Enterprise Security

CMSC 23200, Spring 2025, Lecture 17

Grant Ho

University of Chicago, 05/20/2025

Logistics

Assignment 6 due Thursday, May 22 by 11:59pm

Final Exam Location: KPTC 106

- Wed, May 28 from 10am – 12pm: BOTH SECTIONS!
- Closed notes
- SDS Accommodations: email me & your SDS point of contact ASAP if you haven't gotten an email from SDS

“Cyber attack”

Spooky!


Tech Firm Ubiquiti Suffers $46M Cyberheist
Networking firm Ubiquiti
stole $46.7 million
communications from
international wire
WIRED
BACKCHANNEL BUSINESS CULTURE GEAR IDEAS POLITICS SCIENCE SECURITY MERCH
SIGN IN
KIM ZETTER SECURITY NOV 3, 2014 6:30 AM
Today's Lecture:
What actually happens in these "cyber attacks"?
What can enterprises do to protect themselves?
Millions of Anthem Customers Targeted in Cyberattack
BY ALEX ALTMAN AND ALEX FITZPATRICK DECEMBER 17, 2014 9:13 PM EST
Sony Pictures Entertainment said late Wednesday that it's pulling The Interview, a comedy about two journalists tasked with killing North
ransomware strikes
2 October 2019

What is an “Enterprise”?

Enterprise: a company / organization / institution

- The collection of machines, employees, and digital assets (e.g., datasets) that are owned by one such entity

Companies

Organizations & Institutions
(Government, Nonprofit, etc.)

What is “Enterprise Security”?

(Software / tech companies)
How do we keep our customers & software secure?
“Product Security”, “AppSec”, “Trust & Safety”

- Software Products / Public Websites
- User Interactions / Hate & Harassment
- User Accounts / Login

Enterprise Security
How do we keep our company’s digital assets secure?

- Corporate Machines / Devices
- Money & Trade Secrets
- Datasets

Outline

- What is enterprise security?
- Structure of enterprise networks & basic defenses
- Attacks on enterprises
- Common enterprise defenses

What do enterprises look like?

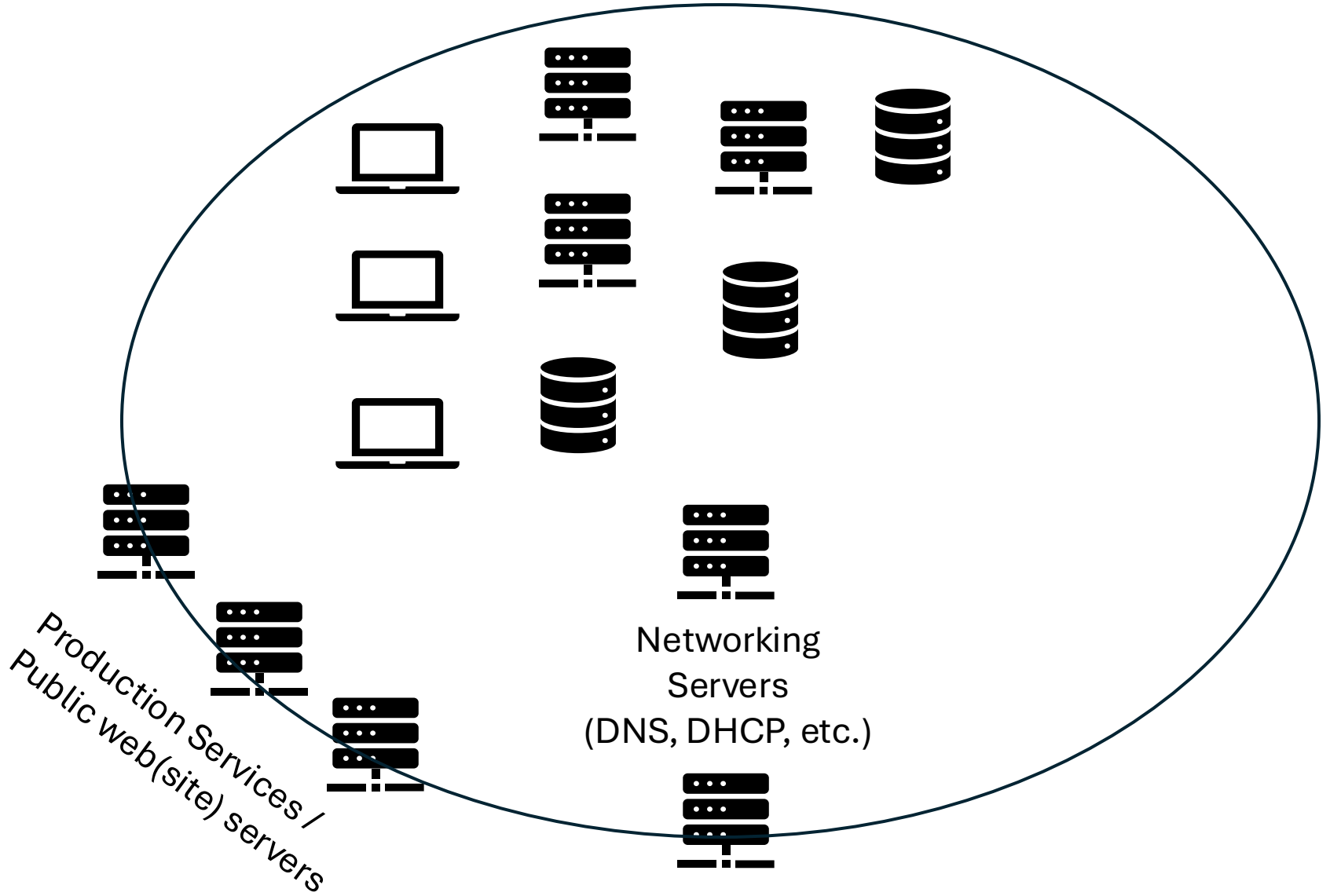
Enterprise network: the set of all devices & digital assets an enterprise owns

- Laptops, servers, cloud services, datasets, etc.
- (Outside this class: can also refer to just the networking infrastructure & configuration)

Huge variation in how enterprises networks are structured

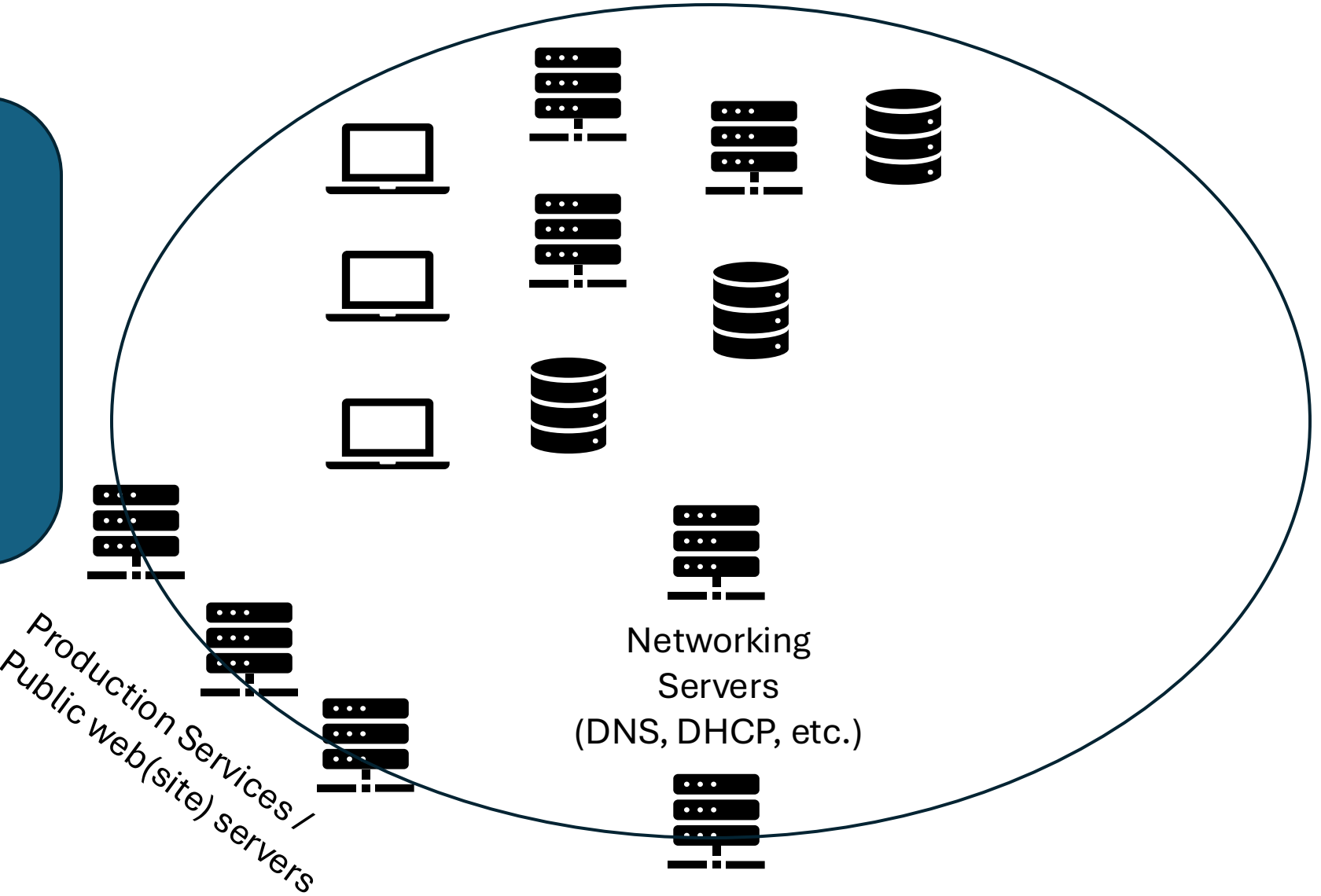
- On-premise (old-school): company physically owns all machines
- Cloud hosted: servers & services hosted in the cloud-providers (company's systems & data lives in cloud VMs or services)
- Hybrid: some systems & services hosted on-prem and some hosted in cloud

Example: (Simplified) Enterprise Network

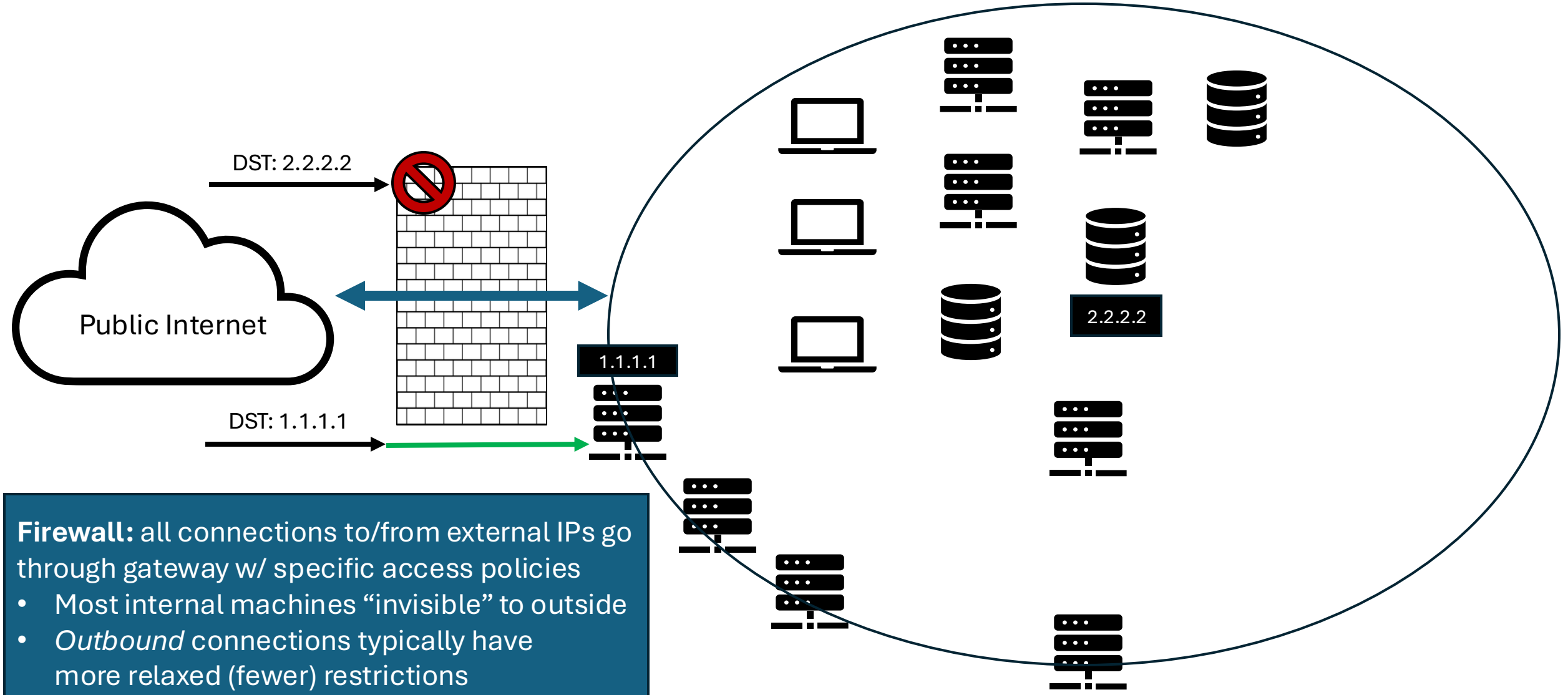


Basic Enterprise Security

Basic idea: only ***authorized*** **employees** allowed to access internal resources



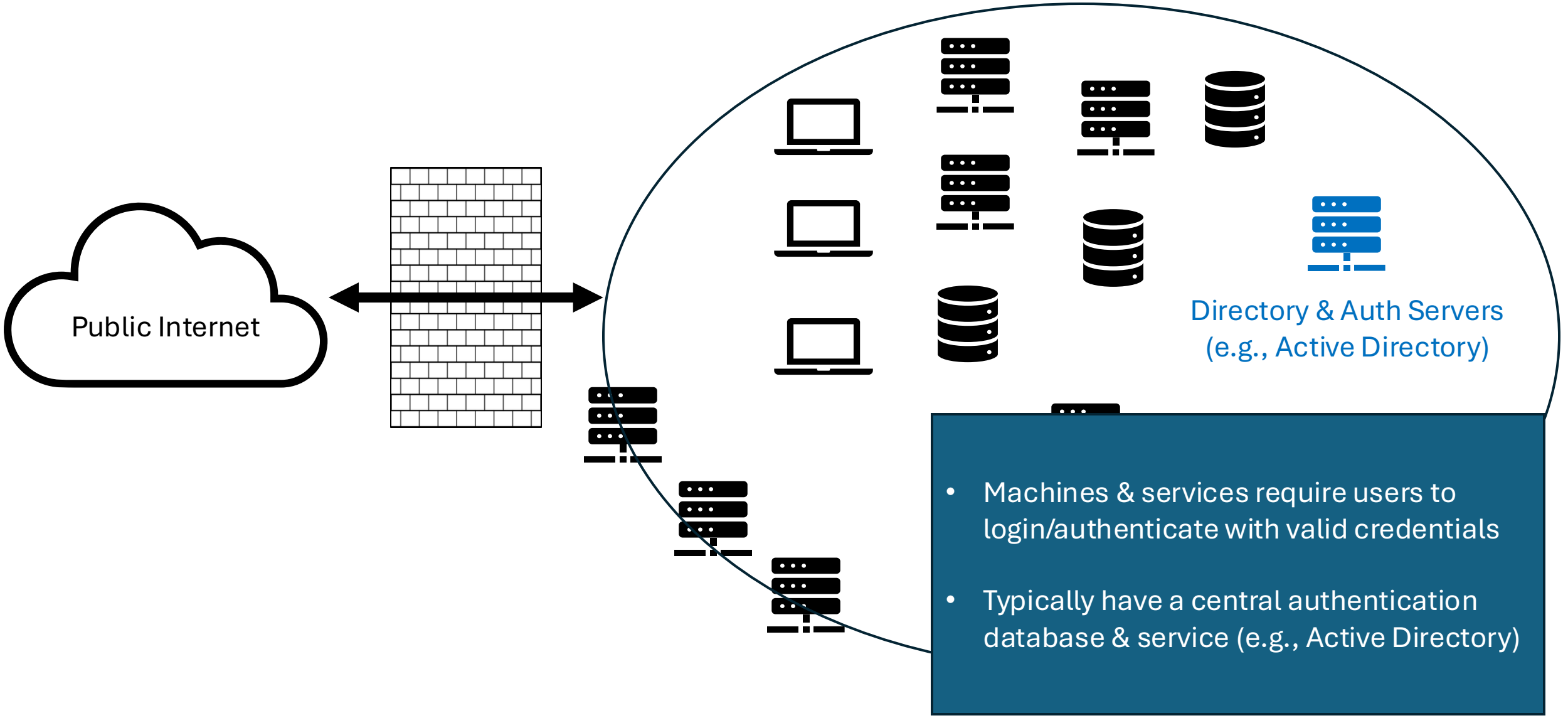
Basic Enterprise Security: Border Firewalls



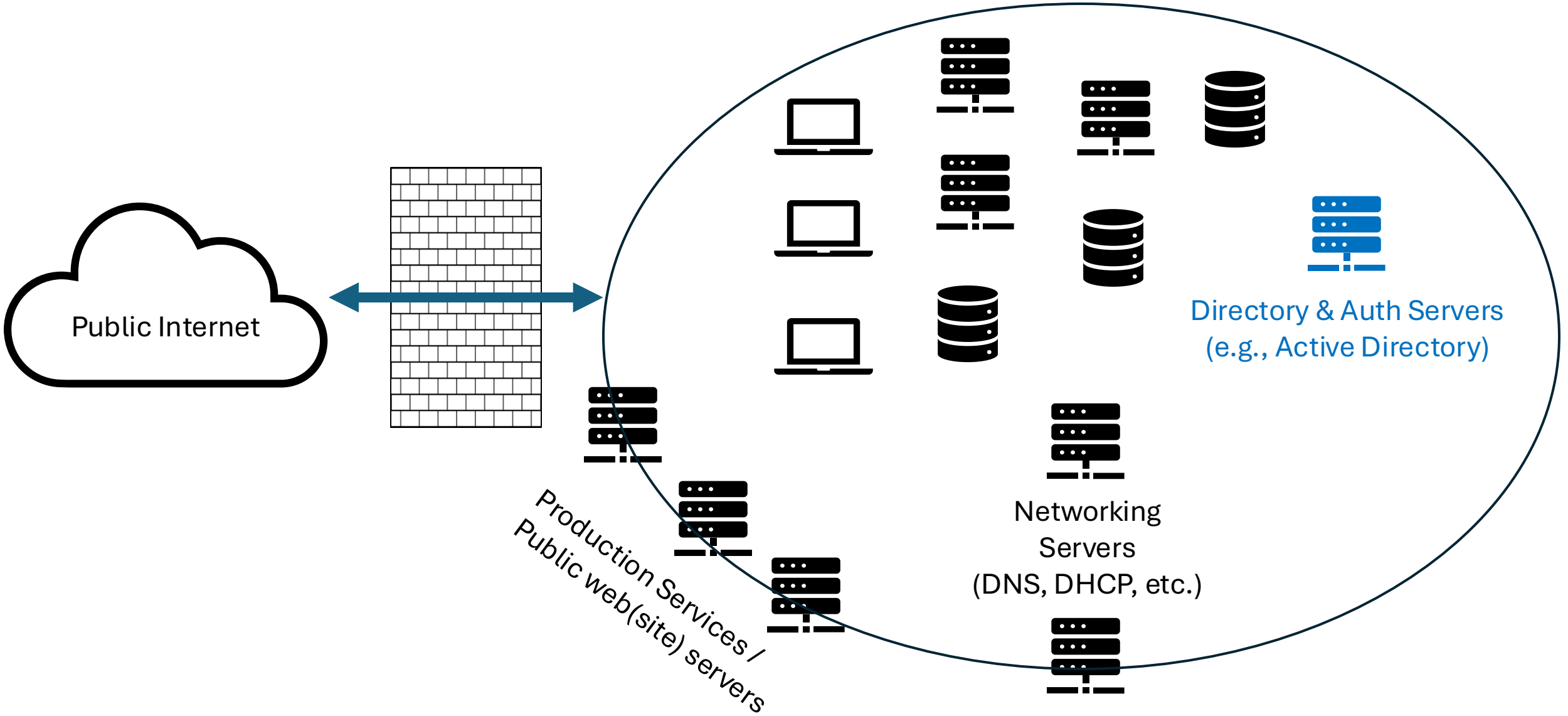
Firewall: all connections to/from external IPs go through gateway w/ specific access policies

- Most internal machines "invisible" to outside
- *Outbound* connections typically have more relaxed (fewer) restrictions

Basic Enterprise Security: User Authentication



Example: (Simplified) Enterprise Network



Outline

- What is enterprise security?
- Structure of enterprise networks & basic defenses
- Attacks on enterprises
- Common enterprise defenses

Common types of enterprise attacks

- Data breach & Theft

Common types of enterprise attacks

- Data breach & Theft
- Denial of Service: [D]DoS
- Destruction & Defacement

Pennsylvania courts resume business after weekend DDoS attack

Pennsylvania state courts officials said they've resumed work after their website was knocked offline by a distributed denial-of-service attack over the weekend.

BY SOPHIA FOX-SOWELL • FEBRUARY 5, 2024

Common types of enterprise attacks

- Data breach & Theft
- Denial of Service: [D]DoS
- Destruction & Defacement

- Ransomware: extort enterprise for money by hijacking enterprise data and/or machines (e.g., encrypt enterprise data w/ attacker key)

Common types of enterprise attacks

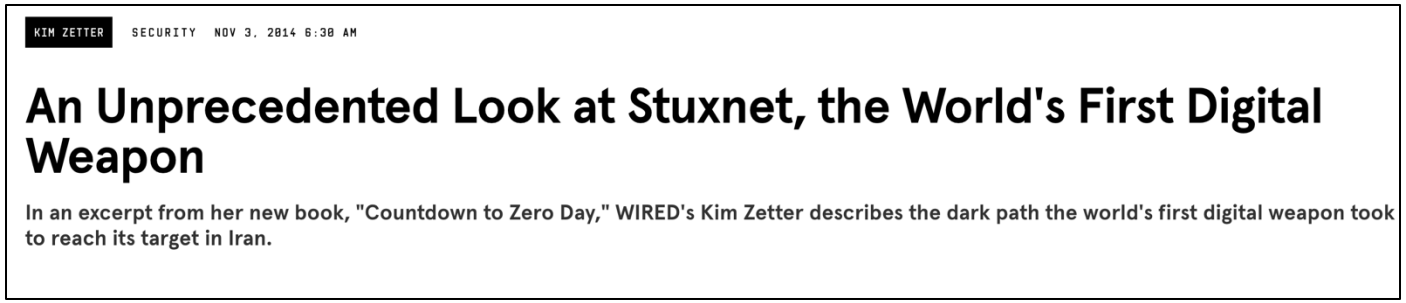
- Data breach & Theft
- Denial of Service: [D]DoS
- Destruction & Defacement
- Ransomware

Helga Labus, Managing Editor, Help Net Security
November 9, 2023

Share

Sandworm hackers incapacitated Ukrainian power grid amid missile strike

Russia-backed ATP group Sandworm is behind the cyberattack that caused disruption of parts of the Ukrainian power grid in late 2022, according to Mandiant.



KIM ZETTER SECURITY NOV 3, 2014 6:30 AM

An Unprecedented Look at Stuxnet, the World's First Digital Weapon

In an excerpt from her new book, "Countdown to Zero Day," WIRED's Kim Zetter describes the dark path the world's first digital weapon took to reach its target in Iran.

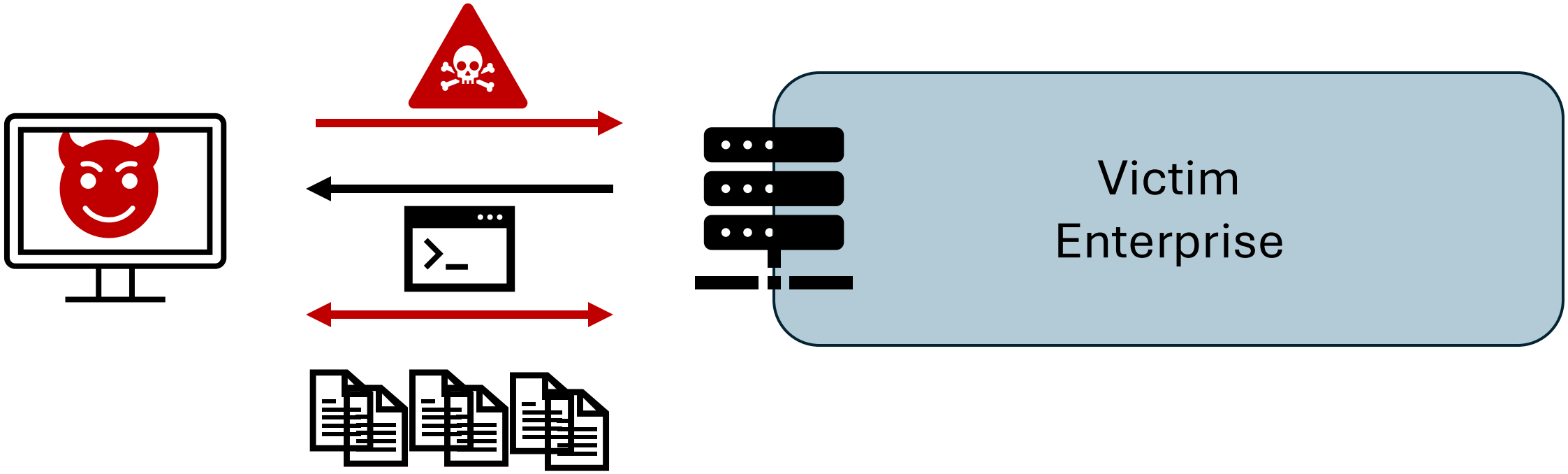
- Functionality & physical-world attacks: hijack & use enterprise machines with useful functionality (e.g., control speed of nuclear centrifuges)

What actually happens in a “cyberattack”?

Simple data breach: Command injection attack

- e.g., Buffer overflow in server software or SQL injection attack

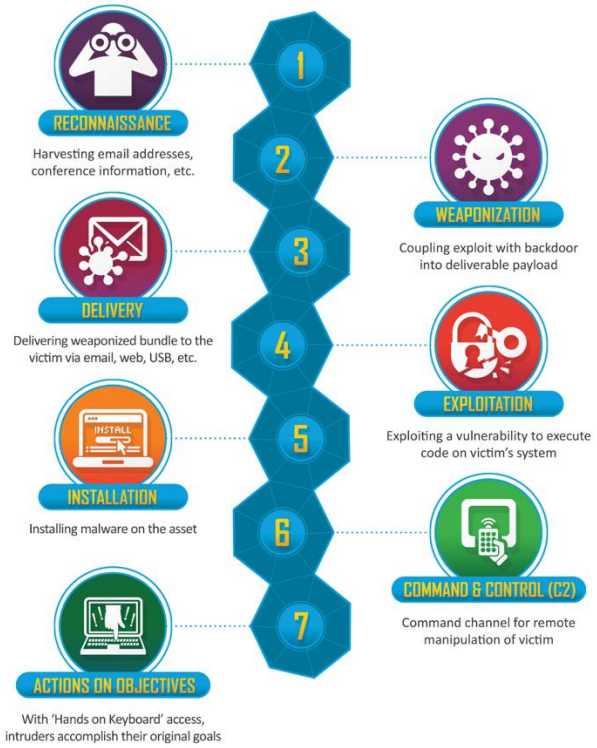
“…/bin/sh…x24\xf6\xff\xbfAAA…”



What about more complicated attacks?

More complex attacks : “the cyber killchain” or “APT lifecycle”

- Sequence of common *attack stages* seen in real attacks



Lockheed Killchain

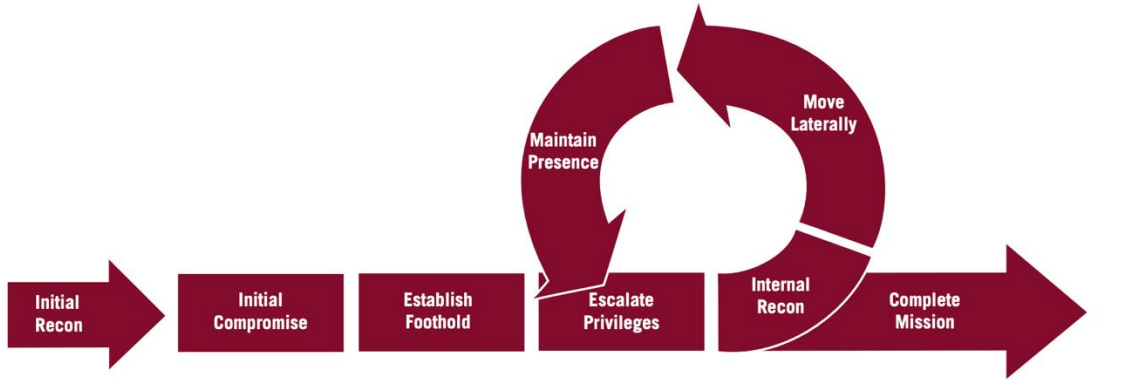
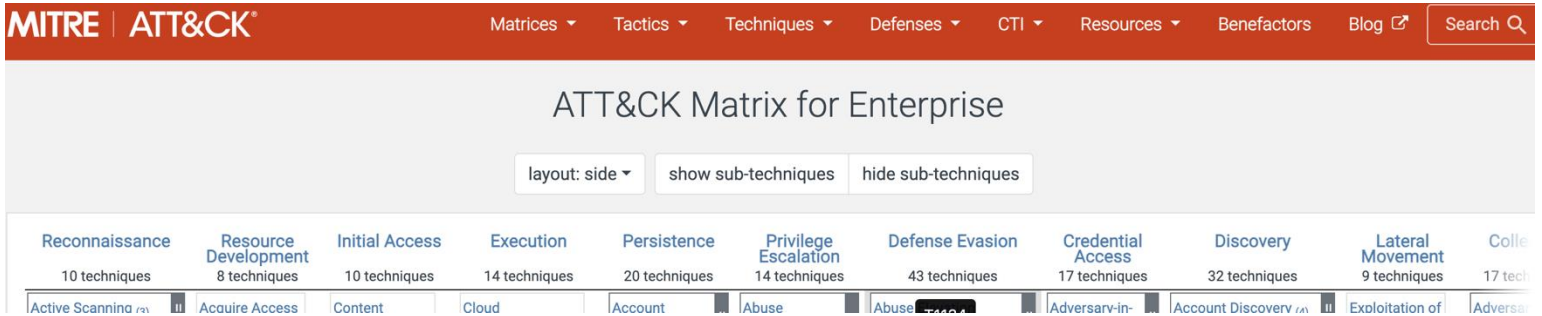


FIGURE 14: Mandiant's Attack Lifecycle Model



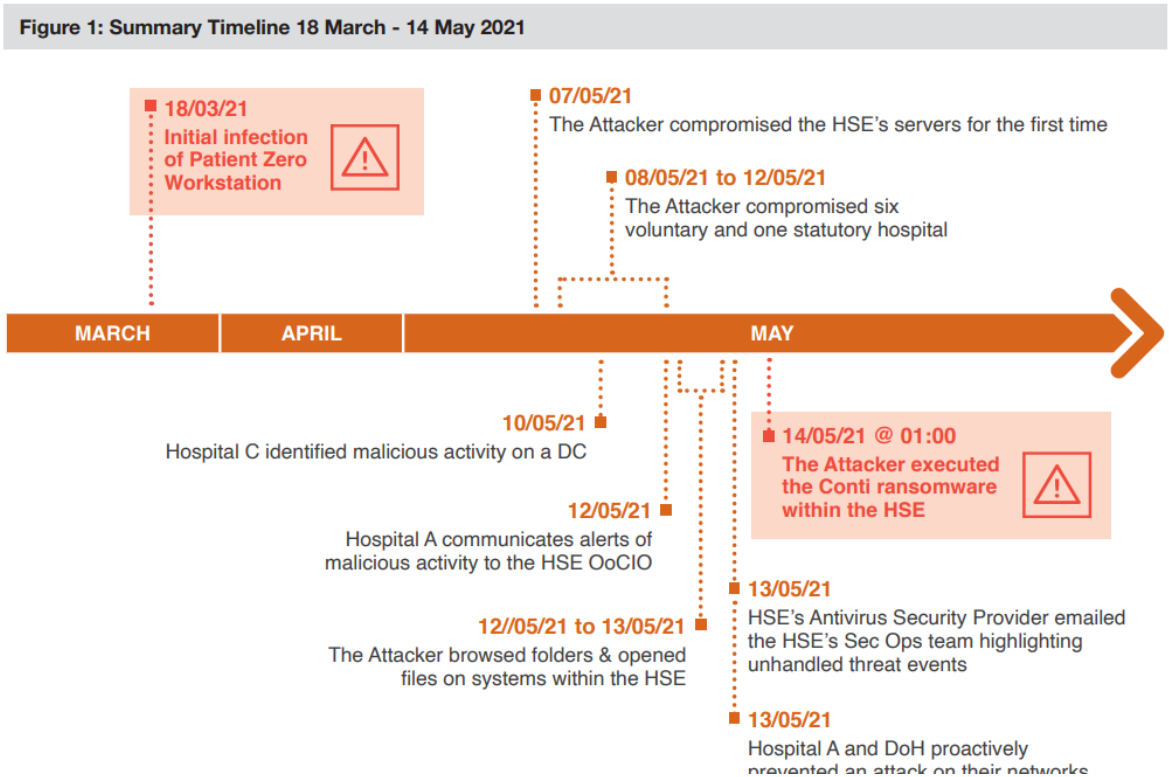
The Conti Ransomware Attack on Ireland's HSE (Healthcare System)

Ireland's HSE: Health Services Executive

- National healthcare system w/ 54 hospitals

2021: major ransomware attack + data breach (700 GB exfiltrated)

- 4 months to remediate & recover
- Damage estimates over $50 million

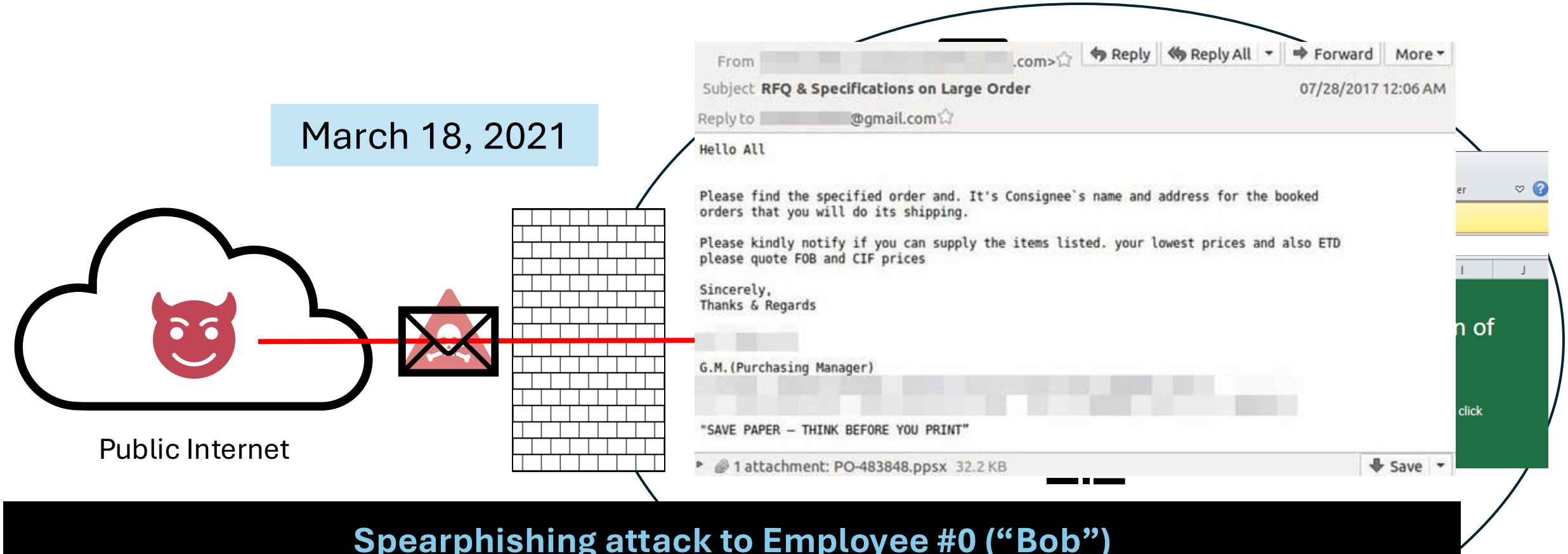


The Conti Ransomware Attack on Ireland's HSE (Healthcare System)

Several exact details are redacted, so some speculative analysis.

Conti Attack on HSE: Initial Compromise

March 18, 2021

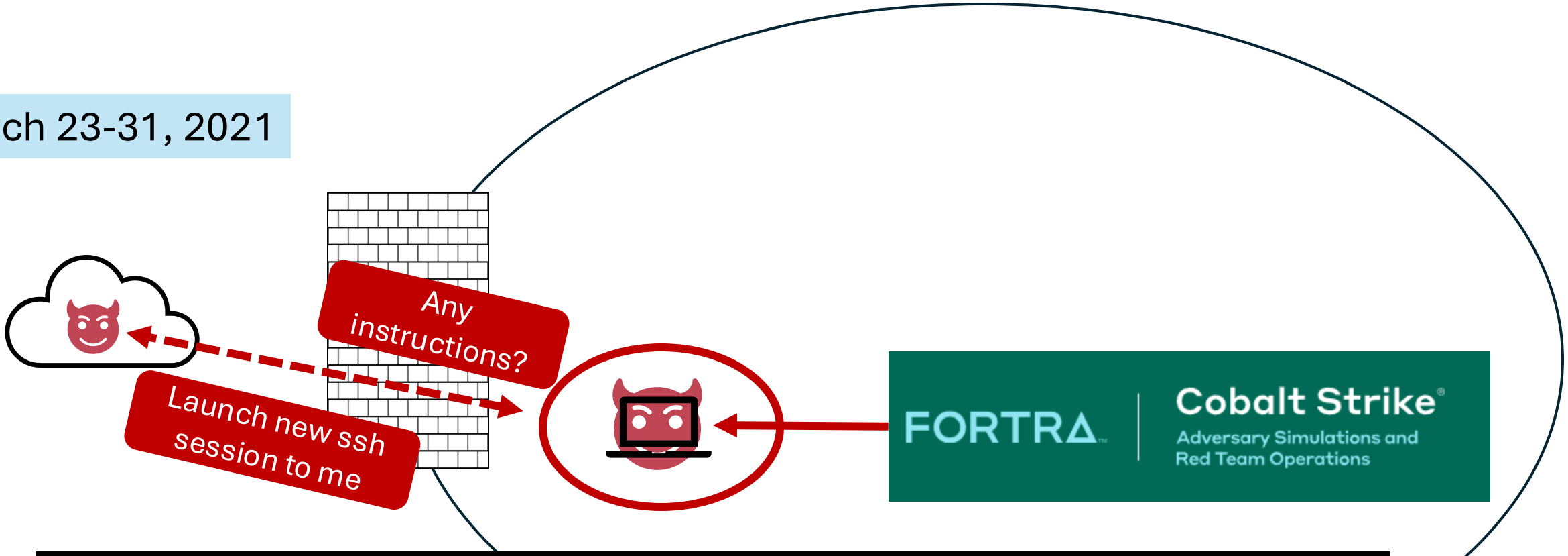


Spearphishing attack to Employee #0 (“Bob”)

- **Email Attachment:** Microsoft Excel file with malicious macro
  (Code plug-in that runs if enabled; e.g., can launch & command other apps: shell / cmd.exe)
- Successfully installs malware on Bob’s machine

Conti Attack on HSE: Establish Foothold

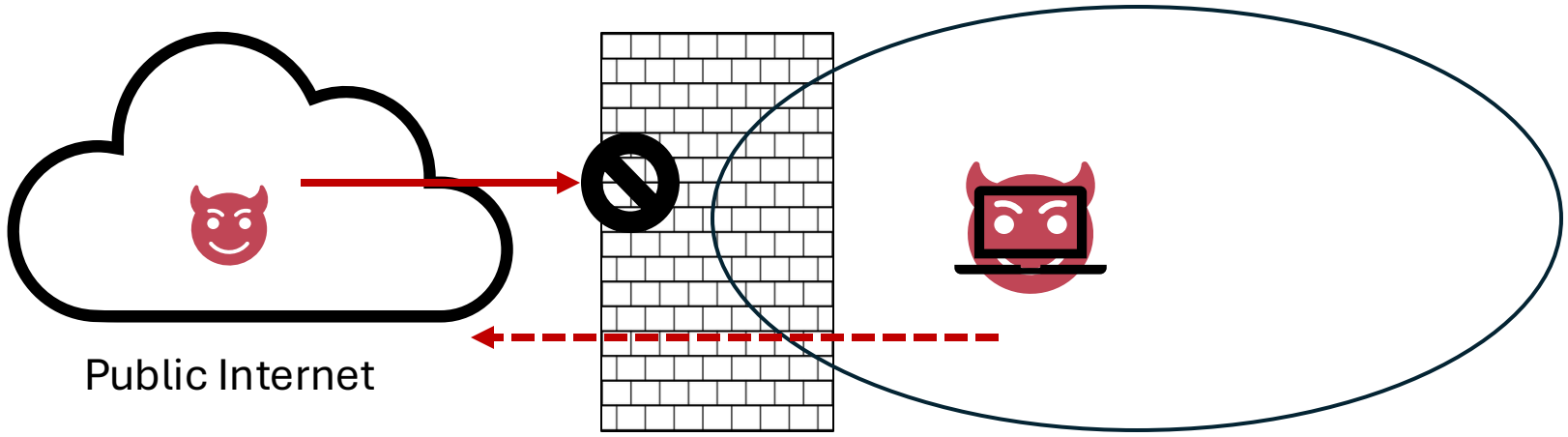
March 23-31, 2021



Establish Foothold: Persistent access and communication

- Persistence: ensure malware runs / attacker has access even if system reboots
  - e.g., modify startup program list, add attacker key to SSH authorized keys, etc.
- Command & Control (C2): maintain (stealthy) line of communication w/ attacker

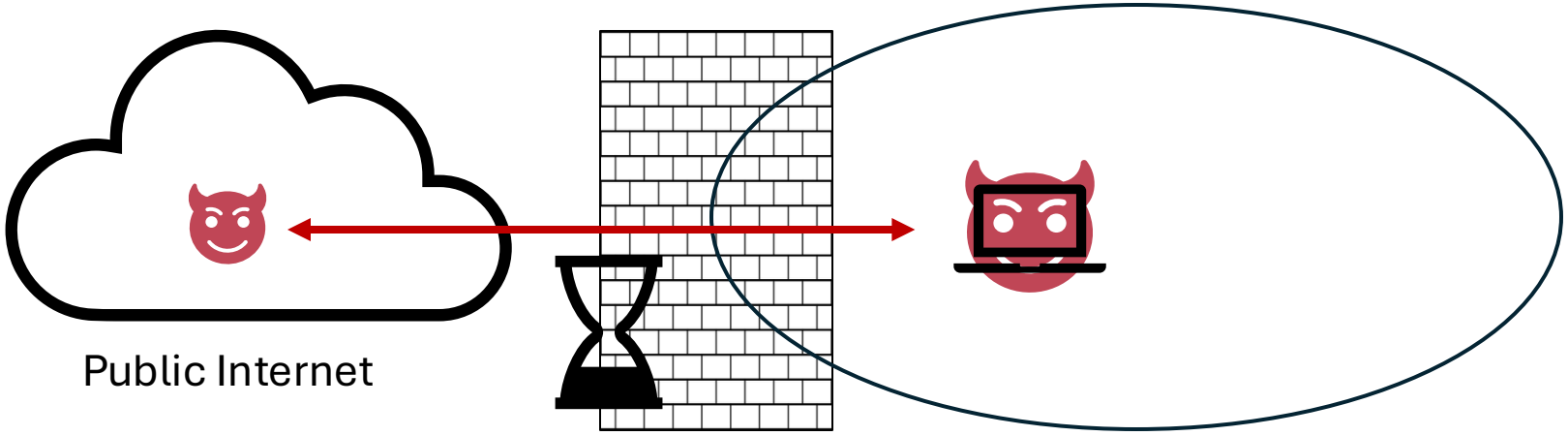
Understanding Command & Control (C2)



Why do attackers need C2 protocols / mechanisms?

- Firewall blocks the outside attacker from initiating comm with infected machine
  - Need the infected machine to initiate communication to external entity

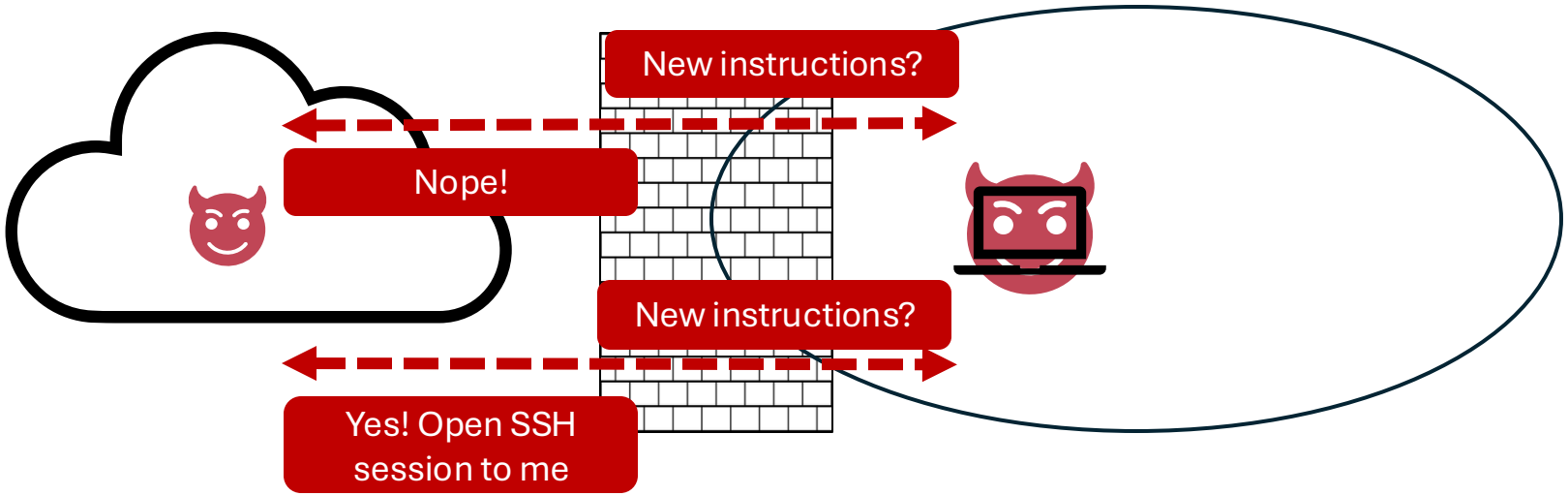
Understanding Command & Control (C2)



Why do attackers need C2 protocols / mechanisms?

- Firewall blocks the outside attacker from initiating comm with infected machine
- Attacks can take days -> months to fully execute
  - Very suspicious & impractical to keep one network session open for that long

Understanding Command & Control (C2)

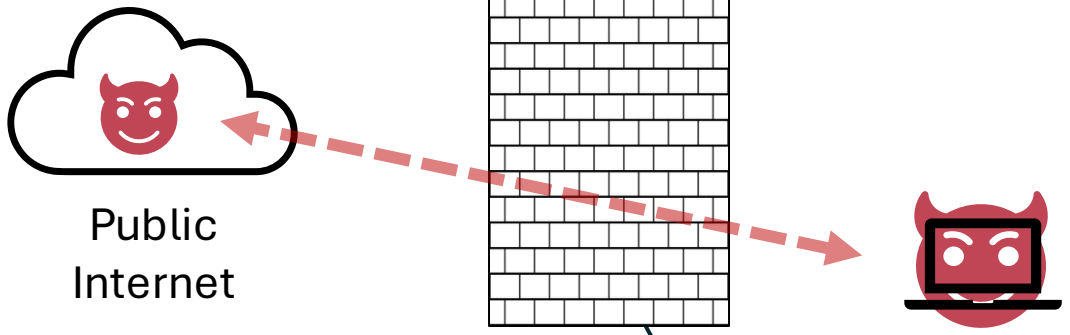


Why do attackers need C2 protocols / mechanisms?

- Firewall blocks the outside attacker from initiating comm with infected machine
- Very suspicious & impractical to keep one network session open for days -> months
- C2 protocols solve these problems for the attacker (e.g., “beaconing”)
  - Infected machine periodically contacts attackers’ server(s) for new instructions

Conti Attack on HSE: Privilege Escalation

Mar-May? 2021



README

mimikatz

`mimikatz` is a tool I've made to learn `C` and make somes experiments with Windows security.

It's now well known to extract plaintexts passwords, hash, PIN code and kerberos tickets from memory. `mimikatz` can also perform pass-the-hash, pass-the-ticket or build *Golden tickets*.

```
  .#####.   mimikatz 2.0 alpha (x86) release "Kiwi en C" (Apr  6 2014 22:02:03)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with  13 modules * * */


mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords
```

(Developed by Benjamin Delpy)

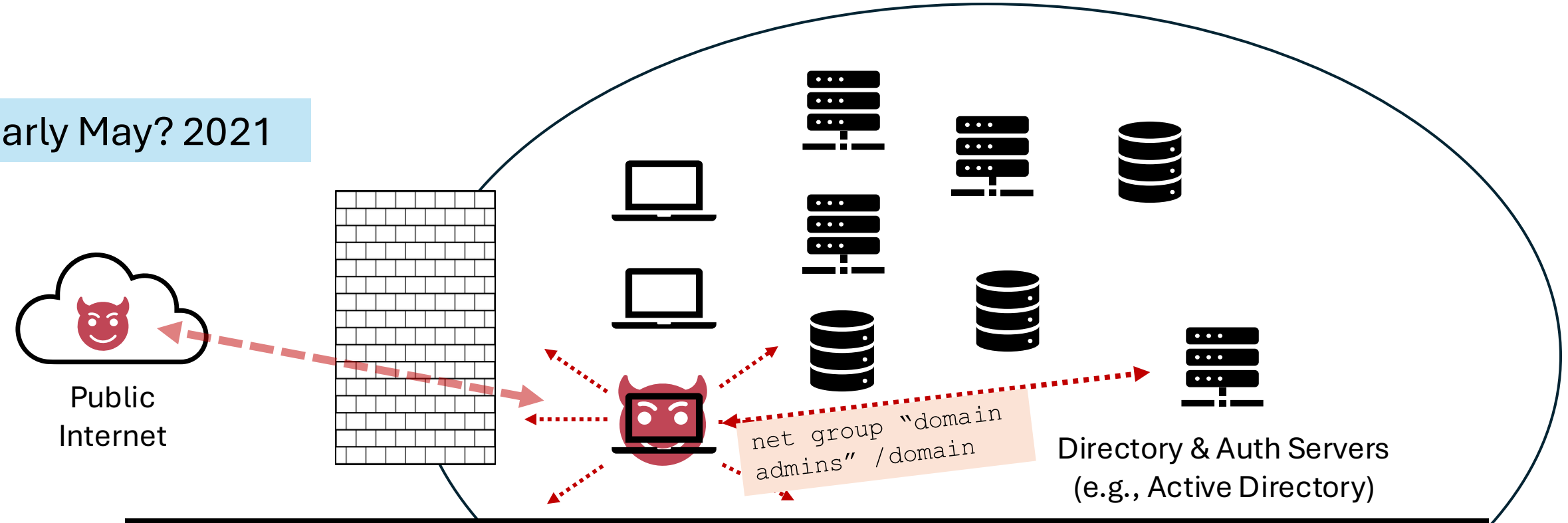
Privilege Escalation: Gain administrative privileges/credentials

(This stage often blends with internal reconnaissance: next slide)

- Credential cracking / attacks (e.g., keylogging, password cracking, Mimikatz)
- Exploiting vulnerabilities in the OS / applications of infected machine

Conti Attack on HSE: Internal Reconn

Early May? 2021



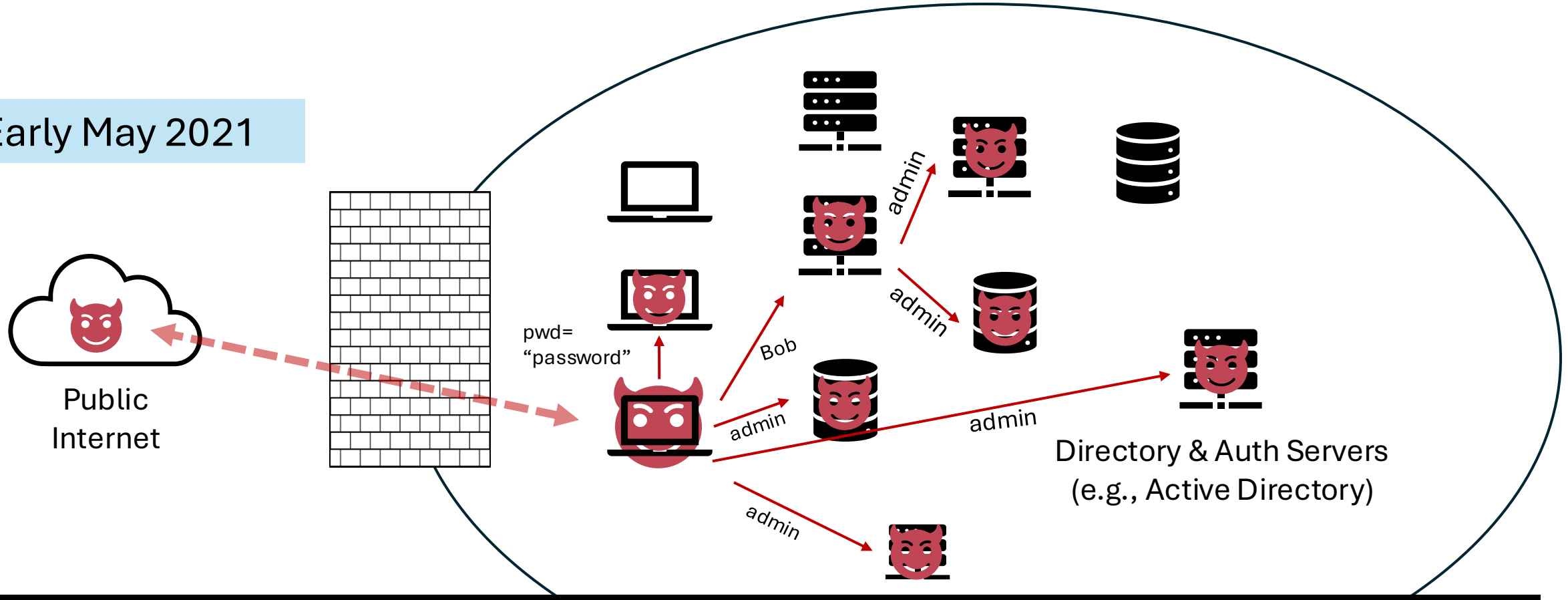
Internal Reconnaissance ("Discovery")

Identify other machines in the enterprise: what they have & how to access

- Local + Passive reconn: look through infected machine (e.g., browser/shell/VPN/app history)
- Active Directory reconn: query central authentication & directory databases
- Network scanning: probe IP addresses to find machines & vulnerable services

Conti Attack on HSE: Lateral Movement

Early May 2021

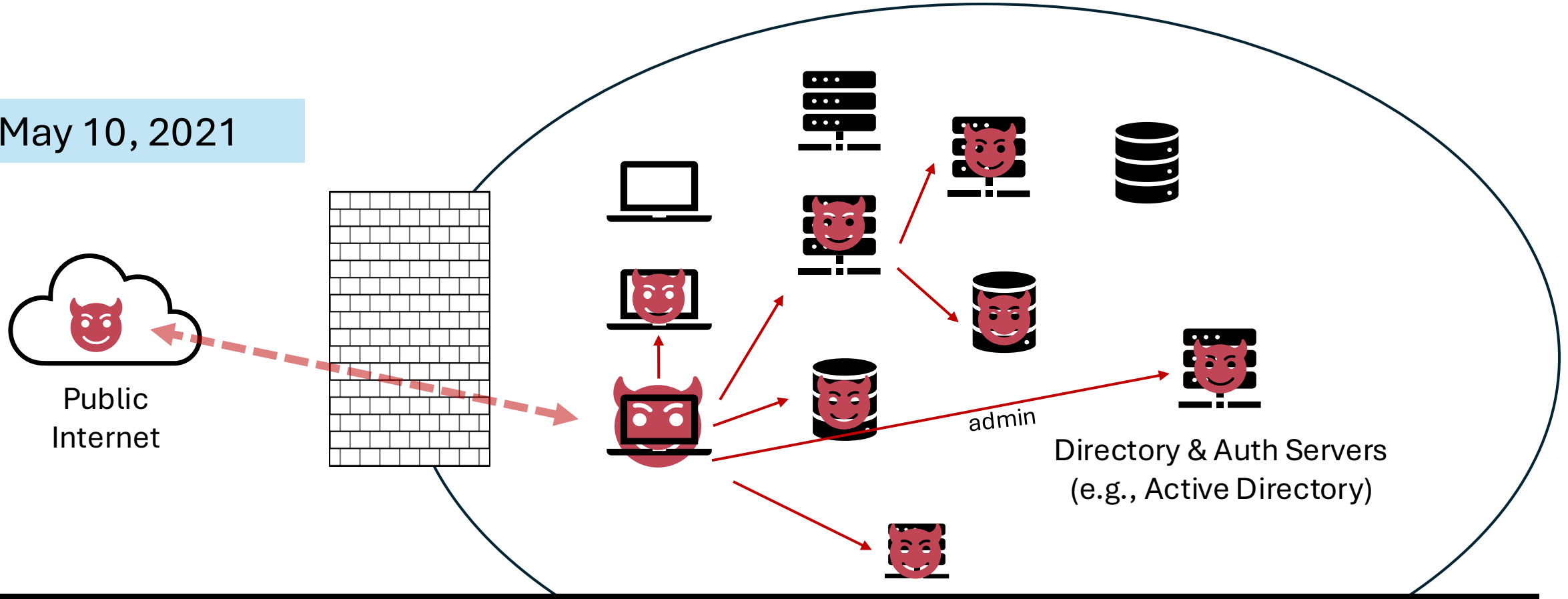


Lateral Movement: Expand to more machines & Repeat

- Use stolen credentials to access more machines (from: Victim #0 machine + Internal Reconn + Brute-forcing)
- Exploit vulnerable software/services on other machines
- Repeat process (persistence/C2/privilege escalation/etc.) on newly compromised machine

Conti Attack on HSE: Complete Mission

May 10, 2021

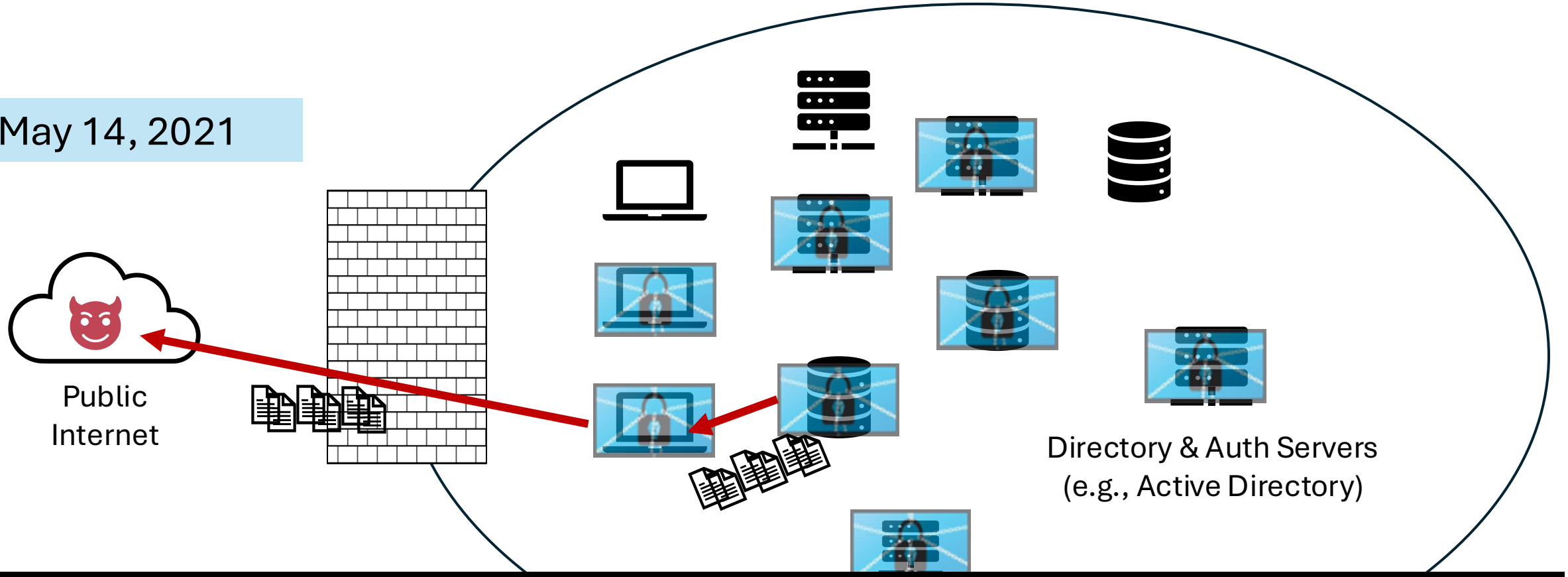


Data Exfiltration + Launch Ransomware

- May 10-12: HSE security teams began noticing & responding to detection alerts

Conti Attack on HSE: Complete Mission

May 14, 2021



Data Exfiltration + Launch Ransomware

- May 10-12: HSE security teams began noticing & responding to detection alerts
- May 14: Ransomware activated to encrypt & disable systems/data
  - Same time or potentially earlier: attackers exfiltrate patient data from systems they have accessed

Conti Attack on HSE: Aftermath

- May 14, 202
  - HSE refuse
- May 20, 202
- Sep 21, 2021

demand, and threat to

ftware (very lucky fc

d restore 99% of apps

BLEEPINGCOMPUTER

Search Site

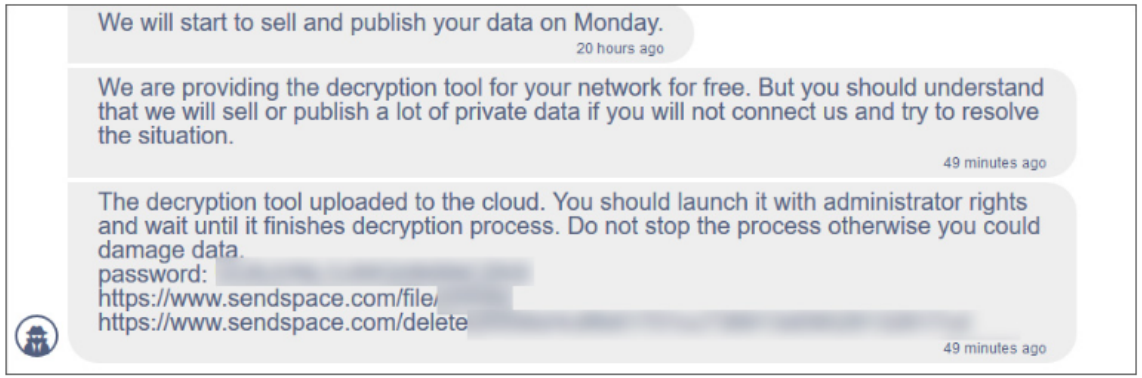
NEWS ▾ TUTORIALS ▾ VIRUS REMOVAL GUIDES ▾ DOWNLOADS ▾ DEALS ▾ VPNS

Free decryptor released

Today, the ransomware gang posted a link to a free decryptor in their negotiation chat page for the HSE that can be used use to recover encrypted files for free.

However, the threat actors warn that they will still be selling or publishing the stolen private data if a ransom of $19,999,000 is not paid.

"We are providing the decryption tool for your network for free. But you should understand that we will sell or publish a lot of private data if you will not connect us and try to resolve the situation," says the Conti ransomware gang on their Tor payment site.



Free decryptor released for HSE

As the ransomware sample used in the attacks on HSE is publicly available, security researcher MalwareHunterTeam and BleepingComputer have confirmed that the decryptor can decrypt files that were encrypted during this attack.

Cyber “Killchain” : Typical Attack Structure

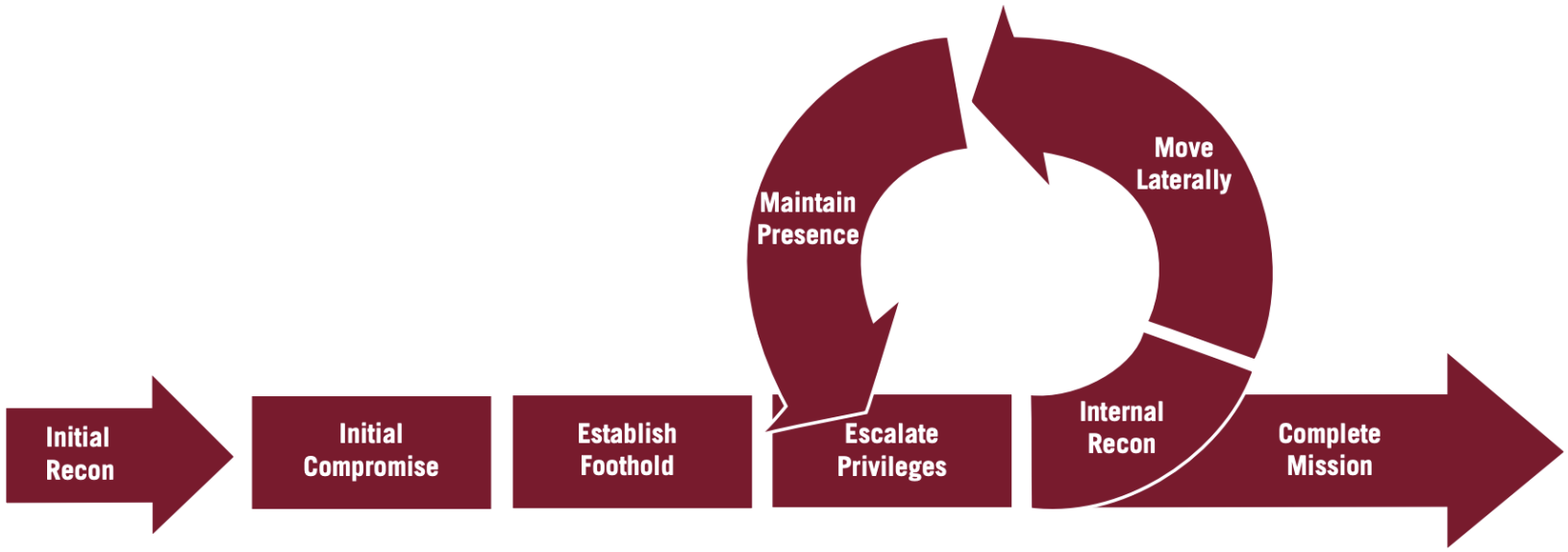


FIGURE 14: Mandiant’s Attack Lifecycle Model

1. **Initial Reconnaissance [Step 1]:** find unpatched vulnerabilities, email addresses of employees to phish, etc.
2. **Initial Access & Foothold [Steps 2-3]:** get access to an enterprise machine/account
3. **Expand Internal Access [Steps 4-7]:** more machines/accounts/privileges
4. **Complete Mission [Step 8]:** steal data / launch ransomware / cause destruction / etc.

Outline

- What is enterprise security?
- Structure of enterprise networks & basic defenses
- Attacks on enterprises
- Common enterprise defenses

General Security Hygiene

Data Backups: Mitigates damage of ransomware & destructive attacks

- Issues: Storage Costs, Potentially increased risk of data breach

Policies: Managed software & devices, Use policies, Employee Training

- Issues: Unclear (potentially harmful) efficacy, Human costs

Regular patching and Vulnerability scanning

- Issues: Compatibility & downtime, Misaligned responsibilities & ownership

Defenses: Stronger Authentication & Isolation

Basic authentication: if username + password correct, allow access

Stronger authentication: Multi-factor authentication (MFA / 2FA)

- Require correct password AND additional hardware/physical verification

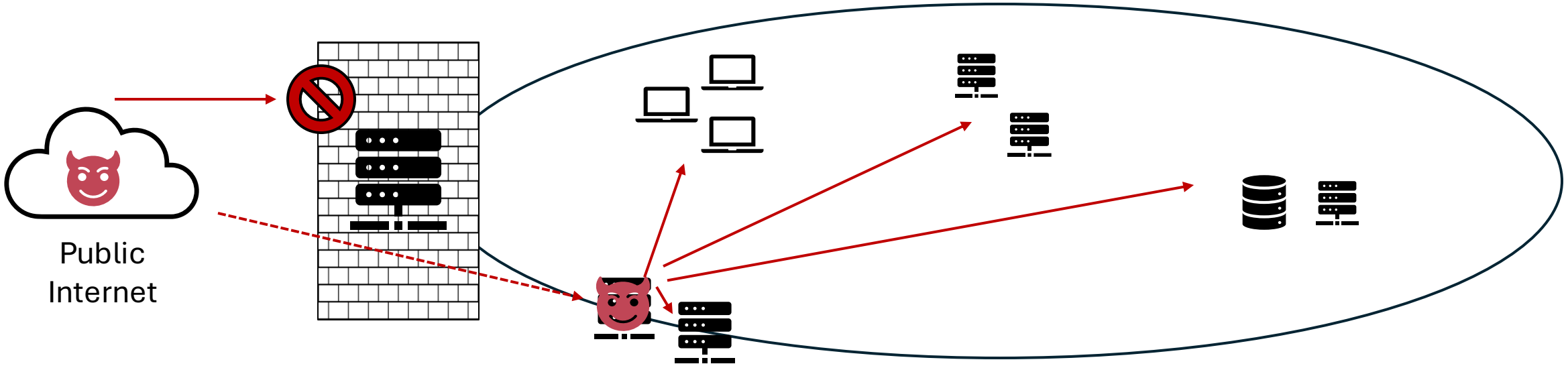
Least privilege: Dedicated admin / highly-privileged accounts

- “grantho” vs. “grantho-admin” : different passwords & permissions

Defenses: Stronger Authentication & Isolation

Basic network separation: Border firewalls keep external entities out

- Limitation: Once an attacker has an initial foothold: no more security!



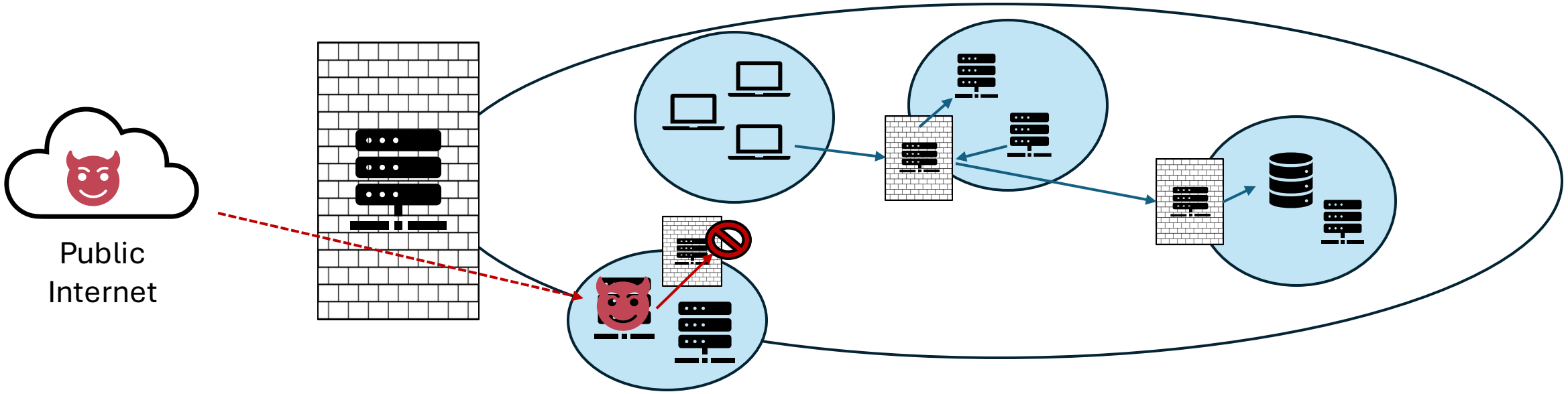
Defenses: Stronger Authentication & Isolation

Basic network separation: Border firewalls keep external entities out

- Limitation: Once an attacker has an initial foothold: no more security!

Stronger Isolation: Network segmentation & bastion hosts

- Add *internal firewalling* that
  1. Creates specific machine groups and
  2. Restricts access to/from a group via their "bastion" machine or specific conditions



Defenses: Zero Trust Model

Require ***all*** accesses to machines & data to be strongly authenticated, and only grant minimum permissions needed

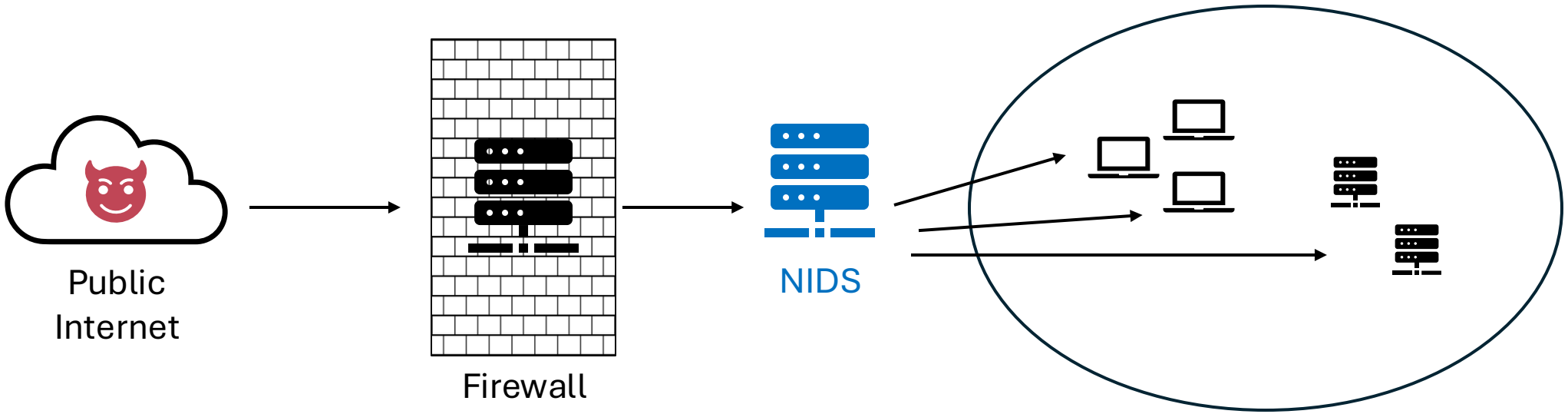
With Zero Trust: authenticating requests typically involves at least user password & 2FA, but can also involve other checks such as:

- Time-of-request
- Network properties of requesting device
- Specific device requirements (e.g., “managed” enterprise device, system and applications up-to-date, recently run anti-virus scan, etc.)

Network Intrusion Detection (NIDS)

NIDS: Typically combination of software + hardware

- Detect & terminate malicious or disallowed network traffic
- Lots of systems in real-world: Zeek, Suricata, Snort, etc.

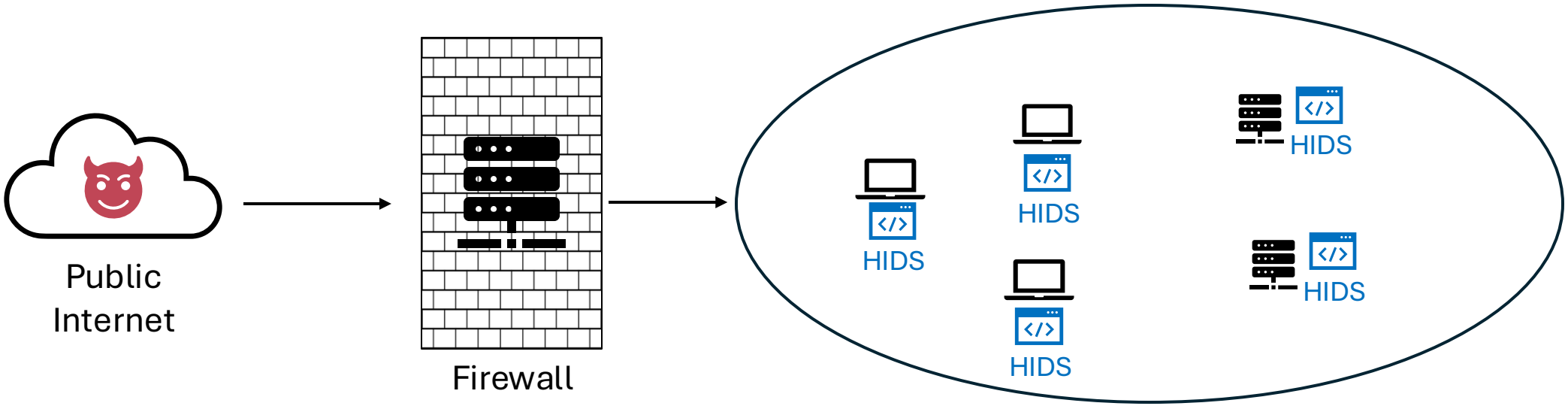


Host-Based Intrusion Detection (HIDS / EDR)

Software program on a machine that detects & remediates malicious activity (e.g., detect, stop, remove malware on employee's laptop)

Traditionally known as anti-virus (AV)

- Modern rebranding: EDR (Endpoint Detection & Response)
  (Provides more centralized control and functionality than older AV software)



Several NIDS vs. HIDS Tradeoffs

NIDS

- Cheaper deployment & maintenance
- Robust against tampering

Challenges

- Traffic Visibility: Internal and/or encrypted
- Ambiguity & evasion
- Performance & scalability

HIDS

- Deeper visibility
- Protects against non-network attacks on hosts

Challenges

- Expensive deployment costs
- Still faces evasion & higher tampering risk

Implementing Detection & Response

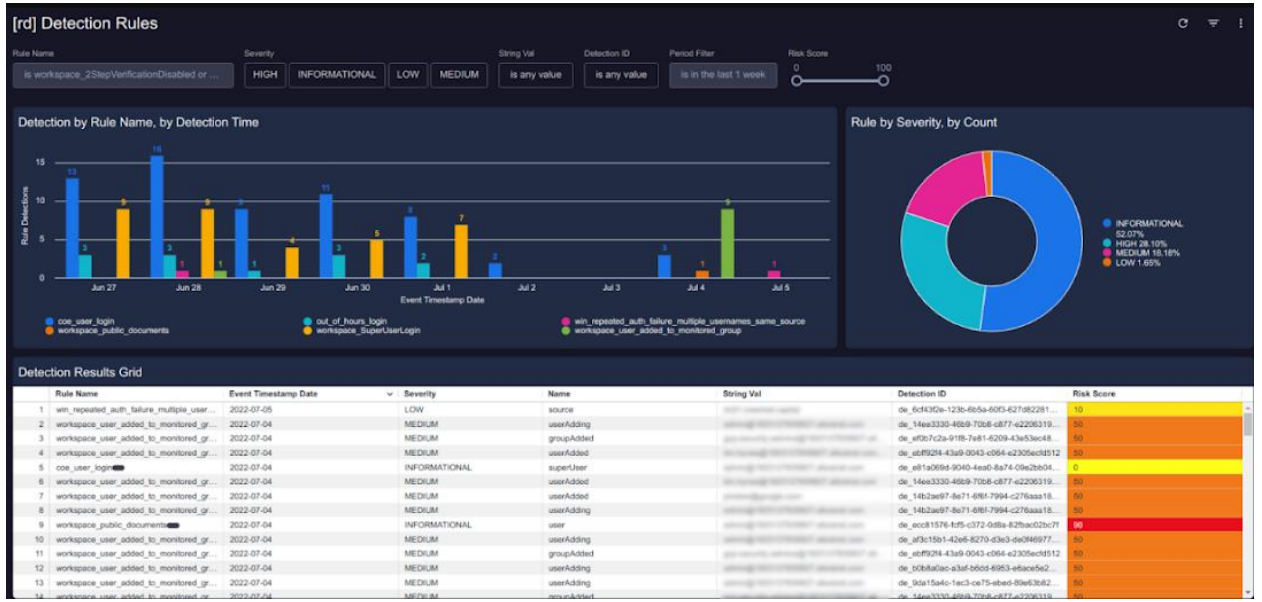
Most enterprises deploy a combination of NIDS & HIDS for detection

- Additionally: Aggregate their logs + additional logs from systems & applications into a centralized SIEM
- SIEM: Security information and event management system
  Perform detection & analysis on aggregated data

elastic Security

Chronicle

splunk>



General Detection Strategies

Exact Detection (Rule Based)

Signature-based Detection: write exact rules about what is an attack

Specification-based Detection: write exact rules about legitimate behavior; everything else is an attack

ML-Based Detection

Supervised Detection: learn characteristics of attacks

- Train model w/ prior attacks

Anomaly Detection: learn what benign behavior looks like; everything else is an attack

Detection Metrics

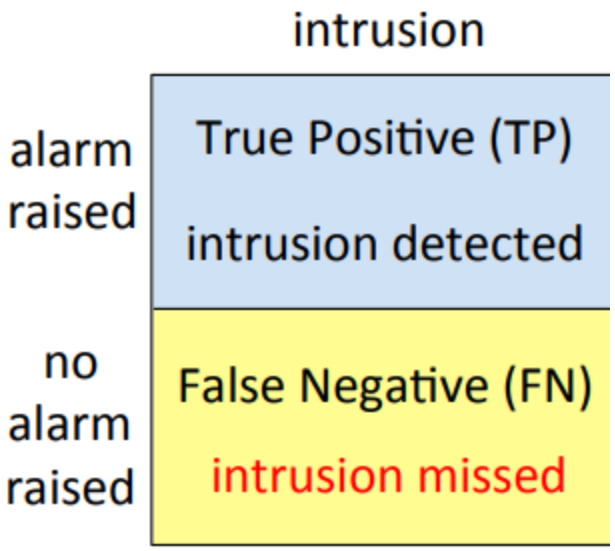
Data consists of attack events and benign events

For all the attack events:

- True Positives: labeled as an attack
- False Negatives: labeled as benign

For all the benign events:

- False Positives: labeled as attack
- True Negatives: labeled as benign



Some Key Challenges for Detection

Fundamental challenge: balancing false positives & false negatives

- Base rate fallacy: attacks are very rare but there are many, many benign events
  - A detector has a 100% TP Rate & 0.1% FP Rate… Good or Bad?
  - If network traffic: 50 attack packets & 10 million benign / day = 10,000 false alarms / day

Evasion: Attackers constantly adapting methods to evade detection

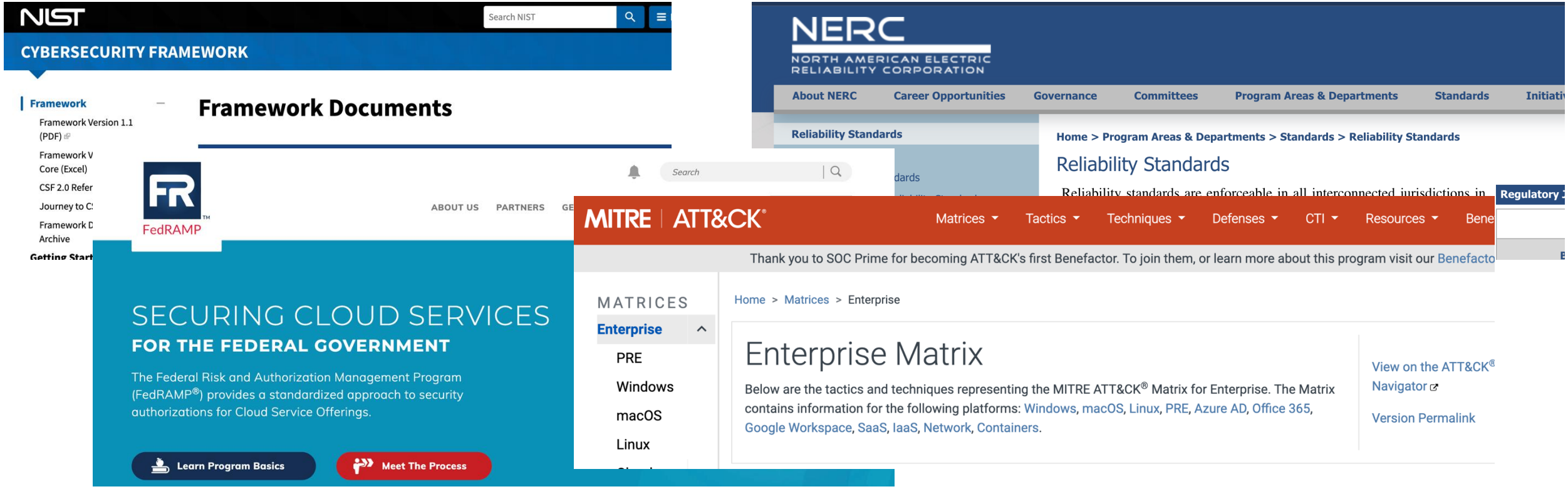
- Simple C2 strategy: infected machine contacts same malicious server on random IP address
- Stealthy C2 strategy: infected machine & malicious server communicate via a OneDrive folder

Compute & Data storage

- One machine can generate millions of events per day… 1,000s of machines at many org's
- Attacks happen over multiple machines and potentially multiple months

Broader Enterprise Security Challenges

- No unified and universal guidelines of security best practices

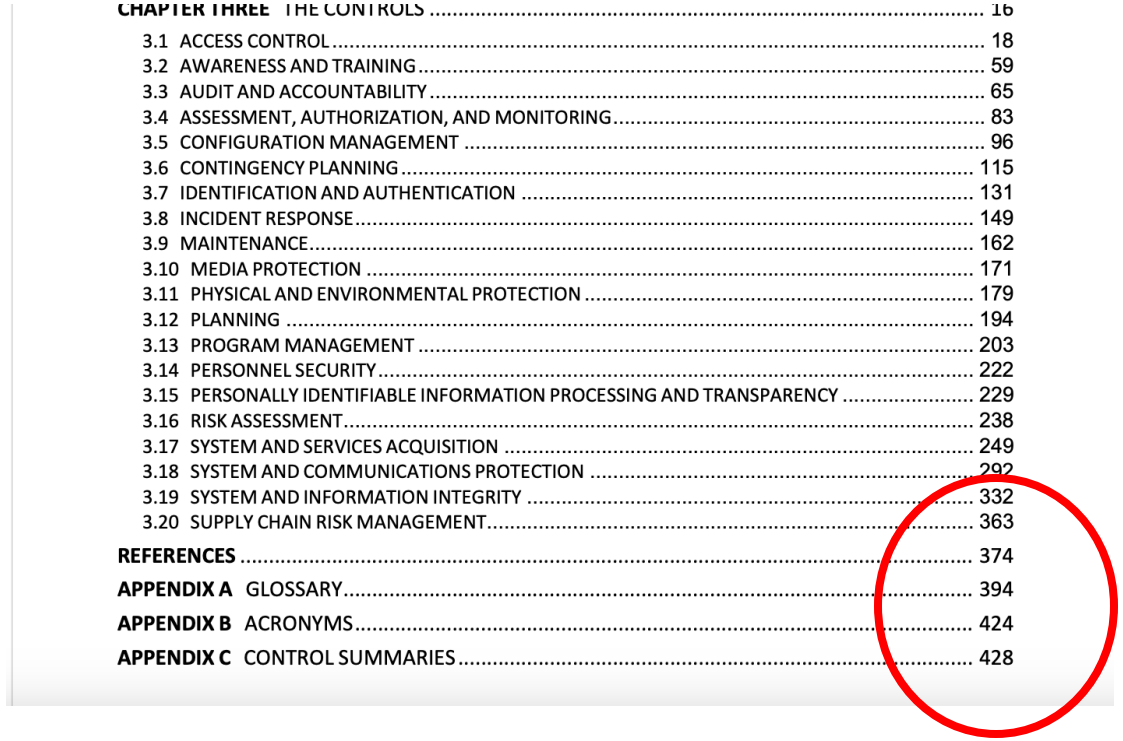


Broader Enterprise Security Challenges

- No unified and universal guidelines of security best practices
- Way too much advice out there & discrepancies / ambiguities

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations



Broader Enterprise Security Challenges

- No unified and universal guidelines of security best practices
- Way too much advice out there & discrepancies / ambiguities
- No good advice on what to prioritize

to *prioritize* this advice. For example, experts perceive 89% of the hundreds of studied behaviors as being effective, and identify 118 of them as being among the "top 5" things users should do, leaving end-users on their own to prioritize and

Elissa M. Redmiles, Noel Warford, Amritha Jayanti, and Aravind Koneru, *University of Maryland;* Sean Kross, *University of California, San Diego;* Miraida Morales, *Rutgers University;* Rock Stevens and Michelle L. Mazurek, *University of Maryland*

https://www.usenix.org/conference/usenixsecurity20/presentation/redmiles

(Security advice for end users)

Several Components for Good Enterprise Security

- Strong authentication for systems and services
- Limit administrative & sensitive privileges (least privilege)
- Deploy comprehensive detection and audit logging
- Frequent patching for applications & OS across machines
- Periodic and secured back-up for critical data