cybereason®

What's Next In The Fight Against Ransomware

RVASEC Session

November 4, 2021

Confidential

AGENDA AND SPEAKERS

1. Ransomware research and Nocturnus
2. The technical evolution of ransomware
3. A historical tangent
4. The attacker perspective
5. Crisis management and the true cost to business
6. How Cybereason defeats ransomware
7. Q&A session

Maggie MacAlpine
Security Strategist
Cybereason
Twitter: @MaggieMacAlpine

VISION

Protect people and information in the new and open connected world

MISSION

Reverse the adversary advantage by empowering defenders with ingenuity and technology to end cyber attacks

NOCTURNUS

Expert Research & Analysis on Today’s Latest Threats

Darkside

Began tracking months before breach activity

REvil

Long term research, Sodinokibi Group behind Travelex, JBS, Acer & Kaseya

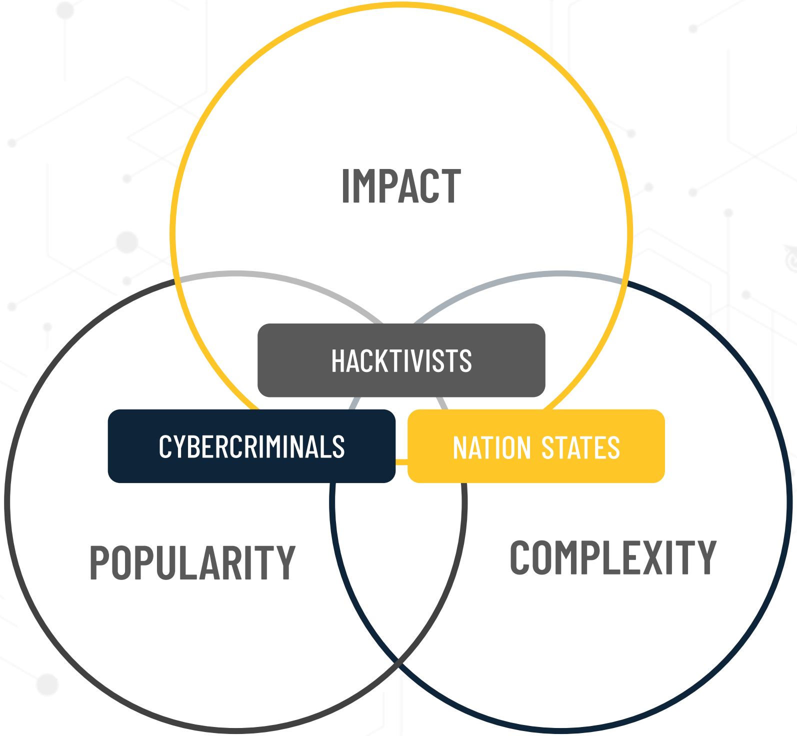
NOTPETYA

Discovered a ransomware vaccine to prevent machine infection

cybereason®

WHY DO ATTACKERS USE RANSOMWARE?

Ransomware:
A type of malware designed to block access to systems or data until a ransom is paid.



RANSOMWARE

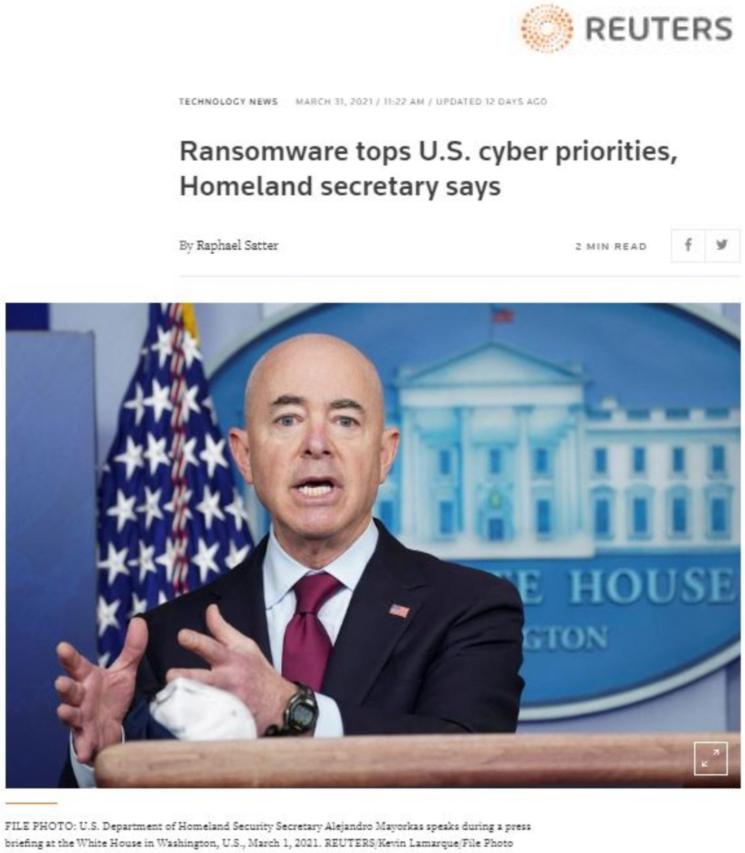
More of an issue than ever

105% Increase in ransomware attacks since the start of the COVID-19 pandemic

73% Success rate in ransomware attempts

51% Organizations have encountered ransomware in their environment

"Ransomware is a problem that's continuing to get bigger"
-Verizon Data Breach Investigations Report, 2020



REUTERS

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

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

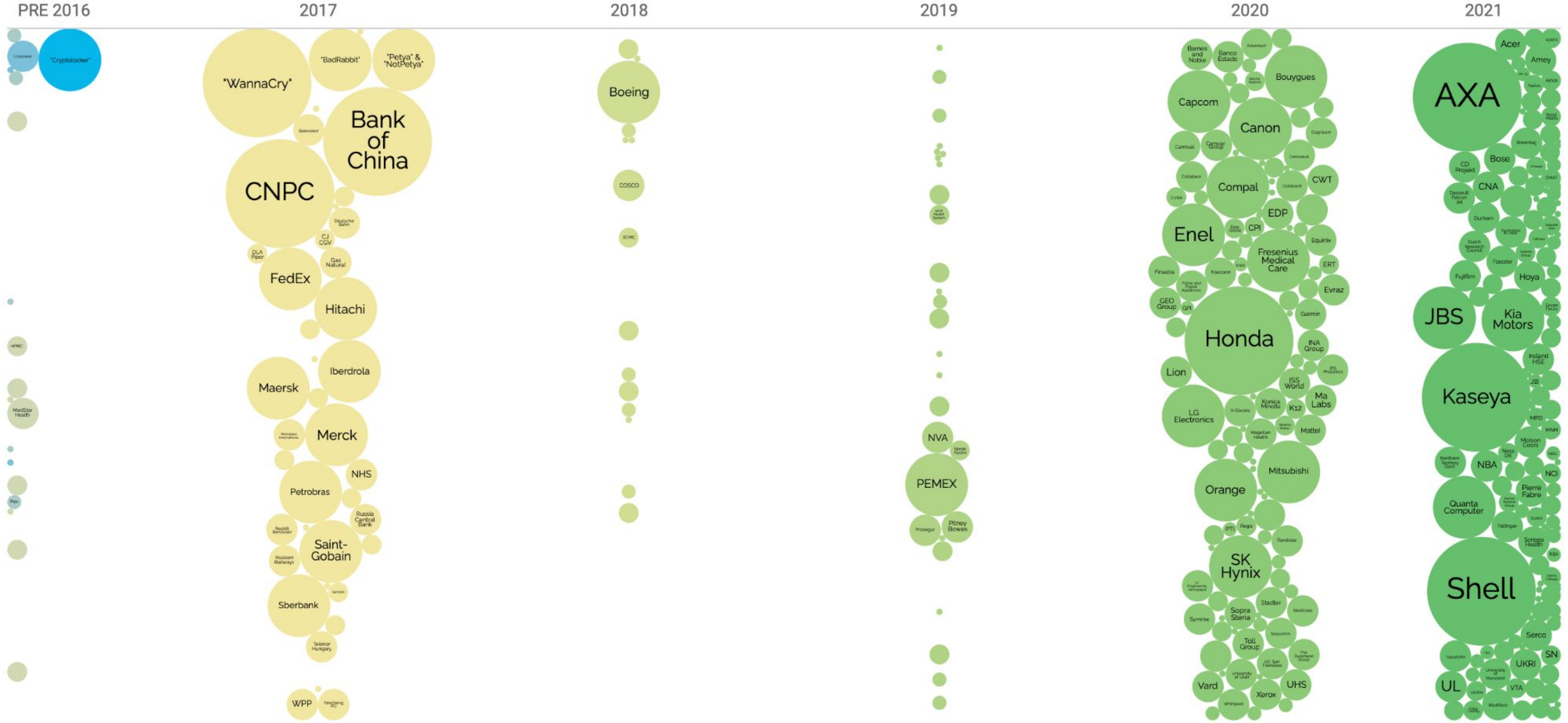
By Raphael Satter 2 MIN READ

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

source

Ransomware Attacks BETA

size = size of organisation



THE ATTACKER TOOLKIT

Factors leading to preferential use of ransomware in cyber attacks

1

Ransomware is extremely lucrative for adversaries

2

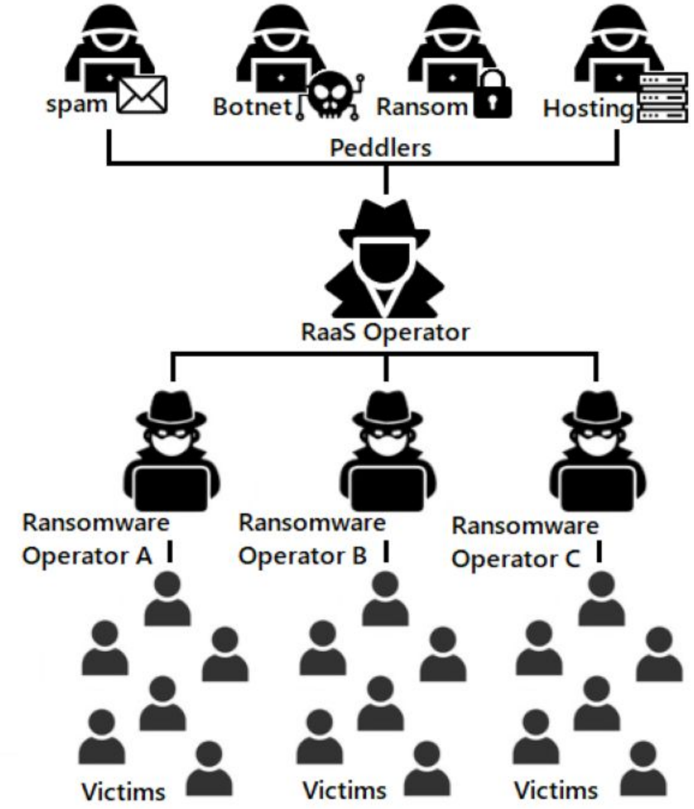
There is a lower bar of entry to deploy a ransomware attack

3

Double extortion, triple extortion = added leverage

CYBERCRIME ECOSYSTEM

THE RaaS MODEL



RANSOMWARE AND CRYPTO

Anonymous Currency Enables Adversaries

Crypto is connected to the RaaS Model

Cryptocurrency - Anonymous & decentralized

Payment without the personal details

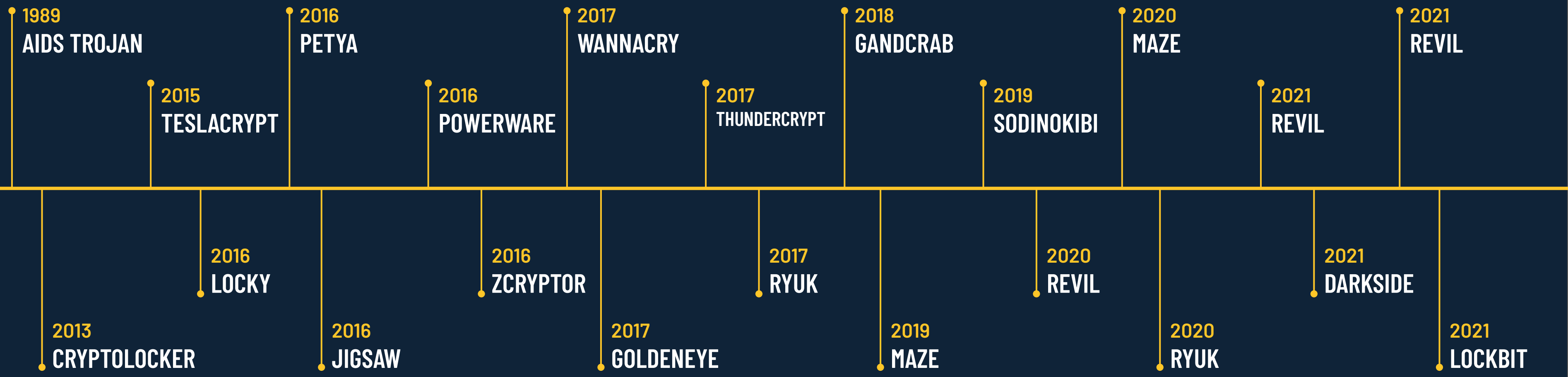
Banks aren’t involved

Funds are (mostly) untraceable

Not limited to Bitcoin - Monero, ZCash

The Evolution of Ransomware

THE EVOLUTION OF RANSOMWARE



1989
AIDS TROJAN

2013
CRYPTOLOCKER

2015
TESLACRYPT

2016
LOCKY

2016
PETYA

2016
JIGSAW

2016
POWERWARE

2016
ZCRYPTOR

2017
WANNACRY

2017
GOLDENEYE

2017
THUNDERCRYPT

2017
RYUK

2018
GANDCRAB

2019
MAZE

2019
SODINOKIBI

2020
REVIL

2020
MAZE

2020
RYUK

2021
REVIL

2021
DARKSIDE

2021
REVIL

2021
LOCKBIT

EVOLUTION OF RYUK

Known Malware

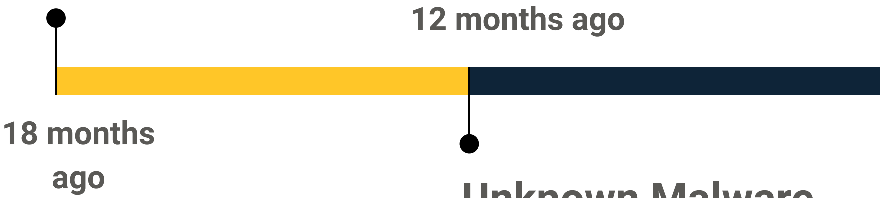
Reused parts of existing malware

18 months ago

EVOLUTION OF RYUK

Known Malware

Reused parts of existing malware



Unknown Malware

Moved to using packers and encoders
to bypass signature detections (AVs)

EVOLUTION OF RYUK

18 months ago

Known Malware

Reused parts of existing malware

12 months ago

Unknown Malware

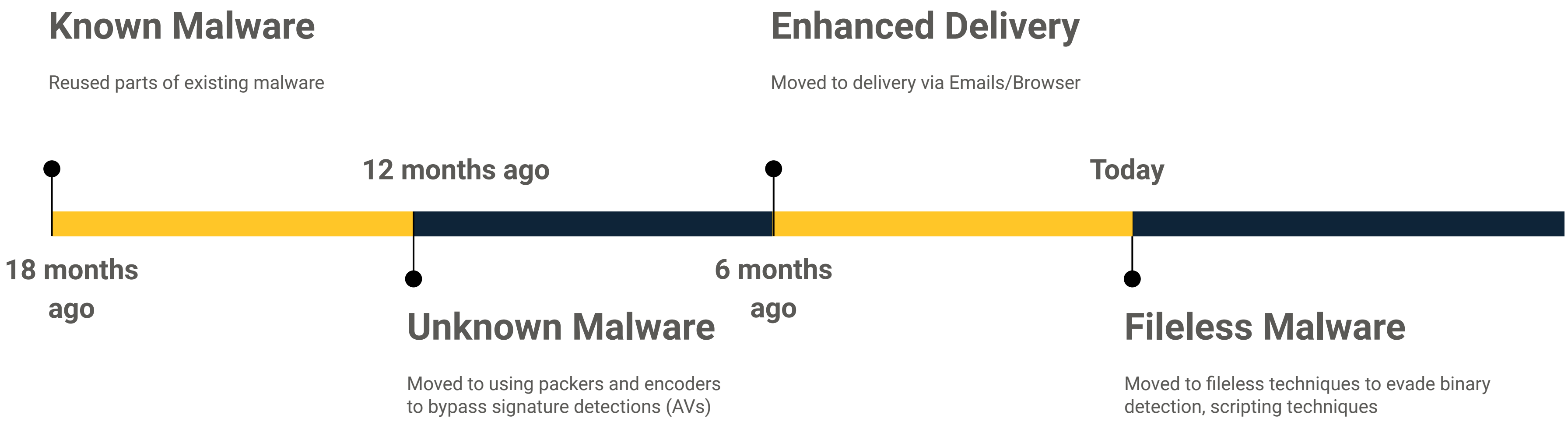
Moved to using packers and encoders to bypass signature detections (AVs)

6 months ago

Enhanced Delivery

Moved to delivery via Emails/Browser

EVOLUTION OF RYUK



18 months ago

Known Malware

Reused parts of existing malware

12 months ago

Unknown Malware

Moved to using packers and encoders to bypass signature detections (AVs)

6 months ago

Enhanced Delivery

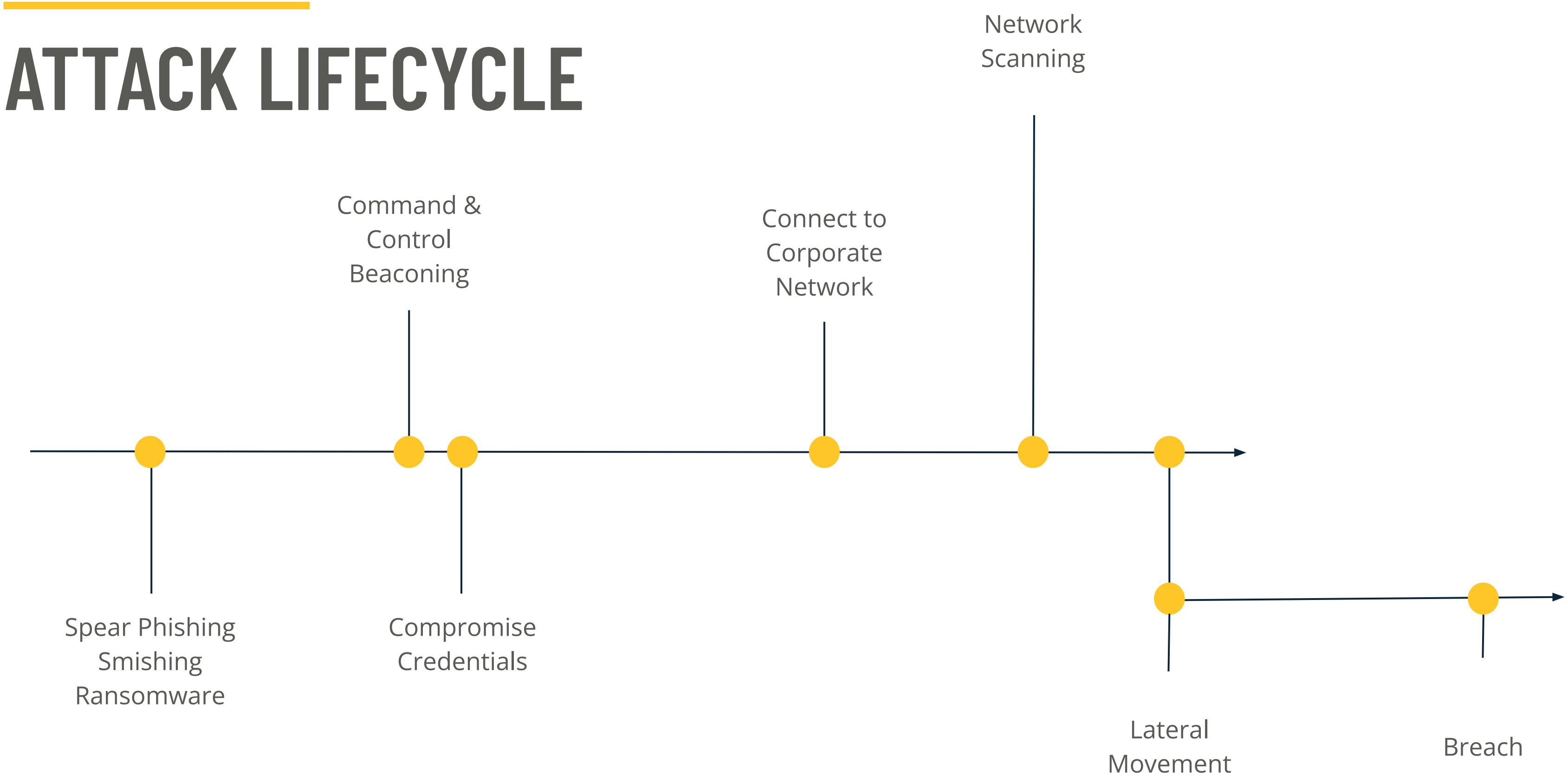
Moved to delivery via Emails/Browser

Today

Fileless Malware

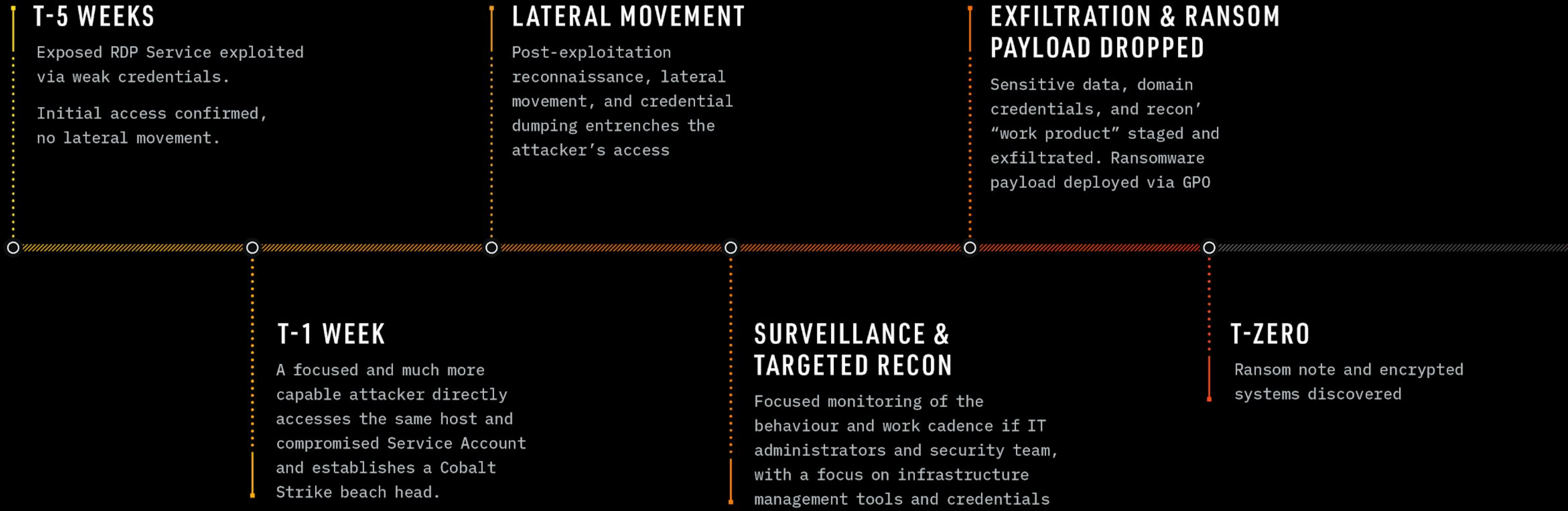
Moved to fileless techniques to evade binary detection, scripting techniques

ATTACK LIFECYCLE



Attacker’s Perspective

RANSOMWARE TIMELINE



T-5 WEEKS

Exposed RDP Service exploited via weak credentials.

Initial access confirmed, no lateral movement.

T-1 WEEK

A focused and much more capable attacker directly accesses the same host and compromised Service Account and establishes a Cobalt Strike beach head.

LATERAL MOVEMENT

Post-exploitation reconnaissance, lateral movement, and credential dumping entrenches the attacker’s access

SURVEILLANCE & TARGETED RECON

Focused monitoring of the behaviour and work cadence if IT administrators and security team, with a focus on infrastructure management tools and credentials

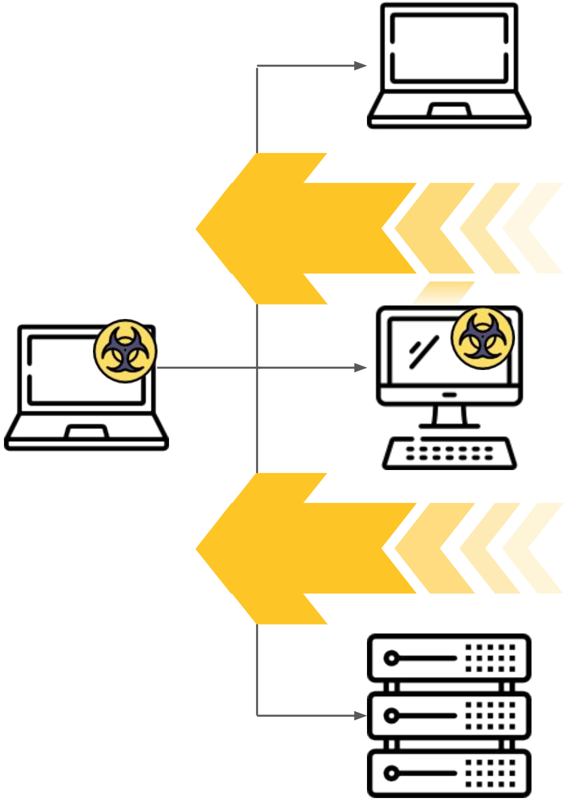
EXFILTRATION & RANSOM PAYLOAD DROPPED

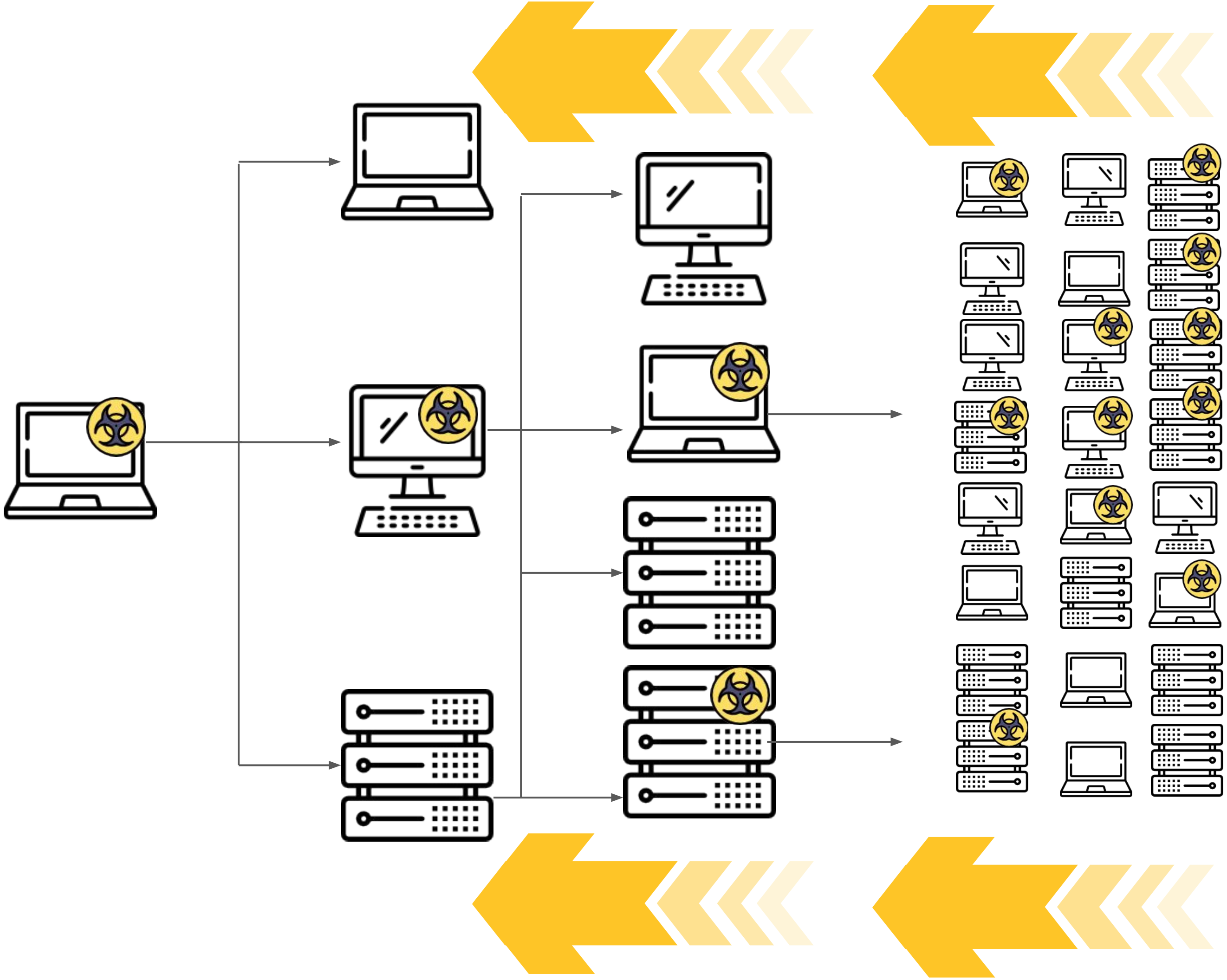
Sensitive data, domain credentials, and recon’ “work product” staged and exfiltrated. Ransomware payload deployed via GPO

T-ZERO

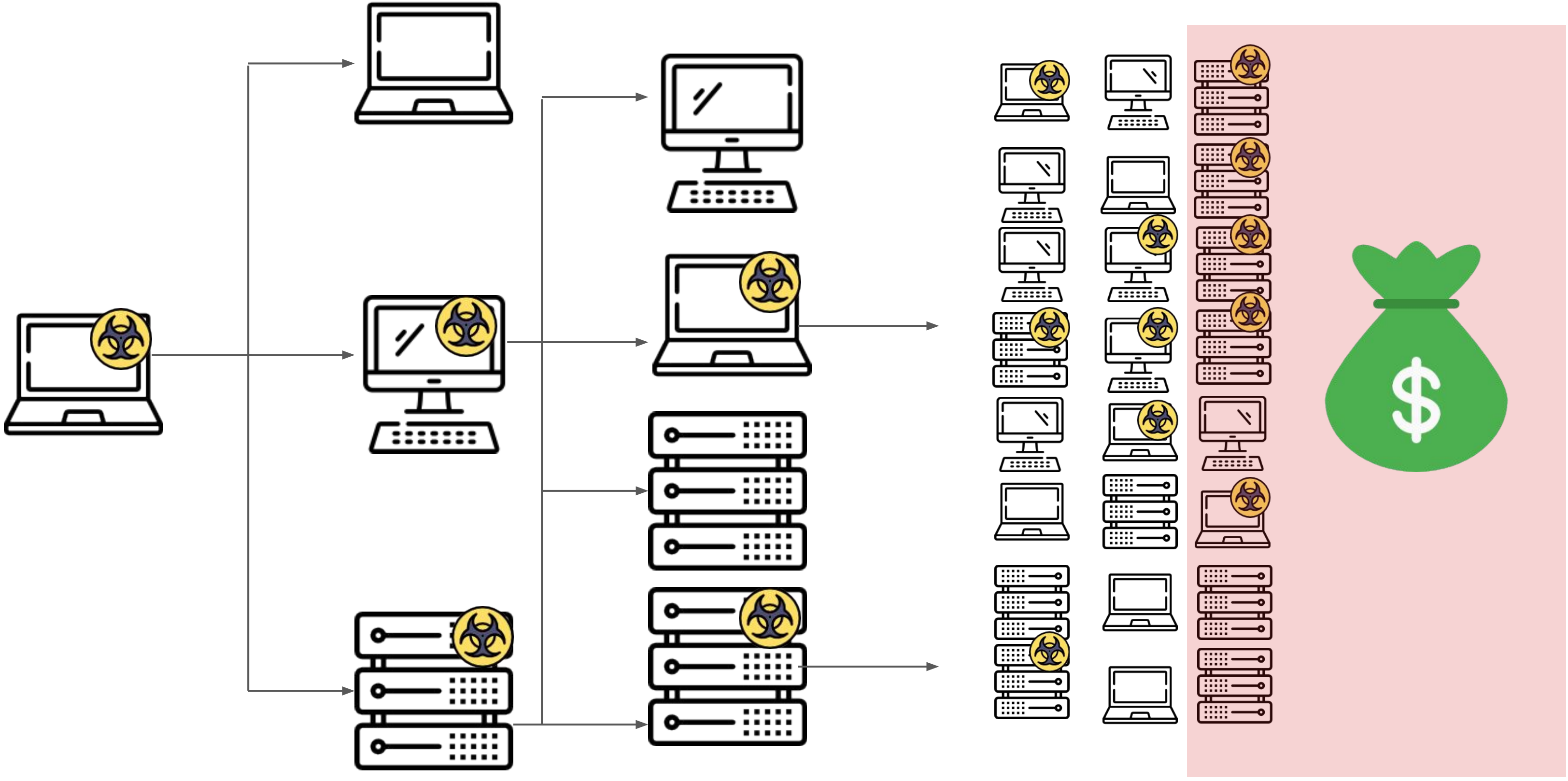
Ransom note and encrypted systems discovered

THE ANATOMY OF A REAL ATTACK





cybereason



cybereason

ACTIONS ON OBJECTION: ATT&CK MAPPING

Discovery

- T1046 → Network Service Scanning

Privilege Escalation

- T1078 → Valid Accounts

Execution

- T1059 → Command & Scripting Interpreter

Defense Evasion

- T1090 → Connection Proxy
- T1078 → Valid Accounts
- T1108 → Redundant Access

Defense Evasion

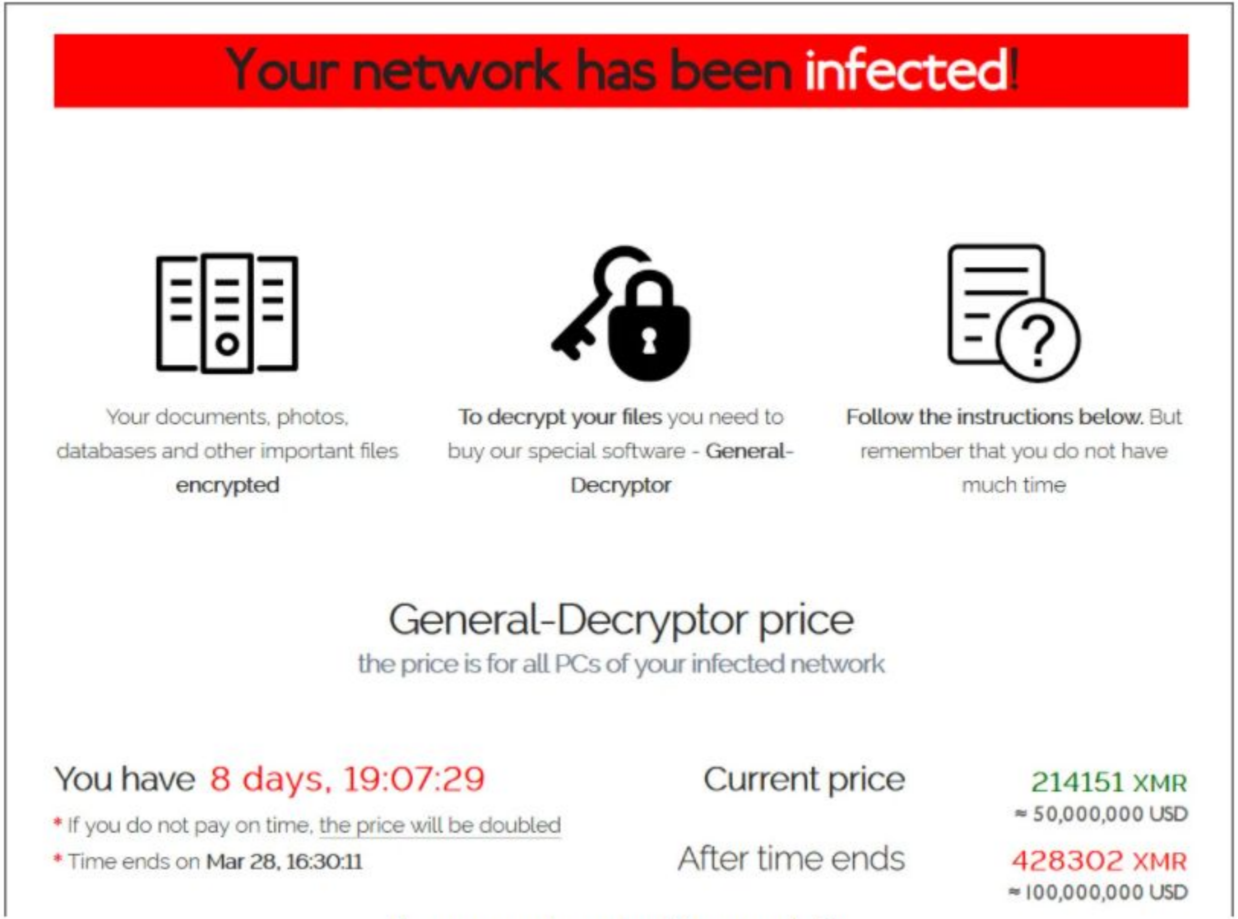
- T1036 Masquerading
- T1140 Deobfuscate/Decode Files or Information
- T1070 → Indicator Removal on Host
- T1553 → Subvert Trust Controls

Lateral Movement

- T1021 → Remote Services
- T1076 → Remote Desktop Protocol

Impact

- T1486 → Data Encrypted for Impact



Your network has been infected!

Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **General-Decryptor**

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

You have 8 days, 19:07:29

* If you do not pay on time, the price will be doubled

* Time ends on **Mar 28, 16:30:11**

Current price 214151 XMR

≈ 50,000,000 USD

After time ends 428302 XMR

≈ 100,000,000 USD

Acer ransom demand on Tor payment site

THE GOLDEN AGE OF RANSOMWARE: A HISTORICAL TANGENT

cybereason®

A Threat We've Seen Before...

- Holding goods for ransom is hardly a new business model for criminals, all that has changed is the medium.

- The Internet has matured to the point where cyberspace resembles international waters during the Age of Sail more than the "Wild West".

- Pirates, or rather privateers as many were state-sanctioned to varying degrees, serve as a historic parallel to modern ransomware gangs.

- Like their maritime counterparts, ransomware gangs:
  - Strike/retreat quickly
  - Mask their country of origin by flying false flags (for whom they may also work informally)
  - Create their own economic ecosystem of wild profitability for highly skilled workers who may otherwise lack opportunities to gain such wealth, ie the rewards far outweighs the risk.

...And a Threat We Know How to Face

- If we shift our view of the current threat landscape to see navies, privateers, and pirates, rather than amorphous levels of state-support for criminal hackers, we empower our thinking with historic and recent naval military models of how to respond.
- Luckily, we also have a model for how to deal with such threats. While it won't be easy, we are not flying blind.
- Going after the means of payment, limiting opportunities, and removing safe harbors, are key steps.
- Violent whack-a-mole will not work. This criminal model *cannot* be stopped so long as the incentives remain.

Piracy is a nontraditional security threat that cannot be solved through military solutions . . . piracy should be rooted out by attacking sources of their strength on land, disrupting their organizational structure, and isolating them from their sources of support. In particular, this means destroying their bases and hideouts; cutting off their sources of capital, technology, and recruitment; and crippling the middlemen and markets that allow them to dispose of their loot.*

- Graham Gerard Ong-Webb, “Piracy in Maritime Asia: Current Trends,” in Violence at Sea: Piracy in the Age of Global Terrorism, Peter Lehr, ed. (New York: Routledge, 2007), 90.

Crisis Management

RANSOMWARE RECOVERY

Organizations may think

○ Cyber insurance

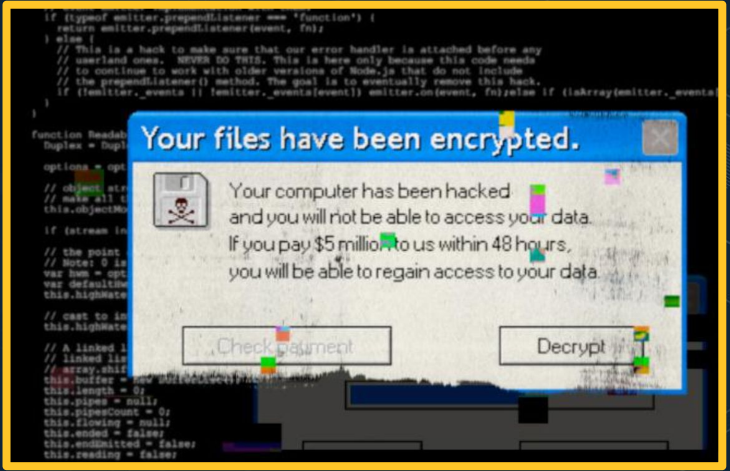
○ Data backups

○ Ability to complete recovery

Are enough - ***but have you considered other risks?***

RANSOMWARE ATTACKS: IMPACT TO BUSINESS

- **66%** of organizations reported loss of revenue
- **53%** reported brand and reputation damage
- **32%** of organizations reported losing C-Level talent
- **29%** reported employees layoffs following a ransomware attack



```
  if (typeof emitter.prependListener === 'function') {
    return emitter.prependListener(event, fn);
  } else {
    // This is a hack to make sure that our error handler is attached before any
    // userland ones.  NEVER DO THIS. This is here only because this code needs
    // to continue to work with older versions of Node.js that do not include
    // the prependListener() method. The goal is to eventually remove this hack.
    if (!emitter._events || !emitter._events[event]) emitter.on(event, fn);else if (isArray(emitter._events
  }
}

function Readab
  Duplex = Dupl

  options = opt

  // object str
  // make all t
  this.objectMo

  if (stream in

  // the point
  // Note: 0 is
  var hwm = opt
  var defaultHw
  this.highWate

  // cast to in
  this.highWate

  // A linked l
  // linked lis
  // array.shif
  this.buffer = new BufferList();
  this.length = 0;
  this.pipes = null;
  this.pipesCount = 0;
  this.flowing = null;
  this.ended = false;
  this.endEmitted = false;
  this.reading = false;
```

Your files have been encrypted.

Your computer has been hacked and you will not be able to access your data. If you pay $5 million to us within 48 hours, you will be able to regain access to your data.

CRISIS MANAGEMENT

Ransomware attacks are more than a technical crisis

Technical Crisis - locked out of systems

Legal Crisis - exposed customer data and IP

Marketing Crisis - brand damage, consumer trust

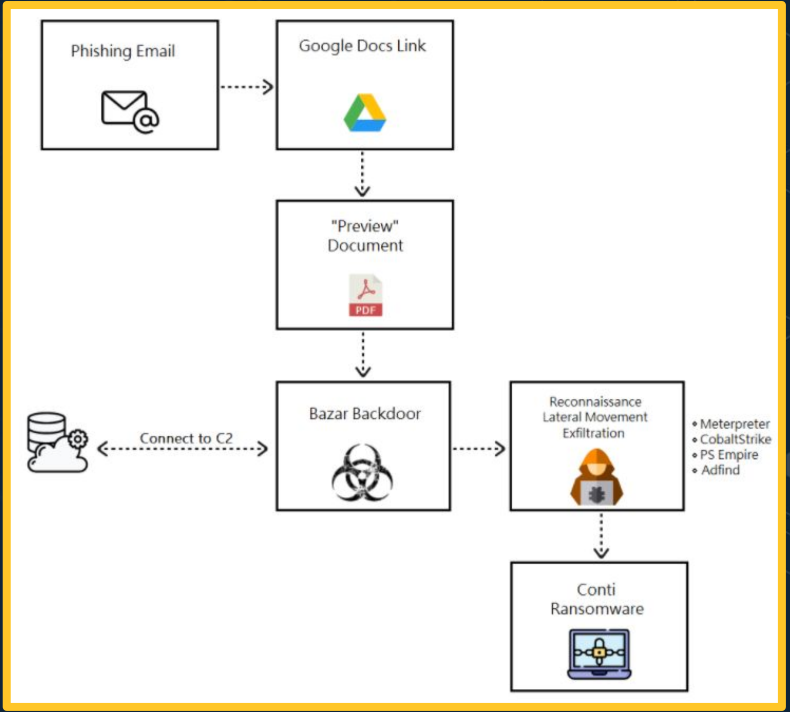
Boardroom Crisis - liability for the breach

TO PAY OR NOT TO PAY?

- **80%** who paid ransom were attacked again
- **46%** who paid regained access to data, but some or all was corrupted
- **42%** reported cyber insurance policy did not cover all losses

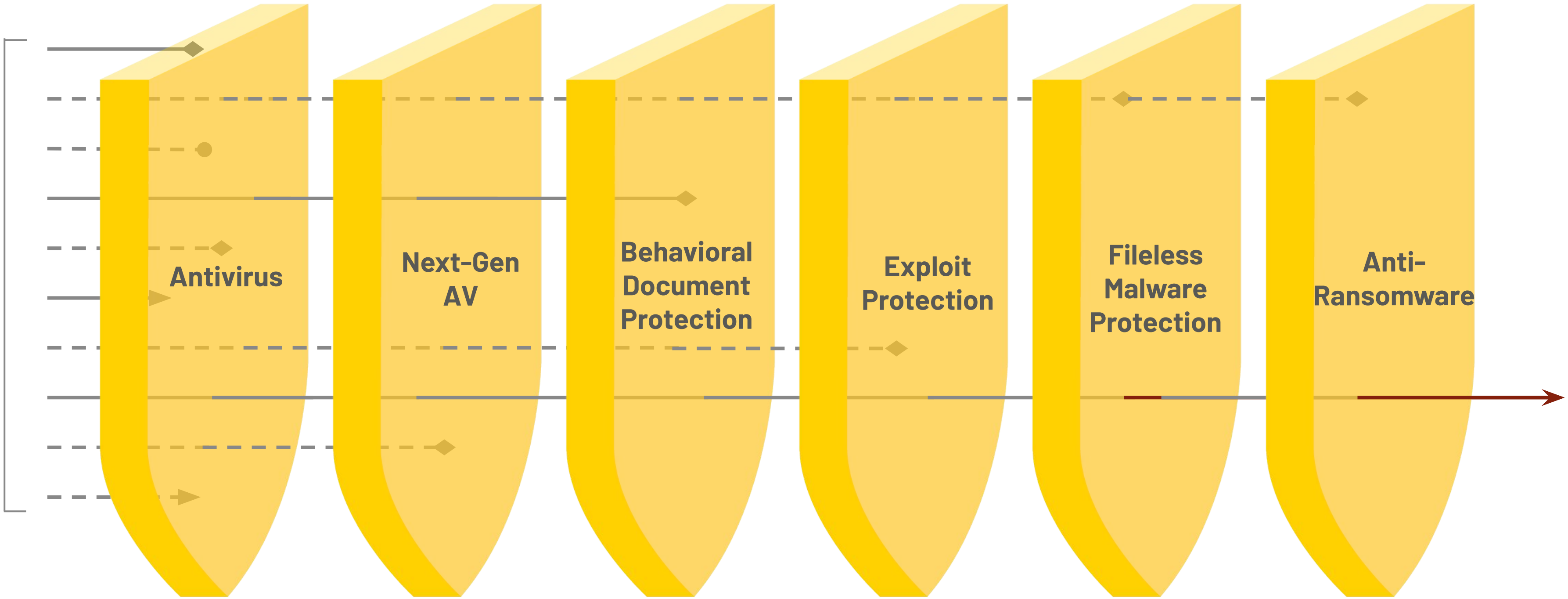
FAILURE TO PLAN IS PLANNING TO FAIL

- **73%** reported they have the right policies
- **42%** believe they have the right people
- **< 50%** reported having antivirus
- Only **30%** reported having an EDR solution
- Only **44%** invested in EPP and/or EDR after a ransomware attack



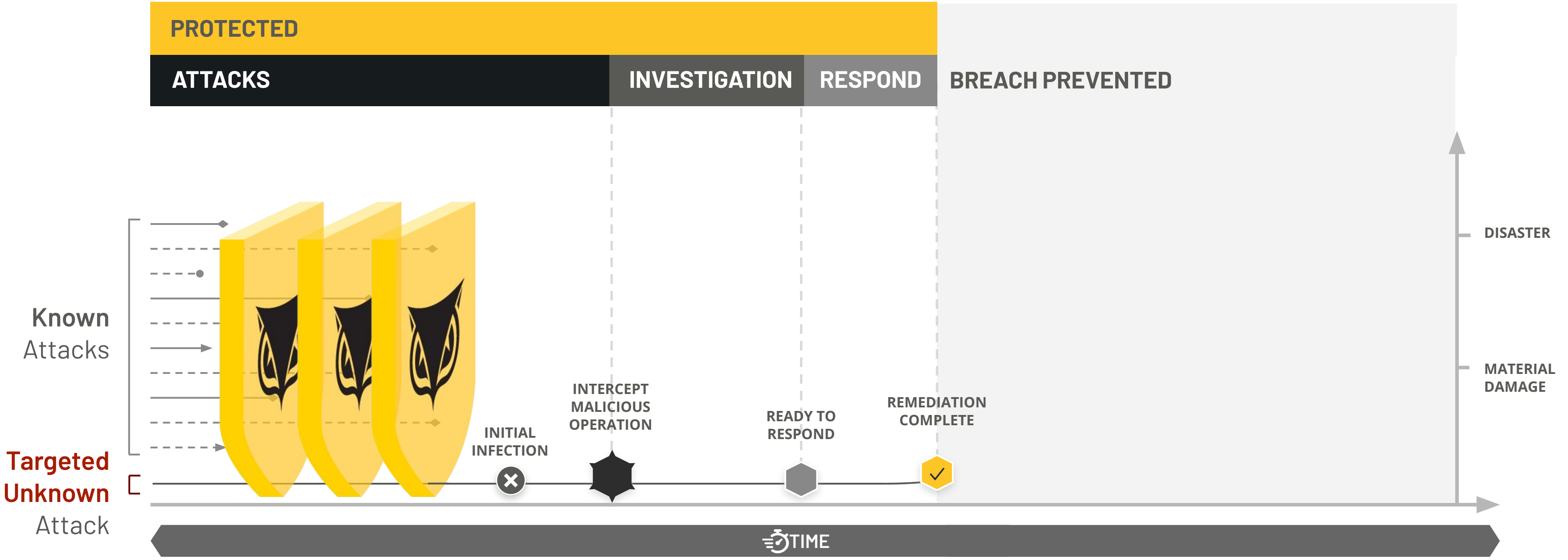
Cybereason Methodologies and Capabilities

MULTI-LAYERED PREVENTION



OPERATION-CENTRIC SECURITY

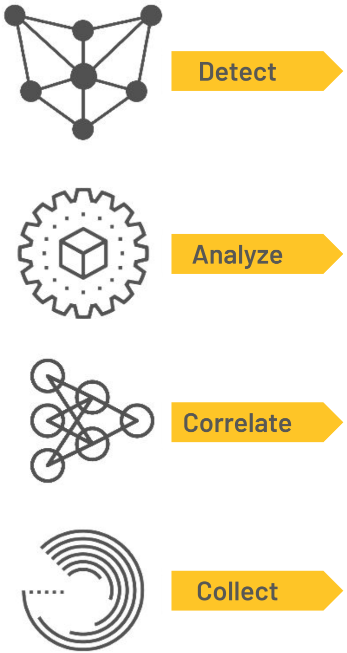
The Ideal State

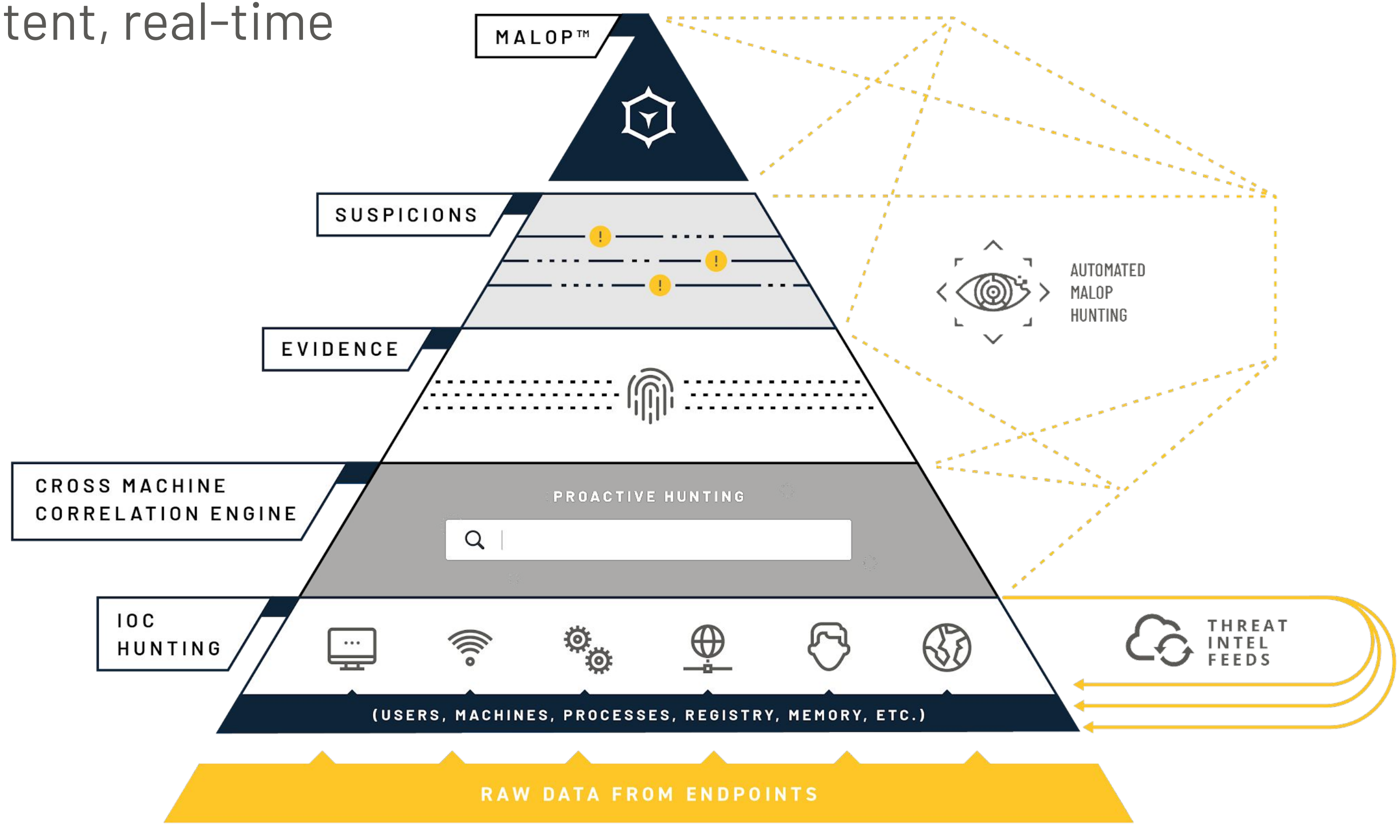


cybereason®

CYBEREASON ANALYSIS MODEL

Dynamic, persistent, real-time





Cybereason Anti-Ransomware

Undefeated in the fight against ransomware

Confidently defeat ransomware

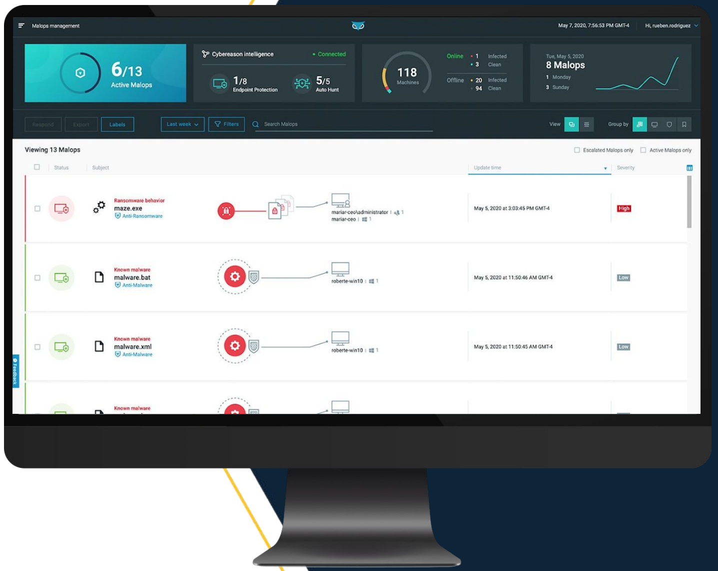
Multiple layers of defense based on behaviors and sophisticated intelligence deliver protection against modern and sophisticated ransomware.

Complement your existing security stack

Operate with and alongside the existing products in your security stack with a single, lightweight endpoint sensor.

Achieve immediate time to value

Simple, rapid deployment delivers instant protection and a less that 1% false positive rate that won't add additional work or administrative overhead.



Status	Subject		Update time	Severity
	Ransomware behavior maze.exe Anti-Ransomware	mariar-ceo\administrator 1 mariar-ceo 1	May 5, 2020 at 3:03:45 PM GMT-4	High
	Known malware malware.bat Anti-Malware	roberte-win10 1	May 5, 2020 at 11:50:46 AM GMT-4	Low
	Known malware malware.xml Anti-Malware	roberte-win10 1	May 5, 2020 at 11:50:45 AM GMT-4	Low
	Known malware			

cybereason®

Q&A

THANK YOU