

# Cyber Threat Landscape, Response, and Reporting

TxICC Conference

November 13, 2023

Any recommendations are offered solely for your consideration, to the extent applicable to your circumstances. Any 3rd party views and opinions do not necessarily reflect those of DIR or its employees. By sharing this material, DIR does not endorse any particular person, entity, product or service.



Texas Department of Information Resources

Transforming How  
Texas Government  
Serves Texans

[dir.texas.gov](http://dir.texas.gov) | [@TexasDIR](https://twitter.com/TexasDIR) | [#DIRisIT](https://twitter.com/DIRisIT)

# What Are We Covering Today?

DIR Overview and CIRT Overview

Cyber Threat Landscape

Incident Response Planning

Incident Reporting and the TX-ISA0

# Our Mission and Vision

## DIR Mission

To serve Texas government by:

- Leading the state's technology strategy,
- Protecting state technology infrastructure, and
- Offering innovative and cost-effective solutions for all levels of government.

## DIR Vision

Transforming How Texas Government Serves Texans



# What's the CIRT, and How Can They Help?

## CIRT Services and Resources

- Incident response support and guidance.
- Dark web monitoring and alerting for Texas organizations.
- Tabletop exercise development and delivery.
- Incident response team Redbook training.
- Connection to state and federal law enforcement.
- Guidance for Managed Security Services (MSS) supporting resources.

*The DIR Cybersecurity Incident Response Team (CIRT) provides incident response support to eligible organizations to safeguard the state's critical assets.*

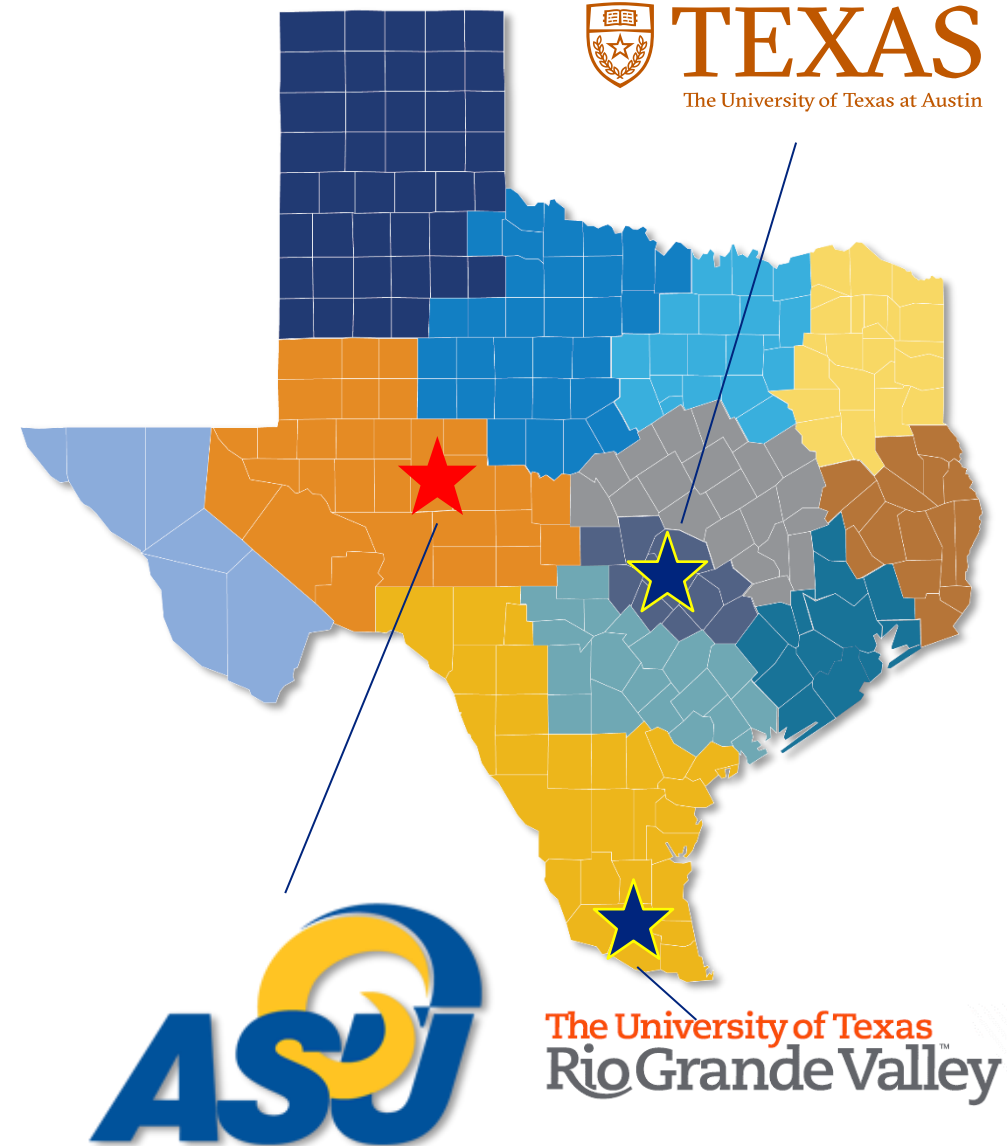


# Regional Security Operations Center (RSOC)

## Entities eligible for RSOC services include:

- Cities and counties
- Independent school districts
- Special districts
- Independent organization as defined by Section 39.151, Utilities Code
- State agencies and public junior colleges

Regional Security Operations Center				
Real-time Security Monitoring	Security Alerts and Guidance	Immediate Response	Policy and Planning	Cyber Education and Awareness
Student Engagement and Workforce Development				



# Texas Volunteer Incident Response Team (VIRT)



Assist with cybersecurity incidents in Texas

## What's Needed to Join?

- Experience in cybersecurity, incident response, or other related skills.
- Complete and submit application.
- Pass fingerprint agency background check.

## The Benefits of Giving Back

- Network with cybersecurity professionals.
- Travel and per diem reimbursements.
- Training opportunities.
- Exposure to high level incidents.
- Satisfaction of serving those in need.
- 100% volunteer deployment.

For more information, please visit DIR's [Texas VIRT Webpage](#), or send inquiries to [texasvirt@dir.texas.gov](mailto:texasvirt@dir.texas.gov).

# Cyber Threat Landscape

Intelligence and Observations  
Gathered by the CIRT



# Worldwide Ransomware Trends

## September 2023

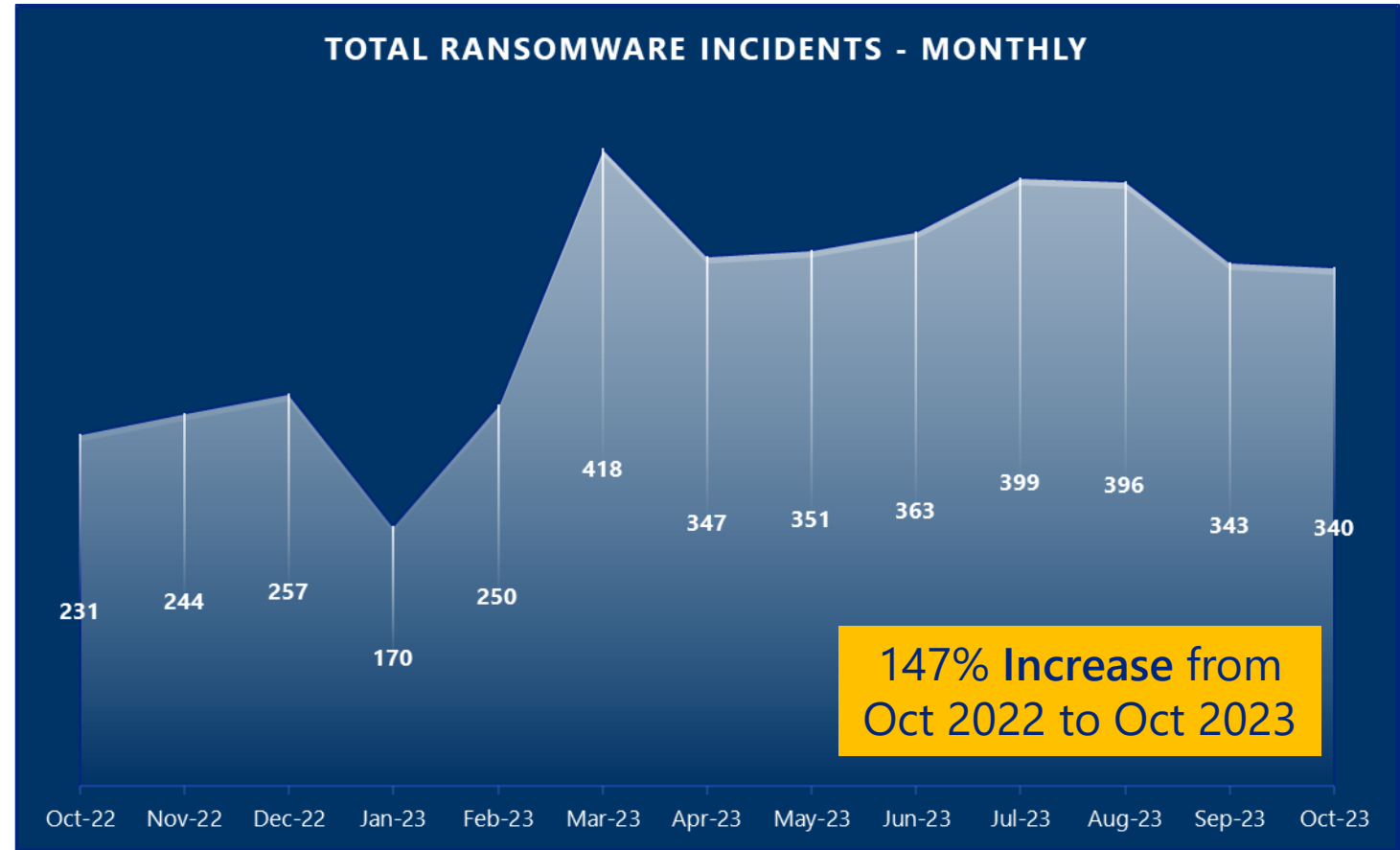
1. Lockbit: 65
2. BlackCat (AlphV): 40
3. Play: 25
4. Cactus: 21
5. No Escape: 20

Total  
Victims  
343

## October 2023

1. Lockbit: 54
2. Play: 40
3. No Escape: 31
4. BlackCat (AlphV): 24
5. 8Base: 8

Total  
Victims  
340





A dark blue background with a network diagram consisting of light blue nodes and connecting lines, creating a web-like pattern.

# **New Ransomware Groups Targeting Texas Entities**

# Akira Ransomware Group

## Group Origination

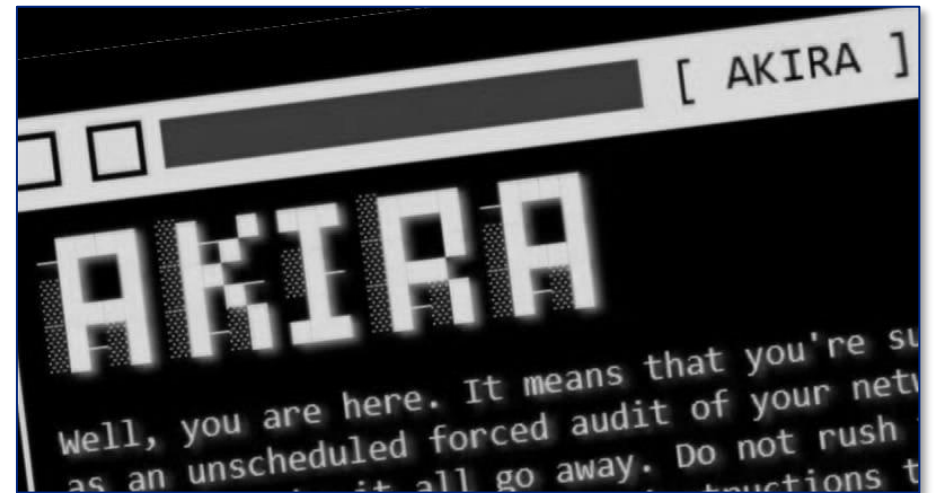
- Initially observed in **March/April 2023**.
- Appears to focus on **small- to medium-sized** businesses.
- Tactics include phishing emails and exploiting unpatched vulnerabilities in software; known for attacking **Cisco VPN** “using Single Factor authentication”.

## Ties to Conti

- Akira ransomware has similarities to leaked Conti v2.
- In at least three separate transactions, Akira sent the full amount of their ransom payment to Conti-affiliated cryptocurrency wallets.

## Decryptor

- Released in **June 2023**.
- Threat actor modified their ransomware.
- The decryptor will no longer work in all cases.



# Rhysida

Threat actors may “test” new malware/ransomware in Central and South America before targeting the United States.

## Group Origination

- First spotted in **May 2023**.
- First major target was the **Chilean Army** in late May 2023.
- Does **not target a particular sector**, but past victims have included:
  - Education services sector.
  - Internet software and service providers.
  - Prospect Medical Holdings.

## Tactics, Techniques, and Procedures (TTPs)

- Operates as **Ransomware-as-a-Service (RaaS)**.
- **Does not** have a DarkWeb forum presence.
- Uses **sophisticated phishing lures** to gain access to systems.
- Deploys via **Cobalt Strike** then establishes a **foothold and spreads** across networks.



A dark blue background with a network diagram consisting of light blue nodes and connecting lines, creating a web-like pattern.

# Recent Vulnerabilities Exploited

# Progress WS\_FTP Server

## Attack Timeline

- **September 27, 2023**
  - Progress advised the WS\_FTP team discovered vulnerabilities in the following systems:
    - WS\_FTP Server Ad hoc Transfer Module.
    - WS\_FTP Server Manager Interface.
- **September 27, 2023**
  - Progress released Versions 8.7.4 and 8.8.2.
- **October 2, 2023**
  - Attackers began **exploiting** these vulnerabilities in the wild.
- **October 3, 2023**
  - Progress released Versions 8.7.5 and 8.8.3.
- **October 5, 2023**
  - CVE-2023-40044 added to CISA's Known Exploited Vulnerability (KEV).

It took multiple patches by Progress to address all the MOVEit vulnerabilities.



CVE-2023-40044  
CRITICAL - CVSS: 10

CVE-2023-42657  
CRITICAL - CVSS: 9.9

CVE-2023-40045  
HIGH - CVSS: 8.3

CVE-2023-40046  
HIGH - CVSS: 8.2

CVE-2023-40047  
HIGH - CVSS: 8.3

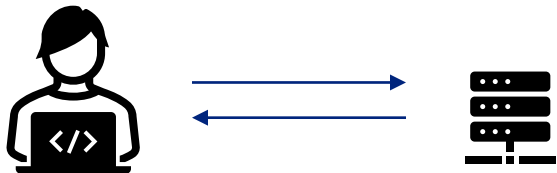
# Rapid Reset, a DDoS Attack

## Timing and Background

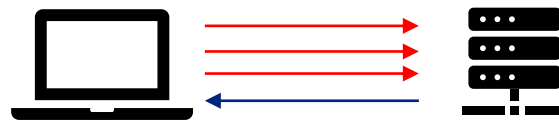
- August 2023
  - A “feature” within the HTTP/2 protocol begins to be exploited.
  - Exploitation allows for **very large** distributed denial-of-service (DDoS) attacks using relatively modest botnets.
- Methodology
  - Using this feature, threat actor requested a website, then immediately canceled the request.
  - Attackers skipped waiting for responses, resulting in **massive** attacks.

## What’s a Denial-of-Service (DoS) Attack?

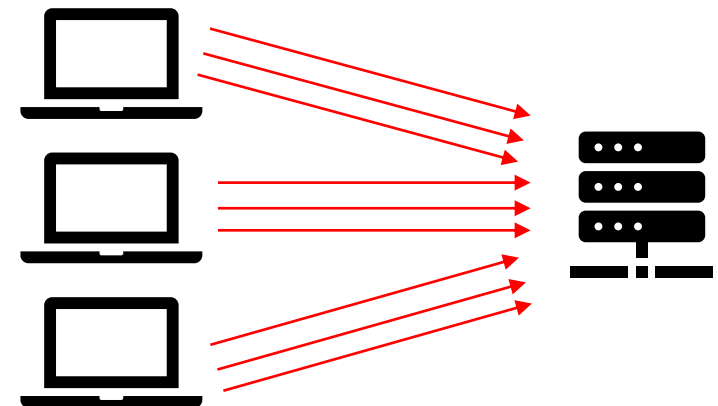
Normal Traffic



DoS Attack

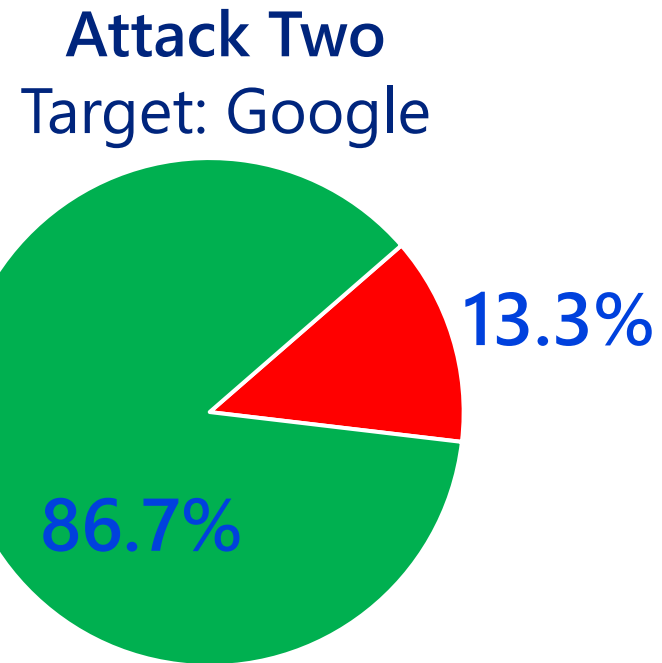
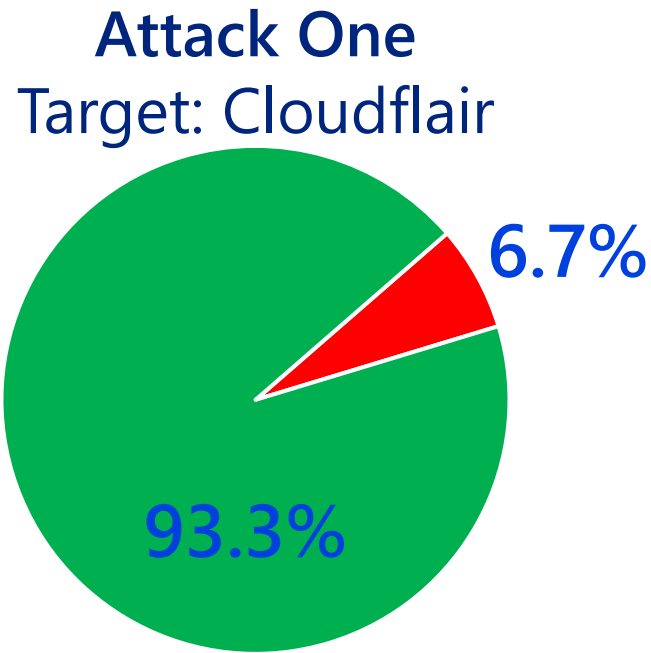


Distributed DoS Attack



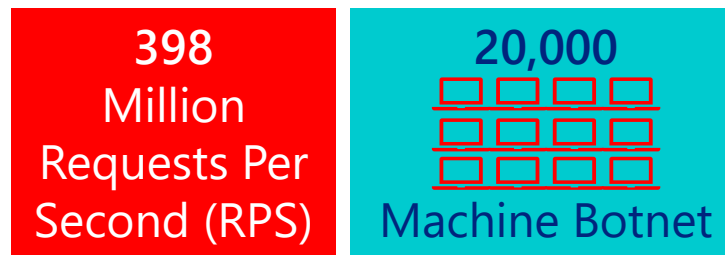
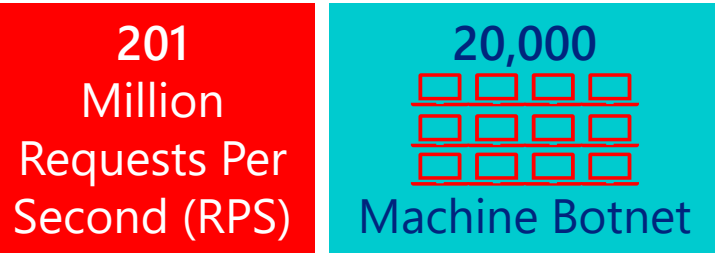
# Rapid Reset, a DDoS Attack

How Severe Were These Attacks?

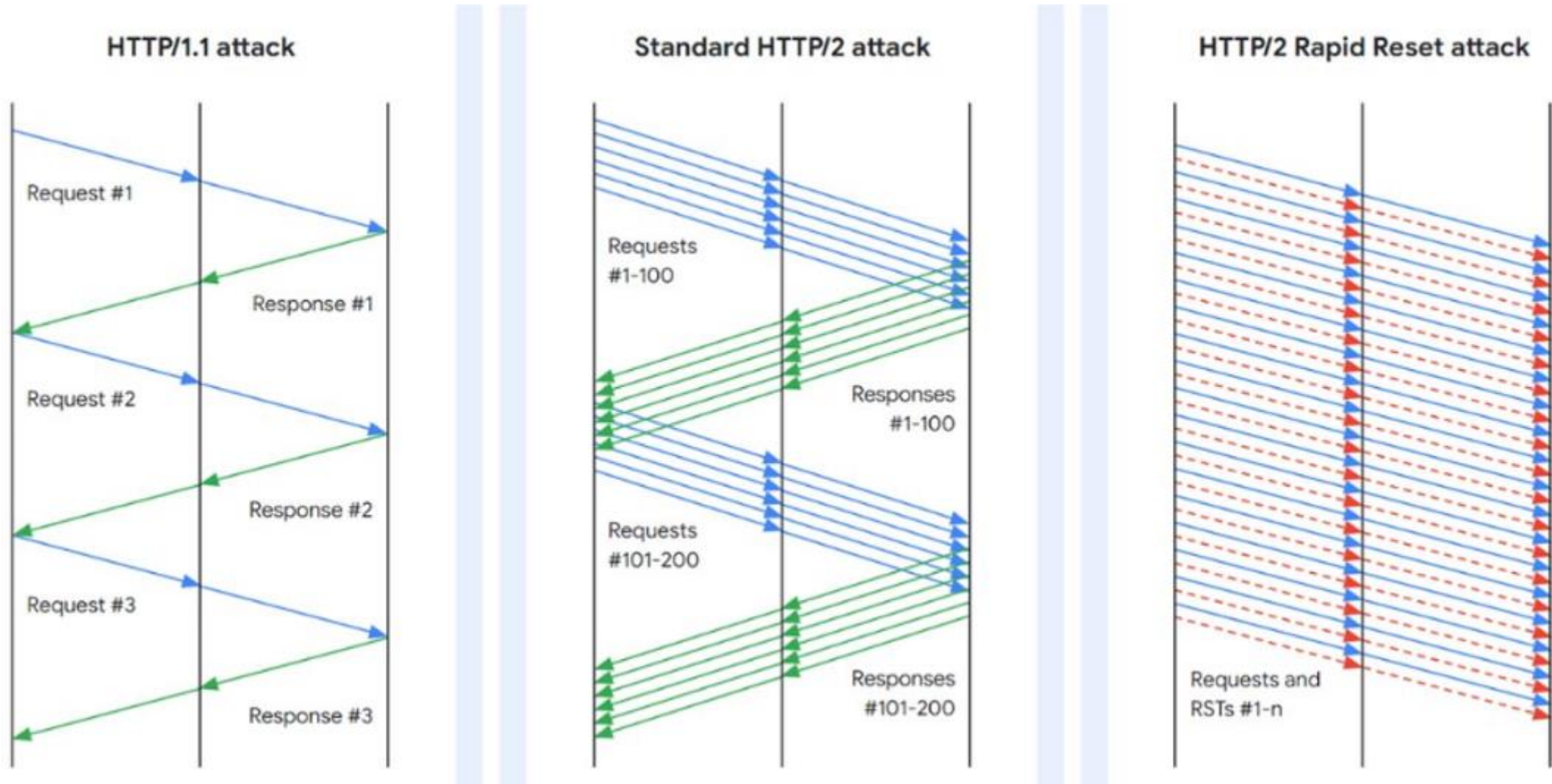


Normal web traffic is typically 1–3 billion RPS.

Percentages represent amount of attack traffic compared to normal internet traffic.



# Rapid Reset, a DDoS Attack





# Cisco IOS XE Software

## Vulnerability Overview

- Allows a remote, unauthenticated attacker to create an account on a vulnerable system.
- The attacker can then use that account to gain control of the affected system.

## Timeline

- **October 16, 2023**
  - Vulnerability announced with observed exploitation in the wild.
  - No patch available, but mitigation recommendations were provided.
- **October 18, 2023**
  - Cisco releases a script to help investigate the potential vulnerability and exploitation of systems.
- **October 23, 2023**
  - Cisco releases patches to address the vulnerability.

The background of the slide is a dark blue color with a faint, light blue network diagram. The diagram consists of several circular nodes connected by thin lines, forming a complex web-like structure. The nodes are of varying sizes and are scattered across the background, with some appearing more prominent than others. The overall aesthetic is clean and modern, typical of a professional presentation.

# Attack Overview

# Recent “Dropbox PDF” Phishing Email Campaign

## Attack Background

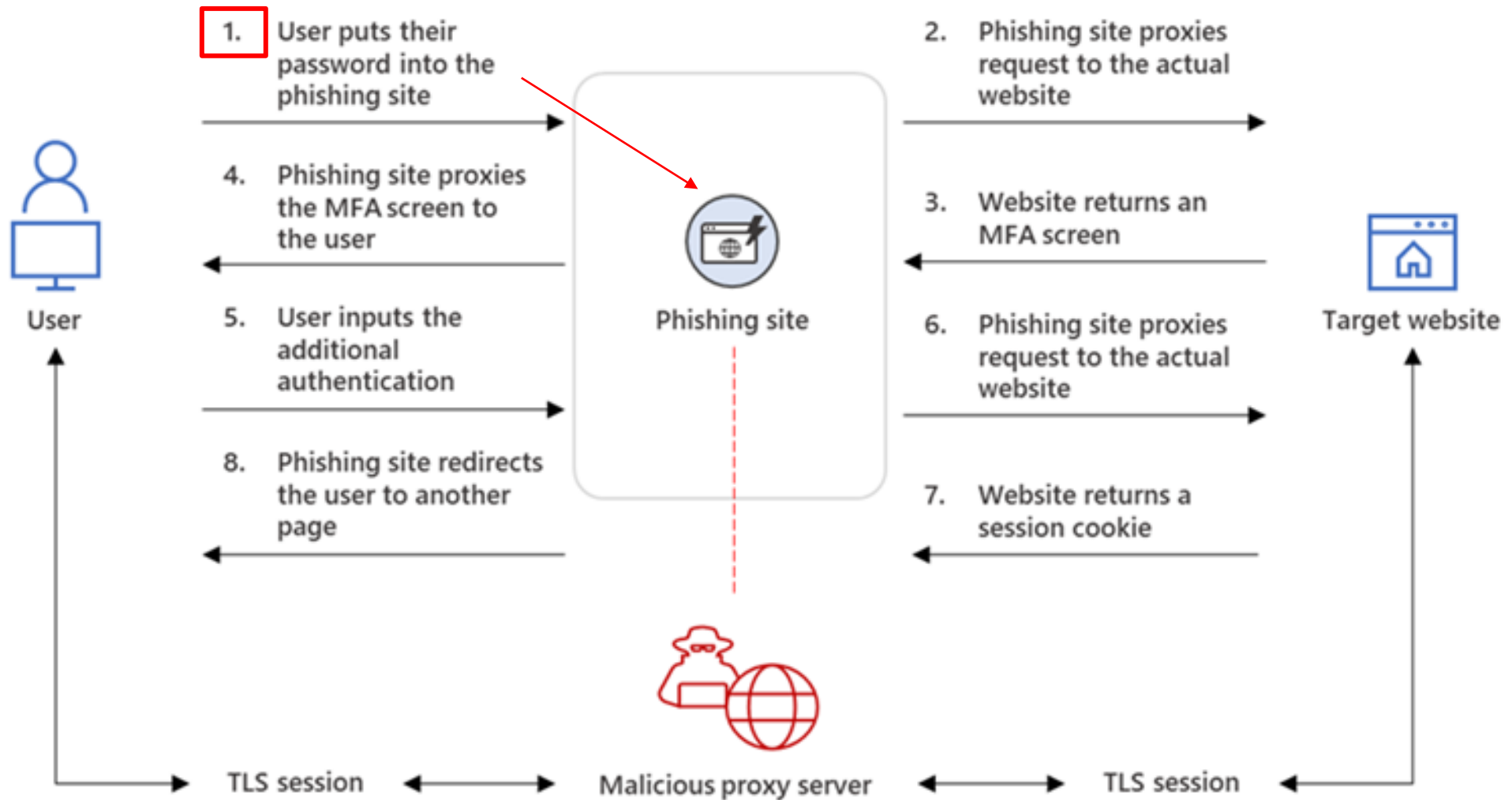
- Campaign uses compromised **legitimate/valid** email accounts to send emails.
  - Since emails are coming from legitimate accounts, they **will not be filtered**.
- Campaign’s phishing link is hosted with Dropbox.
  - Unless you are blocking file share sites, web filtering will **not block the Dropbox link**.

## Attack Goal

- Get victim to provide credentials and MFA to access a “PDF.”
- This is an example of an Adversary-in-the-Middle (AitM) phishing attempt.
  - AitMs work as a proxy between the victim and the target site.
  - AitM attacks not only phish username and password, but they also prompt for MFA to get session cookies/tokens.

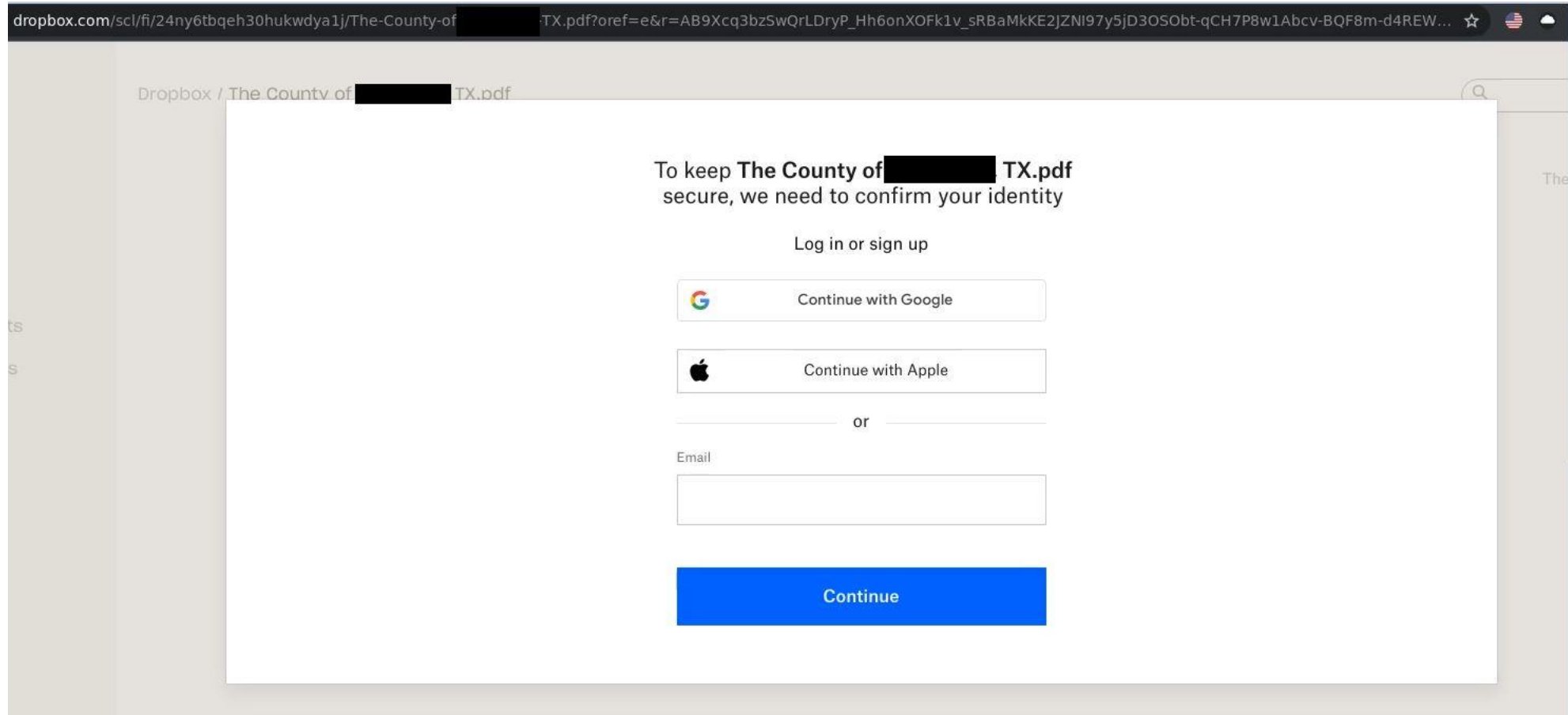
**In the next few slides, we will break down how an AiTM phishing email works.**

# Adversary-in-the-Middle (AitM)



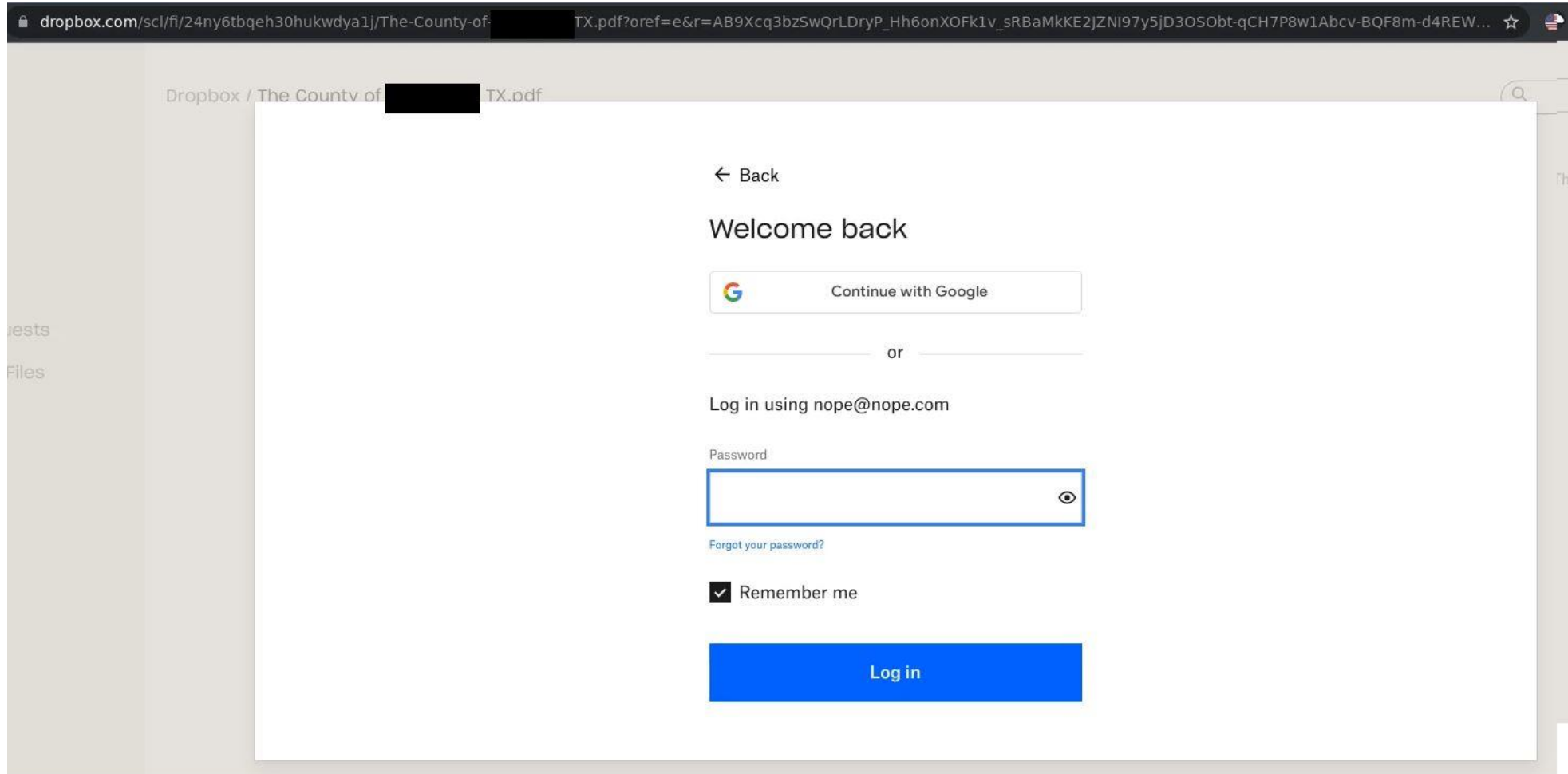
# Adversary-in-the-Middle (AitM)

## “Dropbox” Phishing Email Link – Username Prompt

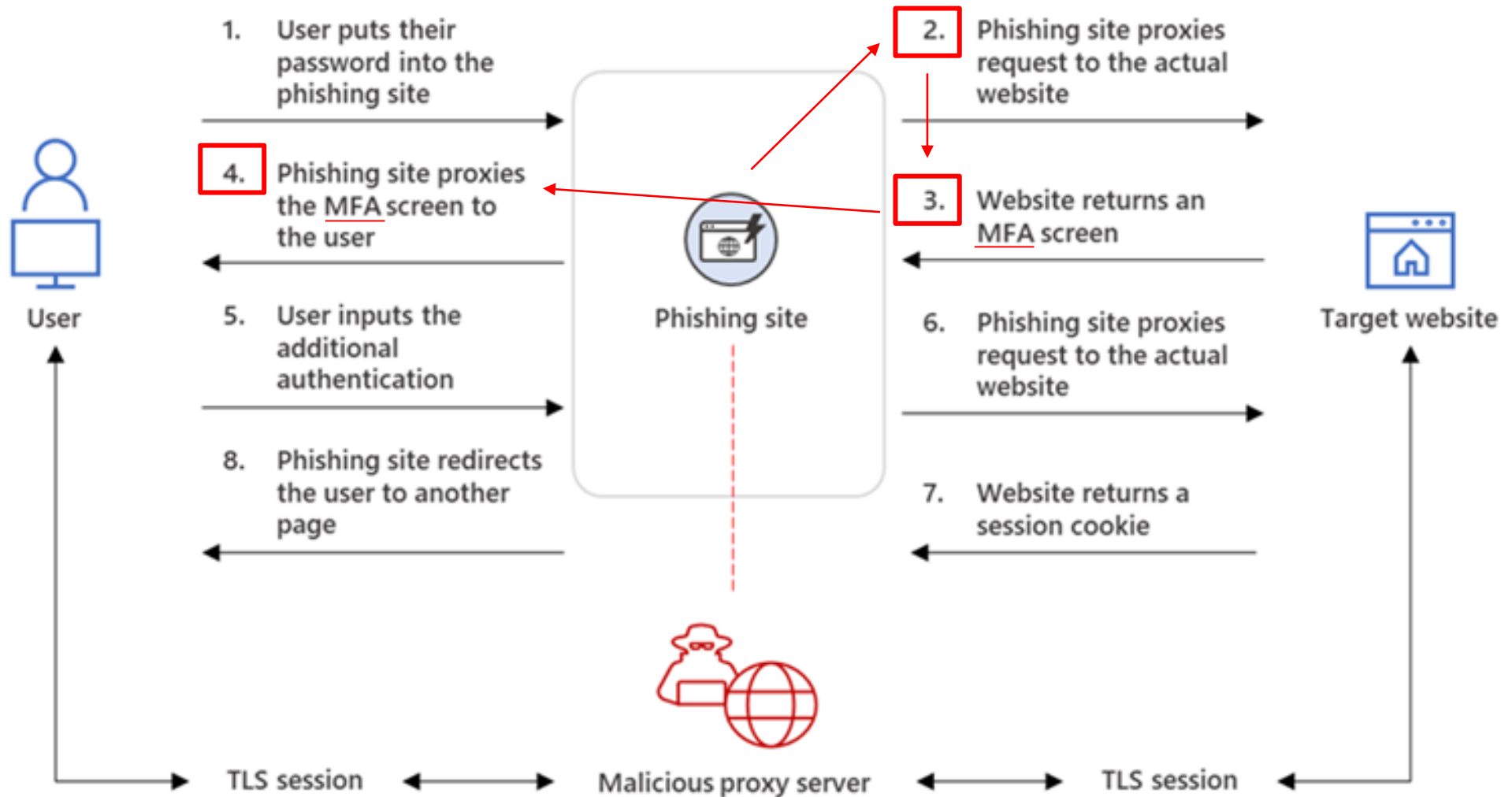


# Adversary-in-the-Middle (AitM)

## “Dropbox” Phishing Email Link – Password Prompt

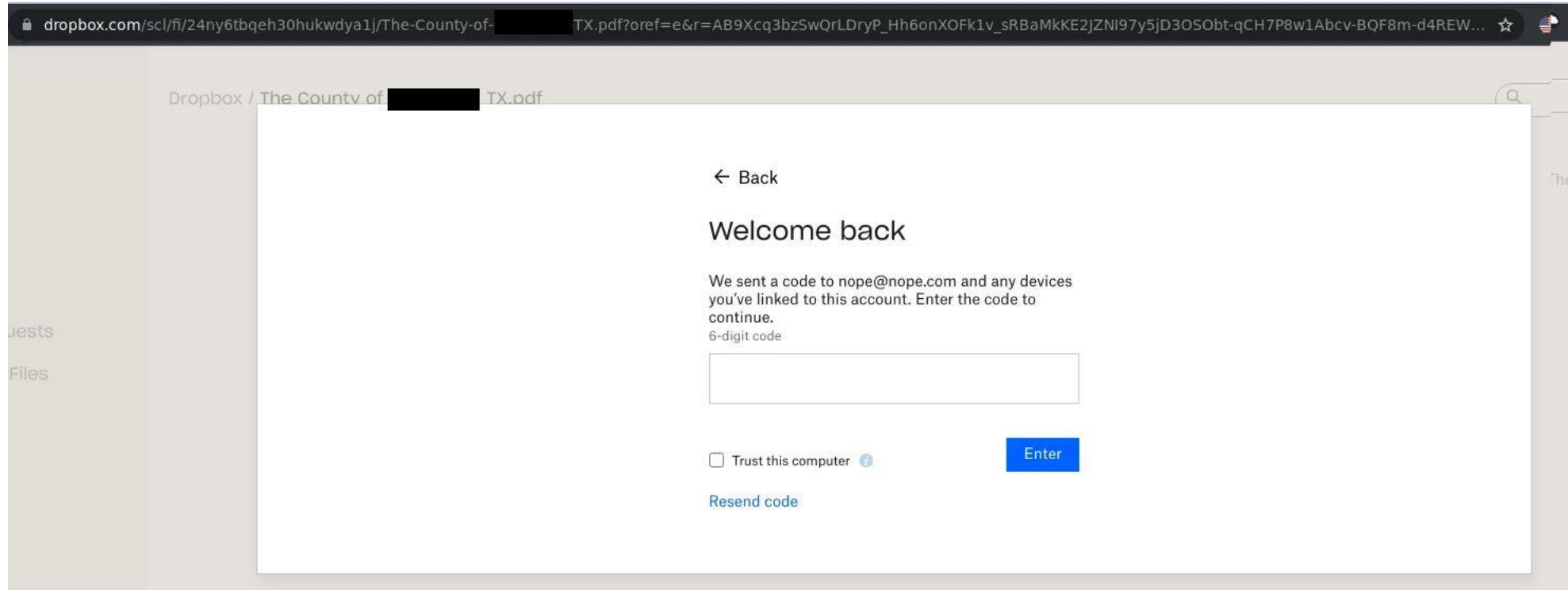


# Adversary-in-the-Middle (AitM)



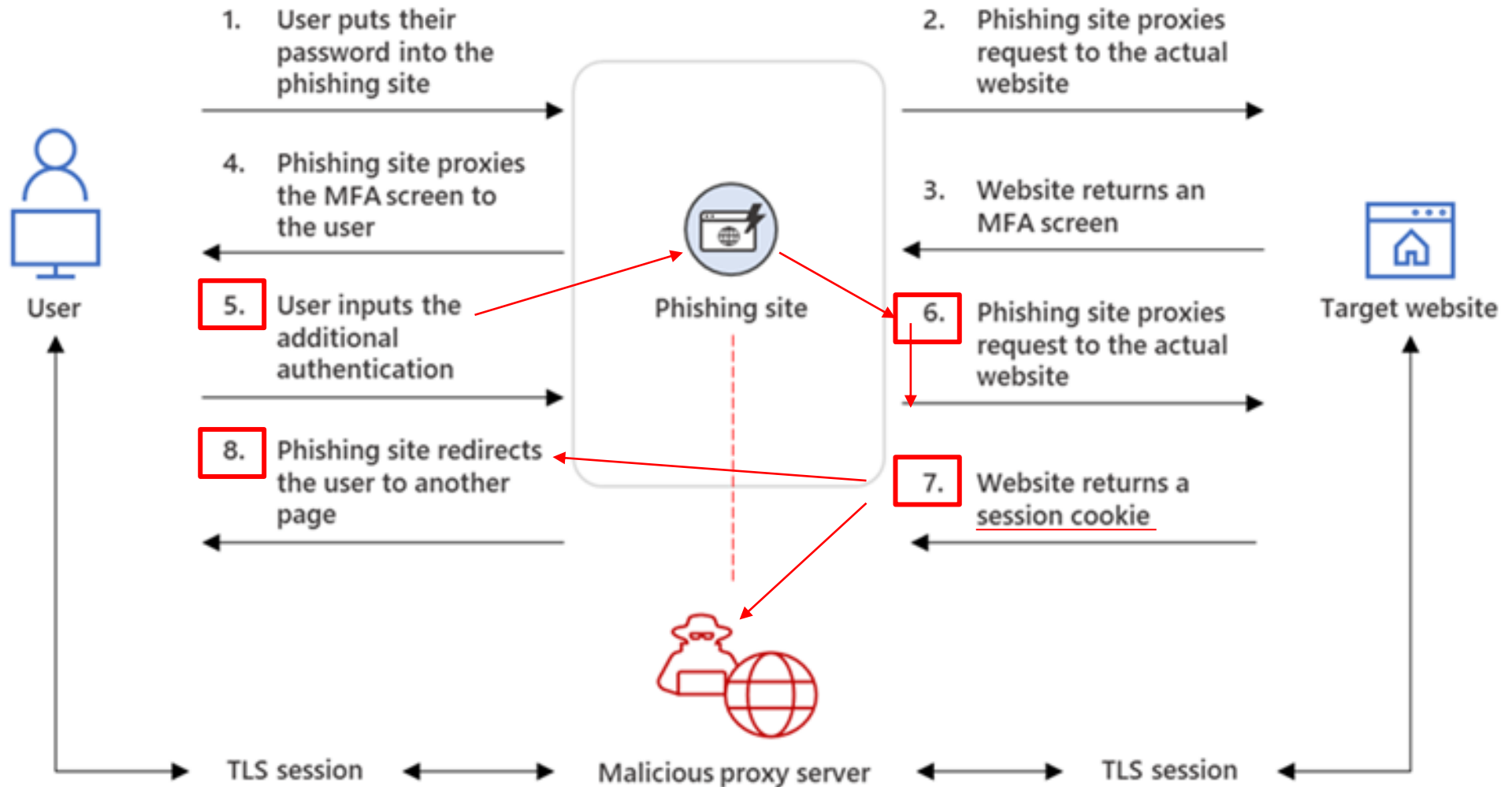
# Adversary-in-the-Middle (AitM)

## “Dropbox” Phishing Email Link – MFA Prompt





# Adversary-in-the-Middle (AitM)



# Adversary-in-the-Middle (AitM)

## How can you protect against AitM phishing?

- Phishing training and user awareness are key to stopping/preventing this attack.
- Enable conditional access policies.
- In Microsoft O365, you can setup a “US Only” geo-blocking conditional access policy that only allows sign ins from US.
- Continuously monitor for suspicious or anomalous activities.

# Malicious Advertisements

## Google Ads Abuse

- Practice of taking out a Google advertisement to promote a malicious website impersonating a legitimate project.
- “cbridge.ceieler.network” instead of “cbridge.celer.network”.

## Impacts

- The result is pushed to the top of the search result page, tricking unsuspecting victims into believing it's a legitimate search result.

The screenshot shows a Google search for "celer bridge". The search bar contains "celer bridge" and the browser tab is "cbridge.celer.network". Below the search bar are navigation buttons for News, Images, Twitter, Crypto, Protocol, Reddit, Network Twitter, Videos, and Shopping. The search results show "About 671,000 results (0.49 seconds)". A red banner at the top right reads "Google Search Ad Phishing". The first result is a sponsored ad for "cbridge.celer.network" with the URL "https://cbridge.celer.network". A red arrow points from this URL to a red box containing the malicious URL "https://cbridge.ceieler.network/". Below the ad is the text "Celer Bridge - Official Website" and a description of cBridge as a multi-chain, cross-layer asset bridge. The second result is for "Celer cBridge" with the URL "https://cbridge.celer.network".

Celer Bridge is a decentralized non-custodial asset bridge for cryptocurrency and one user lost \$900,000 via this malicious Google Ad

# How Can We Start Planning for Cyber Incident Response?



# Questions to Ask During Incident Response Planning

Who is on your incident response team?

What are your incident reporting requirements?

What external resources can help you respond?

What systems, data, and technology do you have?

What will you do during each phase of incident response?

What are the incident reporting thresholds?

How can you continuously improve?

Do we have a culture of cybersecurity?

# Consider What Goes in Your Incident Response Plan

## Identify Your Team

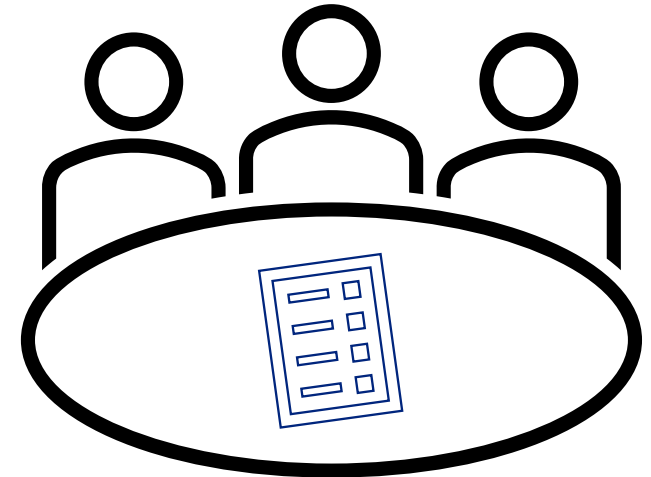
- Who will be on the incident response team? Will we have several team components?

## Decide Who Gets Notified and When

- Who will be notified when we activate our incident response plan? Who makes those decisions?

## Document Your Environment

- Do we have an inventory of our systems? Do we need to develop a network diagram? Have we classified our data?



# Begin Drafting Your Incident Response Plan

## Identify What Resources Can Assist You

- What resources will assist with incident response? Will these resources be from inside or outside of the organization?

## Define Your Response Strategy

- How will we contain an incident? What will we do to eradicate the threat so recovery can begin?



# Does DIR Offer Any Additional Services?

TX-ISAO and Cybersecurity  
Incident Response Team (CIRT)





# Texas Information Sharing and Analysis Organization (TX-ISAO)

## TX-ISAO Services Include

- Access to the TX-ISAO Portal and discussions module.
- Cybersecurity bulletins (including advisories and actionable intelligence).
- Monthly ISAO member meetings.
- Weekly actionable cyber threat intelligence.
- Cybersecurity training for Law Enforcement.
- Tabletop exercise packages.



### **Become a Member**

[Join the TX-ISAO](#) to receive intelligence and educational opportunities, and participate in information sharing.

# Security Incident Reporting Requirement FAQs

## What bill/statute requires local incident reporting?

- SB 271, which was passed during the 88<sup>th</sup> Legislative Session.

## When is this statute effective?

- September 1, 2023.

## Who is required to report incidents?

- Local governments including counties, municipalities, special districts, school districts, junior college districts, and other political subdivisions of the state.

## Are any organizations/incidents exempt from reporting to DIR?

- Yes. These requirements do not apply to incidents that are already required to be reported to an independent organization certified by the Public Utilities Commission under the Texas Utilities Code.

# Security Incident Reporting Requirement FAQs

## What's the definition of a security incident?

- A breach or suspected breach of system security (as defined by Section 521.053, Business & Commerce Code); the introduction of ransomware into a computer, network, or system (as defined by Section 33.023, Penal Code).

## Do I have to report security incidents immediately?

- Covered entities are required to report to DIR within 48 hours of discover.

## Do I submit only one report?

- No. You must submit a close out report 10 days after incident eradication, closure, and recovery, which includes details of the security incident and an analysis of the cause of the incident.

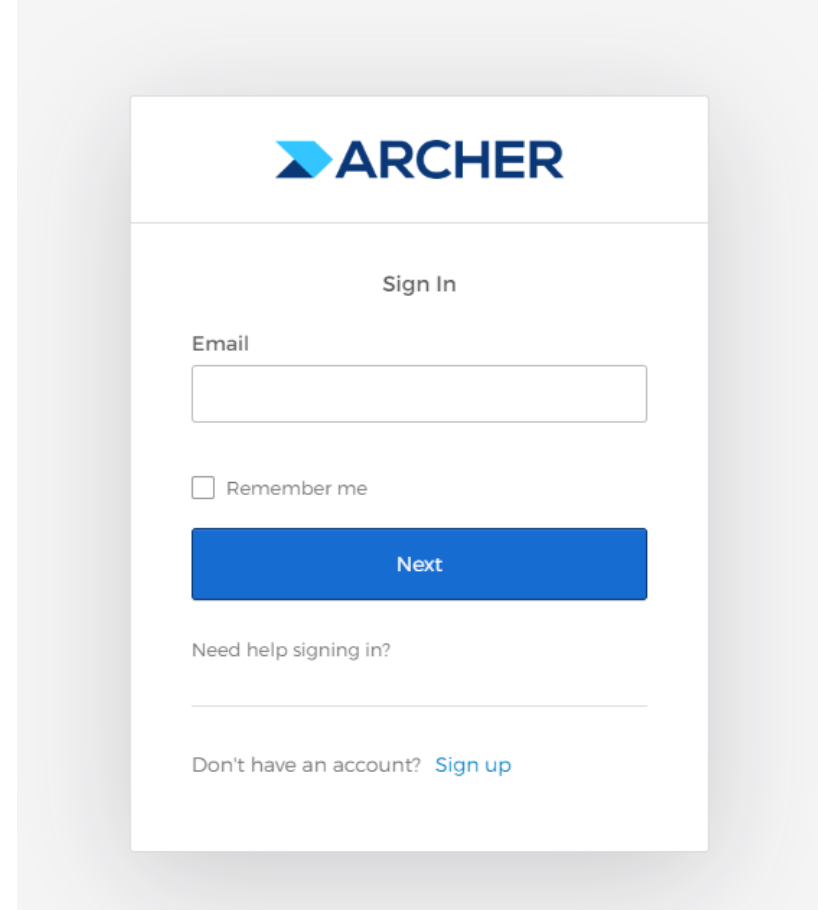
## Is my report safe and confidential?

- Yes. DIR works diligently to protect your organization's information.

# Need to Report a Security Incident?

## Visit the [DIR SB 271 Security Incident Webpage](#)

1. Create an Archer Engage account (first-time only).
2. Log into Engage (enter username and password; submit one-time verification code).
3. Submit incident report and receive email confirmation (retain email confirmation with incident ID).
4. Submit incident closure and receive email confirmation.

A screenshot of the Archer Engage Sign In page. The page features the Archer logo at the top left, which consists of a blue triangle pointing right followed by the word "ARCHER" in blue. Below the logo is the text "Sign In". There is an input field labeled "Email" with a light gray border. Below the input field is a checkbox labeled "Remember me". A blue button with the text "Next" is positioned below the checkbox. At the bottom of the page, there is a link that says "Don't have an account? Sign up".

**ARCHER**

Sign In

Email

Remember me

Next

Need help signing in?

Don't have an account? [Sign up](#)

# Are There Any Additional Free or Low-cost Resources?

# Informational Resources

## Guides

- DIR
  - [Incident Response Team Redbook](#)
  - [OCISO Services Guide](#)
  - [Technology Legislation Tracker](#)
- MS-ISAC/CISA
  - [Joint Ransomware Guide](#)
  - [First Steps Within a Cybersecurity Program](#)
- American Public Power Association
  - [Public Power Cyber Incident Response Playbook](#)

## Training

- Federal Virtual Training Environment (FedVTE)
  - [Free Online Cybersecurity Training](#)
- DIR
  - [Statewide Cybersecurity Awareness Training Resources](#)

## Membership

- Texas ISAO
  - [TxISAO Mailing List Access Request Form](#)
- MS-ISAC
  - [Join MS-ISAC](#)
- InfraGard
  - [New Application](#)

# Response Resources

## ISAO Contact Information

- Website: <https://dir.texas.gov/information-security/txisao>
- Mailing list sign up and threat reporting form
- Email: [ISAO@dir.texas.gov](mailto:ISAO@dir.texas.gov)

## DIR Cyber Operations (NSOC)

- Submit phishing emails as attachments for analysis: [security-alerts@dir.texas.gov](mailto:security-alerts@dir.texas.gov)

## DIR Cyber Incident Response Support

- 24x7x365 incident response and assistance hotline for state and local government organizations: [1-877-DIR-CISO](tel:1-877-DIR-CISO) (1-877-347-2476)

## Incident Response Resources

- DIR [Managed Security Services](#)
- Major Texas base cyber insurance risk pools:
  - [Texas Association of Counties \(TAC\)](#)
  - [Texas Municipal League \(TML\)](#)
  - [Texas Association of School Boards \(TASB\)](#)

# Building and Sustaining an Effective Security Program

## A Quote from Paul Proctor at Gartner

“Current thinking aligns to treating security like magic and security people like wizards who cast spells to protect the organization.”<sup>1</sup>

## People

- Empower your security professionals.
- Conduct realistic training and exercises for the entire organization.

## Processes

- Develop clear policies and procedures.
- Update and socialize documentation.

## Tools

- Conduct a proof of concept for new equipment.
- Ensure tools are effective and support your security program.





# Thank You

[CIRT@DIR.texas.gov](mailto:CIRT@DIR.texas.gov)

1-877-DIR-CISO (1-877-347-2476)



Texas Department of Information Resources

Transforming How  
Texas Government  
Serves Texans

[dir.texas.gov](http://dir.texas.gov) | [@TexasDIR](https://twitter.com/TexasDIR) | [#DIRisIT](https://twitter.com/hashtag/DIRisIT)