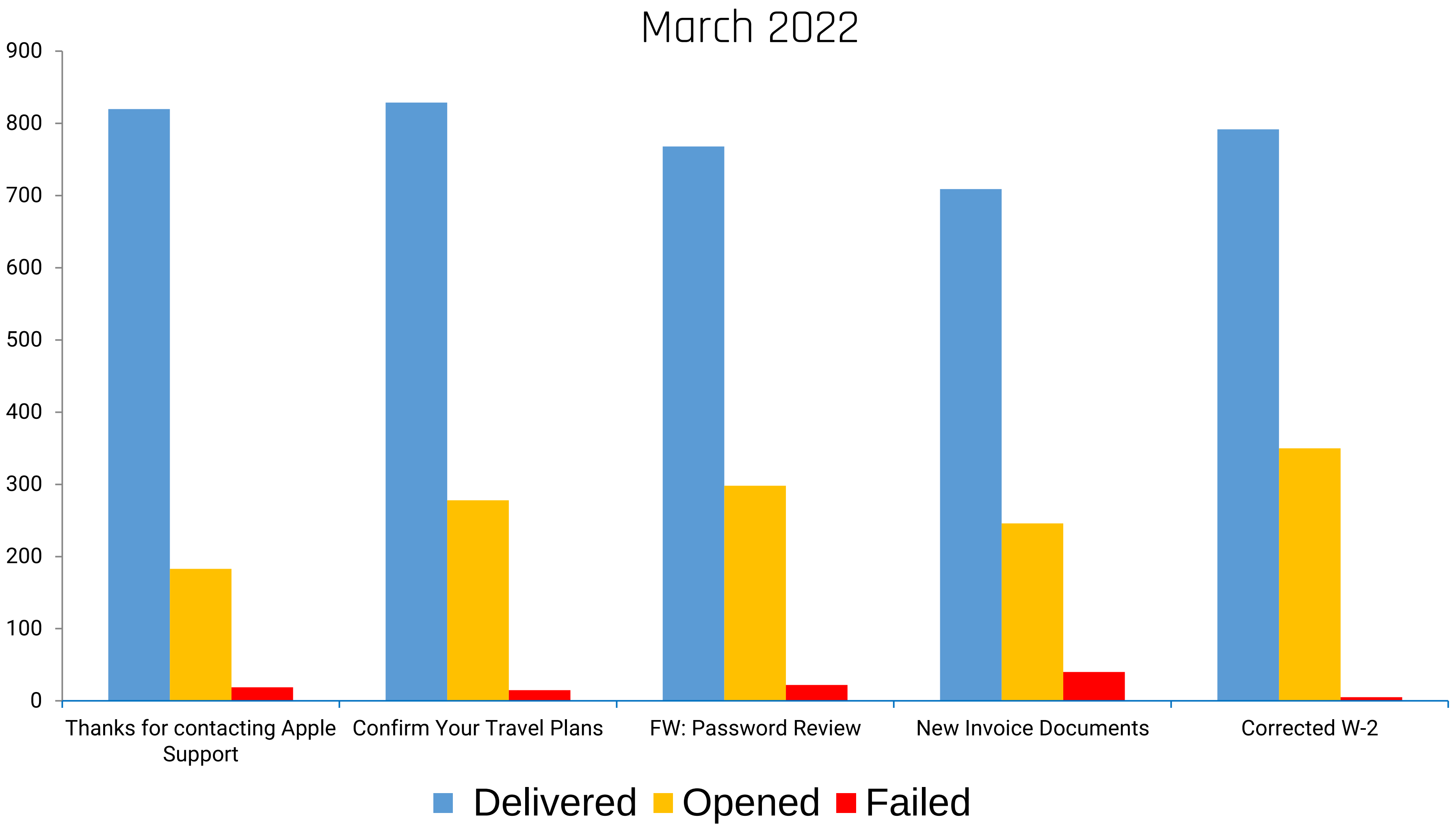


RESULTS BY PHISHING MESSAGE SMALL AGENCIES



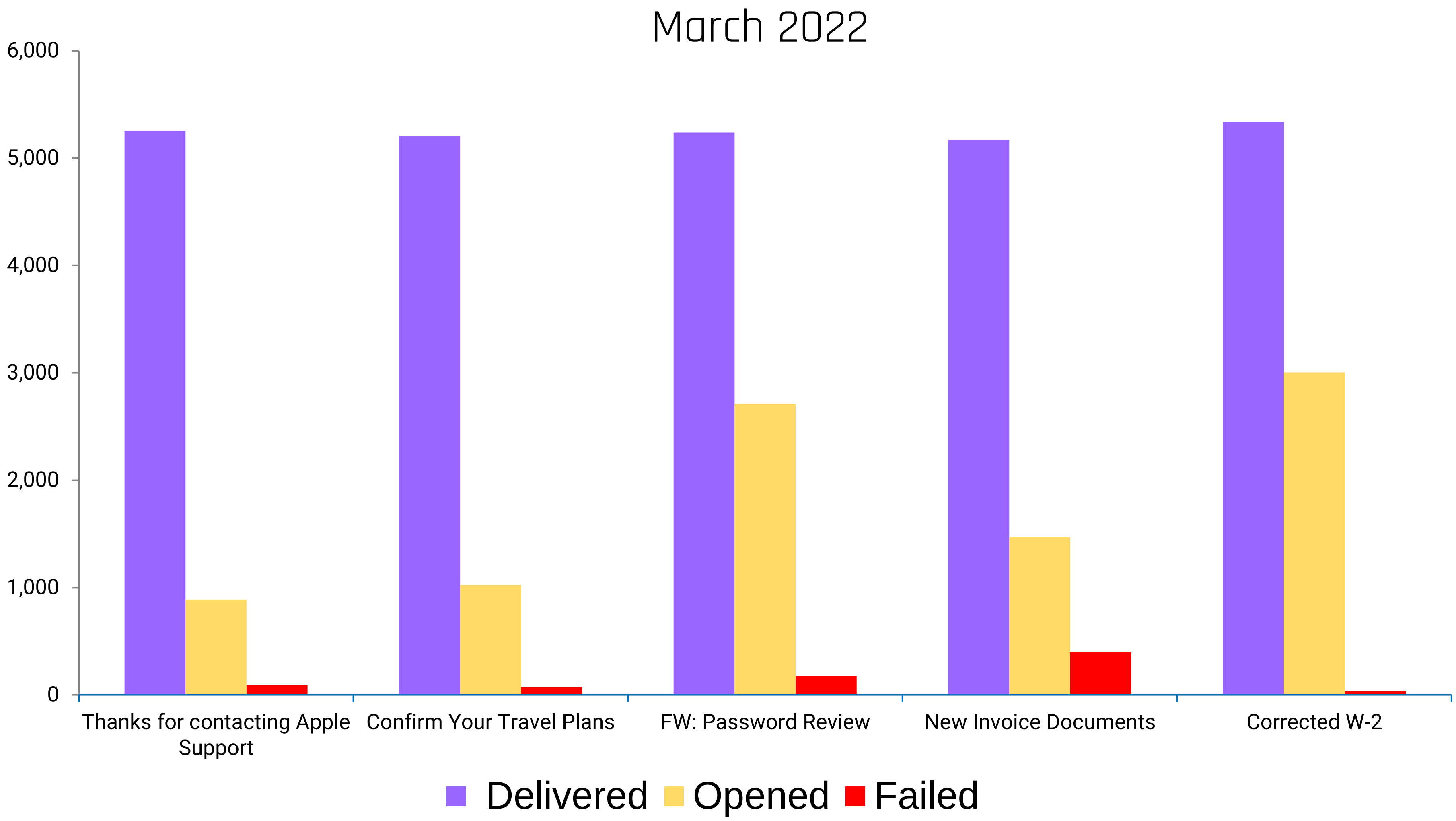
VIRGINIA IT AGENCY

RESULTS BY PHISHING MESSAGE MEDIUM AGENCIES

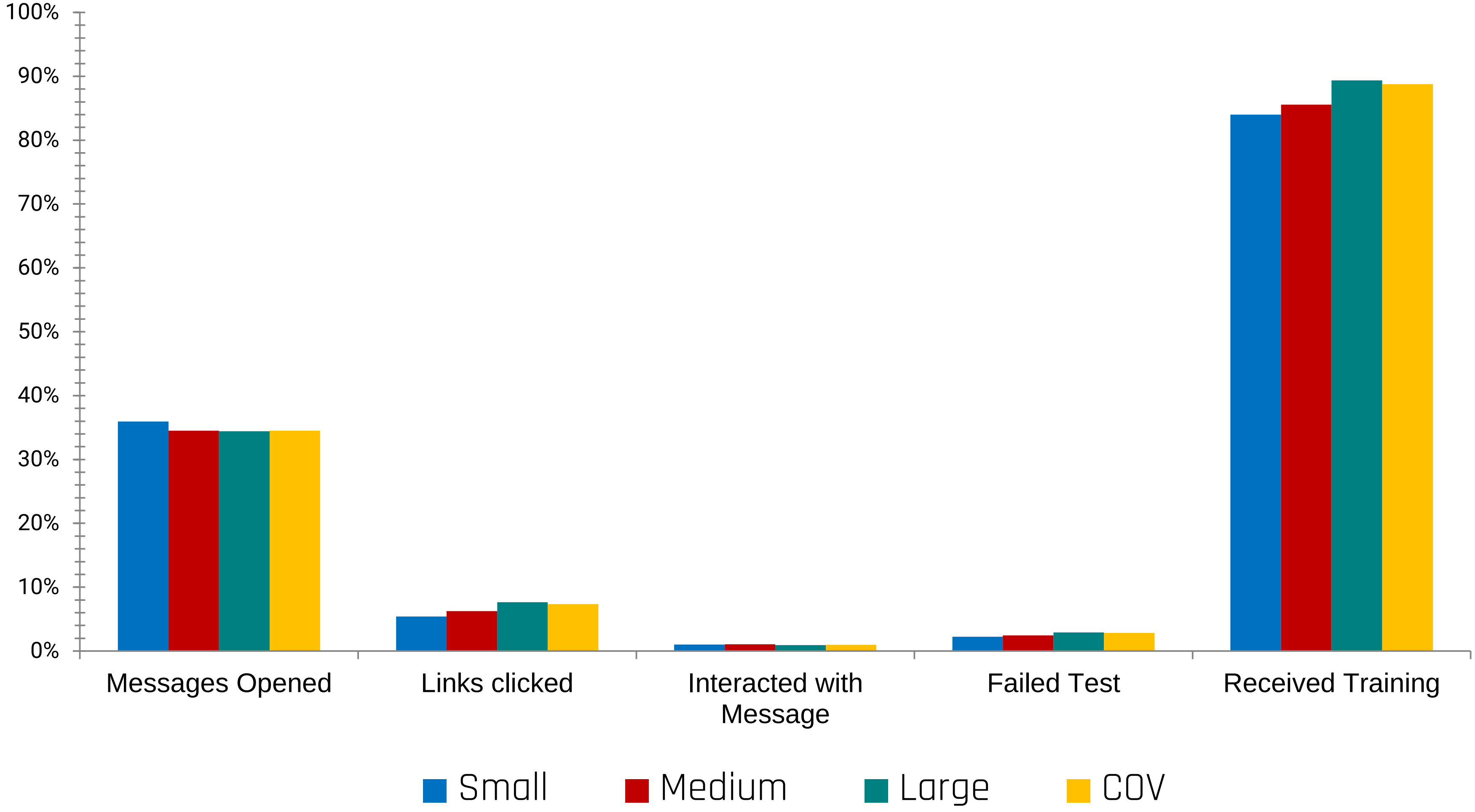


VIRGINIA IT AGENCY

RESULTS BY PHISHING MESSAGE LARGE AGENCIES

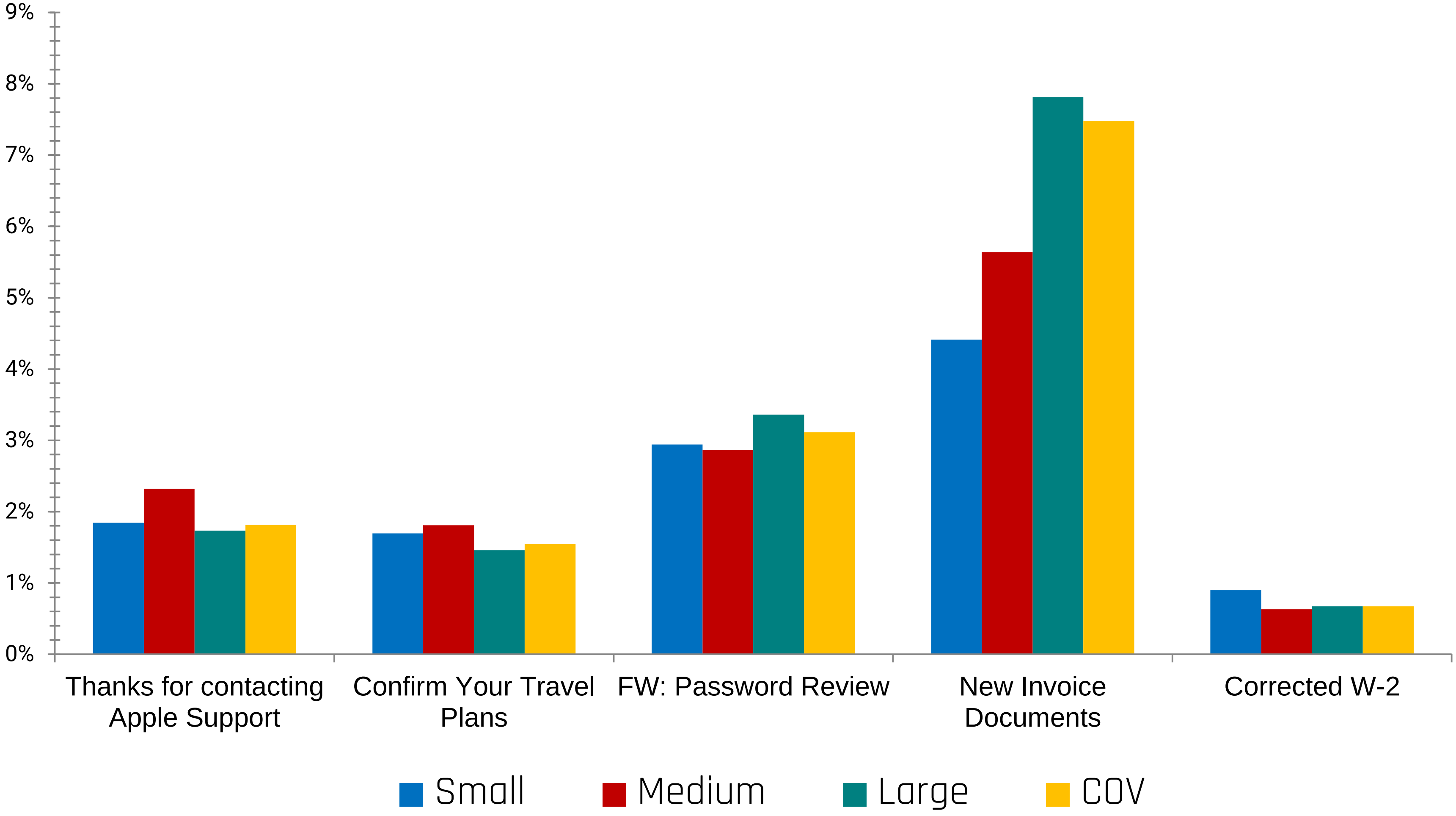


COV VS AGENCY ACTIONS TAKEN MARCH 2022



VIRGINIA IT AGENCY

SUCCESS RATE OF PHISHING MESSAGES MARCH 2022



VIRGINIA IT AGENCY

EXAMPLE REPORTS

REPORTING RESULTS

There are three types of reports that CSRM pulls once a phishing campaign has been completed. These are:

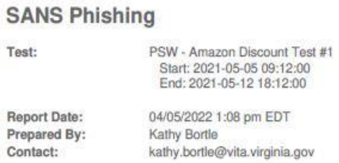
- Full Report
- Exhaustive Report
- Repeat Offenders Report – this report will be available after the user participates in multiple campaigns
- CSV Export - this file will contain all results for that test.

EXAMPLE REPORTS - FULL REPORT

FULL REPORT

INCLUDES:

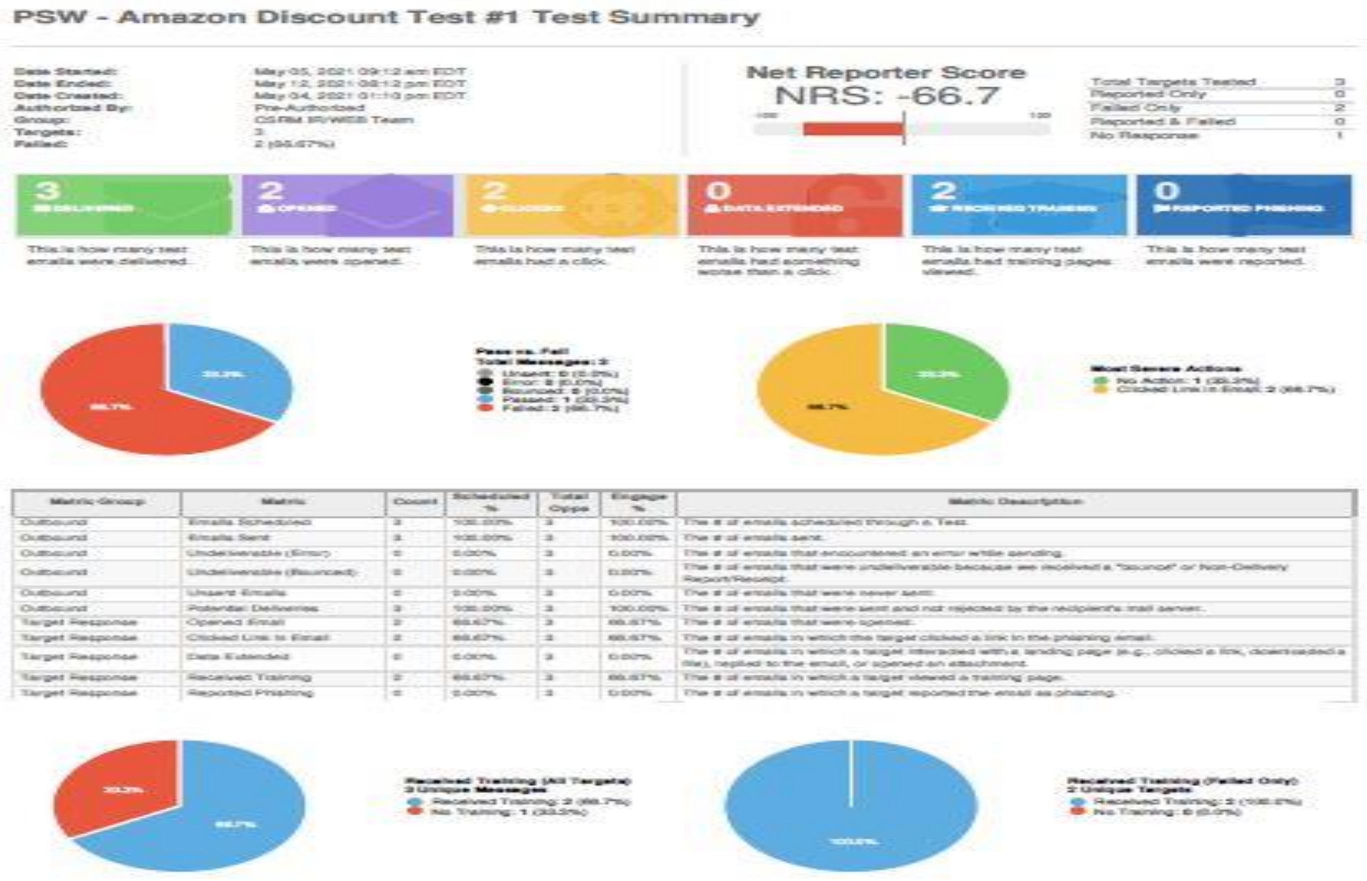
- TEST SUMMARY
- PHISHING TERM APPENDIX



SANS Phishing

Test:	PSW - Amazon Discount Test #1 Start: 2021-05-05 09:12:00 End: 2021-05-12 18:12:00
Report Date:	04/05/2022 1:08 pm EDT
Prepared By:	Kathy Bortle
Contact:	kathy.bortle@vita.virginia.gov

FULL REPORT TEST SUMMARY



PSW - Amazon Discount Test #1 Test Summary

Date Started:	May 05, 2021 09:12 am EDT
Date Ended:	May 12, 2021 08:12 pm EDT
Date Created:	May 04, 2021 01:10 pm EDT
Authorized By:	Pre-Authorized
Group:	CSRM IR/WSS Team
Targets:	3
Failed:	2 (66.67%)

Net Reporter Score

NRS: -66.7

Total Targets Tested	3
Reported Only	0
Failed Only	2
Reported & Failed	0
No Response	1

3 DELIVERED — This is how many test emails were delivered.

2 OPENED — This is how many test emails were opened.

2 CLICKED — This is how many test emails had a click.

0 DATA EXTENDED — This is how many test emails had something worse than a click.

2 RECEIVED TRAINING — This is how many test emails had training pages viewed.

0 REPORTED PHISHING — This is how many test emails were reported.

Pass vs. Fail
Total Messages: 3
- Unsent: 0 (0.0%)
- Error: 0 (0.0%)
- Bounced: 0 (0.0%)
- Passed: 1 (33.3%)
- Failed: 2 (66.7%)

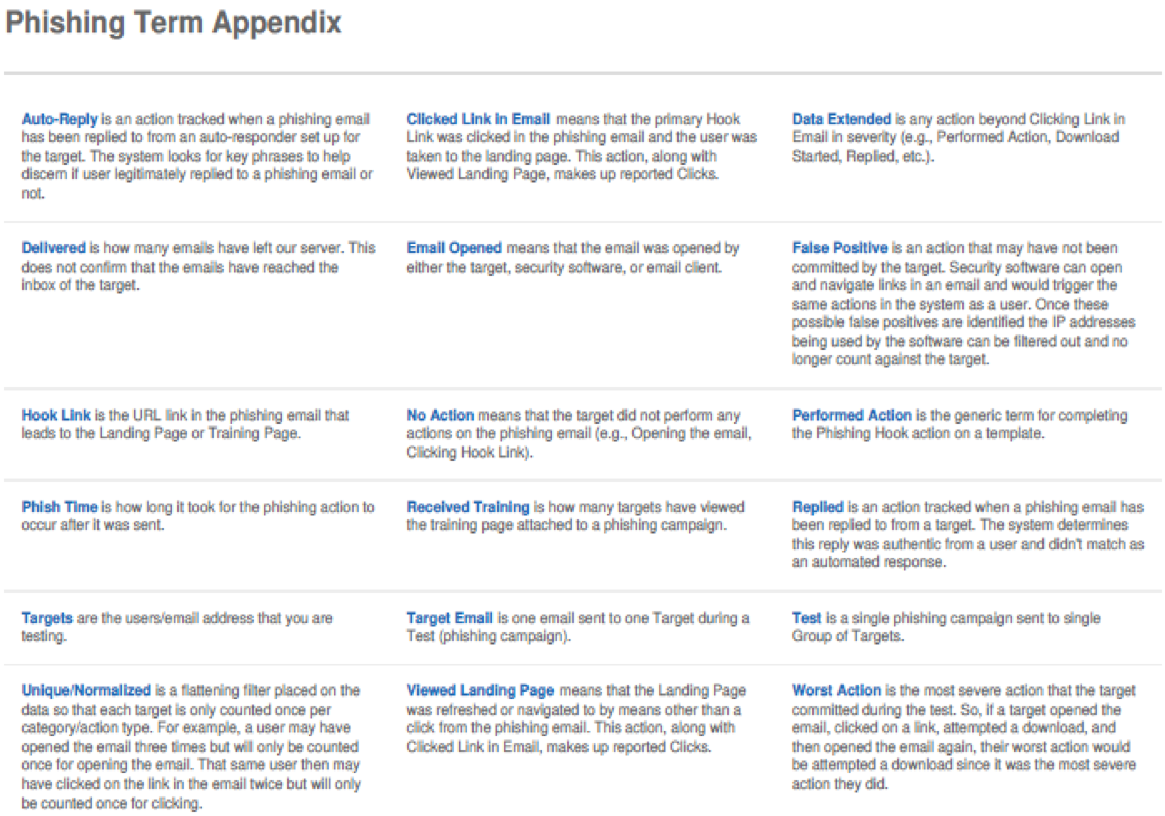
Most Severe Actions
- No Action: 1 (33.3%)
- Clicked Link in Email: 2 (66.7%)

Metric Group	Metric	Count	Scheduled %	Total Opps	Engage %	Metric Description
Outbound	Emails Scheduled	3	100.00%	3	100.00%	The # of emails scheduled through a Test.
Outbound	Emails Sent	3	100.00%	3	100.00%	The # of emails sent.
Outbound	Undeliverable (Error)	0	0.00%	3	0.00%	The # of emails that encountered an error while sending.
Outbound	Undeliverable (Bounced)	0	0.00%	3	0.00%	The # of emails that were undeliverable because we received a "bounce" or Non-Delivery Report/Receipt.
Outbound	Unsent Emails	0	0.00%	3	0.00%	The # of emails that were never sent.
Outbound	Potential Deliveries	3	100.00%	3	100.00%	The # of emails that were sent and not rejected by the recipient's mail server.
Target Response	Opened Email	2	66.67%	3	66.67%	The # of emails that were opened.
Target Response	Clicked Link In Email	2	66.67%	3	66.67%	The # of emails in which the target clicked a link in the phishing email.
Target Response	Data Extended	0	0.00%	3	0.00%	The # of emails in which a target interacted with a landing page (e.g., clicked a link, downloaded a file), replied to the email, or opened an attachment.
Target Response	Received Training	2	66.67%	3	66.67%	The # of emails in which a target viewed a training page.
Target Response	Reported Phishing	0	0.00%	3	0.00%	The # of emails in which a target reported the email as phishing.

Received Training (All Targets)
3 Unique Messages
- Received Training: 2 (66.7%)
- No Training: 1 (33.3%)

Received Training (Failed Only)
2 Unique Targets
- Received Training: 2 (100.0%)
- No Training: 0 (0.0%)

FULL REPORT – PHISHING TERM APPENDIX



Phishing Term Appendix

Auto-Reply is an action tracked when a phishing email has been replied to from an auto-responder set up for the target. The system looks for key phrases to help discern if user legitimately replied to a phishing email or not.

Clicked Link In Email means that the primary Hook Link was clicked in the phishing email and the user was taken to the landing page. This action, along with Viewed Landing Page, makes up reported Clicks.

Data Extended is any action beyond Clicking Link in Email in severity (e.g., Performed Action, Download Started, Replied, etc.).

Delivered is how many emails have left our server. This does not confirm that the emails have reached the inbox of the target.

Email Opened means that the email was opened by either the target, security software, or email client.

False Positive is an action that may have not been committed by the target. Security software can open and navigate links in an email and would trigger the same actions in the system as a user. Once these possible false positives are identified the IP addresses being used by the software can be filtered out and no longer count against the target.

Hook Link is the URL link in the phishing email that leads to the Landing Page or Training Page.

No Action means that the target did not perform any actions on the phishing email (e.g., Opening the email, Clicking Hook Link).

Performed Action is the generic term for completing the Phishing Hook action on a template.

Phish Time is how long it took for the phishing action to occur after it was sent.

Received Training is how many targets have viewed the training page attached to a phishing campaign.

Replied is an action tracked when a phishing email has been replied to from a target. The system determines this reply was authentic from a user and didn't match as an automated response.

Targets are the users/email address that you are testing.

Target Email is one email sent to one Target during a Test (phishing campaign).

Test is a single phishing campaign sent to single Group of Targets.

Unique/Normalized is a flattening filter placed on the data so that each target is only counted once per category/action type. For example, a user may have opened the email three times but will only be counted once for opening the email. That same user then may have clicked on the link in the email twice but will only be counted once for clicking.

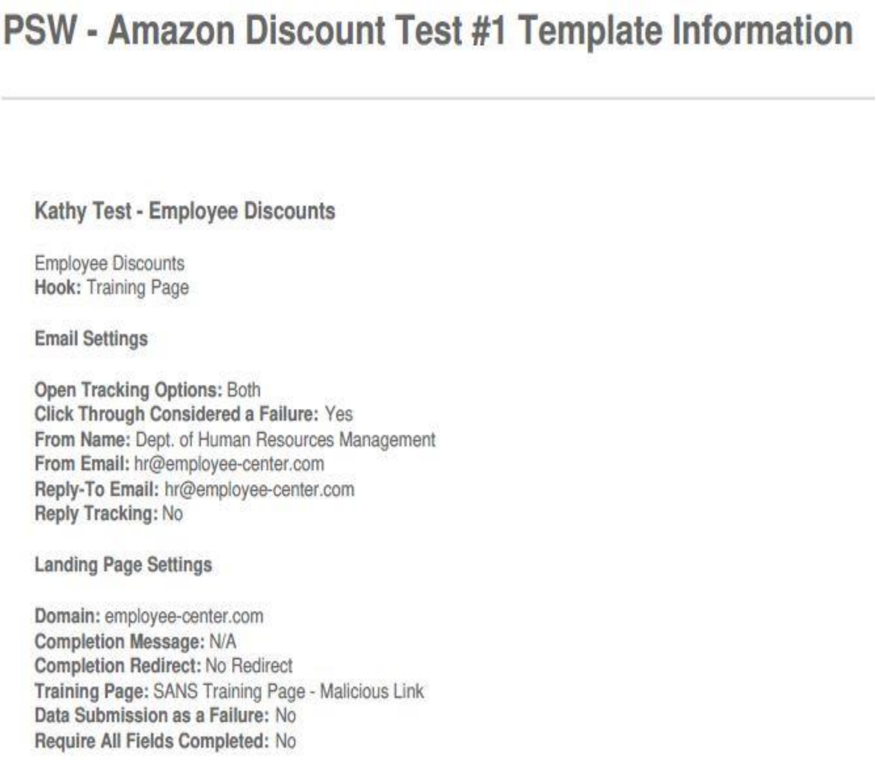
Viewed Landing Page means that the Landing Page was refreshed or navigated to by means other than a click from the phishing email. This action, along with Clicked Link in Email, makes up reported Clicks.

Worst Action is the most severe action that the target committed during the test. So, if a target opened the email, clicked on a link, attempted a download, and then opened the email again, their worst action would be attempted a download since it was the most severe action they did.

EXHAUSTIVE REPORT

INCLUDES:

- TEST SUMMARY (SAME AS FULL REPORT)
- TEMPLATE INFORMATION
- ACTION BREAKDOWN (LIMITED TO 2500 ROWS)
- IP ADDRESS USER HIT LOCATIONS
- PHISHING TERM APPENDIX



PSW - Amazon Discount Test #1 Template Information

Kathy Test - Employee Discounts

Employee Discounts
Hook: Training Page

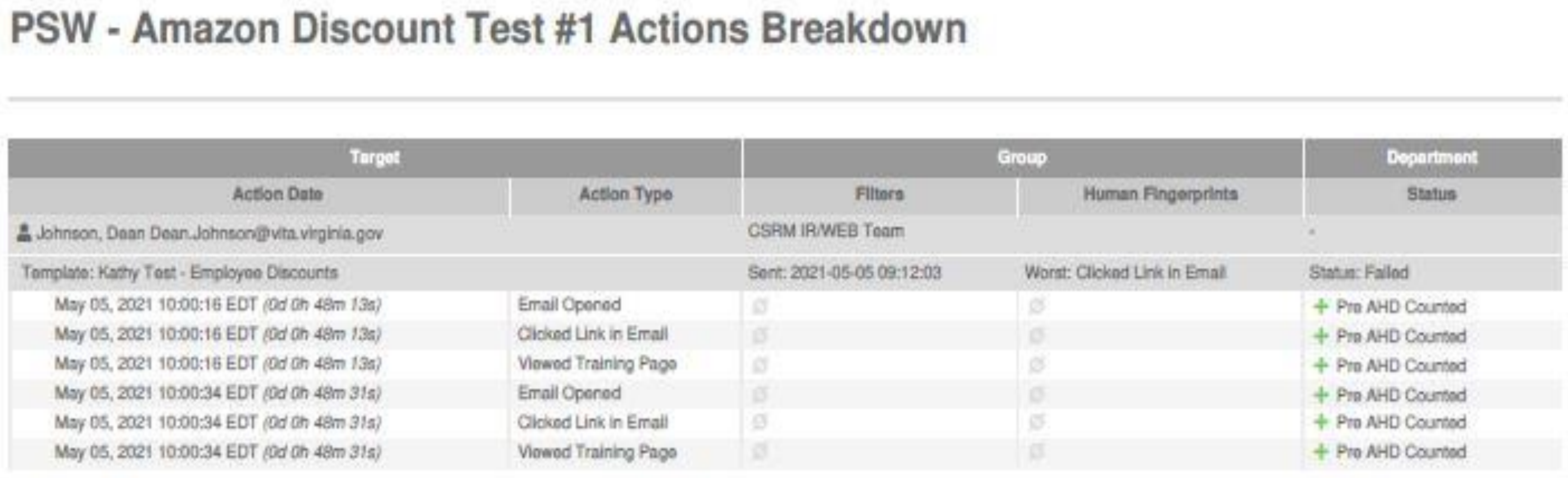
Email Settings

Open Tracking Options: Both
Click Through Considered a Failure: Yes
From Name: Dept. of Human Resources Management
From Email: hr@employee-center.com
Reply-To Email: hr@employee-center.com
Reply Tracking: No

Landing Page Settings

Domain: employee-center.com
Completion Message: N/A
Completion Redirect: No Redirect
Training Page: SANS Training Page - Malicious Link
Data Submission as a Failure: No
Require All Fields Completed: No

EXHAUSTIVE REPORT ACTION BREAKDOWN TABLE*



PSW - Amazon Discount Test #1 Actions Breakdown

Target		Group		Department
Action Date	Action Type	Filters	Human Fingerprints	Status
Johnson, Dean Dean.Johnson@vita.virginia.gov		CSRM IR/WEB Team		-
Template: Kathy Test - Employee Discounts		Sent: 2021-05-05 09:12:03	Worst: Clicked Link in Email	Status: Failed
May 05, 2021 10:00:16 EDT *(0d 0h 48m 13s)*	Email Opened			+ Pre AHD Counted
May 05, 2021 10:00:16 EDT *(0d 0h 48m 13s)*	Clicked Link in Email			+ Pre AHD Counted
May 05, 2021 10:00:16 EDT *(0d 0h 48m 13s)*	Viewed Training Page			+ Pre AHD Counted
May 05, 2021 10:00:34 EDT *(0d 0h 48m 31s)*	Email Opened			+ Pre AHD Counted
May 05, 2021 10:00:34 EDT *(0d 0h 48m 31s)*	Clicked Link in Email			+ Pre AHD Counted
May 05, 2021 10:00:34 EDT *(0d 0h 48m 31s)*	Viewed Training Page			+ Pre AHD Counted

* Table is limited to 2500 rows

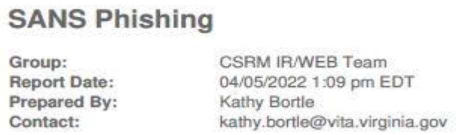
EXAMPLE REPORTS – REPEAT OFFERS REPORT

REPEAT OFFENDERS REPORT

INCLUDES:

- REPEAT OFFENDERS
- PHISHING TERM APPENDIX

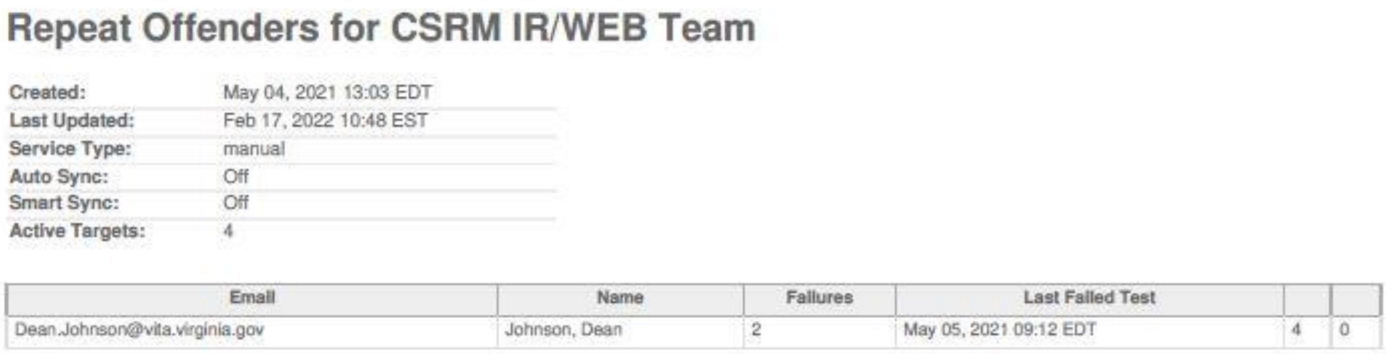
Repeat Failures-By Date Report



SANS Phishing

Group:	CSRM IR/WEB Team
Report Date:	04/05/2022 1:09 pm EDT
Prepared By:	Kathy Bortle
Contact:	kathy.bortle@vita.virginia.gov

REPEAT OFFENDERS REPORT DETAIL

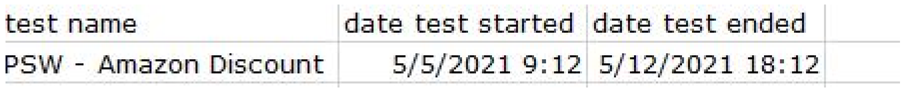


Repeat Offenders for CSRM IR/WEB Team

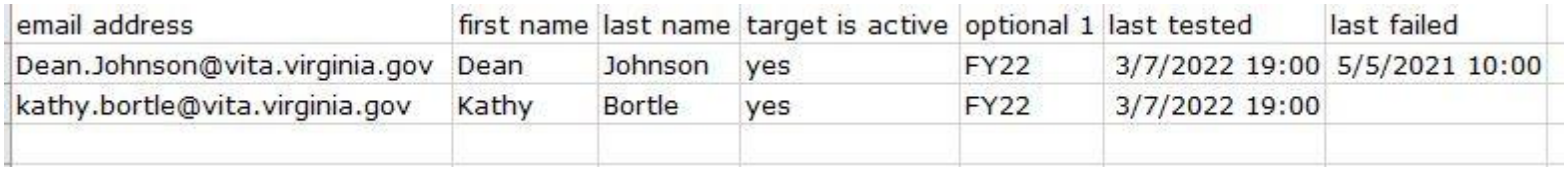
Created:	May 04, 2021 13:03 EDT
Last Updated:	Feb 17, 2022 10:48 EST
Service Type:	manual
Auto Sync:	Off
Smart Sync:	Off
Active Targets:	4

Email	Name	Failures	Last Failed Test		
Dean.Johnson@vita.virginia.gov	Johnson, Dean	2	May 05, 2021 09:12 EDT	4	0

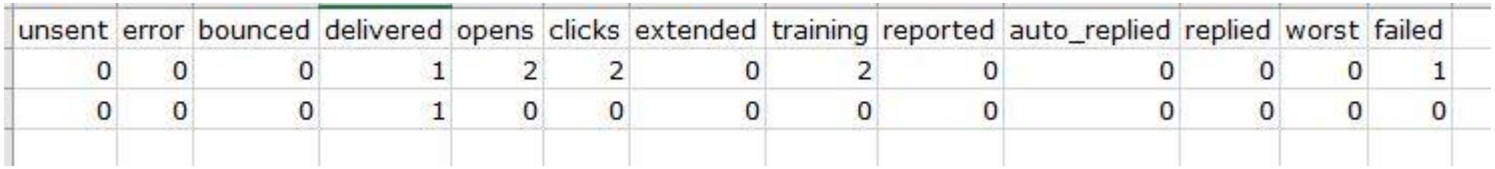
CSV FILE OF FULL RESULTS – IMPORTANT FIELDS



test name	date test started	date test ended
PSW - Amazon Discount	5/5/2021 9:12	5/12/2021 18:12



email address	first name	last name	target is active	optional 1	last tested	last failed
Dean.Johnson@vita.virginia.gov	Dean	Johnson	yes	FY22	3/7/2022 19:00	5/5/2021 10:00
kathy.bortle@vita.virginia.gov	Kathy	Bortle	yes	FY22	3/7/2022 19:00	



unsent	error	bounced	delivered	opens	clicks	extended	training	reported	auto_replied	replied	worst	failed
0	0	0	1	2	2	0	2	0	0	0	0	1
0	0	0	1	0	0	0	0	0	0	0	0	0

GOING FORWARD

QUARTERLY PHISHING CAMPAIGNS

The CSRM Threat Management Team will be performing COV Wide Phishing Campaigns once a quarter.

- The next campaign will be scheduled for June 2022.
- All details for the campaign will be shared with the ISOs, ATOS and the MSI prior to campaign start.
- All account verification will be completed prior to campaign start.
- ISOs will receive results once verified following the campaign.
- Results will include:
  - Full Report
  - Exhaustive Report if user actions are displayed
  - CSV files of all results
  - Repeat Offender reports if applicable
- Starting in July, we will be switching to the FY23 users for our phishing campaigns. These folks will be tested for the first time in Q3 2022.

QUESTIONS?

CONTACT INFO

Dean Johnson, Director of Threat Management

Dean.Johnson@vita.Virginia.gov

804-416-8785

Kathy Bortle , Incident Response Specialist

Kathy.borle@vita.Virginia.gov

804-416-6061

Jim Sturdevant, Sr., Incident Response Specialist

Jim.sturdevant@vita.Virginia.gov

804-416-6038

VIRGINIA IT AGENCY

Upcoming events

THE COMMONWEALTH OF VIRGINIA SECURITY CONFERENCE WILL BE HELD ON AUG. 18, 2022, VIRTUALLY.

MORE DETAILS WILL BE FORTHCOMNG.

MAY 2022 ISOAG

May 4, 2022, from 1 to 4 p.m.

Presenters:

Scott Debb/NSU

John Joseph/Obtegocyber

Samuel “Gene” Fishel/OAG

VIRGINIA IT AGENCY

THANK YOU FOR ATTENDING!