

A wireframe illustration of a robotic hand holding a keyboard. The hand is composed of a grid of lines, and the keyboard keys are also represented by wireframe models. A solid orange horizontal line is positioned above the main title.

RANSOMWARE DECODED

Understanding And Preventing
Modern Ransomware Attacks



~\$ WHOAMI



Kraig Faulkner

Lead Sales Engineer
Cybereason

AGENDA

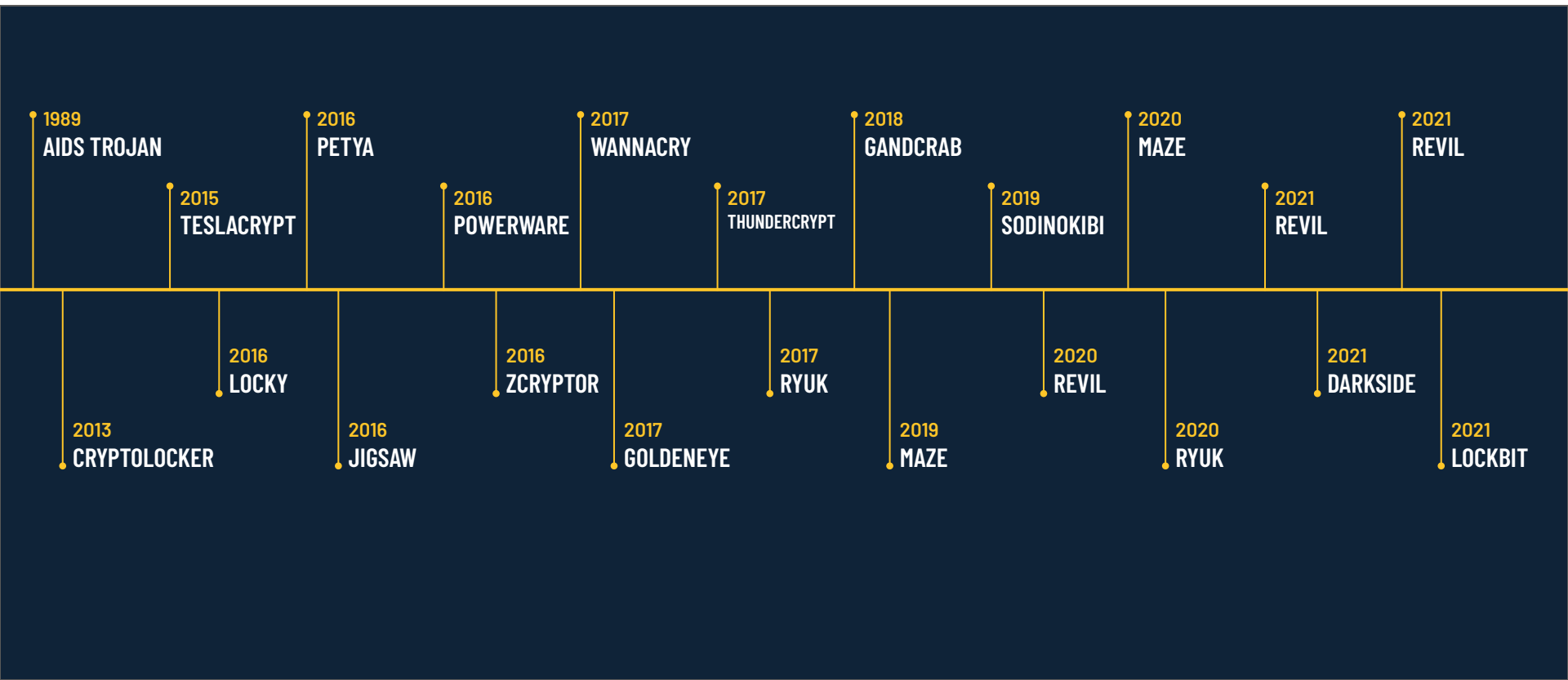
1. History of Modern Ransomware
2. Why Ransomware?
3. Insights & Trends
4. The Golden Age of Ransomware
5. Ransomware Defense



A large, stylized wireframe graphic of an owl's head, composed of a grid of white lines on a dark blue background. The owl is facing forward, with its head slightly tilted. The wireframe is dense and detailed, showing the contours of the owl's face, ears, and feathers.

HISTORY OF MODERN RANSOMWARE

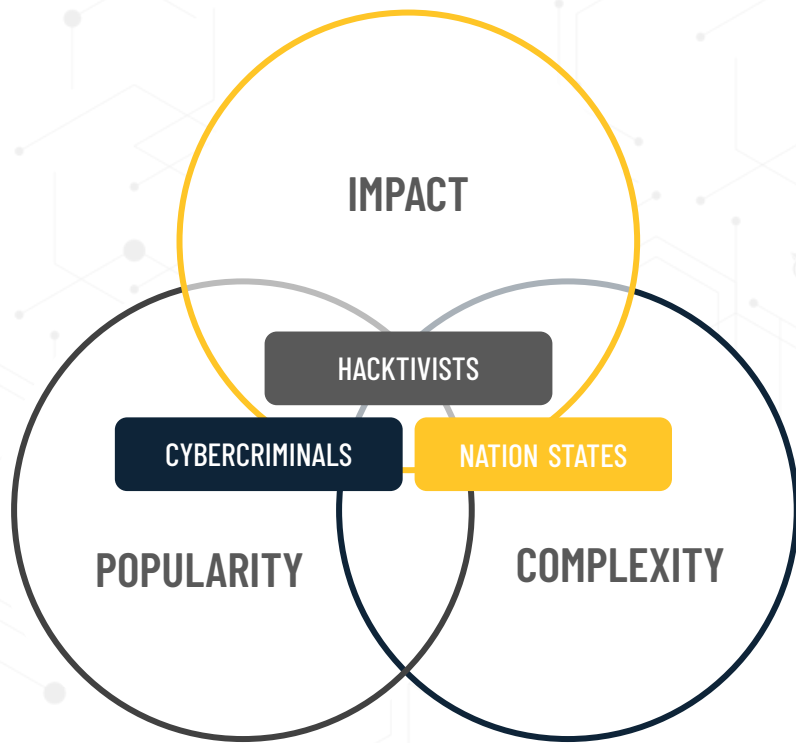
THE EVOLUTION OF RANSOMWARE



A wireframe illustration of an owl's head, rendered in a light blue color against a dark blue background. The owl is facing forward, with its large, detailed eyes and sharp beak clearly visible. The wireframe lines create a mesh-like texture across the entire head.

WHY RANSOMWARE?

WHY DO ATTACKERS USE RANSOMWARE?



THE LATEST

MUST READ: Ransomware: Take these three steps to protect yourself from attacks and make it easier to recover

TECHNOLOGY NEWS MARCH 31, 2021 / 11:22 AM / UPDATED 12 DAYS AGO

Ransomware tops U.S. cyber priorities, Homeland secretary says

By Raphael Satter

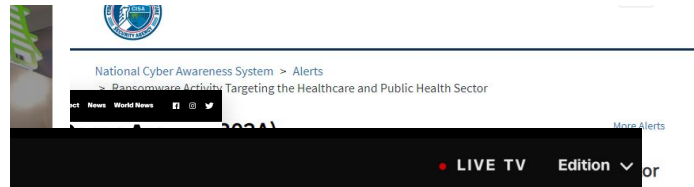
2 MIN READ



FILE PHOTO: U.S. Department of Homeland Security Secretary Alejandro Mayorkas speaks during a press briefing at the White House in Washington, U.S., March 1, 2021. REUTERS/Kevin Lamarque/File Photo

REvil ransomware group resurfaces after brief hiatus

The 'Happy Blog' run by the group was back on Tuesday.



LATEST Amazon offers to pay college tuition for most US workers

e attack also led to personal

WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA) announced the Reduce the Risk of Ransomware Campaign today, a focused, coordinated and sustained effort to encourage public and private sector organizations to implement best practices, tools and resources that can help them mitigate this cybersecurity risk and threat.

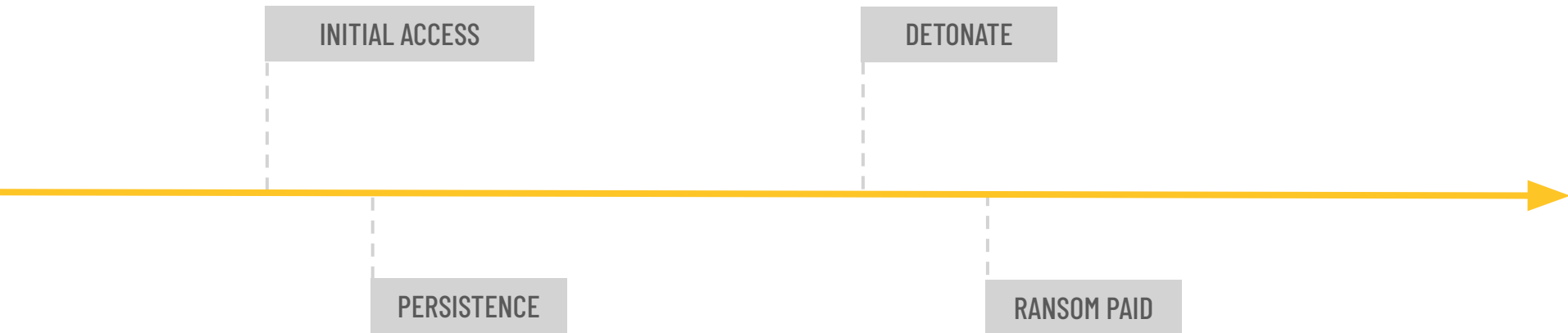
WHY PRIORITIZE RANSOMWARE DEFENSE?

- Ransom Payment \$\$\$
- Business Continuity
 - Downtime costs
 - Loss of data
- IR & security costs
- IT costs
- Insurance coverage
- Reputational damage
- Regulatory fines
- Loss of Human Life

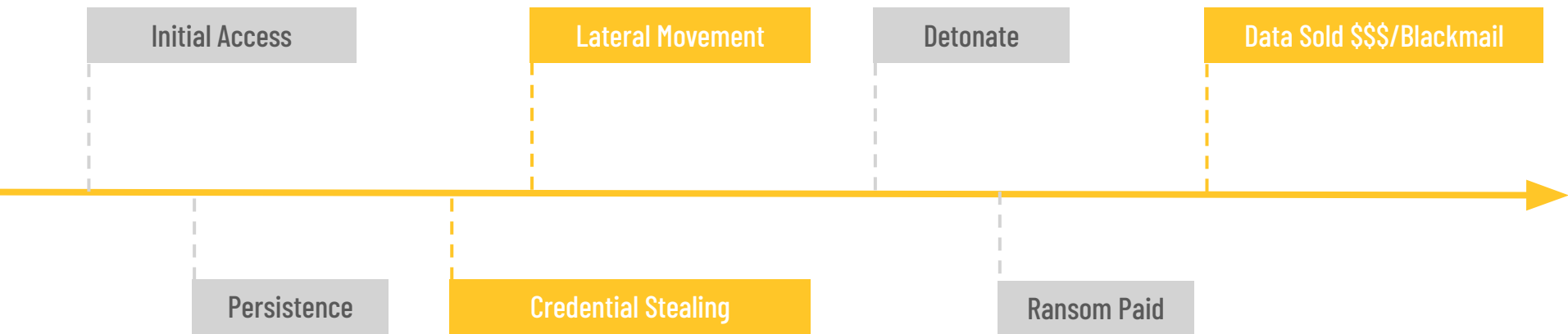


INSIGHTS & TRENDS

SINGLE STAGE RANSOMWARE



MULTISTAGE RANSOMWARE



WHAT CHANGED?

Decline of “Spray and Pray”:

- Up until 2016, most ransomware attacks indiscriminately targeted individuals and organizations alike.

Bigger Risk, Bigger Payout:

- Since 2016, targeted attacks against organizations have increased dramatically.
- Average ransom rose from \$115k in 2019 to \$312k in 2020

Average Ransom Payment by Quarter

Amounts are in USD



WHAT MAKES A GOOD TARGET?

1

Those who require 99.999% uptime.

2

Those with small IT teams.

3

Those who use legacy systems.

HOW ARE ATTACKERS DOING IT?

Get Philadelphia at a Special Price!

\$389
Unlimited License

Unlimited Builds

Unlimited Campaigns

No monthly fees or % rate

Constant Updates

Bitcoin Payment Autodetect

Plain-English help file

No dependencies (.net or whatever)

[Get In Touch!](#)

Alpha Locker

Нажмите здесь, чтобы посмотреть исходное изображение.

ALPHA LOCKER

ABOUT

Alpha locker is written in C #, it has a minimum weight of up to 50 kb
The unique key for each pc
Locker encrypts all drives connected to the pc
Continues to encrypt files when the computer is turned off
Decryption can decrypt the chosen file or an entire folder
Admin panel has statistics and general information
The scripts back up and restore the database increases data reliability
Communication for the decryptor via e-mail
We can add features to your liking


PRICE

BUILD

65\$

[BUY NOW](#)

CONTACT

 + **OTR**

ALPHALOCKER@EXPLOIT.IM

FROM RANSOM TO BLACKMAIL

Concerning Trend:

**Shifting to
BLACKMAIL**

HOW CYBERCRIMINALS NOW FORCE VICTIMS TO PAY?

- Controlling the network can be used to steal data
- Data exfiltration at scale & stealth
- Don't want to pay? All your data will be sold to the highest bidder
- Exploiting the fear of legal ramifications (GDPR, HIPAA, PCI DDS, GLBA)

PAYING THE RANSOM



FinCEN ADVISORY

FIN-2020-A006

October 1, 2020

Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments

Detecting and reporting ransomware payments are vital to prevent and deter cybercriminals from deploying malicious software to extort individuals and businesses and hold ransomware attackers accountable for their crimes.

This Advisory should be shared with:

- Chief Executive Officers
- Chief Operating Officers
- Chief Compliance Officers
- Chief Risk Officers
- Chief Information Officers
- AML/BSA Departments
- Legal Departments
- Cyber and Security Departments
- Customer Service Agents
- Bank Tellers

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to predominant trends, typologies, and potential indicators of ransomware and associated money laundering activities. This advisory provides information on: (1) the role of financial intermediaries in the processing of ransomware payments; (2) trends and typologies of ransomware and associated payments; (3) ransomware-related [financial red flag indicators](#); and (4) reporting and sharing information related to ransomware attacks.

The information contained in this advisory is derived

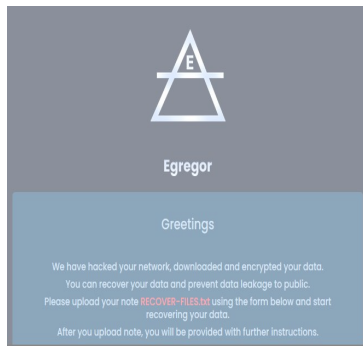
The background is a dark blue field filled with a complex, light gray geometric pattern. This pattern consists of interconnected lines, dots, and various polygons, including hexagons and squares, creating a sense of a digital network or circuitry. A single, solid orange horizontal line is positioned above the main title text.

THE GOLDEN AGE OF RANSOMWARE

2020: The Year of Ransomware?

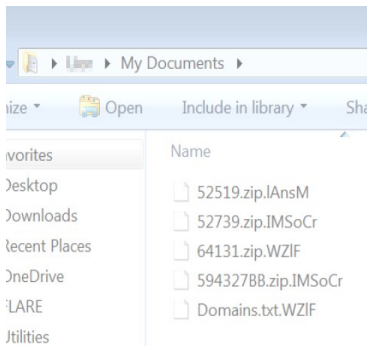
MORE AGGRESSIVE THAN EVER

The most prominent
threat in 2020



PARADIGM SHIFT

Classic Ransom Demand
→
Double Extortion



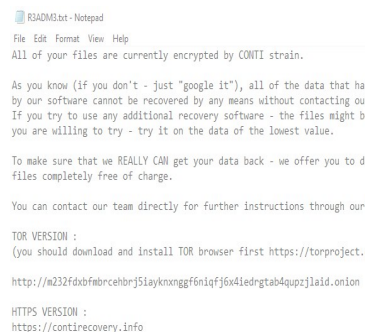
CYBERCRIMINAL COLLABORATION

Joint operations with
various commodity
malware



COMMON INFECTION VECTORS

Credentials on
underground markets,
vulnerable assets, phishing



Ransomware Stats for 2020

Top affected Industries

- Manufacturing
- Government
- Education
- Services
- Healthcare

Top affected countries / Regions

- North America
- North-West Europe
- Commonwealth countries (UK, Australia, South Africa)
- Japan
- India



SUPPLY CHAIN ATTACKS

CYBEREASON VS EGREGOR RANSOMWARE



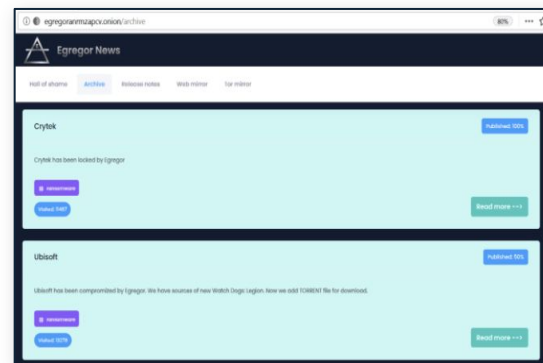
REGIONS:



INDUSTRIES:



- **RaaS Model:** Ties to the former Maze Cartel
- **Double extortion Scheme:** with a leaks website
- **Infection chain:** phishing email -> Qakbot -> Eggegor



COMMODITY MALWARE AS A PRECURSOR OF AN ATTACK

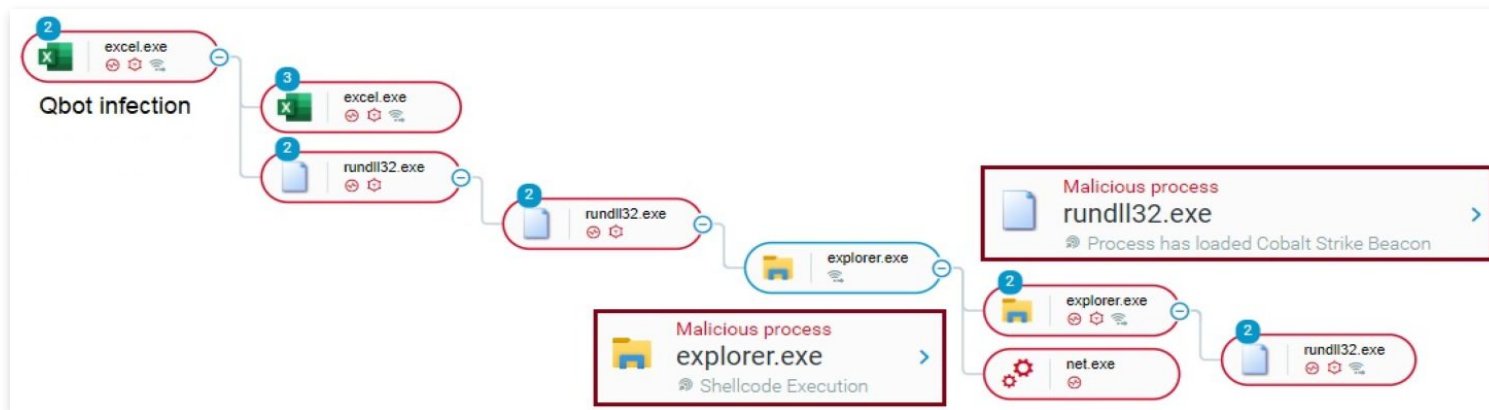
COMMODITY MALWARE INFECTION

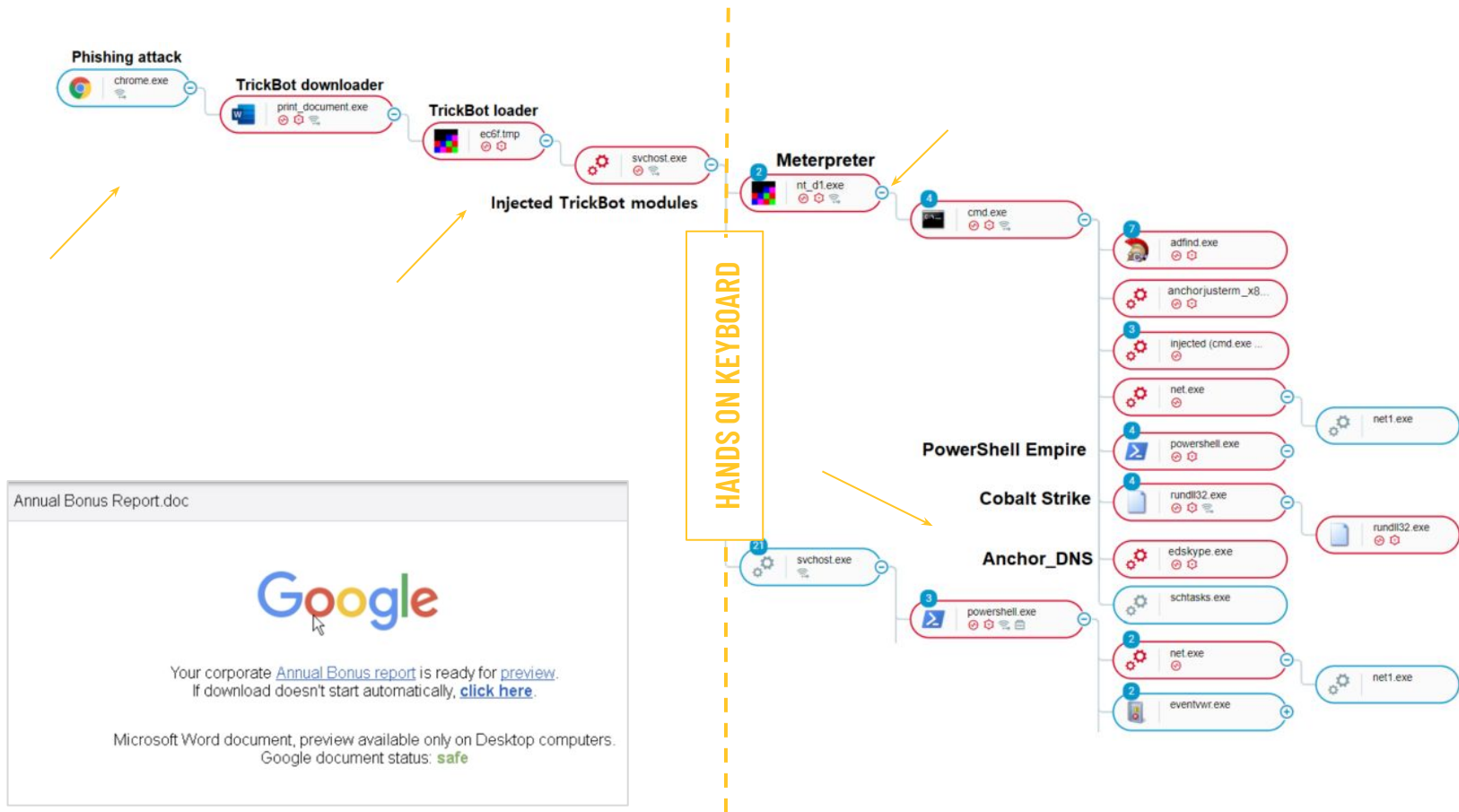
RECONNAISSANCE

- Who is the victim?
- Collect data about the user / domain

COURSE OF ACTION

- **Hacktools & penetration testing frameworks** (Metasploit, Cobalt Strike, adfind)
- **Lateral movement** attempts (WMI, PowerShell, Pass-the-Hash, Pass-the-Ticket)







RANSOMWARE DEFENSE

TODAY'S CHALLENGES

- Easier than ever to run a RaaS operation
- More threat actors focus on organizations
- More payouts than ever before, prices go up
- Ransom → Blackmail: Not paying increasingly becomes a scarier option
- Government regulations with steep fines come into play

THE UPSIDE

- “Low and Slow”: Dwell time > 1 month (up to 9 months!)
- History repeats itself: Most ransomware attacks are not novel!
- Next-gen AV and Behavior-based protection prove effective
- Good hygiene, procedures, and layered defense can prevent most attacks

PROTECTING YOUR ORGANIZATION

- Reevaluate or identify crown jewels (and paths to them)
- Evaluate and reduce cyber risk through prioritization
- Update legacy systems
- Prevent the preventable
- Detection mindset
- Implement user training
- Communicate the risk to the business
- Build relationships with executives
- Prepare in peacetime

WANT TO LEARN MORE?



THANK YOU