Ransomware:
Protecting your Money and Assets

Partner Firms:

VIPRE Security
David Corlette
Director, Product Management

Arcserve
Christophe Bertrand
VP of Product Marketing

VLP Law Group LLP
Melissa Krasnow
Partner

Thank you for logging into today's event. Please note we are in standby mode. All Microphones will be muted until the event starts. We will be back with speaker instructions @ 11:55am. Any Questions? Please email: info@theknowledgegroup.org

Group Registration Policy

Please note ALL participants must be registered or they will not be able to access the event.
If you have more than one person from your company attending, you must fill out the group registration form.

We reserve the right to disconnect any unauthorized users from this event and to deny violators admission to future events.

To obtain a group registration please send a note to info@theknowledgegroup.org or call 646.202.9344.

Ransomware:
Protecting your Money and Assets

➢Please note the FAQ.HELP TAB located to the right of the main presentation. On this page you will find answers to the top questions asked by attendees during webcast such as how to fix audio issues, where to download the slides and what to do if you miss a secret word. To access this tab, click the FAQ.HELP Tab to the right of the main presentation when you're done click the tab of the main presentation to get back.

➢For those viewing the webcast on a mobile device, please note:

- These instructions are for Apple and Android devices only. If you are using a Windows tablet, please follow the instructions for viewing the webcast on a PC.
- The FAQ.HELP TAB will not be visible on mobile devices.
- You will receive the frequently asked questions & other pertinent info through the apps chat window function on your device.
- On Apple devices you must tap the screen anywhere to see the task bar which will show up as a blue bar across the top of the screen. Click the chat icon then click the chat with all to access the FAQ's.
- Feel free to submit questions by using the "questions" function built-in to the app on your device.
- You may use your device's "pinch to zoom function" to enlarge the slide images on your screen.
- Headphones are highly recommended. In the event of audio difficulties, a dial-in number is available and will be provided via the app's chat function on your device.

Ransomware:
Protecting your Money and Assets

- Follow us on Twitter, that's @Know_Group to receive updates for this event as well as other news and pertinent info.

- If you experience any technical difficulties during today's WebEx session, please contact our Technical Support @ 866-779-3239. We will post the dial information in the chat window to the right shortly and it's available in the FAQ.Help Tab on the right. Please redial into the webcast in case of connectivity issue where we have to restart the WebEx event.

- You may ask a question at anytime throughout the presentation today via the chat window on the lower right hand side of your screen. Questions will be aggregated and addressed during the Q&A segment.

- Please note, this call is being recorded for playback purposes.

- If anyone was unable to log in to the online webcast and needs to download a copy of the PowerPoint presentation for today's event, please send an email to: info@theknowledgegroup.org. If you're already logged in to the online Webcast, we will post a link to download the files shortly and it's available in the FAQ.Help Tab

Ransomware:
Protecting your Money and Assets

- If you are listening on a laptop, you may need to use headphones as some laptops speakers are not sufficiently amplified enough to hear the presentations. If you do not have headphones and cannot hear the webcast send an email to info@theknowledgegroup.org and we will send you the dial in phone number.

- About an hour or so after the event, you'll be sent a survey via email asking you for your feedback on your experience with this event today - it's designed to take less than two minutes to complete, and it helps us to understand how to wisely invest your time in future events. Your feedback is greatly appreciated. If you are applying for continuing education credit, completions of the surveys are mandatory as per your state boards and bars. 6 secret words (3 for each credit hour) will be given throughout the presentation. We will ask you to fill these words into the survey as proof of your attendance. Please stay tuned for the secret word. If you miss a secret word please refer to the FAQ.Help tab to the right.

- Speakers, I will be giving out the secret words at randomly selected times. I may have to break into your presentation briefly to read the secret word. Pardon the interruption.

Ransomware:
Protecting your Money and Assets

➢We need your insights -- We are conducting some special research to improve The Knowledge Group for you.

➢Give us ten minutes on the phone and we will give you three months of FREE CE webcasts.

➢Please click this link to sign up and participate: https://knowgp.org/2q1zI3b We look forward to hearing from you.

Ransomware:
Protecting your Money and Assets

Sponsors:

VIPRE delivers the best protection at the best price. It is the top-rated, award-winning endpoint security product for small and medium businesses, and home users. VIPRE is powered by next-generation advanced machine learning, one of the world's largest threat intelligence clouds and real-time behavior monitoring to protect millions of users from ransomware, zero-day attacks, phishing, exploit kits, mobile threats and other malware that easily evade traditional signature-based antivirus. Easy to use, simple to license and available at the best price, VIPRE provides the proactive advanced threat defense all users need to protect their data, and all VIPRE customers receive free U.S.-based technical support. To learn more, visit www.VIPREAntivirus.com.

Arcserve is a leading provider of data protection and recovery software that gives organizations the assurance that they can recover their data and applications when needed. Launched in 1990, Arcserve provides a comprehensive solution for cloud, virtual and physical environments, on premise or in the cloud, backed up by unsurpassed support and expertise. Arcserve Unified Data Protection (UDP), available on Arcserve's appliance or your hardware, drives a full range of highly efficient and integrated data protection capabilities through a simple, web-based user console. Arcserve has a customer base of 45,000 end users in more than 150 countries and partners with over 7,500 distributors, resellers and service providers around the world. Arcserve is headquartered in Minneapolis, Minnesota. Visit www.arcserve.com.

Ransomware:
Protecting your Money and Assets

Partner Firm:

VLP LAW GROUP LLP

Founded in 2008, VLP is a business and transactional law firm that delivers top quality legal services from experienced attorneys through an efficient platform. VLP's broad practice includes high tech, life sciences, clean tech, retail, consumer products, edtech, and real estate. VLP's clients range from individual executives and early-stage startups to Fortune 500 companies, including public and private corporations, venture capital investors, private equity funds, educational institutions and companies, nonprofits and individuals. VLP provides general corporate, licensing, contract, intellectual property protection and counseling, securities regulation, financing, merger and acquisition, real estate, commercial lending, tax, employment and other legal services.

Ransomware:
Protecting your Money and Assets

Brief Speaker Bios:

VIPRE Security
David Corlette
Director, Product Management

David Corlette is the Director of Product Management for VIPRE, a top-rated, award-winning internet security product for channel partners and businesses worldwide. For the past decade, David has worked with customers and partners to design and build best-of-breed IT security using innovative threat detection and response solutions. He has broad experience in advanced threat, SIEM, networking, cloud services, security standardization, open source, agile development and technology policy. He chaired the Distributed Management Task Force, a computer software trade group which works to simplify the manageability of network-accessible technologies and holds an A.B. in Electrical Engineering from Harvard University.

Arcserve
Christophe Bertrand
VP of Product Marketing

Christophe Bertrand is the Vice President of Product Marketing at Arcserve. Christophe has spent most of his career in the data storage and data protection space with companies such as Legato Systems (now EMC), VERITAS (now Symantec), Maxtor, Hitachi Data Systems and most recently DataDirect Networks where he ran product, channel and vertical marketing.

Christophe earned an MBA from Bradford University (England), a BA in European Business Administration from Middlesex University (England) and a Maitrise degree from the ESC Reims Business School (France).

Ransomware:
Protecting your Money and Assets

Brief Speaker Bios:

VLP Law Group LLP
Melissa Krasnow
Partner

Melissa Krasnow is a partner at VLP Law Group LLP whose practice encompasses domestic and cross-border privacy and data security, technology transactions and mergers and acquisitions.

She advises companies on responding to data breaches (HIPAA, FERPA, financial services regulatory and PCI DSS), preparing written information security programs, devising incident response plans and facilitating tabletop exercises. Melissa counsels boards of directors and executive officers on privacy and data security risk oversight and developments and reviews cyber liability insurance policies.

Ransomware:
Protecting your Money and Assets

Organizations like yours are concerned about ransomware. Technology leaders Arcserve and VIPRE joined forces to help you defeat those ransomware hoodlums lurking in the dark cyberspace. From preventative measures with VIPRE, to remediation strategies with Arcserve, plus legal and regulatory guidance about ransomware from VLP, you will:

- Watch as we dissect common variants like Locky, Petya, TeslaCrypt and Cerber
- Learn how to stop ransomware attacks before they happen
- Get practical advice on how to get back on your feet if an attacker does get through
- Discover what others have done – without opening their wallets – to defeat the threat

Find out how to fend off and remediate ransomware attacks.

Ransomware:
Protecting your Money and Assets

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

SEGMENT 2:
Christophe Bertrand
VP of Product Marketing
Arcserve

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

► *For more information about the speakers, you can visit:* https://theknowledgegroup.org/event-homepage/?event_id=2218

Ransomware:
Protecting your Money and Assets

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

Introduction

David Corlette is the Director of Product Management for VIPRE, a top-rated, award-winning internet security product for channel partners and businesses worldwide. For the past decade, David has worked with customers and partners to design and build best-of-breed IT security using innovative threat detection and response solutions. He has broad experience in advanced threat, SIEM, networking, cloud services, security standardization, open source, agile development and technology policy. He chaired the Distributed Management Task Force, a computer software trade group which works to simplify the manageability of network-accessible technologies and holds an A.B. in Electrical Engineering from Harvard University.

Ransomware: Protecting your Money and Assets

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

Ransomware on the Rise

Criminal hackers now target hospitals, police stations, and schools

Los Angeles Times

World reels from massive cyberattack that hit nearly 100 countries

CNN

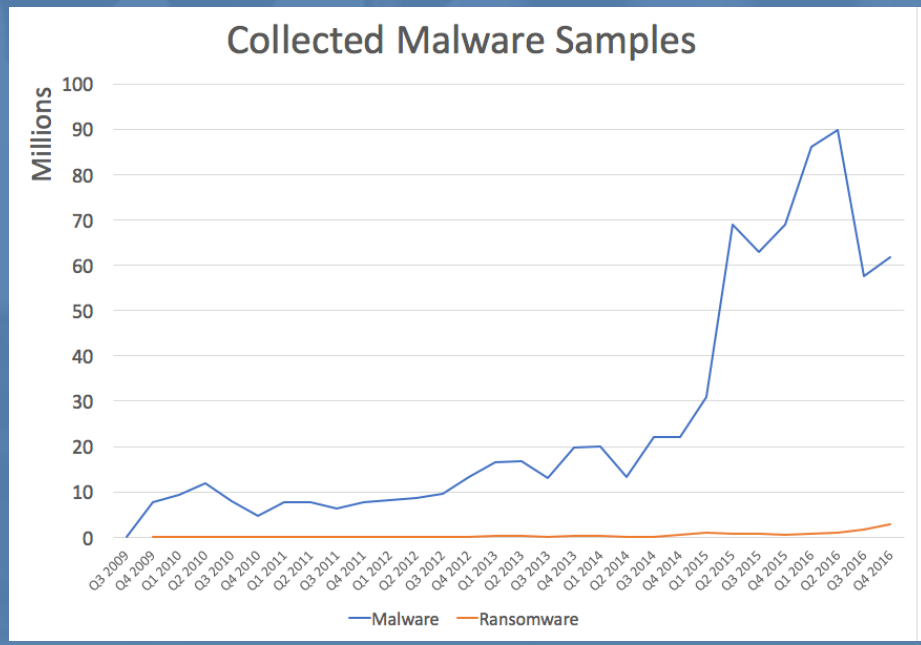
Ransomware Hackers Blackmail U.S. Police Departments

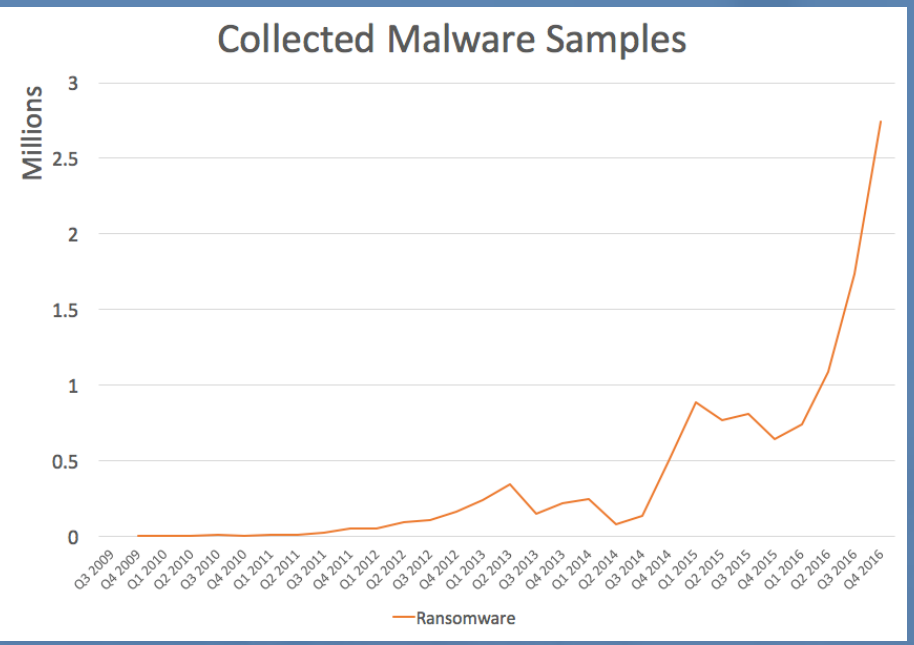
NBC NEWS

Ransomware: Protecting your Money and Assets

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

Malware/Ransomware Samples per Quarter





Ransomware: Protecting your Money and Assets

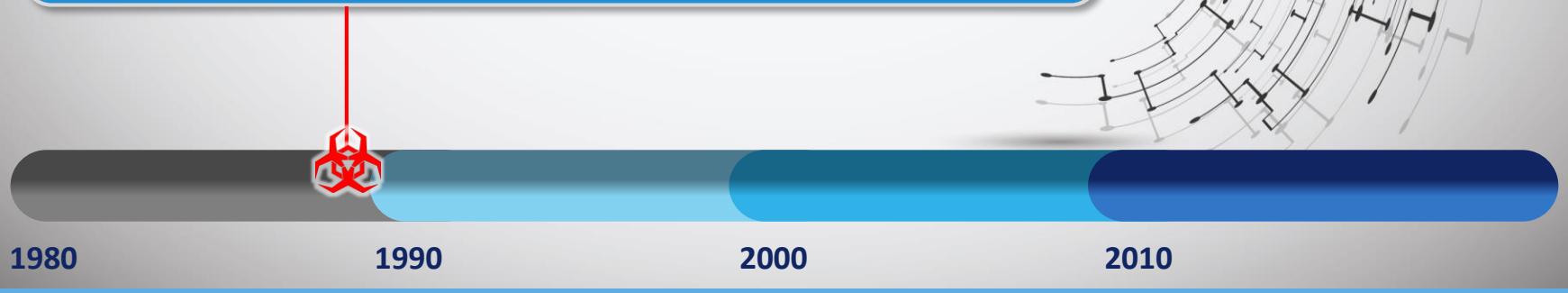
VIPRE

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

The Timeline

First known ransomware program "PS Cyborg (1989)" was created in this period

- Created by disturbed biologist Joseph L. Popp
- Manually distributed by floppy to WHO AIDS conference participants
- Triggered after 90 reboots
- Hid directories and files
- User was supposed to send $189 to a P.O. Box in Panama
- Popp was caught and ransomware was relatively easy to circumvent



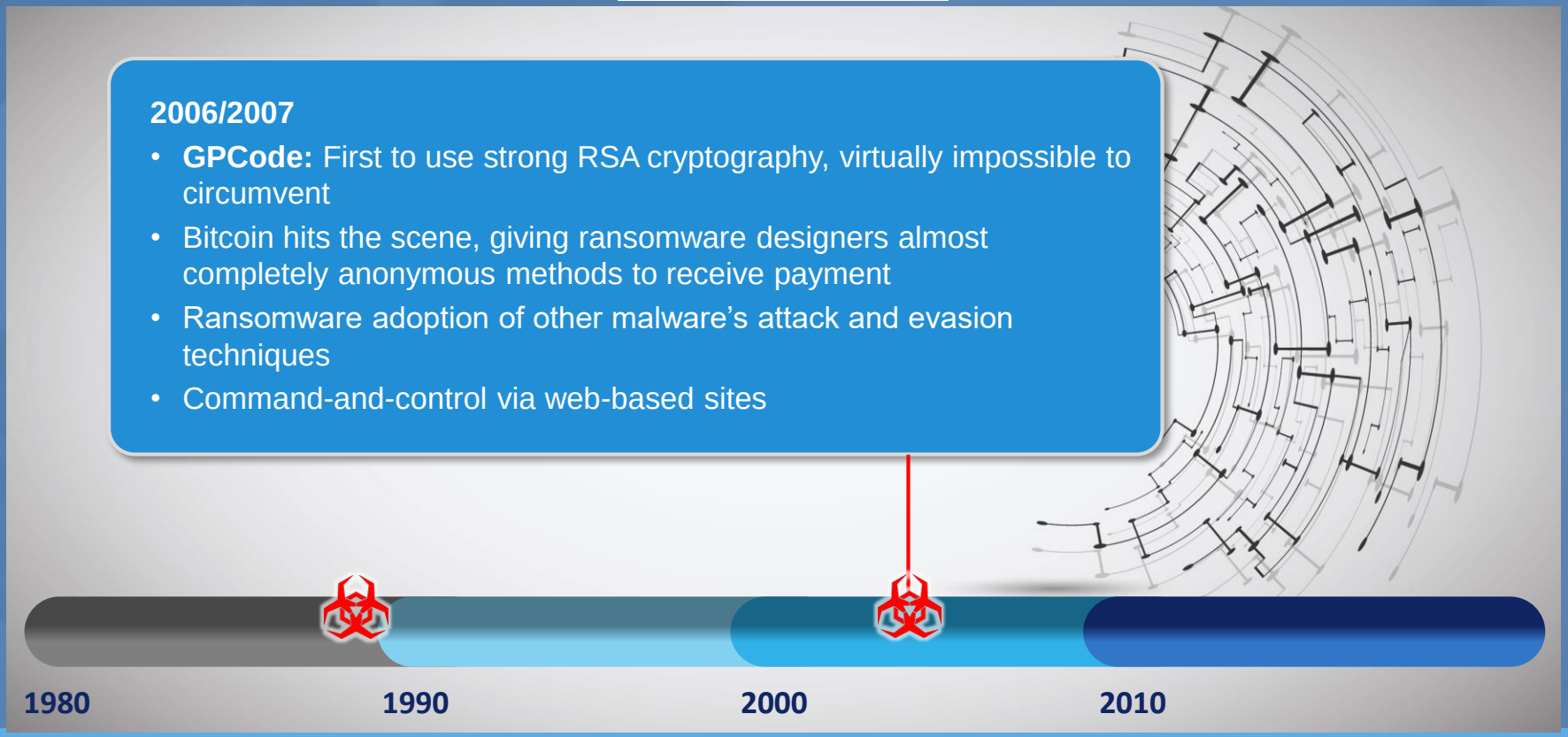
Ransomware: Protecting your Money and Assets

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

Introduction

2006/2007

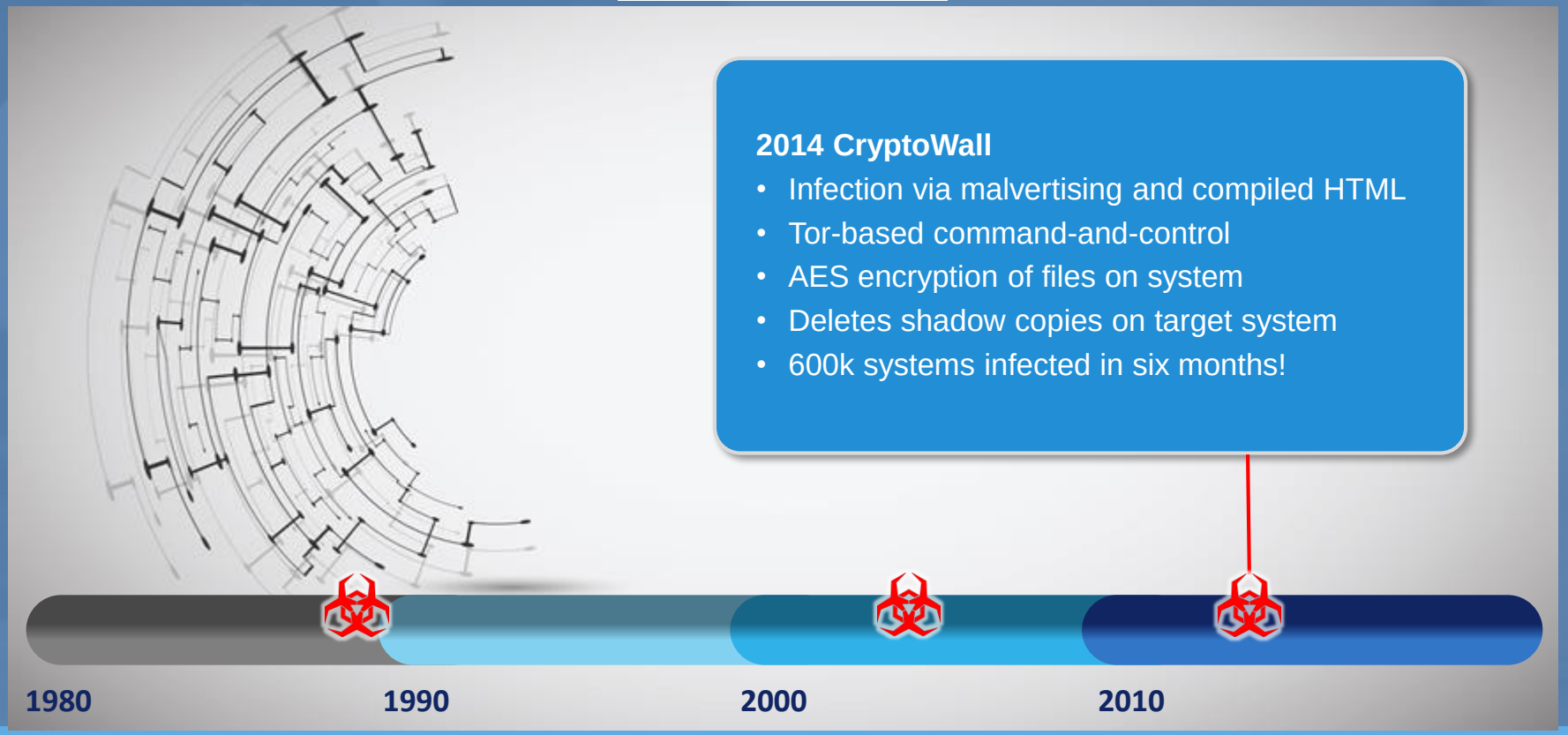
- **GPCode:** First to use strong RSA cryptography, virtually impossible to circumvent
- Bitcoin hits the scene, giving ransomware designers almost completely anonymous methods to receive payment
- Ransomware adoption of other malware's attack and evasion techniques
- Command-and-control via web-based sites



Ransomware: Protecting your Money and Assets

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

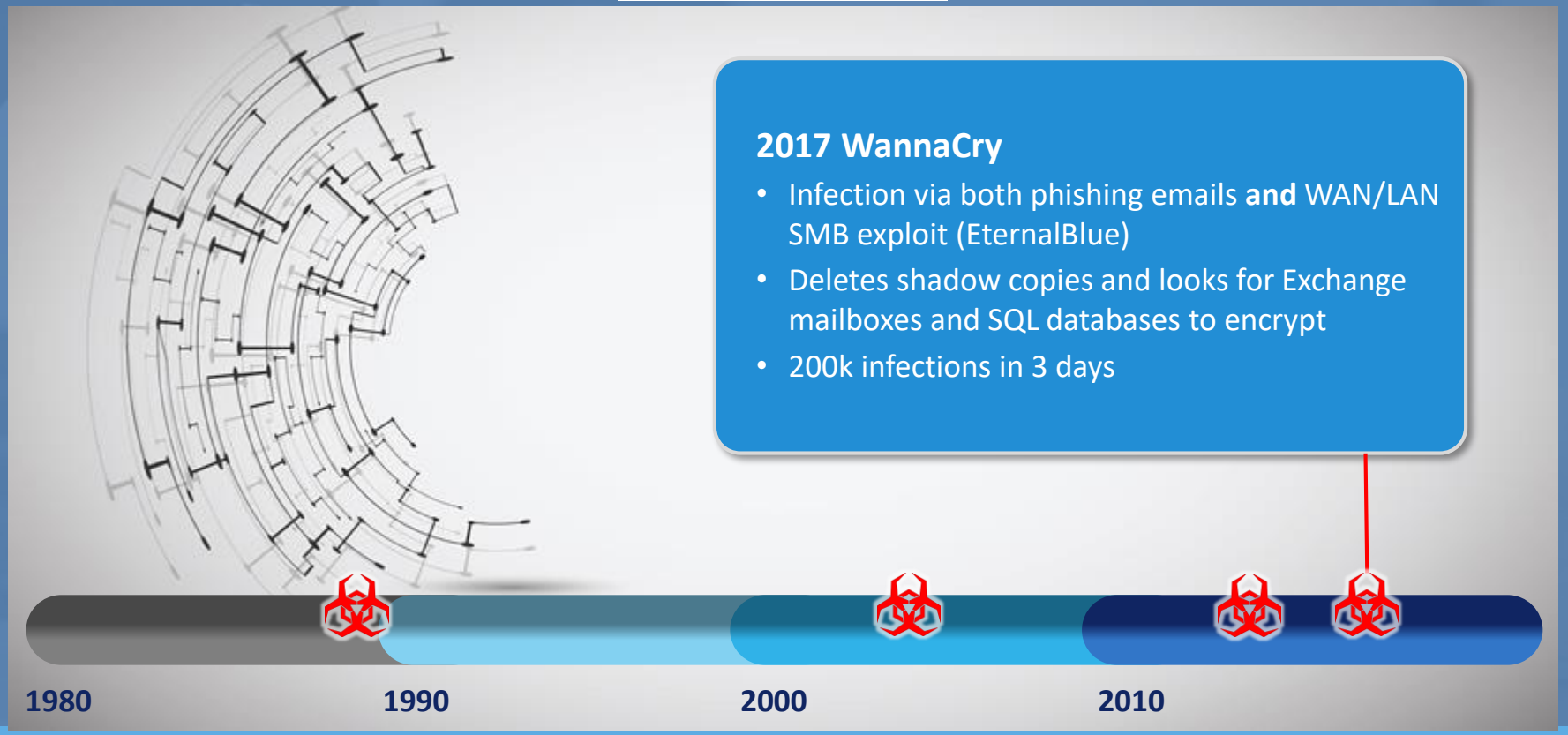
Introduction



Ransomware: Protecting your Money and Assets

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

Introduction



Ransomware: Protecting your Money and Assets

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

Antivirus on the Decline?

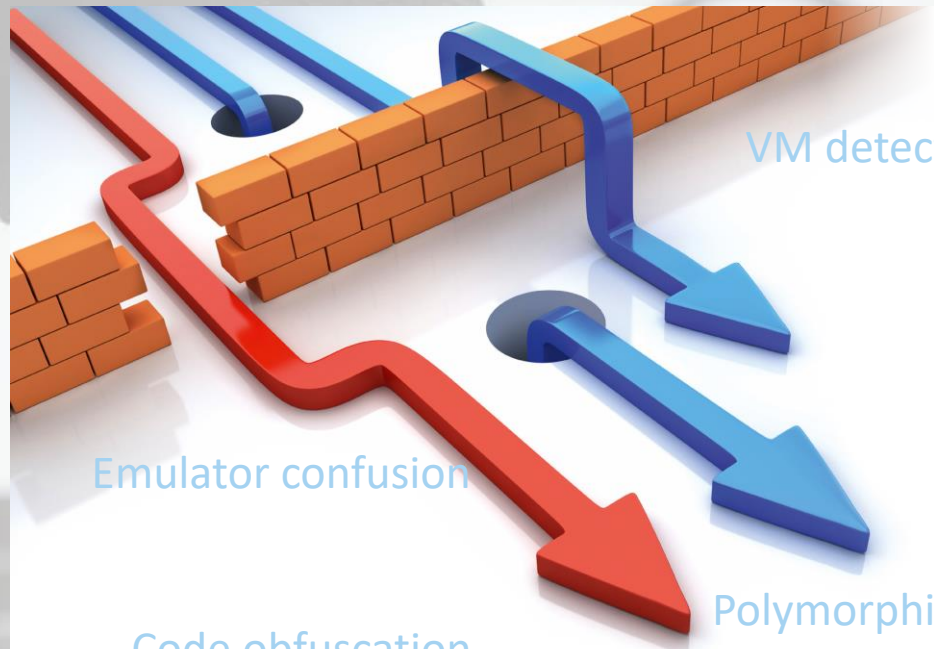
Antivirus is dead, says maker of Norton Antivirus — PCWorld FROM IDG

Antivirus Fails to Stop Ransomware 100% of the Time — infosecurity GROUP

Symantec admits anti-virus software is no longer effective at stopping virus attacks — dotTech

Ransomware: Protecting your Money and Assets

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security



Mouse movement detection

VM detection

Execute attack on 5th start

Wait for N reboots

Emulator confusion

Polymorphism

Code obfuscation

Code encryption

Packing

Return-oriented programming

Sleeps and waits

Wait for Tuesday

Malware Evasive Techniques

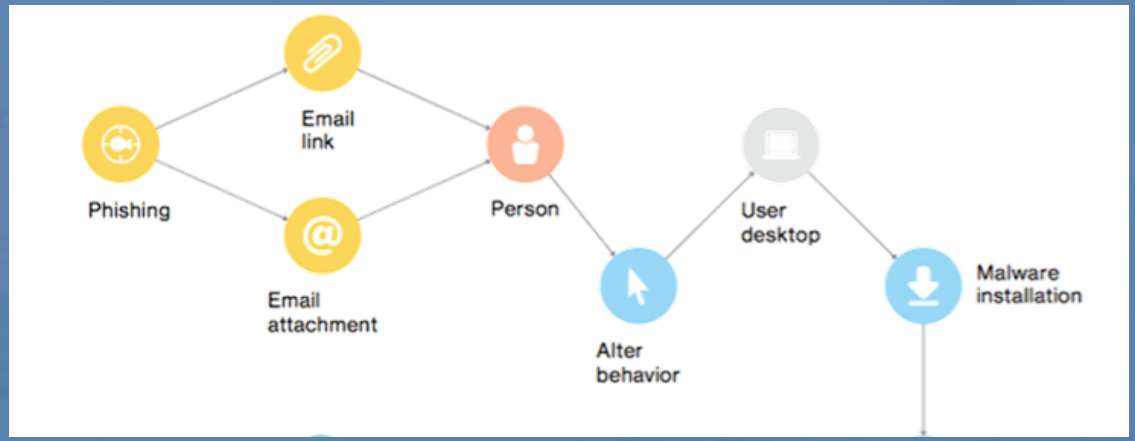
- Polymorphism and obfuscation
- Timing-based evasion
- Environmental detection and hiding
- Behavioral unpredictability

Ransomware: Protecting your Money and Assets

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

The "Kill Chain"

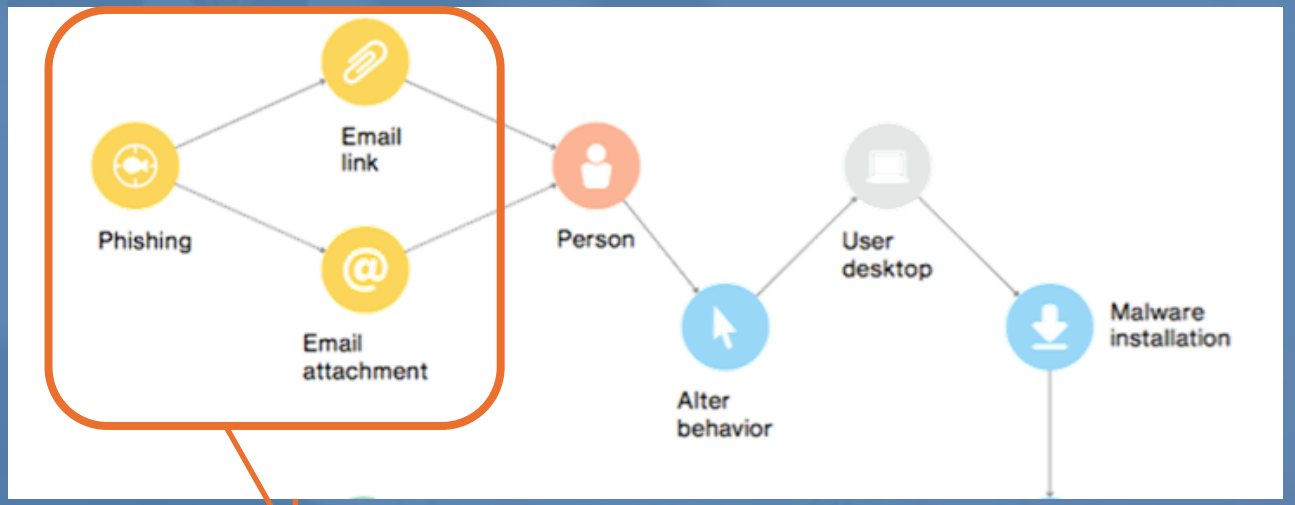
- Verizon Data Breach Investigations Report (DBIR) published a diagram of the "common threat actions."
- Initial beachhead is usually a dropper that then fetches additional modules – a multi-stage attack
- Ransomware may also attempt to spread on internal networks



Ransomware:
Protecting your Money and Assets

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

Breaking the "Kill Chain"

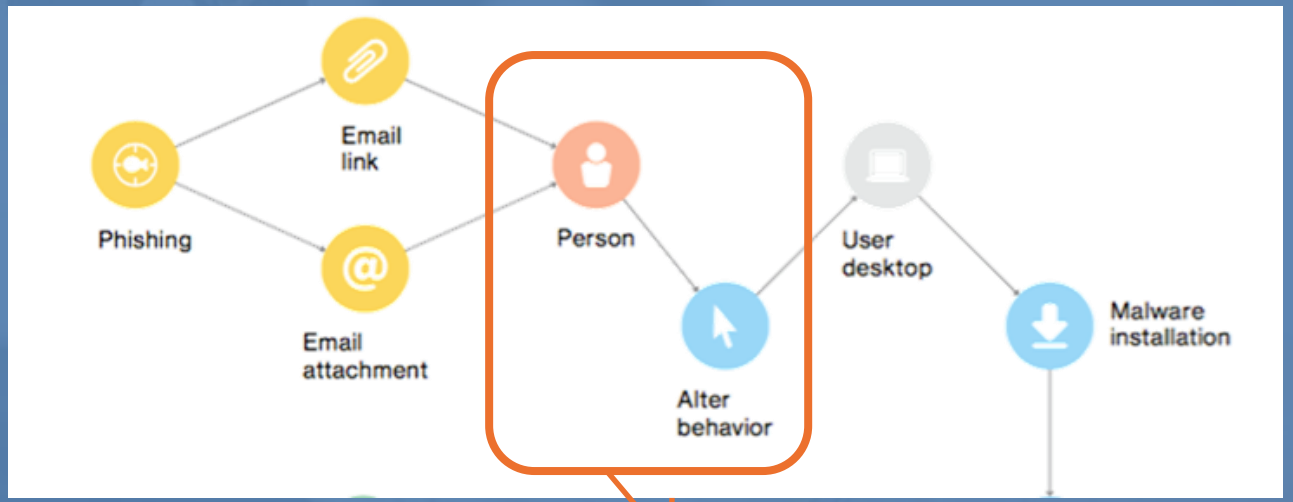


- Anti-phishing
- IDS/IPS
- Email/Network payload analysis

Ransomware:
Protecting your Money and Assets

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

Breaking the "Kill Chain"



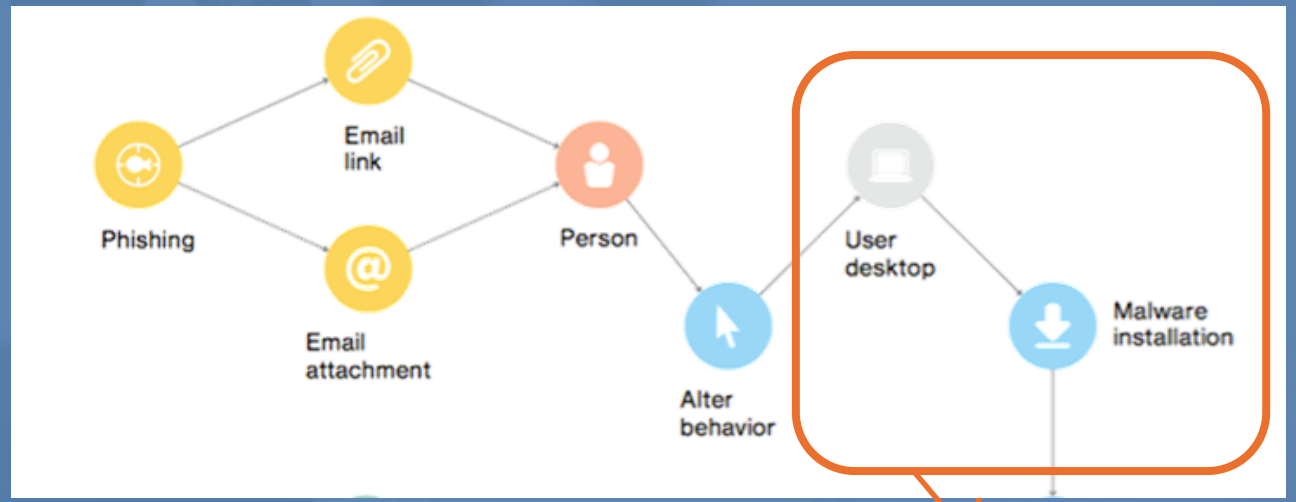
- User training

Ransomware:
Protecting your Money and Assets

VIPRE

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

Breaking the "Kill Chain"

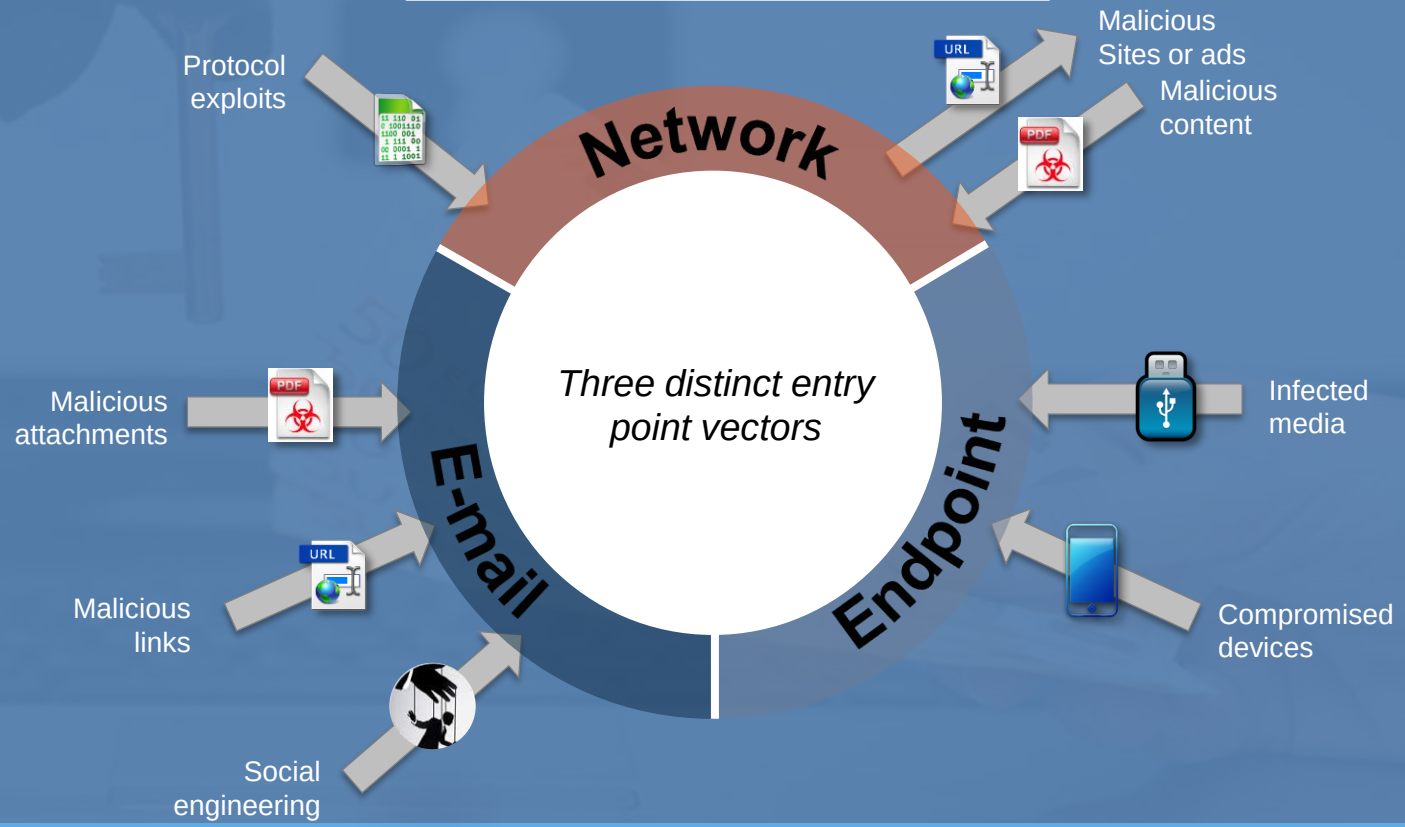


- Secure configuration/patching
- Endpoint protection
- Backups

Ransomware: Protecting your Money and Assets

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

How Attackers Get In

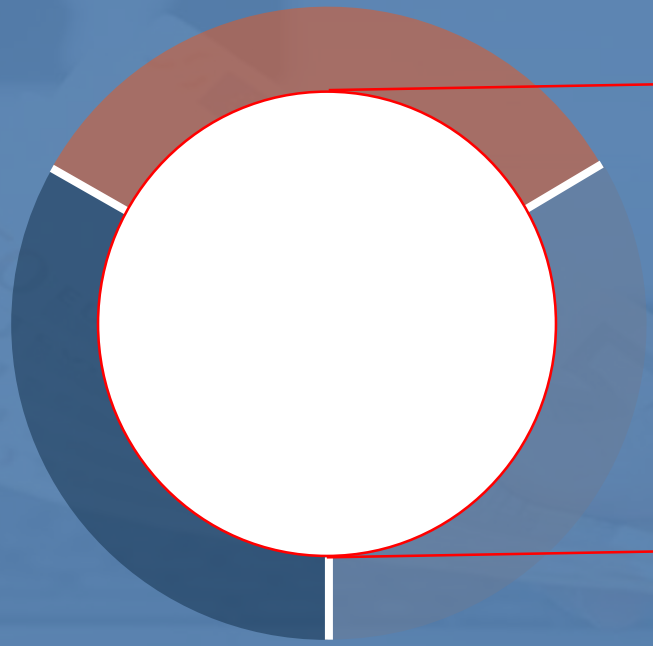


Ransomware: Protecting your Money and Assets

VIPRE

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

Old-school Hash/Signature Detection



Signature-based detection

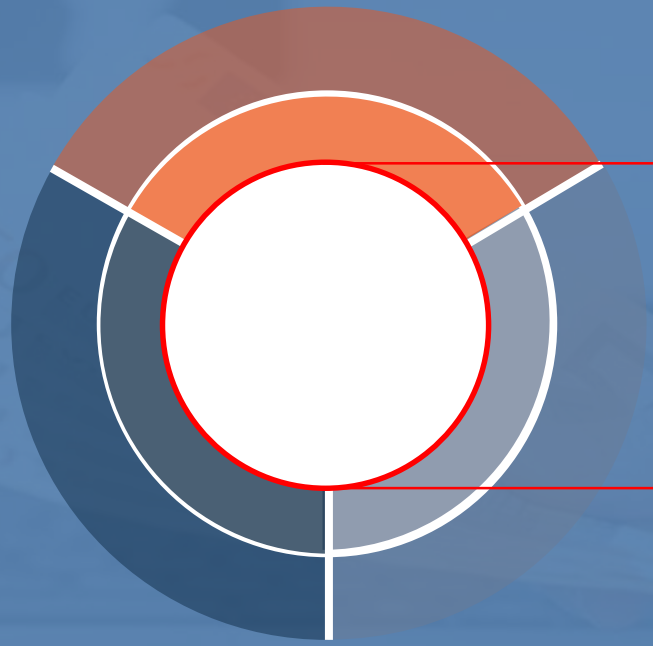
- Original form of detection
- Easily defeated by today's polymorphic malware
- Hashes, however, are good Indicators of Compromise (IoCs) – e.g. for a particular infestation, see how far it has spread
- See Threat Intelligence

Ransomware: Protecting your Money and Assets

VIPRE

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

Old-school Hash/Signature Detection

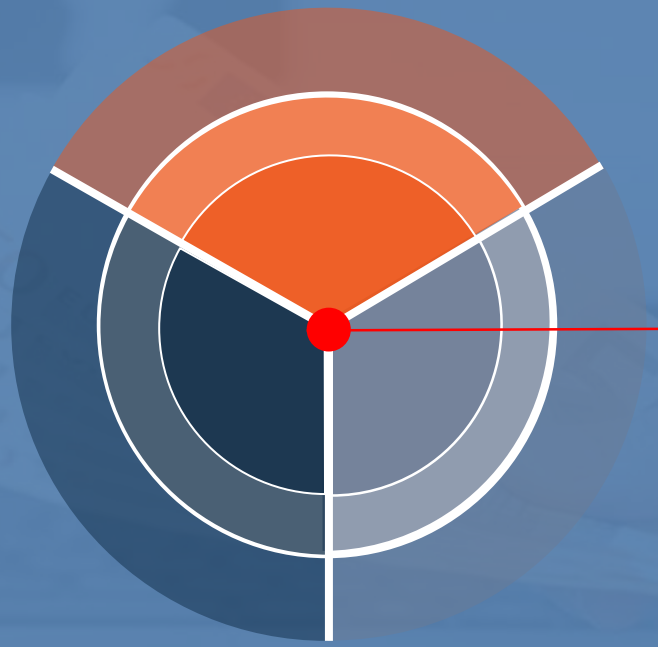


- Rule-based detection
- Expert rules crafted to detect combinations of features
- Detects known malware and simpler forms of evasive malware
- Stops casual, unmotivated attackers
- Issues with false positives
- Classic antivirus (host, e-mail, network) only goes this deep

Ransomware: Protecting your Money and Assets

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

Advanced Malware Detection



Dynamic behavioral models

- Leverage **machine-learned** models of normal behavior to detect abnormal behavior
  - –Malware revealed through its **behavior**
  - –Need to actually **run** the malware – sandbox is safer!
- This is the **hard nut** to crack
- This is where the **risk** is (93% of victims had **"antivirus"** in place)

Ransomware:
Protecting your Money and Assets

SEGMENT 1:
David Corlette
Director, Product Management
VIPRE Security

Call To Action

- ✓ Review the solutions you have protecting your network and endpoints to ensure high-quality layered approaches are used
- ✓ Make sure your users are well-trained to spot the signs of a phishing attempt
- ✓ Ensure that you have a solid system configuration and patching program in place
- ✓ Back up any and all critical data

Ransomware:
Protecting your Money and Assets

arcserve

SEGMENT 2:
Christophe Bertrand
VP of Product Marketing
Arcserve

Introduction

Christophe Bertrand is the Vice President of Product Marketing at Arcserve. Christophe has spent most of his career in the data storage and data protection space with companies such as Legato Systems (now EMC), VERITAS (now Symantec), Maxtor, Hitachi Data Systems and most recently DataDirect Networks where he ran product, channel and vertical marketing.

Christophe earned an MBA from Bradford University (England), a BA in European Business Administration from Middlesex University (England) and a Maitrise degree from the ESC Reims Business School (France).

Ransomware:
Protecting your Money and Assets

arcserve

SEGMENT 2:
Christophe Bertrand
VP of Product Marketing
Arcserve

Talking Points

- Importance of backup for disaster recovery
- Service level dial (levels of protection for different applications)
- Overview of Arcserve UDP
- Ransomware success stories
- Best practices

Ransomware: Arcserve Overview

SEGMENT 2:
Christophe Bertrand
VP of Product Marketing
Arcserve

Worldwide Customer Base & Sales Presence

- 45,000 customers
- >30,000 UDP customers
- 7,500 partners
- Distributed in 150 countries
- WW HQ – Minneapolis, USA
- LATAM HQ – São Paulo, Brazil
- EMEA HQ – Barcelona
- APAC HQ – Singapore
- Japan HQ – Tokyo
- Sales offices in 20+ countries

Industry Recognition

- 3 VMworld Gold Awards
- 2 CRN Channel Chief Awards
- Channel Company Top Midmarket Executive
- MSPBJ Titan of Technology
- 2 PC Pro Recommendations
- 3 IT Pro Recommendations
- DCS Storage Software Product of the Year
- CRN Woman of the Channel
- 4 Storage Awards
- Cloud Hosting DR Product of the Year
- Computer Singapore Readers' Choice Award for Networked Storage

A single, fully-integrated solution portfolio to protect across cloud, virtual and physical environments.

SOFTWARE | APPLIANCES | CLOUD (DRaaS)

Ransomware:
Ransomware in SLA Terms

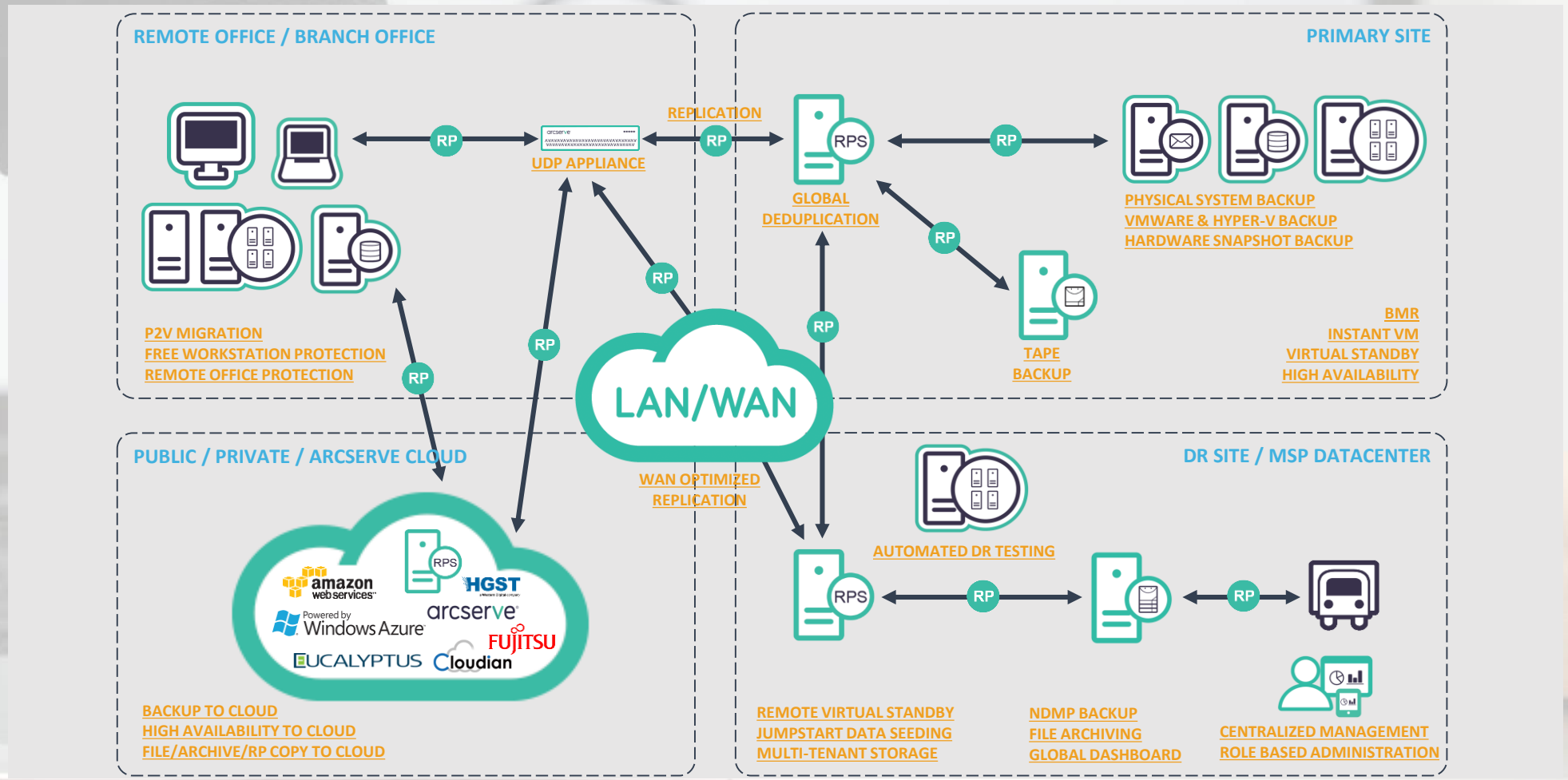
arcserve

SEGMENT 2:
Christophe Bertrand
VP of Product Marketing
Arcserve

Ransomware:
Arcserve Unified Data Protection

arcserve

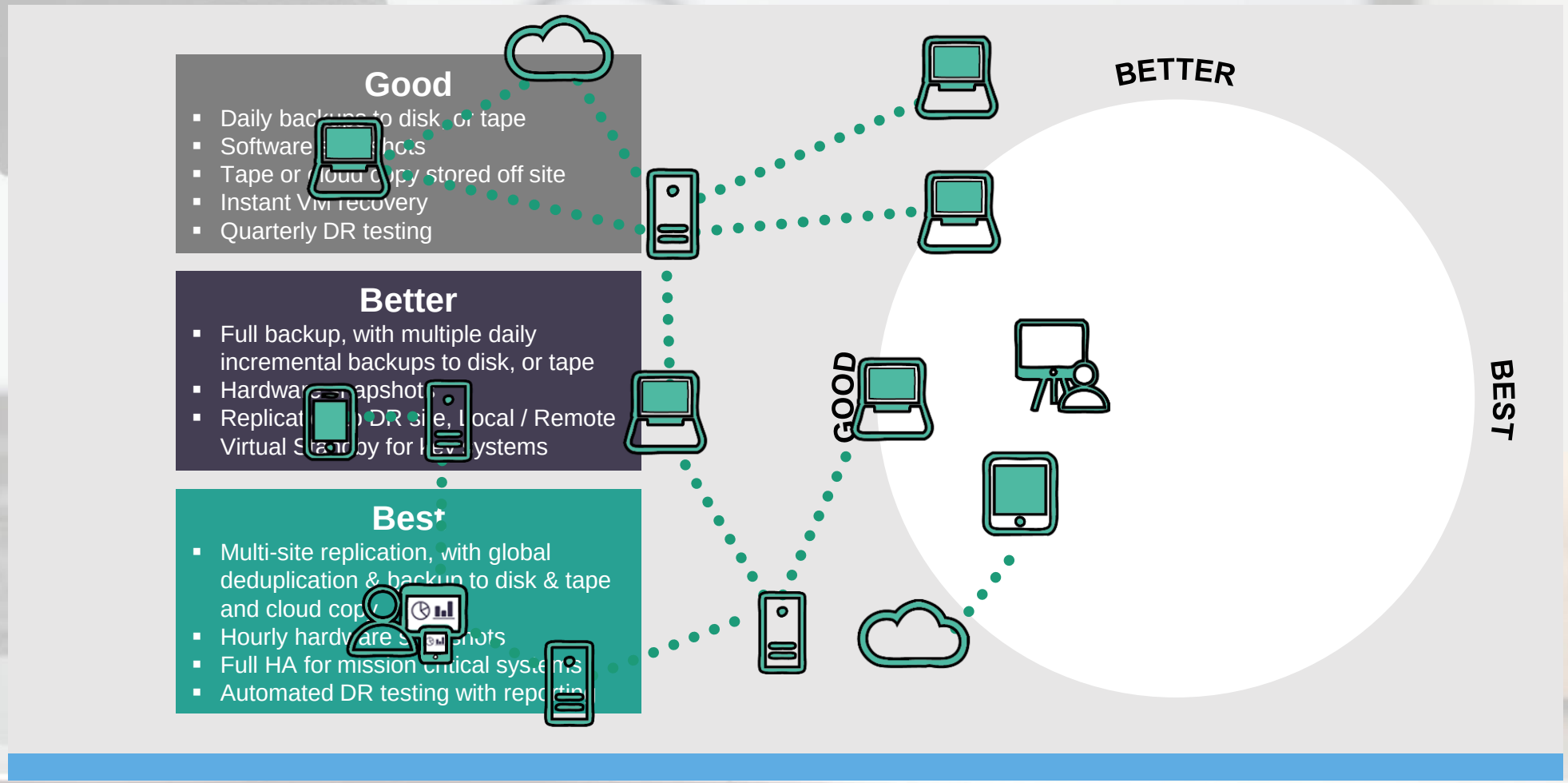
SEGMENT 2:
Christophe Bertrand
VP of Product Marketing
Arcserve



Ransomware:
Ransomware in SLA Terms

arcserve

SEGMENT 2:
Christophe Bertrand
VP of Product Marketing
Arcserve



Ransomware:
Customer Example: Publishing Business

arcserve

SEGMENT 2:
Christophe Bertrand
VP of Product Marketing
Arcserve

1 Customer X supports a few hundred users at this publishing business

2 The corruption came in as an attachment titled Photos.zip with a spoofed email address – who doesn't have "click-happy" end-users?

3 Photos.zip was the infected file sent via email. It was a "bart" type virus

4 Customer X does a 7AM snapshot of his environment and keeps a near line copy of the Recovery Points as a precaution. Best backup practices paid off!!

Result

- Using Arcserve was key to his ability to thwart the attack and recover the affected systems and their data
- It took him 28 hours to determine the source, repair and reverse the damage but there was no publicly visible indication that an attack had taken place
- His ability to contain the attack and mitigate the damage earned him a letter of praise from his CEO

SUCCESS

Ransomware:
Protect The Protector

arcserve

SEGMENT 2:
Christophe Bertrand
VP of Product Marketing
Arcserve

Take precautions to prevent infection in the first place, such as training users to not click on links within emails, downloading attachments from unknown sources and updating software on a timely basis. Rigorous access control is also critical.

Perform regular backups, which may include rethinking your service level agreements to ensure critical business data is backed up more frequently.

3 2 1

Follow the 3-2-1 strategy for backup: one of the copies should be offline, and at least one of the copies should be offsite. Leverage DRaaS capabilities!

Make sure your chosen backup solution includes virtual standby for critical systems so that you can get back on your feet very quickly.

Ransomware:
Protect Source Machines

arcserve

SEGMENT 2:
Christophe Bertrand
VP of Product Marketing
Arcserve

Replicate data to offsite / cloud

If your backup server gets infected or if your backup data is on a shared network share that is accessible from an infected machine, ransomware can encrypt backup data as well. It sounds obvious, but it's important to remember!

Periodically, copy recovery points to offline media, such as USB disks. Consider leveraging tape as a backup medium for critical data (yes tape!). This oldie but goodie comes in handy to send periodic recovery points offline.

Ransomware:
THANK YOU!

arcserve

SEGMENT 2:
Christophe Bertrand
VP of Product Marketing
Arcserve

arcserve

Download a trial at www.arcserve.com

Call for more info: 844.639.6792

Ransomware:
Protecting your Money and Assets

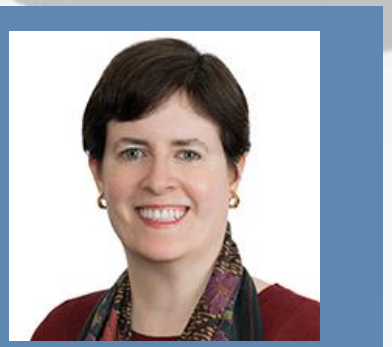
SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Introduction

Melissa Krasnow is a partner at VLP Law Group LLP whose practice encompasses domestic and cross-border privacy and data security, technology transactions and mergers and acquisitions.

She advises companies on responding to data breaches (HIPAA, FERPA, financial services regulatory and PCI DSS), preparing written information security programs, devising incident response plans and facilitating tabletop exercises. Melissa counsels boards of directors and executive officers on privacy and data security risk oversight and developments and reviews cyber liability insurance policies. She advises companies on responding to regulatory inquiries and complying with state, federal and international privacy and data security and related laws. Melissa is a Certified Information Privacy Professional/US (CIPP/US) and a National Association of Corporate Directors Board Leadership Fellow.

Ransomware: Protecting your Money and Assets



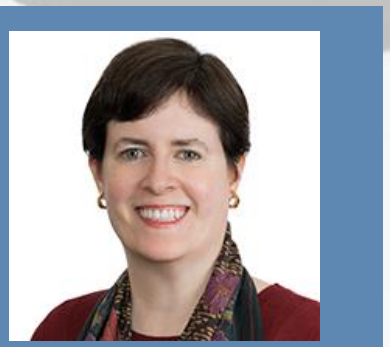
SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

What is Ransomware?

Ransomware is a form of malicious software that infiltrates computer systems or networks and uses tools like encryption to deny access or hold data "hostage" until the victim pays a ransom, frequently demanding payment in Bitcoin. Source: FTC Business Blog at https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look

After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted. Source: FBI brochure at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-ceos.pdf/view

Ransomware: Protecting your Money and Assets



SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

How is Ransomware Delivered?

Ransomware often arrives through e-mail phishing campaigns, which typically require the user to take an action such as clicking on a link or downloading a malicious attachment. Other campaigns use drive-by downloads, where a user visits a malicious website or a site that has been compromised, and the act of loading the site causes the ransomware to automatically download onto the user's computer. In addition, ransomware is delivered through "malvertising" campaigns, where malicious code is hidden in an online ad that infects the user's computer….Attackers also have exploited server-side vulnerabilities to deliver ransomware payloads by searching for networks that had failed to patch known vulnerabilities. Source: FTC Business Blog at https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look

Ransomware: Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Federal Trade Commission's Recommended Steps Regarding WannaCry

- Keep software up-to-date - download security updates as soon as they are available – no matter what operating system.
- Back up important files routinely.
- Think twice before clicking on links or downloading attachments and apps. Source: FTC Business Blog at https://www.ftc.gov/news-events/blogs/business-blog/2017/05/wannacry-worries-update-now

Ransomware: Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Federal Trade Commission Remarks About Ransomware

A company's unreasonable failure to patch vulnerabilities known to be exploited by ransomware might violate the FTC Act….businesses play a critical role in ensuring that they adequately protect consumers' information, particularly as security threats like ransomware escalate.
Source: Opening Remarks of FTC Chairwoman Edith Ramirez Fall Technology Series: Ransomware at https://www.ftc.gov/system/files/documents/public_s

Ransomware:
Protecting your Money and Assets

VLP LAW GROUP LLP

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Department of Health and Human Services Guidance

When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule. Source: FACT SHEET: Ransomware and HIPAA at https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Ransomware:
Protecting your Money and Assets

VLP LAW GROUP LLP

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Department of Homeland Security US-CERT Alert Regarding WannaCry

Recommended steps for prevention.

Recommendations for network protection.

Recommended steps for remediation.

Defending against ransomware generally. Source: US-CERT Alert (TA17-132A) at https://www.us-cert.gov/ncas/alerts/TA17-132A; note that this Alert is referenced in https://www.sec.gov/files/risk-alert-cybersecurity-ransomware-alert.pdf

Ransomware:
Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

What Steps Does the FBI Recommend Taking?

Isolate the infected computer immediately, and remove infected systems from the network as soon as possible to prevent ransomware from attacking network or share drives.

Isolate or power off affected devices that have not yet been completely corrupted.

Immediately secure backup data or systems by taking them offline, and ensure backups are free of malware.

Contact law enforcement immediately.

Collect and secure partial portions of the ransomed data that might exist if available.

Ransomware:
Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

What Steps Does the FBI Recommend Taking? (con't)

Change all online account passwords and network passwords after removing the system from the network if possible, and change all system passwords once the malware is removed from the system.

Delete registry values and files to stop the program from loading.

Implement security incident response and business continuity plans.

Ransomware: Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

What Steps Does the FBI Recommend Taking? (con't)

Conduct a post incident review of the response to the incident, and assess the strengths and weaknesses of the incident response plan. Source: FBI brochure at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

Ransomware:
Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Reaching Out to the FBI / Filing a Complaint

The FBI requests that victims reach out to their local FBI office and/or file a complaint with the Internet Crime Complaint Center at https://www.ic3.gov/default.aspx
Source: FBI public service announcement at https://www.ic3.gov/media/2016/160915.aspx

Ransomware: Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Should the Ransom be Paid?

The FBI does not support paying a ransom to the adversary because it does not guarantee the victim will regain access to their data. In fact, some individuals or organizations are never provided with decryption keys after paying a ransom. Paying a ransom emboldens the adversary to target other victims for profit and could provide an incentive for other criminals to engage in similar illicit activities for financial gain. Although the FBI does not support paying a ransom, it recognizes that executives, when faced with inoperability issues, will evaluate all options to protect their shareholders, employees, and customers. Source: FBI public service announcement at https://www.ic3.gov/media/2016/160915.aspx

Ransomware:
Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

FBI on Prevention and Continuity Measures

Regularly back up data and verify the integrity of those backups.

Secure your backups and ensure backups are not connected to the computers and networks they are backing up.

Scrutinize links contained in e-mails and do not open attachments included in unsolicited e-mails.

Only download software – especially free software – from sites you know and trust. When possible, verify the integrity of the software through a digital signature prior to execution.

Ransomware:
Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

FBI on Prevention and Continuity Measures (con't)

Ensure application patches for the operating system, software, and firmware are up to date.

Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.

Disable macro scripts from files transmitted via e-mail.

Implement software restrictions or other controls to prevent the execution of programs in common ransomware locations, such as temporary folders supporting popular Internet browsers, or compression/decompression programs, including those located in the AppData/LocalAppData folder.

Ransomware: Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

FBI on Prevention and Continuity Measures (con't)

Enable strong spam filters to prevent phishing e-mails from reaching the end users, and authenticate inbound e-mail using technologies like Sender Policy Framework, Domain Message Authentication Reporting and Conformance, and DomainKeys Identified Mail to prevent e-mail spoofing.

Scan all incoming and outgoing e-mails to detect threats, and filter executable files from reaching end users.

Configure firewalls to block access to known malicious IP addresses.

Consider disabling Remote Desktop Protocol if it is not being used.

Conduct an annual penetration test and vulnerability assessment. Source: FBI brochure, Ransomware Prevention and Response for CISOs, at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

Ransomware: Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

FBI on Prevention and Continuity Measures (con't)

Focus on awareness and training.

Patch all endpoint device operating systems, software, and firmware as vulnerabilities are discovered.

Manage the use of privileged accounts by implementing the principle of least privilege.

Configure access controls with least privilege in mind.

Use virtualized environments to execute operating system environments or specific programs.

Ransomware: Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

FBI on Prevention and Continuity Measures (con't)

Categorize data based on organizational value, and implement physical/logical separation of networks and data for different organizational units.

Require user interaction for end user applications communicating with Web sites uncategorized by the network proxy or firewall.

Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy. Source: FBI public service announcement at https://www.ic3.gov/media/2016/160915.aspx

Ransomware: Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Additional Considerations

Organizations also should conduct a cyber-security risk analysis of the organization and have and test an incident response plan. FBI brochure at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-ceos.pdf/view

Take into account insurance coverage, namely cyber-liability/cyber-extortion coverage.

See article on kidnap insurance and ransomware at http://www.reuters.com/article/us-cyber-attack-insurance-idUSKCN18F1LU

Ransomware: Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Additional Considerations (con't)

After….[the]….devastating global ransomware attack, now known as WannaCry, directors will once again be questioning management teams to make sure the company is protected. The challenge is that most directors do not know what questions they should be asking.

If I were sitting on a board, this attack would prompt me to ask questions about the following three areas: End of Life (EOL) software; patching; and disaster recovery. Source: https://blog.nacdonline.org/2017/05/questions-to-ask-after-the-wannacry-attack/

Ransomware: Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Cybersecurity Event Recovery

The National Institute of Standards and Technology Guide for Cybersecurity Event Recovery at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf includes an example of a recovery plan in the form of a playbook for a ransomware attack. While the guide applies to US federal agencies, it should be useful to any organization.

Ransomware: Protecting your Money and Assets

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Resources

Ransomware Guidance at https://www.irmi.com/articles/expert-commentary/guidance-on-ransomware

Cyber-Security Event Recovery Plans at https://www.irmi.com/articles/expert-commentary/cyber-security-event-recovery-plans

Directors and Cybersecurity at http://www.vlplawgroup.com/wp-content/uploads/2017/01/M.Krasnow-Bloomberg-Article-1-2017.pdf

Ransomware:
Protecting your Money and Assets

Contact Info:

David Corlette
Director, Product Management
VIPRE Security
David.Corlette@threattrack.com

Christophe Bertrand
VP of Product Marketing
Arcserve
Christophe.bertrand@arcserve.com

Melissa Krasnow
Partner
VLP Law Group LLP
MKrasnow@vlplawgroup.com
(312) 350-1082

Ransomware: Protecting your Money and Assets

Q&A:

David Corlette
Director, Product Management
VIPRE Security
David.Corlette@threattrack.com

Christophe Bertrand
VP of Product Marketing
Arcserve
Christophe.bertrand@arcserve.com

Melissa Krasnow
Partner
VLP Law Group LLP
MKrasnow@vlplawgroup.com
(312) 350-1082

► *You may ask a question at anytime throughout the presentation today. Simply click on the question mark icon located on the floating tool bar on the bottom right side of your screen. Type your question in the box that appears and click send.*

► *Questions will be answered in the order they are received.*

ABOUT THE KNOWLEDGE GROUP

The Knowledge Group is an organization that produces live webcasts which examine regulatory changes and their impacts across a variety of industries. “We bring together the world's leading authorities and industry participants through informative two-hour webcasts to study the impact of changing regulations.”

If you would like to be informed of other upcoming events, please click here.

DISCLAIMER:

The Knowledge Group is producing this event for information purposes only. We do not intend to provide or offer business advice.

The contents of this event are based upon the opinions of our speakers. The Knowledge Group does not warrant their accuracy and completeness. The statements made by them are based on their independent opinions and does not necessarily reflect that of The Knowledge Group‘s views.

In no event shall The Knowledge Group be liable to any person or business entity for any special, direct, indirect, punitive, incidental or consequential damages as a result of any information gathered from this webcast.