WILLIAMS &
CONNOLLY LLP®

Mitigation Strategies for the Emerging Threat Environment

Presenters:

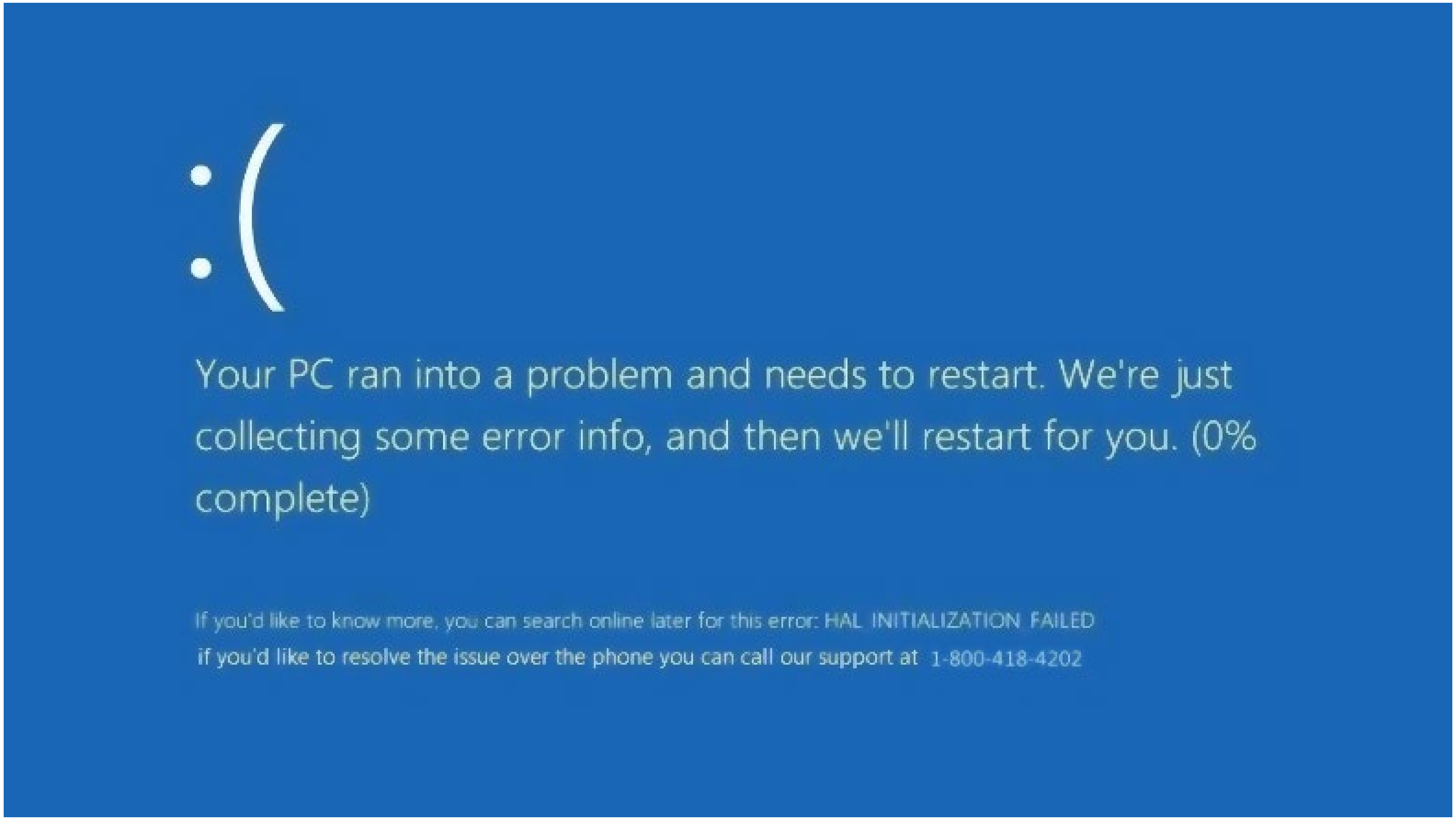
John McNichols
Allie Eisen
Kevin Hughes

May 2023

Outline For Today’s Presentation

- What’s “malware”?
- Where did it come from?
- How does it work?
- What are the risks?
- What are our obligations?
- What’s next?

What is Malware?



:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you. (0% complete)

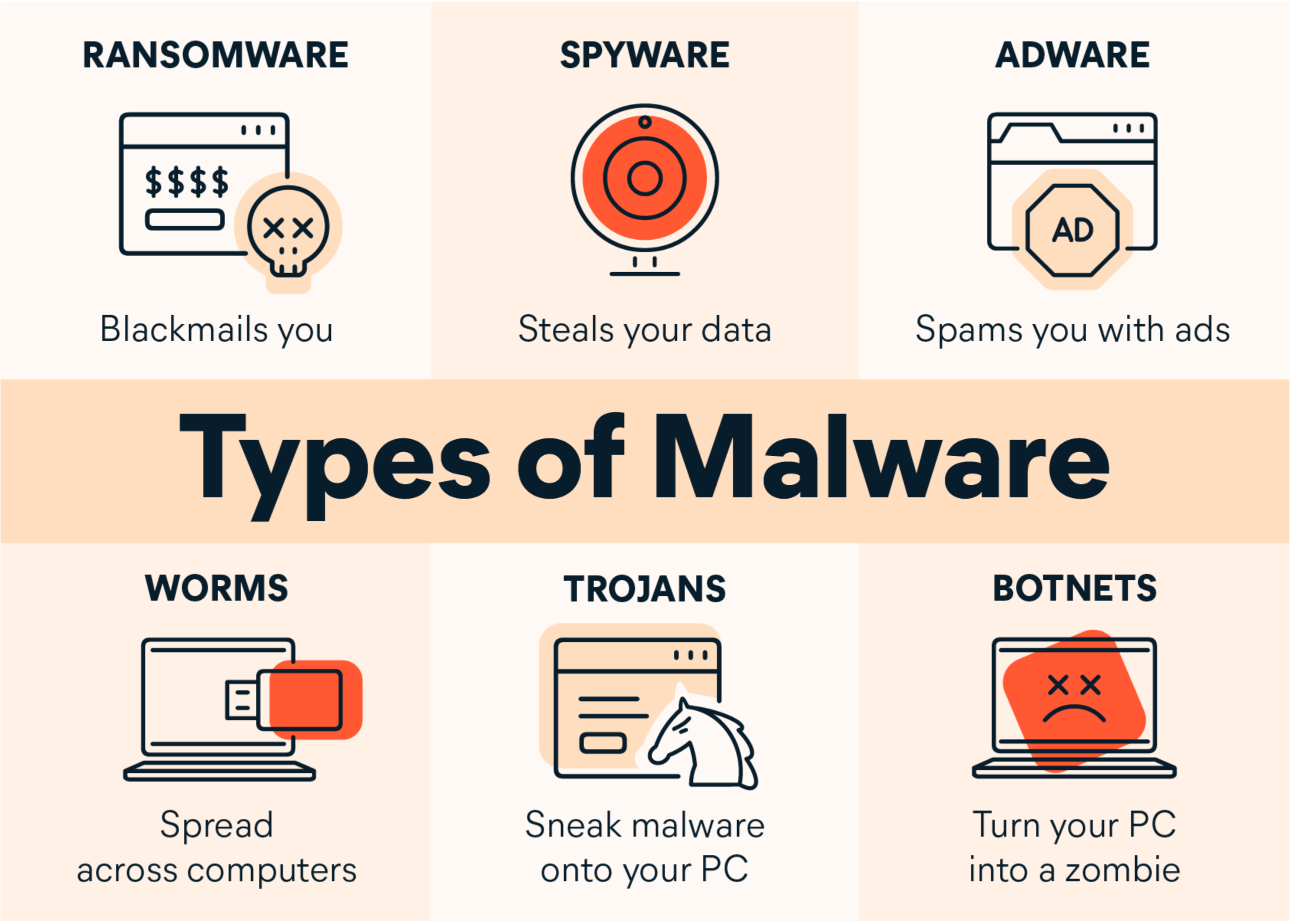
If you'd like to know more, you can search online later for this error: HAL INITIALIZATION FAILED

if you'd like to resolve the issue over the phone you can call our support at 1-800-418-4202

Malware

Software that is specifically designed to **disrupt**, **damage**, or **gain unauthorized access** to a computer system.

Types of Malware



RANSOMWARE

Blackmails you

SPYWARE

Steals your data

ADWARE

Spams you with ads

Types of Malware

WORMS

Spread across computers

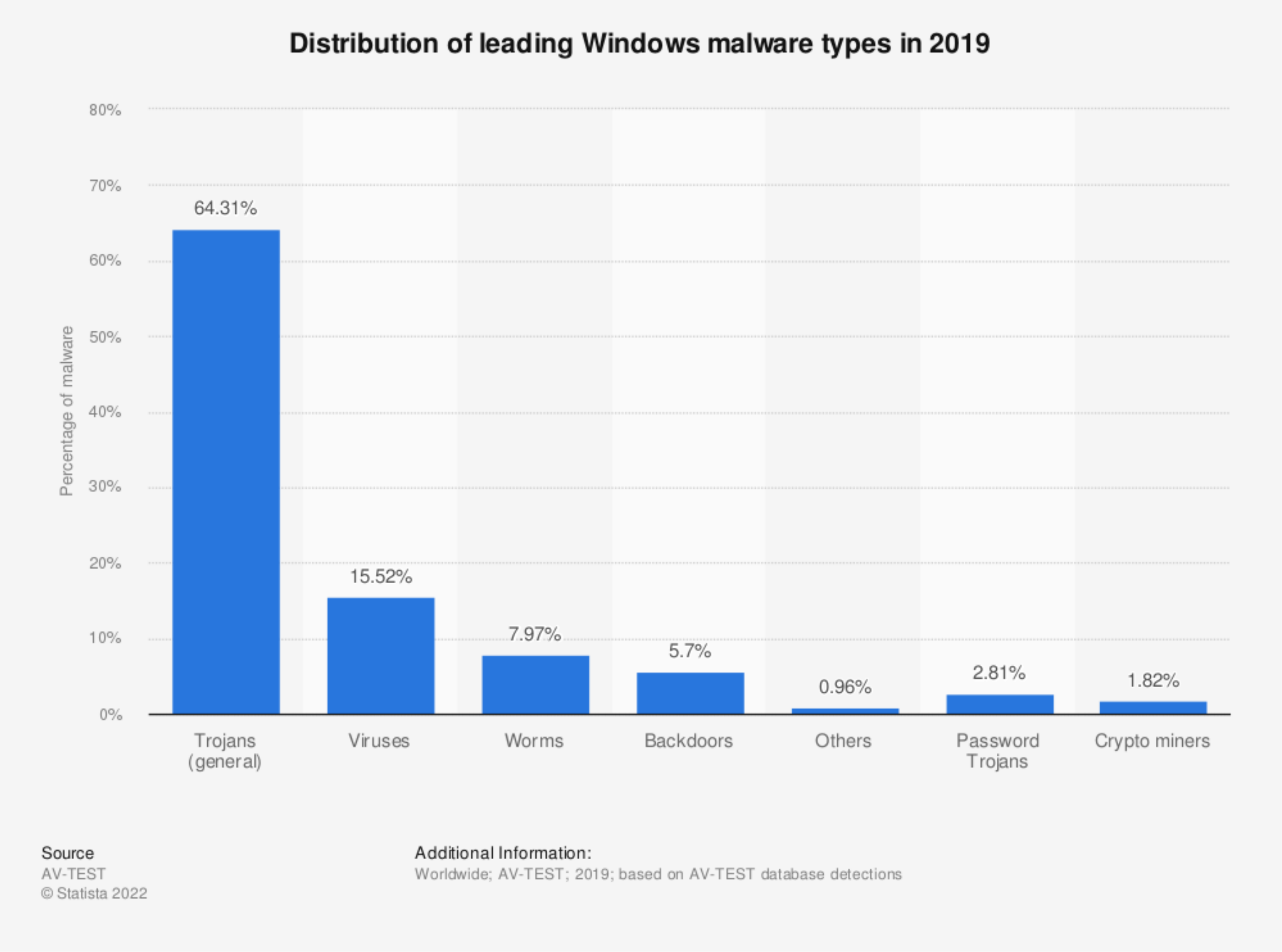
TROJANS

Sneak malware onto your PC

BOTNETS

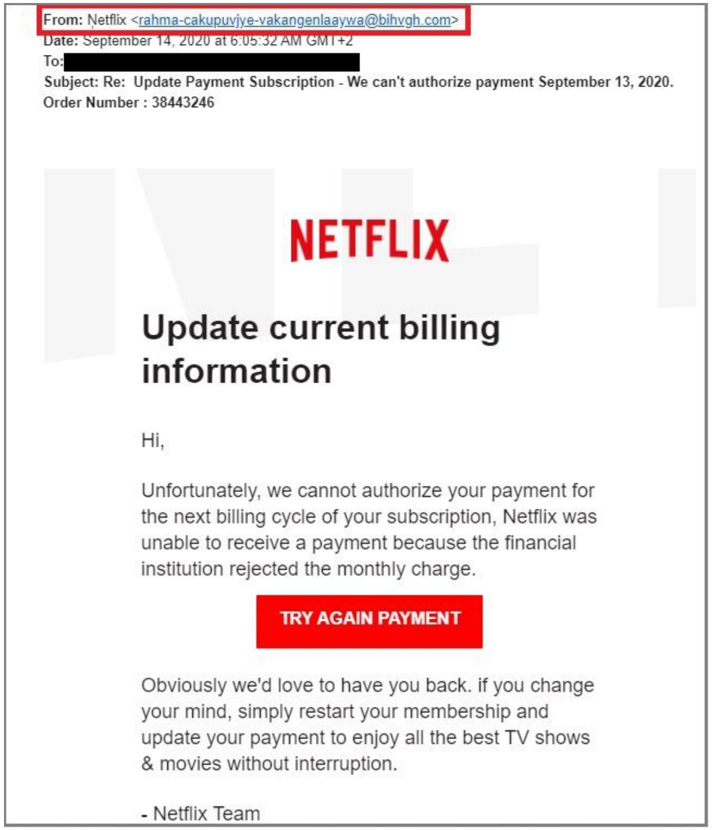
Turn your PC into a zombie

Where Does It Come From?



How Does It Work?

1. Trojan Horses & Worms
2. Unexpected Email Links
3. Office Macros
4. Infected Removable Drives
5. Compromised Web Pages



From: Netflix <rahma-cakupuvjye-vakangenlaaywa@bihvgh.com>
Date: September 14, 2020 at 6:05:32 AM GMT+2
To: [redacted]
Subject: Re: Update Payment Subscription - We can't authorize payment September 13, 2020.
Order Number : 38443246

NETFLIX

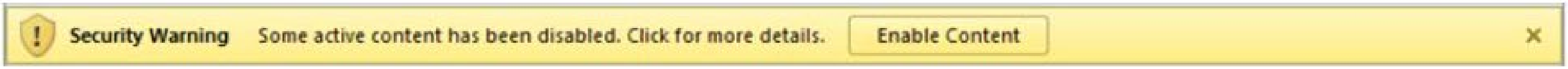
Update current billing information

Hi,

Unfortunately, we cannot authorize your payment for the next billing cycle of your subscription, Netflix was unable to receive a payment because the financial institution rejected the monthly charge.

Obviously we'd love to have you back. if you change your mind, simply restart your membership and update your payment to enjoy all the best TV shows & movies without interruption.

- Netflix Team



Security Warning Some active content has been disabled. Click for more details.

Security Challenges

287

Average number of days to identify and contain a data breach
(IBM Security Research 2021)

600%

The rise in global cost of cybercrime in 2021 to $6T USD, now the third-largest world economy after the USA and China
(Cybersecurity Ventures)

97%

Percentage of companies that have been affected by a cybersecurity breach in their supply chain
(PrivacySharks.com)

$172B

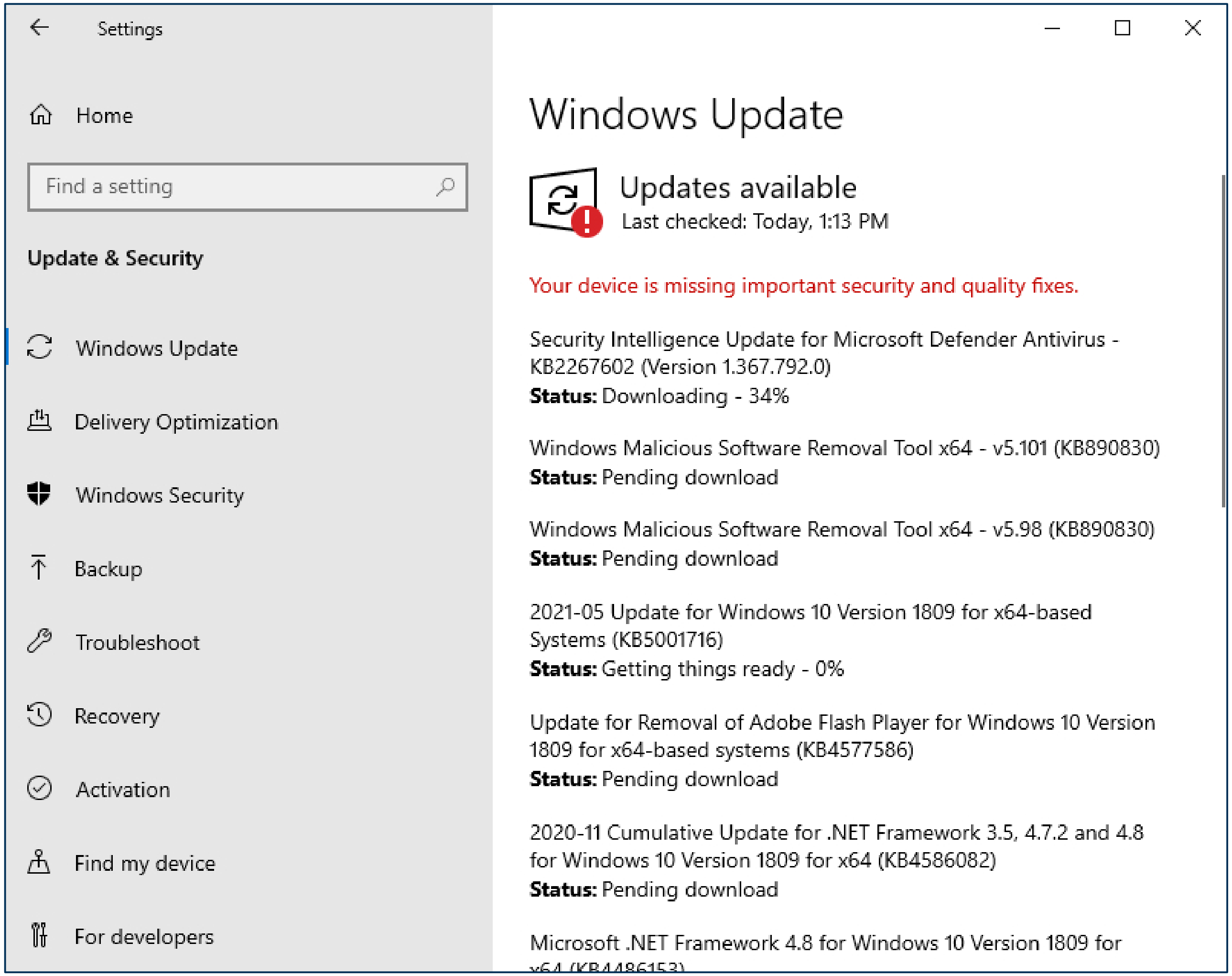
Expected spending on information security solutions in 2022, up 12% from $155 billion in 2021 (Gartner Research)

93%

Percentage of company networks that cyber criminals can penetrate
(Positive Technologies)

Trends in Malware

Hidden Ransomware



Windows Update

Updates available

Last checked: Today, 1:13 PM

Your device is missing important security and quality fixes.

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.367.792.0)
Status: Downloading - 34%

Windows Malicious Software Removal Tool x64 - v5.101 (KB890830)
Status: Pending download

Windows Malicious Software Removal Tool x64 - v5.98 (KB890830)
Status: Pending download

2021-05 Update for Windows 10 Version 1809 for x64-based Systems (KB5001716)
Status: Getting things ready - 0%

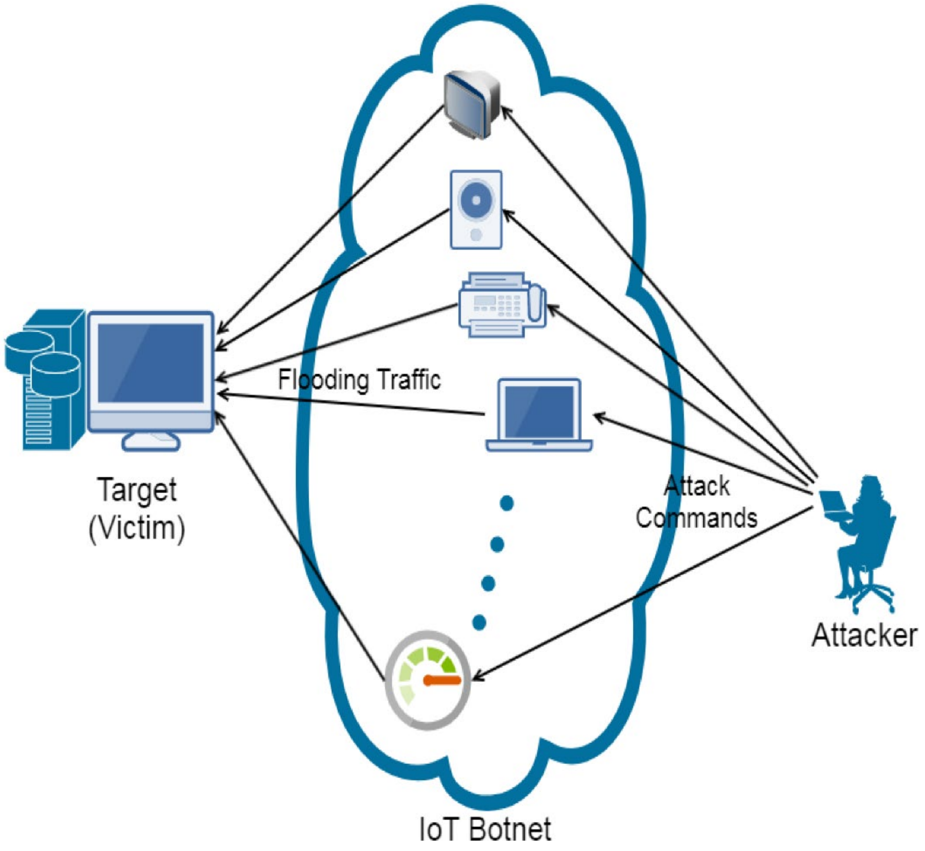
Update for Removal of Adobe Flash Player for Windows 10 Version 1809 for x64-based systems (KB4577586)
Status: Pending download

2020-11 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64 (KB4586082)
Status: Pending download

Microsoft .NET Framework 4.8 for Windows 10 Version 1809 for x64 (KB4486153)

IoT Device Attacks

- IoT = Internet of Things
- Targets smart devices (speakers, video doorbells, baby monitors, etc.)
- Launching off point to access larger network of information
- DDoS attacks



Zeus Gameover

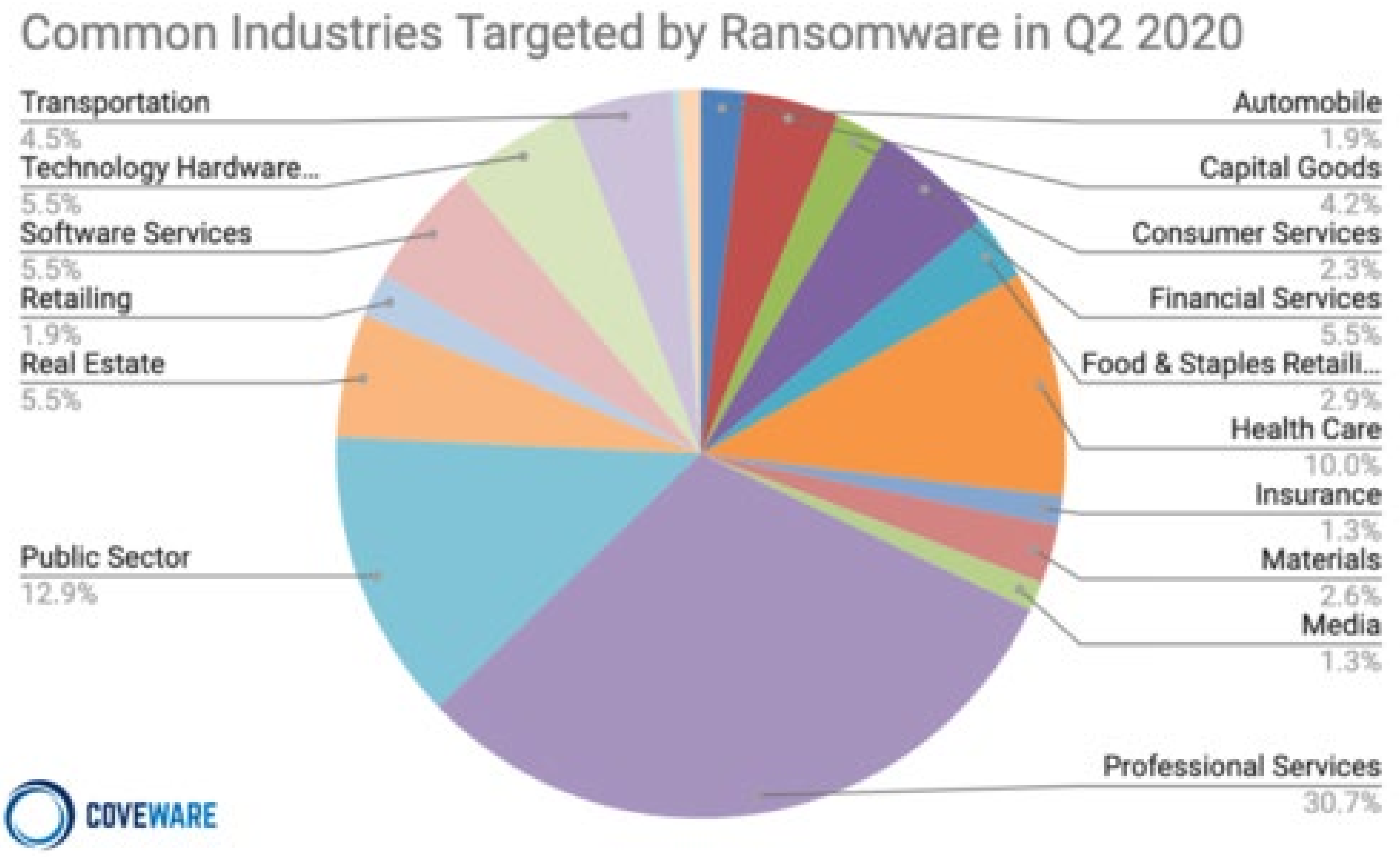
- Type of Trojan
- Bypasses centralized serves
- Cannot trace stolen data
- Popular for financial crimes

Other Trends

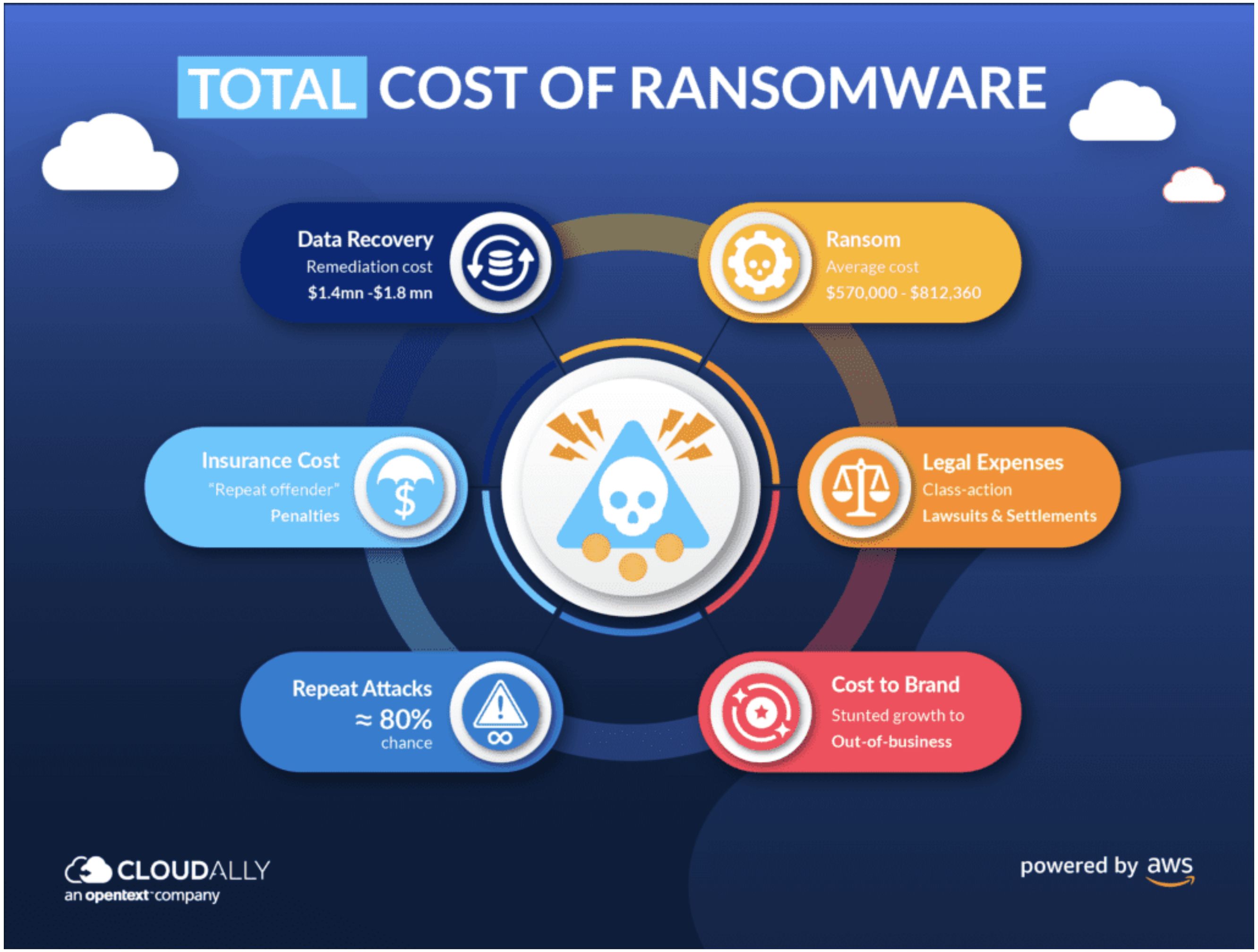
- **Fleeceware**: Charging app users money after apps are deleted; popular on Android devices.
- **RaaS**: “Ransomware as a Service,” contracting out for malware attacks
- **Data Monetization**: Criminals stealing data to sell for profit, particularly to competitors.

Industry Risks

Notable Past Attacks



Legal Exposure & Costs



TOTAL COST OF RANSOMWARE

Data Recovery
Remediation cost
$1.4mn -$1.8 mn

Ransom
Average cost
$570,000 - $812,360

Insurance Cost
"Repeat offender"
Penalties

Legal Expenses
Class-action
Lawsuits & Settlements

Repeat Attacks
≈ 80%
chance

Cost to Brand
Stunted growth to
Out-of-business

Specific Risks to Law Firms

- Law firms are popular targets
    - Six different law firms were targeted in January and February 2023 as part of two disparate threat campaigns distributing GootLoader and FakeUpdates (aka SocGholish) malware strains.
- The number of law firms reporting a security breach increased from 26% in 2019 to 29% in 2020.
- Nearly ¾ of breaches are due to employee actions (either intentional or accidental)
- Cyber Insurance comes into the picture

Notable Past Attacks on Law Firms

PANAMA PAPERS
Die Geheimnisse des schmutzigen Geldes
Das Leak
Doping im Fußball – Jetzt auch die Premier League
Süddeutsche Zeitung
MÜNCHNER NEUESTE NACHRICHTEN AUS POLITIK, KULTUR
Das Streiflicht
Die heimlichen Millionengeschäfte des Putin-Zirkels
Vertrauliche Dokumente enthüllen: Freunde des russischen Präsidenten haben über Briefkastenfirmen offenbar viel Geld ins Ausland geschafft. Die „Panama Papers" zeigen, wie Staatschefs, Diktatoren und Sportstars weltweit ihr Vermögen verschleiern
Sport

Obligations

General Data Privacy Standards

- **Federal:**
  - U.S. Privacy Act of 1974
  - Children's Online Privacy Protection Act
- **State:**
  - California Consumer Privacy Act
  - Maryland Online Consumer Protection Act
- **Industry:**
  - National Institute of Standards and Technology ("NIST")

Unique Obligations for Law Firms

- **Industry-Specific Regulations**
  - Sarbanes-Oxley Act of 2002
  - New York State SHIELD Act
  - HIPPA
- **Ethical Obligations**
  - ABA Model Rule of Professional Conduct 1.6
  - ABA Formal Opinion 483

Trends in Cybersecurity

Mitigation Strategies

- Security Systems
- Advanced Protection Technology
- Education
- Patches
- Tabletop Exercises

Evolving Practices

- Disaster Recovery Plans
- Network Segregation
- Threat Reputation Services

The Solutions:

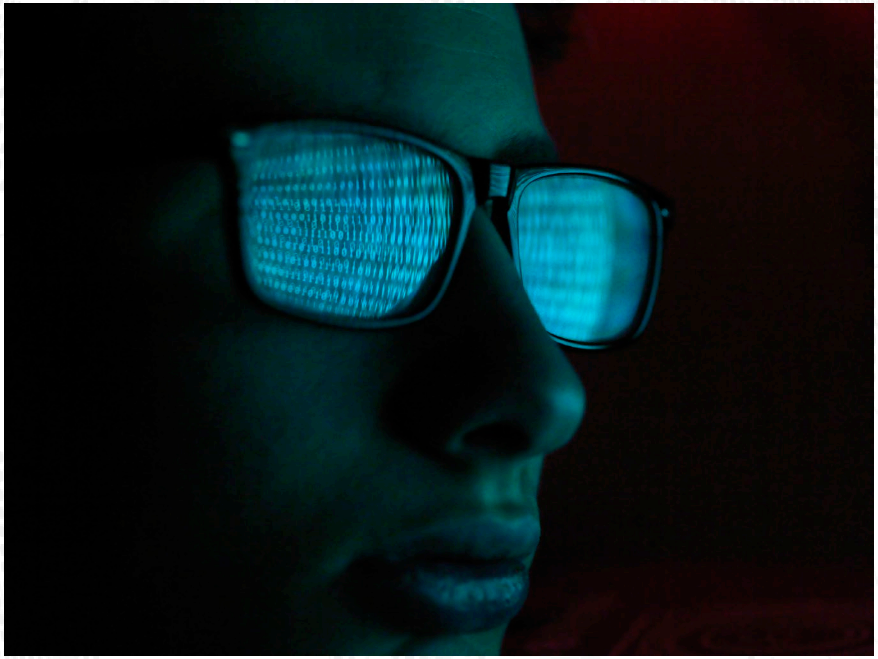
UltraDDR, UltraDDoS Protect and UltraWAF

Why UltraDDR?

Bad actors will always get in if they want to

UltraDDR makes sure their attack won’t be effective

It’s all about real-time visibility into anomalies and adversary communication to stop the attack before it gets started.



Get Proactive and Preventative: Deal With Cyber Risks Before The Attack

Not After You’ve Had To Inform Your C-Suite

Stop connections to attacker infrastructure before adversaries can use it

Prevent attackers from initiating new attacks

Minimize the noise and distraction of false positives and negatives

Deploy in minutes to improve your existing security investments

UltraDDR – Protective DNS Service

UltraDDR

DDR = DNS Detection and Response

Detection

Protect against adversary infrastructure before it's used

Continuous observability to map attacker assets, understand physical locations of attacks, and prepare proactively for new threats

Response

Prevent attackers from initiating new attacks

Mitigate in real-time to render existing intrusions inert

Watch and analyze suspicious communications to move to block or greenlight

Summary & Wrap-Up

Questions?

Presenters

John McNichols

Partner

Williams & Connolly

jmcnichols@wc.com

202-434-5043

Allie Eisen

Associate

Williams & Connolly

aeisen@wc.com

202-434-5354

Kevin Hughes

General Counsel

Vercara

kevin.hughes@vercara.com