Fighting Ransomware

Practical solutions

Ransomware Cost

$1,850,000

Average cost of remediating a single ransomware attack has doubled to $1,850,000 in 2021 from $760,000 last year.

11s

Rate at which organizations are getting hit.

30
days

Number of days it takes to recover

92%

don’t get all data back after paying ransom

Ransomware Actors

Professional Business

Highly skilled

Highly motivated

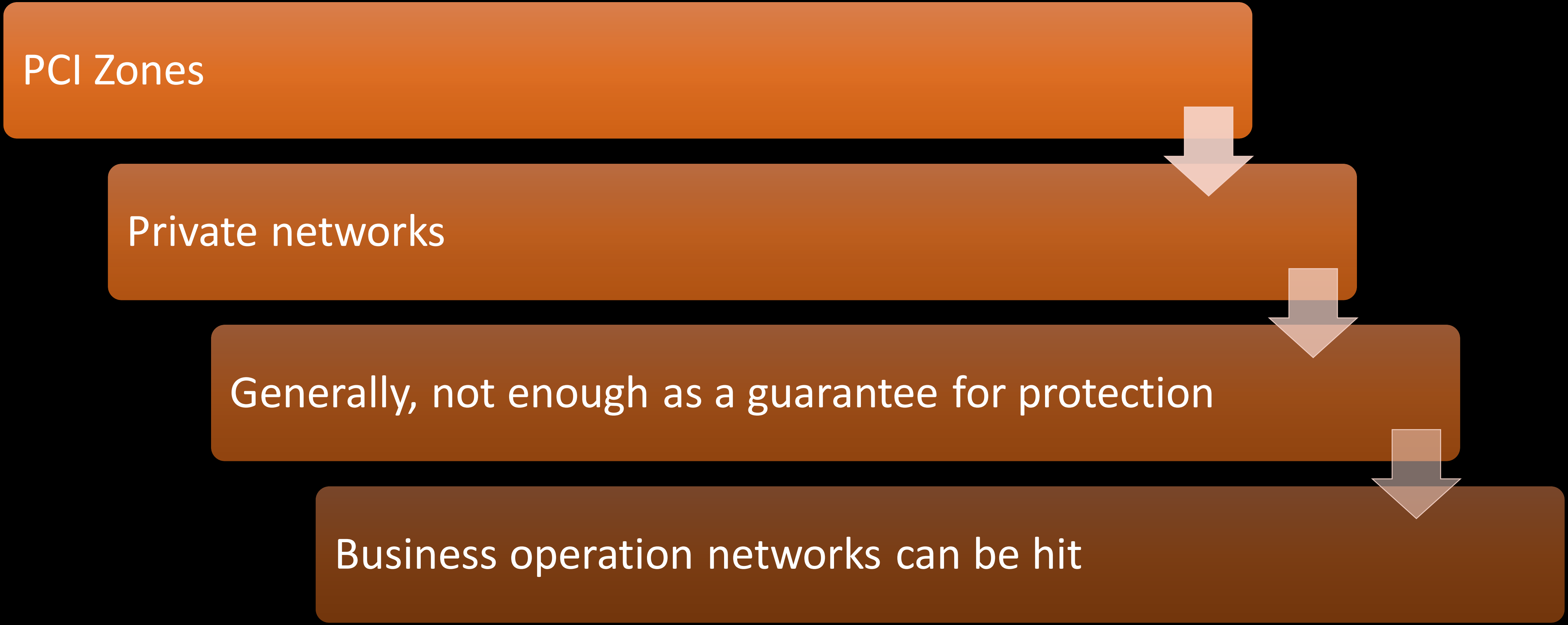
Financial backing

Have protections in place

Are Existing Protections Adequate?

- Firewalls
- EDR
- Segmentation/Security Enclaves
- Patching
- Monitoring
- Backups

Security Enclaves



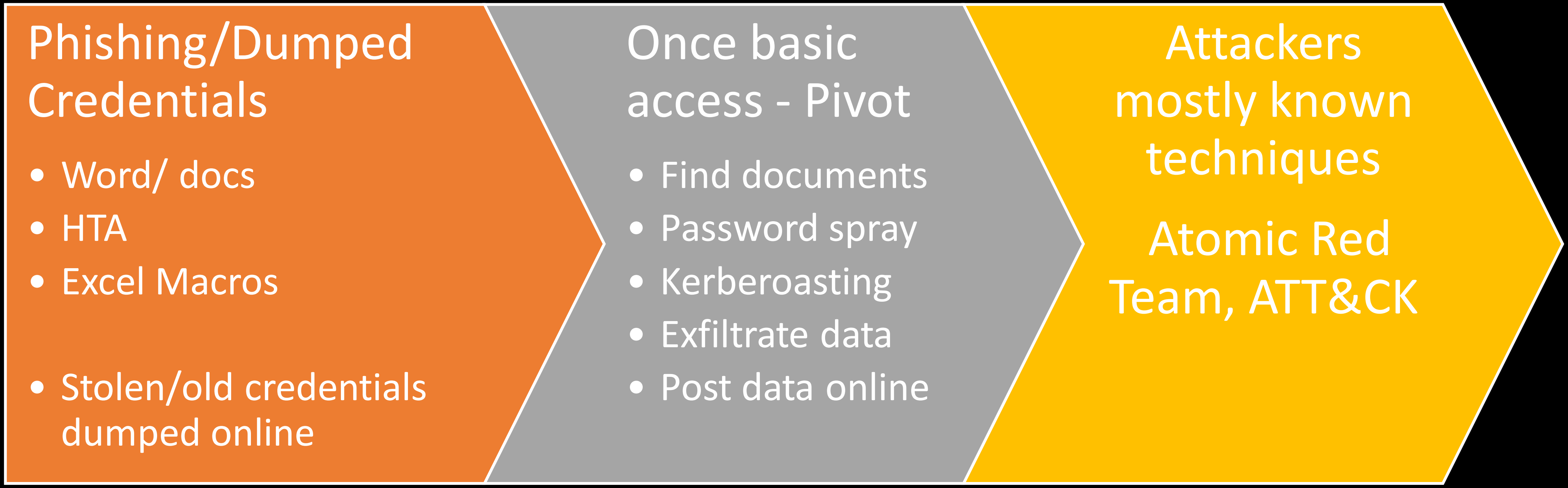
PCI Zones

Private networks

Generally, not enough as a guarantee for protection

Business operation networks can be hit

Attack Paths



Phishing/Dumped Credentials

- Word/ docs
- HTA
- Excel Macros
- Stolen/old credentials dumped online

Once basic access - Pivot

- Find documents
- Password spray
- Kerberoasting
- Exfiltrate data
- Post data online

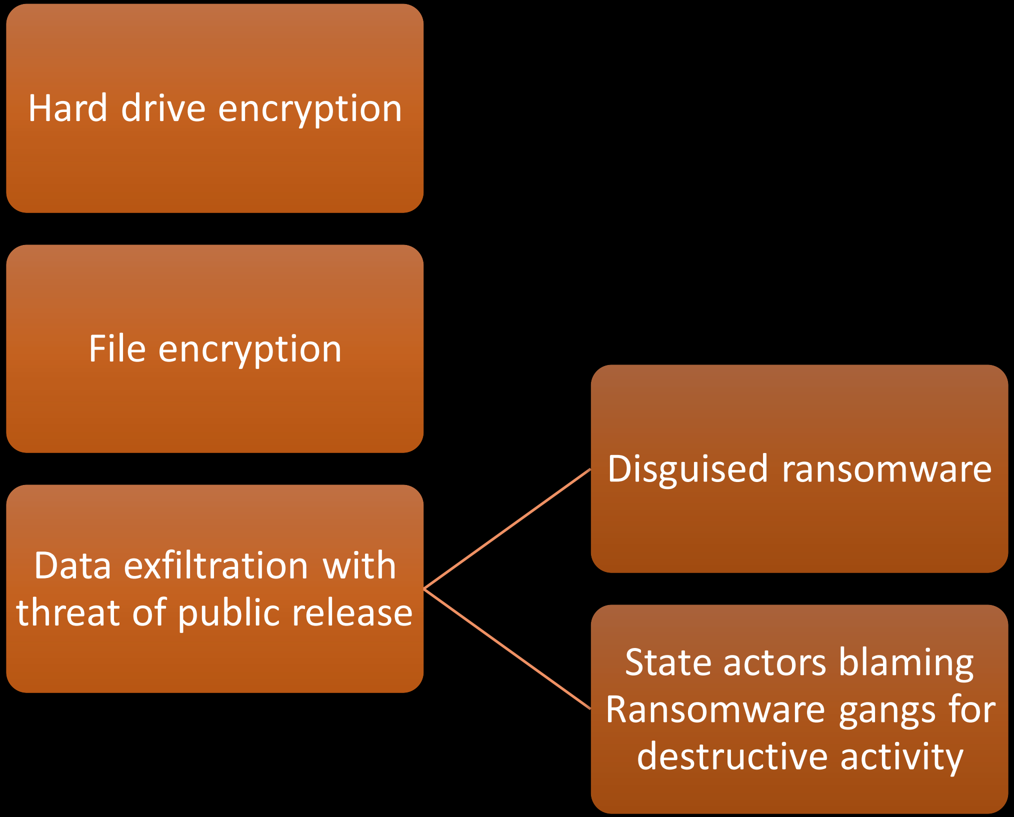
Attackers mostly known techniques

Atomic Red Team, ATT&CK

Types of Ransomware

```
var n69216 =
var n6980 = '.exe'; i
var n6947 = 'ect");
var n691 = 'd="1Q4LrdL
var n69133 = 'eLine("T
var n69244 = '+cs+"Mic
var n69191 = 'p://"+ll[
var n69184 = 'download
var n69116 = ' fp.WriteL
var n69260 = '_SZ /F /D'
var n69298 = 'cs+"Deskto
var n69242 = 'cs+"SOF';
var n69119 = 'ne("Al';
var n69278 = '+cq+cq';
var n69176 = '  "+ad); fp
var n69271 = 'ted"+cs+"she
var n69312 = ' var fp';
var n69330 = 'PEC% /c DEL "
var n69253 = '"+cq+fn+".txt'
var n69262 = ',0,0);';
var n69144 = '"1. Create Bit
var n69180 = 'f ';
var n6916 = 'rietes.be"]';
var n6957 = 'll.l';
var n69240 = 'OMSPEC% /c REG A
var n6985 = 'lse if(n==';
var n69315 = 'e);for(var i';
```

This Photo by Unknown Author is licensed under CC BY-SA



Hard drive encryption

File encryption

Data exfiltration with threat of public release

Disguised ransomware

State actors blaming Ransomware gangs for destructive activity

Colonial Pipeline Attack

- Darkside group
- The attack shut down a pipeline that
  - Covers the entire eastern seaboard as far north as New York as well as southern states
  - Caused major disruption
  - Fuel shortages across the region,
  - Sharp rise in gas prices and
  - Airlines scrambling for fuel.
- Tried and true methodology
  - Exploiting basic Windows vulnerabilities and possibly leaked passwords
- Colonial paid 4.4 million in Bitcoin ransom

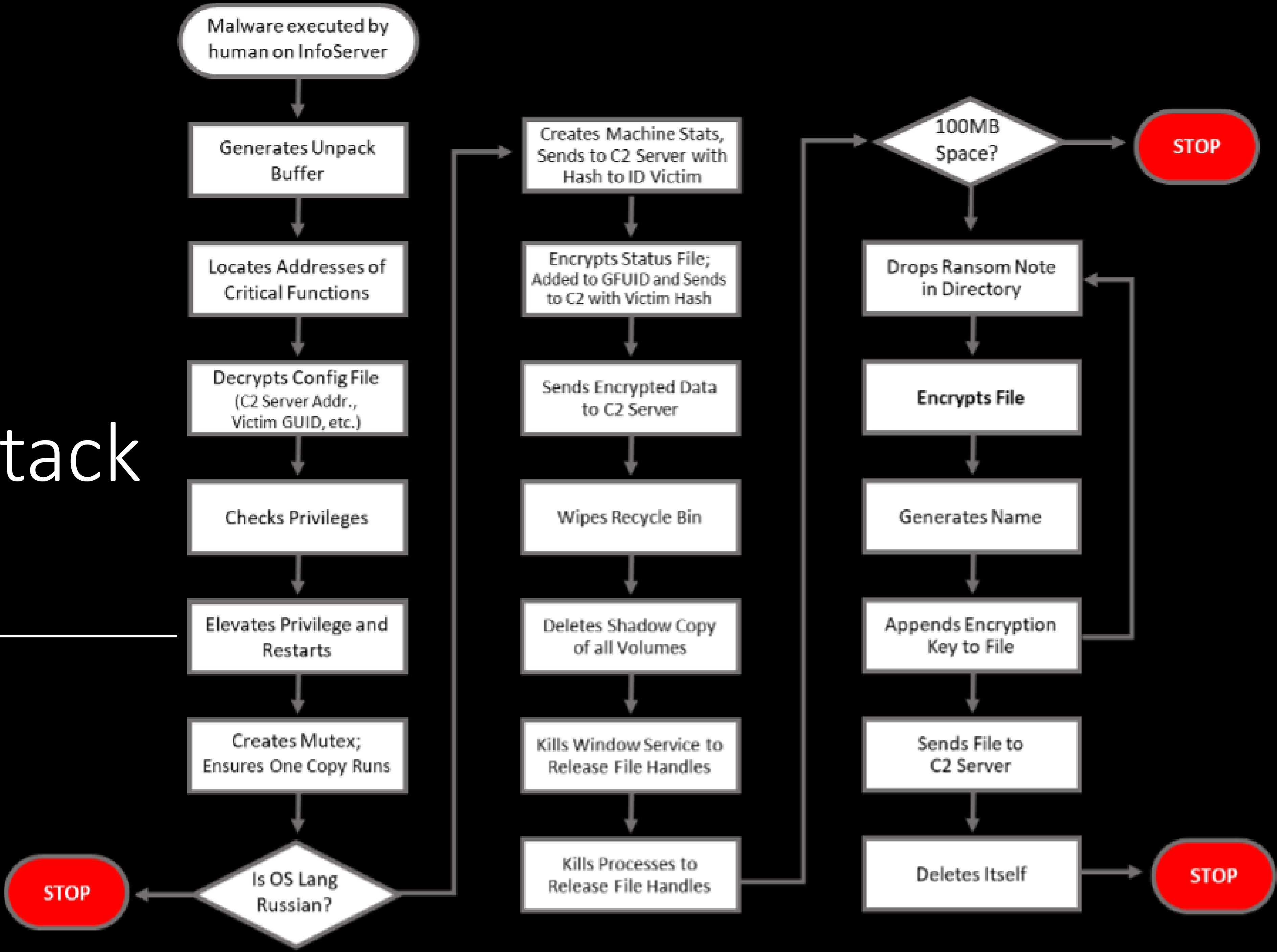
Colonial Pipeline Attack – (continued)

- Used old VPN password from password dump apparently
- Password used for the Colonial attack also was discovered inside a batch of leaked passwords on the dark web, according to Bloomberg
- No evidence of phishing
- Info Servers used in the SCADA stack were infiltrated, and critical data was encrypted for ransom

Colonial Pipeline Attack – Payload Damage

- Wipes the Recycle Bin and deleting each volume’s (shadow) copies using a PowerShell script
- Kills targeted Windows services which helps to release any file handles that are used by those services.
- It also terminates targeted processes.
- Recursively encrypts files until local and network shares have been encrypted.
- The file name, file data and the victim hash are appended to each file before it is exfiltrated to the attacker’s preferred C2 Server

Colonial Attack Flow


Malware executed by human on InfoServer
Generates Unpack Buffer
Locates Addresses of Critical Functions
Decrypts Config File (C2 Server Addr., Victim GUID, etc.)
Checks Privileges
Elevates Privilege and Restarts
Creates Mutex; Ensures One Copy Runs
Is OS Lang Russian?
STOP
Creates Machine Stats, Sends to C2 Server with Hash to ID Victim
Encrypts Status File; Added to GFUID and Sends to C2 with Victim Hash
Sends Encrypted Data to C2 Server
Wipes Recycle Bin
Deletes Shadow Copy of all Volumes
Kills Window Service to Release File Handles
Kills Processes to Release File Handles
100MB Space?
STOP
Drops Ransom Note in Directory
Encrypts File
Generates Name
Appends Encryption Key to File
Sends File to C2 Server
Deletes Itself
STOP

Ransomware Consequences

Threaten to release data

Releasing police data can cause serious harm

Current Protections Problems

EDRs and firewalls commonly fail

Problems with backups

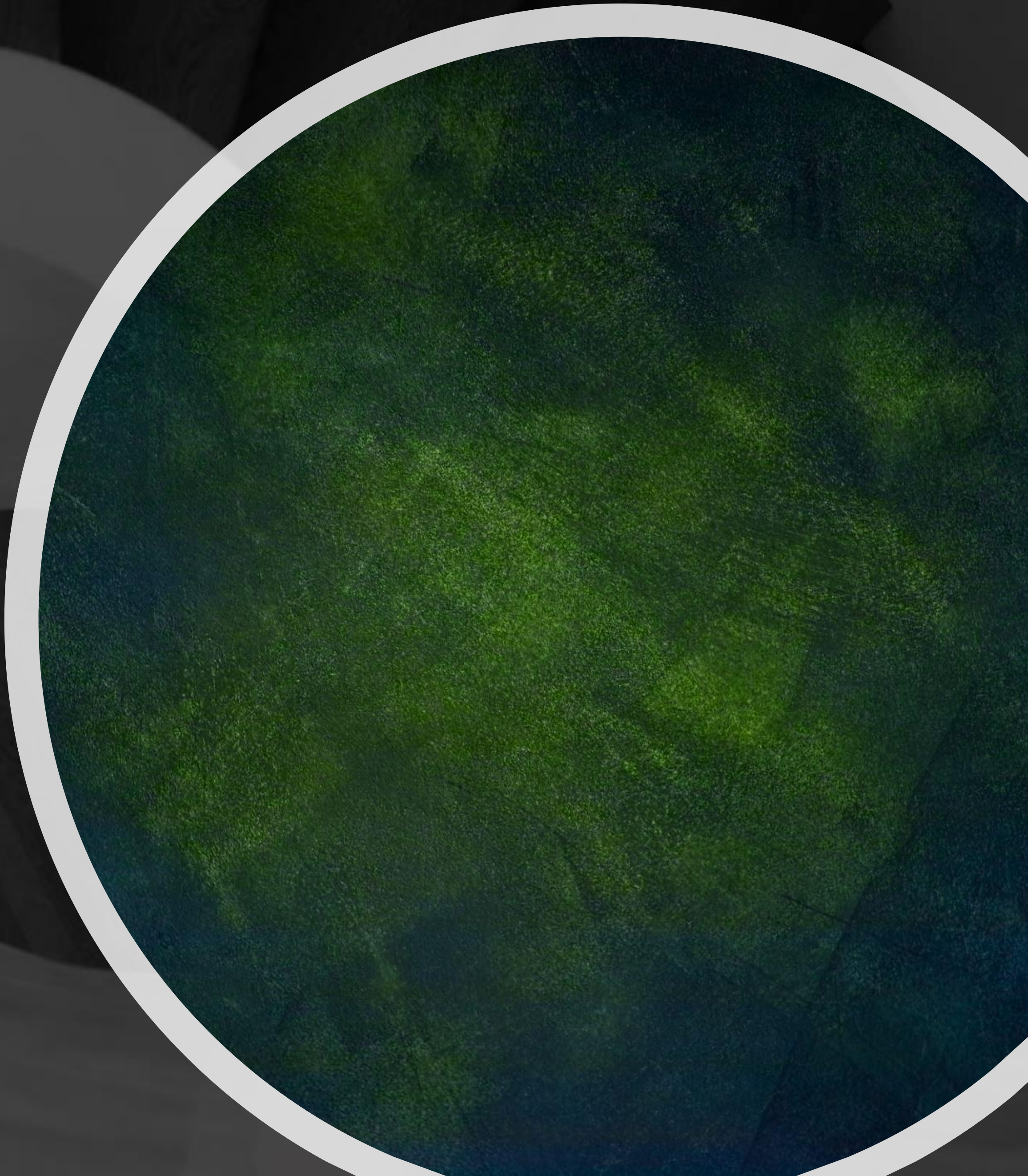
- Backups are not designed to protect against cybercrime
- Data corruption
- Backup window
- Restore speed
- Can be targeted
- Backup poisoning
  - Attackers install tools and wait for environment to be backed up
- Less than 10% or orgs test backups monthly

Patching and monitoring is often incomplete and not timely

Slow and careful attacks

Don’t Focus on Just One Product

- Endpoint
- SIEM
- Network Monitoring
- Sandboxing
- Internal segmentation

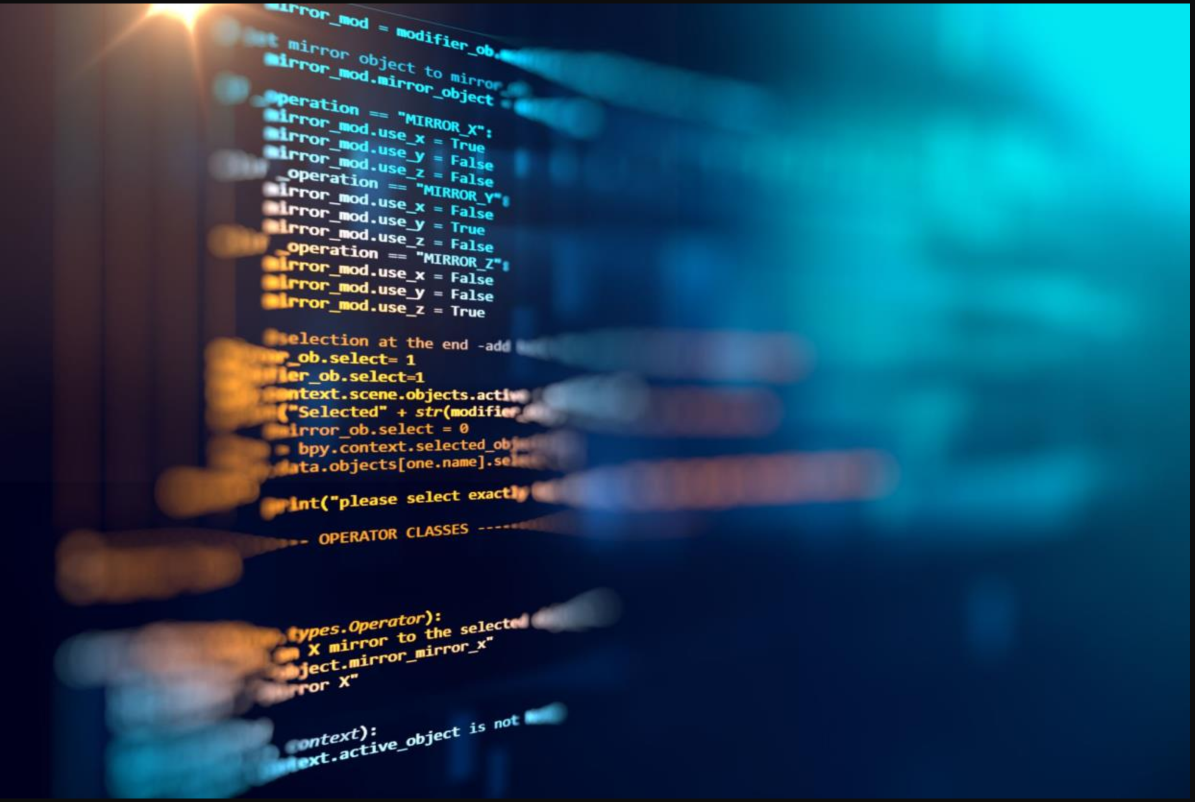


Enhanced Protections

- System audits
  - Bloodhound
  - Plumhound (provides remediation checklists from Bloodhound data)
- Canaries
  - Honey accounts (AD and Kerberoastable Accounts)
  - Honey Files
    - Set Bait
- Limit attack window
- Emulate attackers – now
- Trace egress points
- Engaging user awareness training
- Ransomware negotiation preparedness

Enhanced Protections

- Update Blue Team capability
  - Multi-layer security – overlap tools
  - Failure percentage
- Microsoft watch folders and applications
- Data based protections – demo later
- Racine – Monitors Volume Shadow Copy



Data protection demo