WELCOME TO THE
APRIL 6, 2022
ISOAG MEETING
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
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
## The Matrix of the Model

<table>
<thead>
<tr>
<th></th>
<th>Systems</th>
<th>Analytics</th>
<th>Design</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Education</strong></td>
<td>Aggregating student data</td>
<td>Predictive models for K-12</td>
<td>Push campaigns</td>
<td>Bias and social inequalities</td>
</tr>
<tr>
<td><strong>Finance</strong></td>
<td>Cybersecurity and fraud</td>
<td>Adversarial models for fraud</td>
<td>Investment storytelling</td>
<td>ROI of Data Science</td>
</tr>
<tr>
<td><strong>Digital Humanities</strong></td>
<td>Sensor Network data</td>
<td>Text analytics on corpus</td>
<td>Data representation</td>
<td>Data creation and evaluation</td>
</tr>
<tr>
<td><strong>Public Policy</strong></td>
<td>Aggregating agency data</td>
<td>Predictive policing</td>
<td>COVID dashboards</td>
<td>Security and privacy</td>
</tr>
</tbody>
</table>
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](https://doi.org/10.1038/sdata.2016.18)
Implementing a Sustainable Growth Plan

- Partnership
- Resources
- Program Development
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
  - Creates 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
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
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
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.

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.
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

www.vsp.virginia.gov
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.

www.vsp.virginia.gov
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
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
Multi-Faceted Extortion
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

RESEARCH DEMONSTRATES WHY BREACHES SO FREQUENTLY OCCUR

53%
Organizations are completely missing or unaware of executed attacks
Broken Processes & Misconfigured Tools...

68%
Not preventing over...

On average 91%
Of ransomware attacks...
Of attacks go undetected

SECURITY VALIDATION MARKET

Evolution of the Security Validation Program

Leveraging testing & validation, shifting from establishing a program, to enabling measured business objectives...
## Attacker Dwell Time

**2019 Global Median Dwell Time**: 56 DAYS  
**2021 Global Median Dwell Time**: 21 DAYS

### Year Over Year

### Over A Decade

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>416</td>
<td>243</td>
<td>229</td>
<td>205</td>
<td>146</td>
<td>99</td>
<td>101</td>
<td>78</td>
<td>56</td>
<td>24</td>
<td>21</td>
</tr>
<tr>
<td>External Notification</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>320</td>
<td>107</td>
<td>186</td>
<td>184</td>
<td>141</td>
<td>73</td>
<td>28</td>
</tr>
<tr>
<td>Internal Detection</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>56</td>
<td>80</td>
<td>57.5</td>
<td>50.5</td>
<td>30</td>
<td>12</td>
<td>18</td>
</tr>
</tbody>
</table>
2021 Trends
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**: SamSam
- **2015**: WannaCry / NotPetya
- **2016**: Ryuk
- **2017**: FIN6 incorporates ransomware
- **2018**: Victim Naming and Shaming Trend Begins in Q4
- **2019**: Indictment and Sanctions of SamSam operators
- **2020**: Indictment and Sanctions of Dridex operators ("EvilCorp")
- **2021**: Targeting of Healthcare Organizations

**Key Events**
- **2021**: Colonial Pipeline incident
- **2020**: FBI reclaims partial extortion payment
- **2019**: Revil, DopplePaymer, Conti, Netwalker and others create public shaming sites
- **2018**: Ryuk
- **2017**: Victim Naming and Shaming Trend Begins in Q4
- **2016**: WannaCry / NotPetya
- **2015**: SamSam
- **2014**: SamSam
- **2013**: CryptoLocker
Evolution of Ransomware
Evolution of Ransomware

POST COMPROMISE APPROACH

1ST STAGE
Credential Theft
Internal Reconnaissance
Lateral Movement Tools
Escalate Privileges
Delete Backups

2ND STAGE
Data Theft
(Often)

3RD STAGE
Encryptor Deployment

Attacker → Victim Organization → 1ST STAGE → 2ND STAGE → 3RD STAGE → Encryptor Deployment
Victim Shaming Sites and Data Exposure

Represented here companies attack on their resources. Waiting for the download link will be soon.

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.
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
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, PSEexec, 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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>How <strong>quickly can you recover</strong> your systems and data on your own?</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>How <strong>reliable</strong> is the threat actor?</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Did the threat actor <strong>steal data</strong> before they deployed their encryptors? How sensitive is the data that they stole?</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Does the threat actor still have <strong>active access</strong> to your network?</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>Will <strong>cybersecurity insurance</strong> cover the claim?</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td><strong>If considering payment</strong> - Is the threat actor <strong>sanctioned</strong> by the U.S. Department of Treasury?</td>
</tr>
</tbody>
</table>
## Learnings from Paying Threat Actors

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Threat actors usually have <strong>multiple backdoors</strong> and can technically re-encrypt data if they wanted to</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>You don’t know who you’re paying - some threat actors are <strong>sanctioned</strong></td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Many threat actors are <strong>reliable</strong> – their business model depends on it</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Many threat actors <strong>move on to the next target</strong> when paid – they have plenty of victims to choose from</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td><strong>No guarantees</strong> that stolen data will be deleted (despite providing “proof” of deletion)</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td>Prior to 2019, we observed many threat actors that publicized stolen data and <strong>re-extorted victims</strong> after being paid</td>
</tr>
</tbody>
</table>
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

- **Threat Actor Investment**
  - Low
  - High

- **Attack Surface Reduction & Detection Investment**
  - Low
  - High

- **Depth of Access**
  - External-Facing Applications & Services
  - Brute Forcing
  - Stolen / Compromised Credentials
  - Single Factor Remote Access
  - Phishing
  - Weaponized Documents
  - Supply Chain
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

Threat Research

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

September 05, 2019 | by Matthew McWhirt

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 GP0 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
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
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

<table>
<thead>
<tr>
<th>Action</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opened</td>
<td>11,000</td>
</tr>
<tr>
<td>Clicked</td>
<td>0</td>
</tr>
<tr>
<td>Extended (Interacted)</td>
<td>0</td>
</tr>
<tr>
<td>Failed</td>
<td>0</td>
</tr>
<tr>
<td>Received Training</td>
<td>0</td>
</tr>
</tbody>
</table>
AGENCY RESULTS BY ACTION TAKEN
MARCH 2022

Opened

Clicked

Extended

Failed

Training

0
1000
2000
3000
4000
5000
6000
7000
8000
9000
10000

Large Agencies

Medium Agencies

Small Agencies
RESULTS BY PHISHING MESSAGE
SMALL AGENCIES

March 2022

- Thanks for contacting Apple Support
- Confirm Your Travel Plans
- FW: Password Review
- New Invoice Documents
- Corrected W-2

Legend:
- Green: Delivered
- Yellow: Opened
- Red: Failed
SUCCESS RATE OF PHISHING MESSAGES
MARCH 2022

SUCCESS RATES:
- Thanks for contacting Apple Support: 2%
- Confirm Your Travel Plans: 2%
- FW: Password Review: 3%
- New Invoice Documents: 8%
- Corrected W-2: 1%

SUCCESS RATES PER SIZE:
- Small
- Medium
- Large
- COV
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.
FULL REPORT

INCLUDES:

• TEST SUMMARY

• PHISHING TERM APPENDIX
# Phishing Term Appendix

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auto-Reply</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Clicked Link in Email</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Data Extended</strong></td>
<td>is any action beyond Clicking Link in Email in severity (e.g., Performed Action, Download Started, Replied, etc.).</td>
</tr>
<tr>
<td><strong>Delivered</strong></td>
<td>is how many emails have left our server. This does not confirm that the emails have reached the inbox of the target.</td>
</tr>
<tr>
<td><strong>Email Opened</strong></td>
<td>means that the email was opened by either the target, security software, or email client.</td>
</tr>
<tr>
<td><strong>False Positive</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Hook Link</strong></td>
<td>is the URL link in the phishing email that leads to the Landing Page or Branding Page.</td>
</tr>
<tr>
<td><strong>No Action</strong></td>
<td>means that the target did not perform any actions on the phishing email (e.g., Clicking Hook Link).</td>
</tr>
<tr>
<td><strong>Performed Action</strong></td>
<td>is the generic term for completing the Phishing Hook action on a template.</td>
</tr>
<tr>
<td><strong>Phish Time</strong></td>
<td>is how long it took for the phishing action to occur after it was sent.</td>
</tr>
<tr>
<td><strong>Replied</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Received Training</strong></td>
<td>is how many targets have viewed the training page attached to a phishing campaign.</td>
</tr>
<tr>
<td><strong>Test</strong></td>
<td>is a single phishing campaign sent to single Group of Targets.</td>
</tr>
<tr>
<td><strong>Targets</strong></td>
<td>are the users/email address that you are testing.</td>
</tr>
<tr>
<td><strong>Target Email</strong></td>
<td>is one email sent to one Target during a Test (phishing campaign).</td>
</tr>
<tr>
<td><strong>Viewed Landing Page</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Worst Action</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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
# PSW - Amazon Discount Test #1 Actions Breakdown

<table>
<thead>
<tr>
<th>Target</th>
<th>Action Date</th>
<th>Action Type</th>
<th>Filters</th>
<th>Group</th>
<th>Human Fingerprints</th>
<th>Department</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>May 05, 2021 10:00:16 EDT (0d 0h 48m 13s)</td>
<td>Email Opened</td>
<td></td>
<td>CSRM IR/WEB Team</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>May 05, 2021 10:00:16 EDT (0d 0h 48m 13s)</td>
<td>Clicked Link in Email</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>May 05, 2021 10:00:16 EDT (0d 0h 48m 13s)</td>
<td>Viewed Training Page</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>May 05, 2021 10:00:34 EDT (0d 0h 48m 31s)</td>
<td>Email Opened</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>May 05, 2021 10:00:34 EDT (0d 0h 48m 31s)</td>
<td>Clicked Link in Email</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>May 05, 2021 10:00:34 EDT (0d 0h 48m 31s)</td>
<td>Viewed Training Page</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Table is limited to 2500 rows
REPEAT OFFENDERS REPORT

INCLUDES:

• REPEAT OFFENDERS

• PHISHING TERM APPENDIX
REPEAT OFFENDERS REPORT DETAIL

Repeat Offenders for CSRM IR/WEB Team

<table>
<thead>
<tr>
<th>Created:</th>
<th>May 04, 2021 13:03 EDT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Updated:</td>
<td>Feb 17, 2022 10:48 EST</td>
</tr>
<tr>
<td>Service Type:</td>
<td>manual</td>
</tr>
<tr>
<td>Auto Sync:</td>
<td>Off</td>
</tr>
<tr>
<td>Smart Sync:</td>
<td>Off</td>
</tr>
<tr>
<td>Active Targets:</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email</th>
<th>Name</th>
<th>Failures</th>
<th>Last Failed Test</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:Dean.Johnson@vita.virginia.gov">Dean.Johnson@vita.virginia.gov</a></td>
<td>Johnson, Dean</td>
<td>2</td>
<td>May 05, 2021 09:12 EDT</td>
<td>4</td>
</tr>
</tbody>
</table>
## CSV FILE OF FULL RESULTS - IMPORTANT FIELDS

<table>
<thead>
<tr>
<th>test name</th>
<th>date test started</th>
<th>date test ended</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSW - Amazon Discount</td>
<td>5/5/2021 9:12</td>
<td>5/12/2021 18:12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>email address</th>
<th>first name</th>
<th>last name</th>
<th>target is active</th>
<th>optional 1</th>
<th>last tested</th>
<th>last failed</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:Dean.Johnson@vita.virginia.gov">Dean.Johnson@vita.virginia.gov</a></td>
<td>Dean</td>
<td>Johnson</td>
<td>yes</td>
<td>FY22</td>
<td>3/7/2022 19:00</td>
<td>5/5/2021 10:00</td>
</tr>
<tr>
<td><a href="mailto:kathy.bortle@vita.virginia.gov">kathy.bortle@vita.virginia.gov</a></td>
<td>Kathy</td>
<td>Bortle</td>
<td>yes</td>
<td>FY22</td>
<td>3/7/2022 19:00</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>unsent</th>
<th>error</th>
<th>bounced</th>
<th>delivered</th>
<th>opens</th>
<th>clicks</th>
<th>extended</th>
<th>training</th>
<th>reported</th>
<th>auto_replied</th>
<th>replied</th>
<th>worst</th>
<th>failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
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
Upcoming events
THE COMMONWEALTH OF VIRGINIA SECURITY CONFERENCE WILL BE HELD ON AUG. 18, 2022, VIRTUALLY.

MORE DETAILS WILL BE FORTHCOMING.
May 4, 2022, from 1 to 4 p.m.

Presenters:
Scott Debb/NSU
John Joseph/Obtegocyber
Samuel “Gene” Fishel/OAG
THANK YOU FOR ATTENDING!