# Preparing for Disruptive Intrusions

## Mitigating the Risk of Data Theft, Ransomware, Public Shaming, and Extortion


Charles Carmakal

SVP and CTO

Dr. Lawrence Taub

Senior Manager

# SVP & CTO

- Based in Washington DC, USA
- Leads a team of incident responders that have responded to over a thousand incidents
- 20+ years of experience with incident response and red teaming
- Previously led the security consulting business at a Big 4 consulting firm
- University of Florida alumnus
- charles.carmakal@mandiant.com

Charles Carmakal

Lawrence Taub

## Senior Manager

- 15+ years of security and industry-relevant experience
- Based in Atlanta, Georgia, USA
- Performed Incident Response activities related to ransomware for organizations across all industries and sizes
- Leads the Southeast US IR team that helps investigate, contain, and eradicate attacker access
- University of Florida, Nova Southeastern alumnus
- Adjunct Faculty at Florida Institute of Technology
- lawrence.taub@mandiant.com

# Agenda

- Ransomware Overview
- Ransomware Deployment Tactics
- Payment Considerations
- Risk Reduction Technical Recommendations
- Q&A

# Ransomware Overview

# Ransomware vs. Extortion

## ransomware

[ ran-*suh* m-wair ]

*noun*

1 malware that requires the victim to pay a ransom to access encrypted files

*Examples: Ryuk, Conti, BitPaymer, DoppelPaymer, Maze, etc.*

## extortion

[ ik-stawr-sh*uh*n ]

*noun*

1 the practice of obtaining something, especially money, through force or threats.

*Example: The theft of data and demand for money in exchange for not publicly releasing the stolen data*

# Evolution of Ransomware

Mandiant-branded Locker

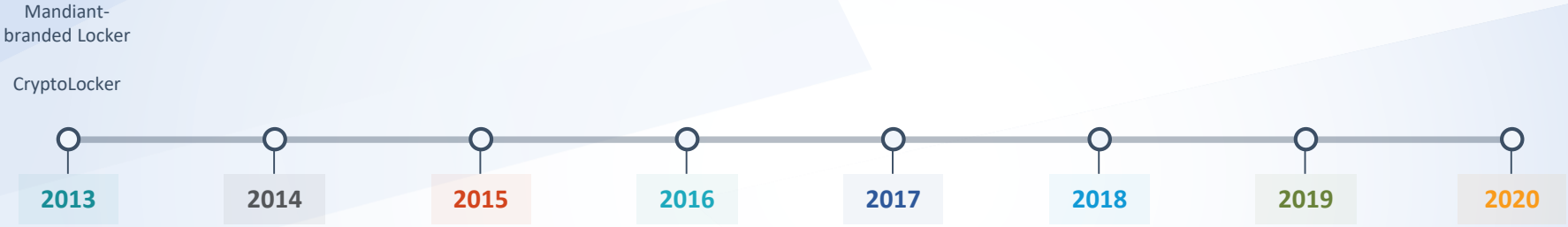
2013 2014 2015 2016 2017 2018 2019 2020

# Mandiant-Branded Locker

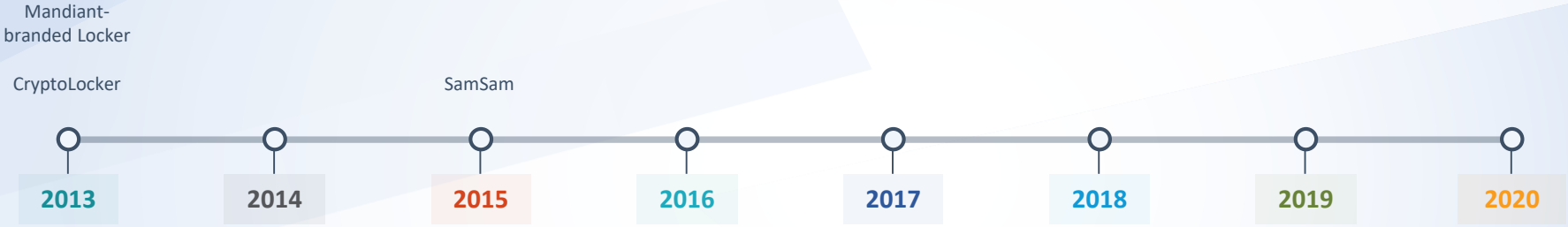

ATTENTION! Your browser has been blocked up for safety reasons. All the actions performed on this PC are fixed. All your files are encrypted. AUDIO AND VIDEO RECORDING IN PROGRESS.

The penalty set must be paid in course of 48 hours as of the breach. On expiration of the term, 48 hours that follow will be used for automatic collection of data on yourself and your misconduct, and criminal case will be opened against you.

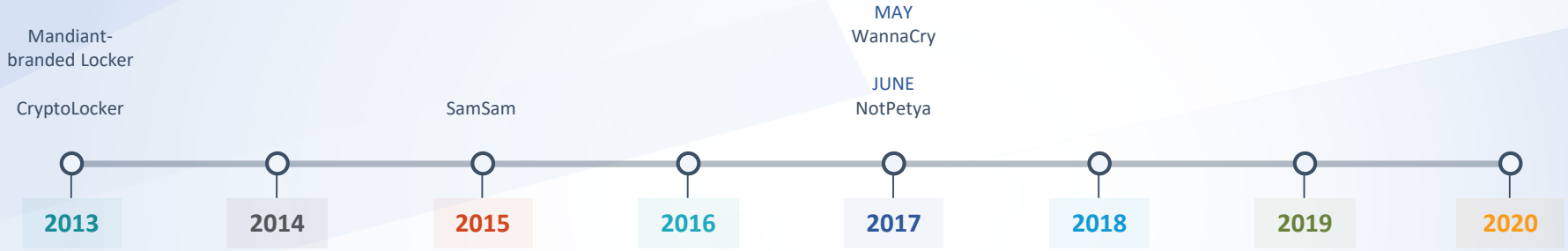
# Evolution of Ransomware



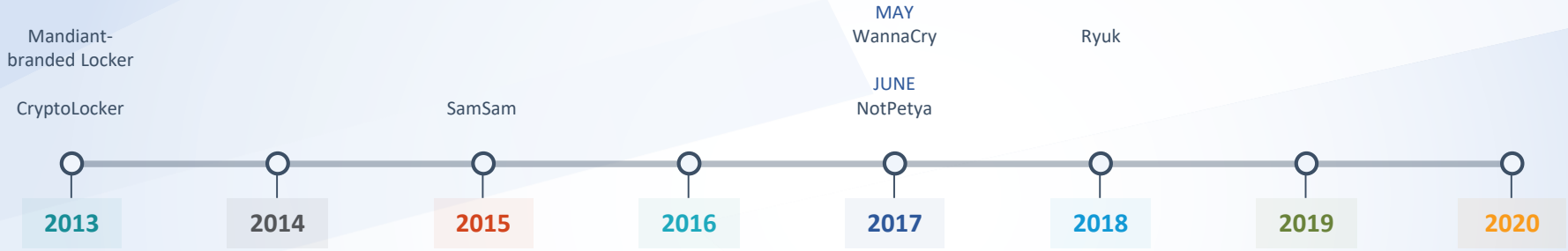
# Evolution of Ransomware



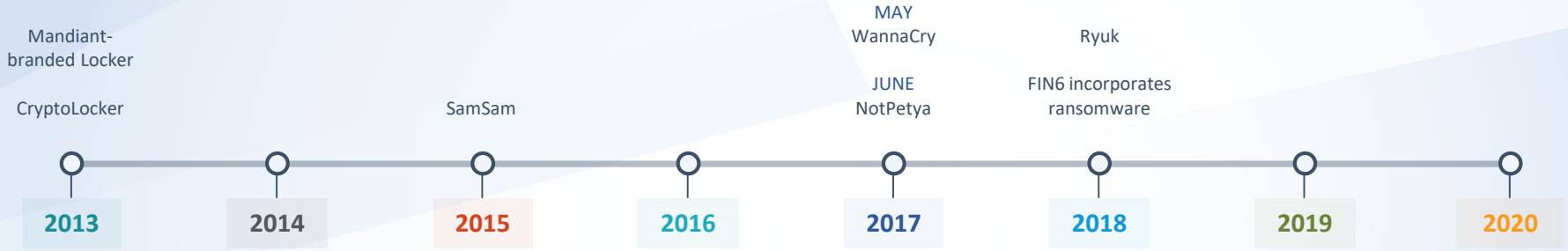
# Evolution of Ransomware



# Evolution of Ransomware



# Evolution of Ransomware



# Evolution of Ransomware

# Evolution of Ransomware

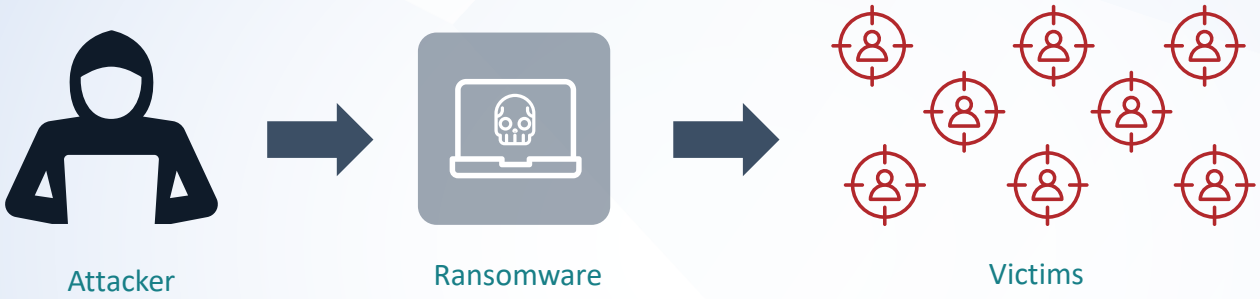
# Evolution of Ransomware

# Evolution of Ransomware

# Ransomware Deployment Tactics

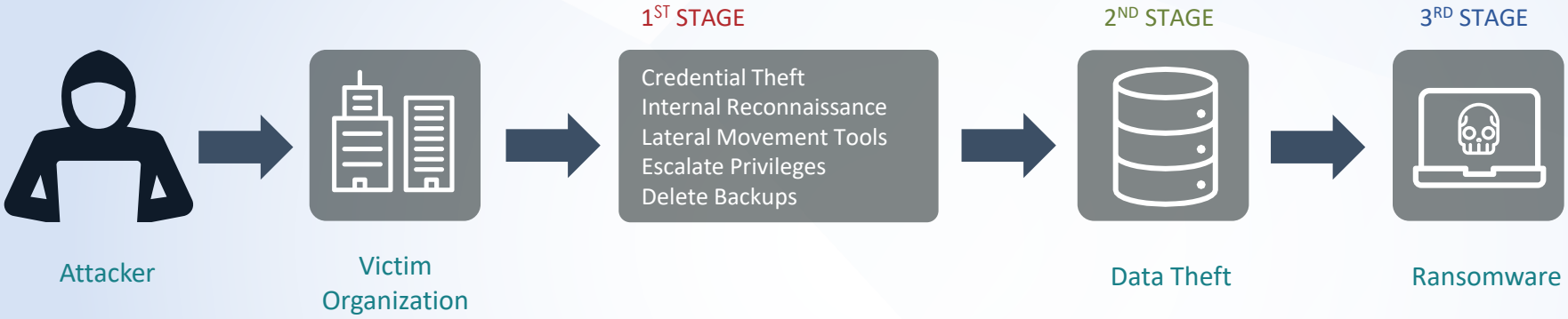
# Shotgun Indiscriminate Approach

SHOTGUN INDISCRIMINATE APPROACH



# Post-Compromise Approach

POST COMPROMISE APPROACH



# Ransomware Deployment Tactics

**Manual deployment** by an attacker **after** they have penetrated an environment and have administrator-level privileges broadly across the environment.

- Tactics:
  - Manually run encryptors on targeted systems.
  - Deploy encryptors across the environment using Windows batch files.
  - Deploy encryptors with Microsoft Group Policy Objects (GPOs).
  - Deploy encryptors with existing software deployment tools utilized by the victim organization.

# Ransomware as a Business

- Some ransomware groups such as MAZE have an affiliate model
- Developers of the MAZE ransomware partner with affiliates who actually deploy it
- Developers receive a commission for every victim ransom paid
- Affiliates may have subcontractors for certain exploitation tasks
  - Some might even be salaried!
- Affiliates can share the customer service infrastructure and public shaming sites

https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html

# Payment Considerations

# Extortion Payment Considerations

1. How **quickly** can you recover your systems and data on your own?
2. Will **paying** the threat actor enable you to recover more quickly?
3. How **reliable** is the threat actor?
4. Did the threat actor **steal data before** they deployed their encryptors? How **sensitive is the data** that they stole?
5. Does the threat actor still have **active access** to your network?
6. Will **cybersecurity insurance** cover the claim?
7. Is the **threat actor sanctioned** by the U.S. Department of Treasury?

Ransomware Advisory, October 1, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001

# Learnings from Paying Threat Actors

1. Threat actors usually have **multiple backdoors** and can technically re-encrypt data if they wanted to
2. You don't know who you're paying - some threat actors operate in countries which with we have an **embargo**
3. Many threat actors are **reliable** – their business model depends on it
4. Many threat actors **move on to the next target** when paid – they have plenty of victims to choose from
5. No guarantees that stolen data will **be deleted** (despite providing "proof" of deletion)
6. Prior to 2019, we observed many threat actors **publicized stolen data** and **re-extorting victims** after being paid

# Risk Reduction & Technical Recommendations

# Ransomware Exploitation Model

Access
+ Credentials
+ Connectivity

---

= $ **PROFIT**

# Proactive Measures – Access Hardening

**Regularly scan** externally facing systems for common ports and protocols open

**Enhance** Vulnerability Management for systems that are external

**Train** end-users on spotting Phishing emails and **regularly** perform phishing campaign exercises

**Harden** external access capabilities with Multifactor Authentication (MFA)

# Proactive Measures – Credential Hardening

**Minimize privileged credential exposure!** Harden systems so that privileged and/or service accounts cannot be used for logons to standard endpoints

**Remove** the capability for local administrative accounts to be used for remote logons to other endpoints

**Randomize** the password for built-in local administrative accounts on endpoints

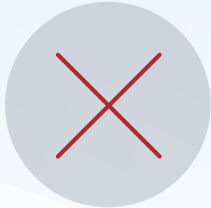
**Harden** endpoints so that clear-text passwords are not stored in memory

# Proactive Measures – Connectivity Hardening

**Restrict** system-to-system communications

**Restrict** egress access, ports, and protocols

**Remove** the capability for privileged accounts to be used for remote logon purposes



**Disable** unnecessary services on endpoints

**Leverage** dedicated privileged access workstations (PAWs) for performing administrative tasks

# Business Continuity Measures

- Ensure up-to-date "hot" and "cold" backups of Servers and Critical systems
- Ensure there is a good offline backup of the SYSVOL directory from a DC (c:\windows\sysvol).
- Ensure that there is a good / clean backup of all existing GPOs

```
backup-gpo -domain "domain.local" -all -path "c:\temp\gpo-backups"
```

- Set the password for the DSRM account (each DC) to a known value

# Questions?

**Charles Carmakal**
SVP & CTO
FireEye Mandiant
charles.carmakal@mandiant.com
+1 864 735 7242
https://www.linkedin.com/in/charlescarmakal

**Lawrence Taub**
Senior Manager
FireEye Mandiant
lawrence.taub@mandiant.com
+1 678 485 7016
https://www.linkedin.com/in/ltaub/