MENLO SECURITY

Zero Trust Through Isolation

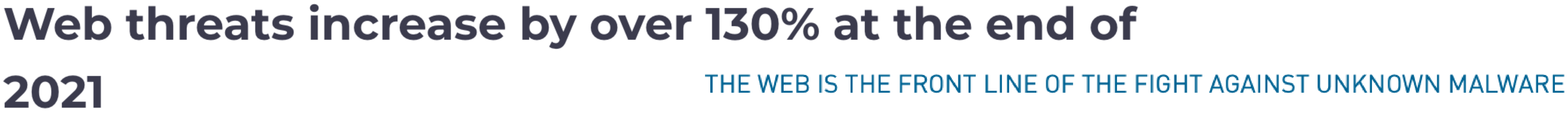
Trust Nothing.

Isolate Everything.

Threats Eliminated.

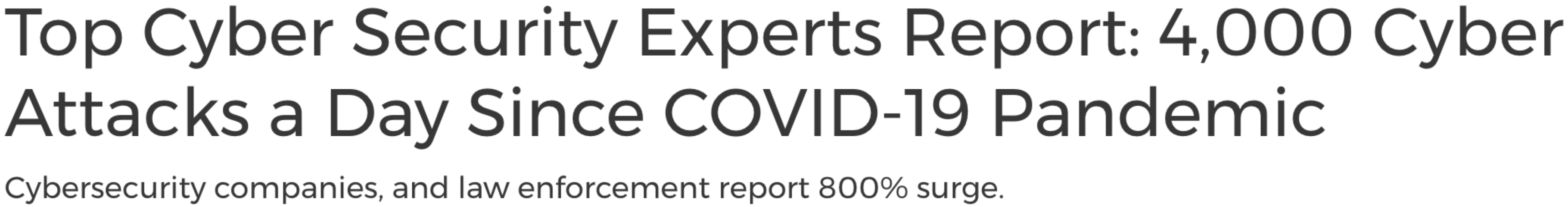
Goals for today

- Provide a technical overview of Browser Isolation and how it delivers on Zero Trust principles
- An overview of HEAT attacks and why customers need to understand these growing threats
- An understanding of the available resources including our HEAT check and how to use it
- Customer successes and use cases for browser isolation across public sector
- Solution demonstrations



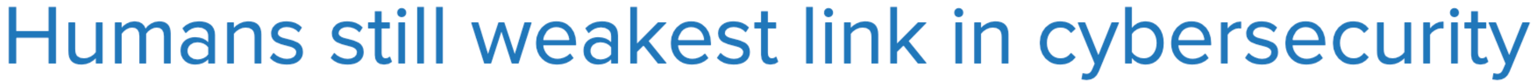
Web threats increase by over 130% at the end of 2021

THE WEB IS THE FRONT LINE OF THE FIGHT AGAINST UNKNOWN MALWARE

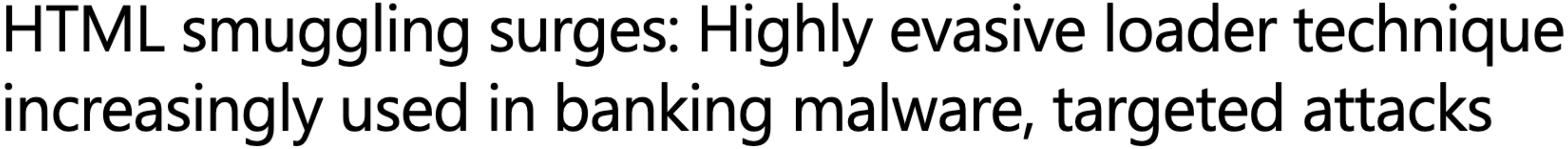


Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic

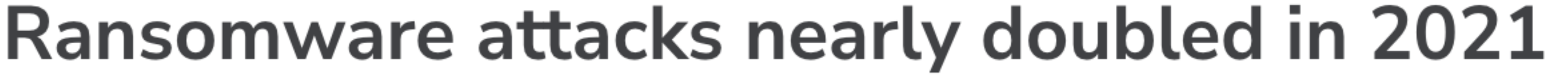
Cybersecurity companies, and law enforcement report 800% surge.



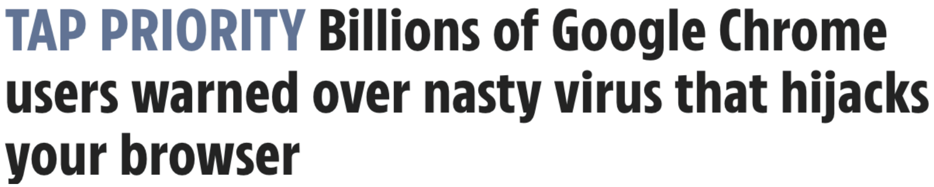
Humans still weakest link in cybersecurity



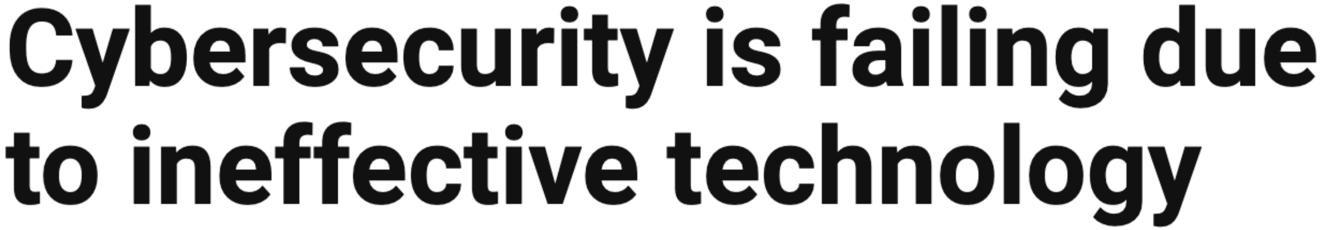
HTML smuggling surges: Highly evasive loader technique increasingly used in banking malware, targeted attacks



Ransomware attacks nearly doubled in 2021



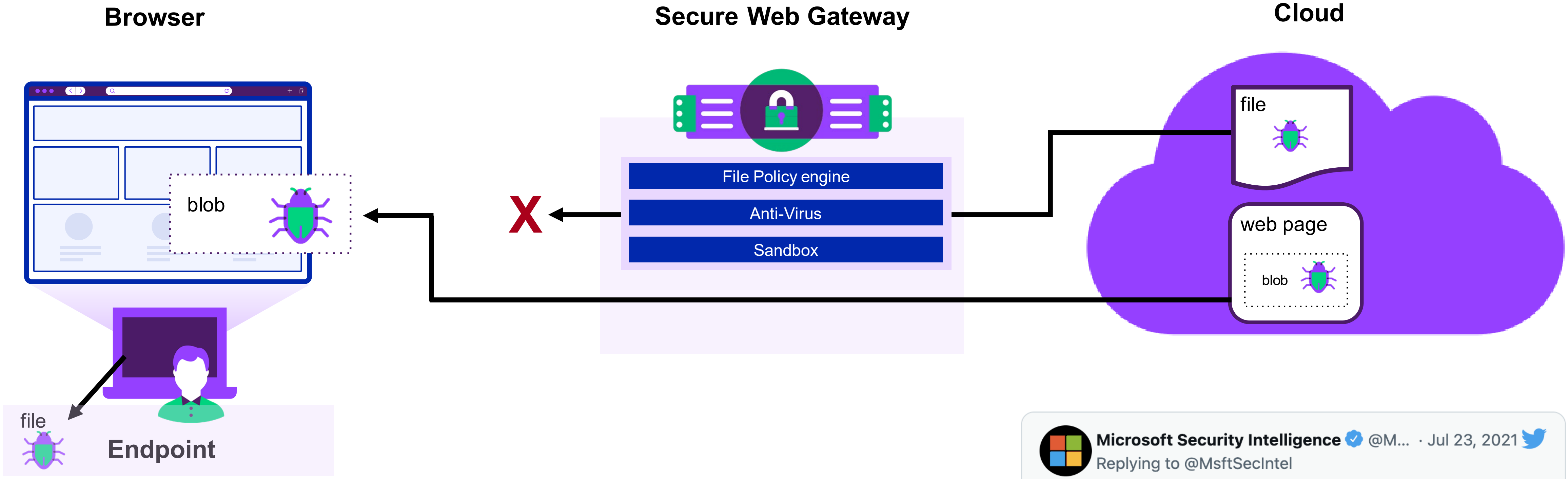
TAP PRIORITY Billions of Google Chrome users warned over nasty virus that hijacks your browser



Cybersecurity is failing due to ineffective technology

High Evasive Adaptive Threat (HEAT)

Tactic: HTML Smuggling



Browser

Secure Web Gateway

Cloud

blob

File Policy engine

Anti-Virus

Sandbox

X

file

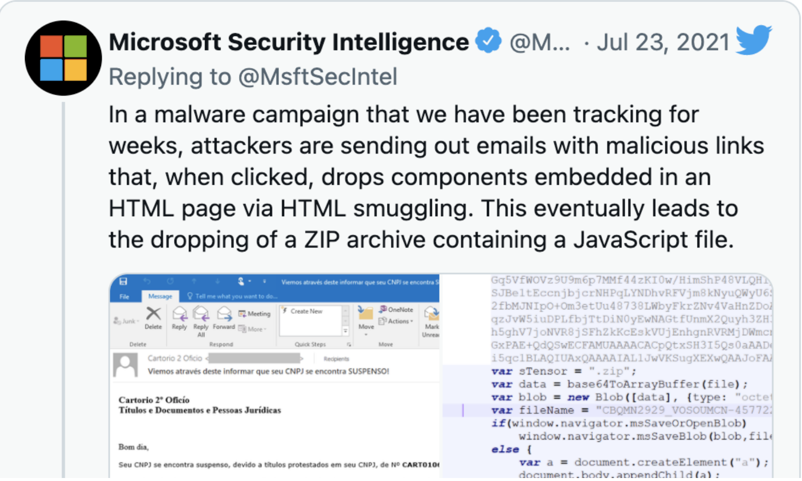
web page

blob

file

Endpoint

1. use evasive **HTML Smuggling technique** where the file content is constructed dynamically in html and JavaScript
2. **Evade content inspection** in the network and in SWG
3. Transparently **bypass file-based policy** and deliver unexpected files to the endpoint thus violating the endpoint posture



Microsoft Security Intelligence @M... · Jul 23, 2021

Replying to @MsftSecIntel

In a malware campaign that we have been tracking for weeks, attackers are sending out emails with malicious links that, when clicked, drops components embedded in an HTML page via HTML smuggling. This eventually leads to the dropping of a ZIP archive containing a JavaScript file.

Cartorio 2 Oficio <[redacted]>

Viemos através deste informar que seu CNPJ se encontra SUSPENSO!

Cartorio 2º Ofício
Títulos e Documentos e Pessoas Jurídicas

Bom dia,

Seu CNPJ se encontra suspenso, devido a títulos protestados em seu CNPJ, de Nº **CART010**

```
Gq5VfWOVz9U9m6p7MMf44zKI0w/HimShP48VLQH1
SJBeltEccnjbjcrNHPqLYNDhvRFVjm8kNyuQWyU6
2fbMJNIpO+Om3etUu48738LWbyFkrZNv4VaHnZDo
qzJvW5iuDPLfbjTtDiN0yEwNAGtfUnmX2Quyh3ZH
h5ghV7joNVR8jSFhZkKcEskVUjEnhgnRVRMjDWmc
GxPAE+QdQSwECFAMUAAAACACpQtxSH3I5Qs0aAAD
i5qc1BLAQIUAxQAAAAIAL1JwVKSugXEXwQAAJoFA
var sTensor = ".zip";
var data = base64ToArrayBuffer(file);
var blob = new Blob([data], {type: "octe
var fileName = "CBQMN2929_VOSOUMCN-45772
if(window.navigator.msSaveOrOpenBlob)
    window.navigator.msSaveBlob(blob,file
else {
    var a = document.createElement("a");
    document.body.appendChild(a);
```

HEAT: Highly Evasive Adaptive Threats

This family of threats uses innovative techniques to evade all existing security defenses.
HEATs usually feature one or more of the following characteristics:

1. Evades URL filtering

Termed Legacy URL Reputation Evasion (LURE), sites classified as benign by categorization engines are compromised and then used for malicious purposes, bypassing indicators of compromise-based detection.

2. Evades email security tools

SEGs and email link analysis are bypassed by leveraging additional phishing avenues outside the email path such as web, social media, professional networks, collaboration tools and SMS phishing techniques.

3. Evades file-based inspection

File content inspection engines completely bypass traditional Secure Web Gateway (SWG) anti-virus or sandbox solutions.

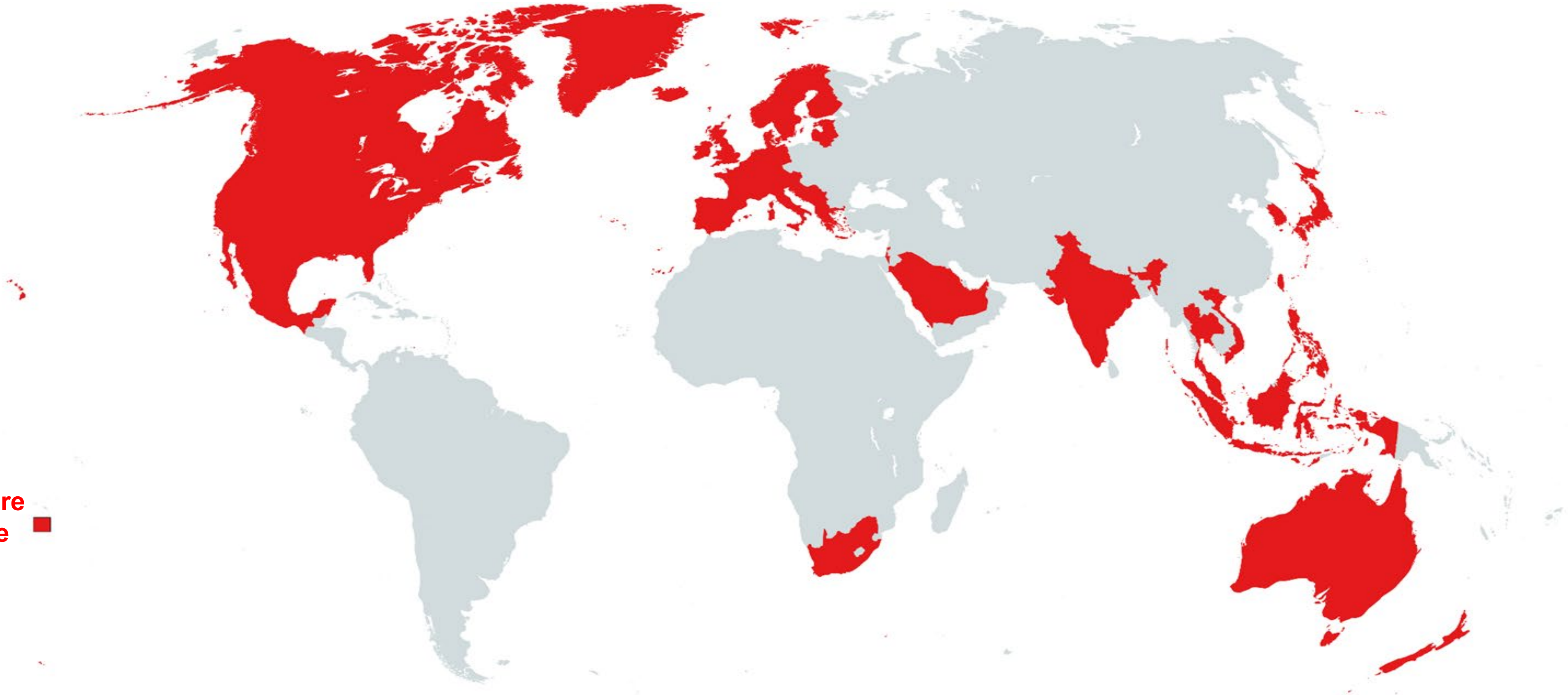
4. Evades HTTP content/page inspection

Malicious content like browser exploits and phishing kit code are hidden or obfuscated to make the Javascript unreadable in order to bypass detection.

Evasive Techniques

Type	Details
URL Filter Reputation Evasion	Malicious sites that evade legacy URL reputation checks - compromised websites, Web hosting sites (e.g., Weebly, Single-use, NRDs
Data Encoding	Refers to all forms of content modification for the purpose of hiding intent
Data Exfiltration (C2)	Use of compression, encryption and packaging to steal data, includes transferring it over command and control (C2) or alternate channels (with size limits on data transmissions).
Code Obfuscation	Source code obfuscation can be defined as making a program unintelligible while maintaining its functionality, intended to make it difficult for a human to understand or reverse-engineer.
HTML Smuggling	Leverages legitimate HTML5 and JavaScript browser features to dynamically generate malicious payloads that bypass existing network-based defenses.
Geo-Fencing	Used to prevent exposure of (threat) capabilities in environments not intended to be compromised or operated within e.g. specific regions.
Malware Engine Bypass e.g. 0-hour malware / not previously seen	Attempts to detect and avoid analysis by sandboxes and malware engines. Includes malware that checks to determine if host is a Virtual machine or presence of Instrumentation / “API Hooks”
File Encryption	Use of encrypted files and archives to deliver malicious payloads. By encrypting the attachment, conventional antivirus programs and malware inspection engines are unable to detect and block hidden malware

HEAT attacks detected in all regions and verticals



Menlo Regions Where HEAT Attacks Have Been Detected 🟥

Telecom

Retail

Manufacturing

Transport

Government

Finance

Utilities

Entertainment

Insurance

Key Trends

50%+

Of HEAT attacks seen come from categorized websites

42%

Of malware delivered as archive (HP Wolf Security Threat Insights Report)

73%

Of Legacy URL Reputation Evasion (LURE) attacks come from categorized websites

70%

Increase In LURE attacks in 2022

90 Day Threat Stats

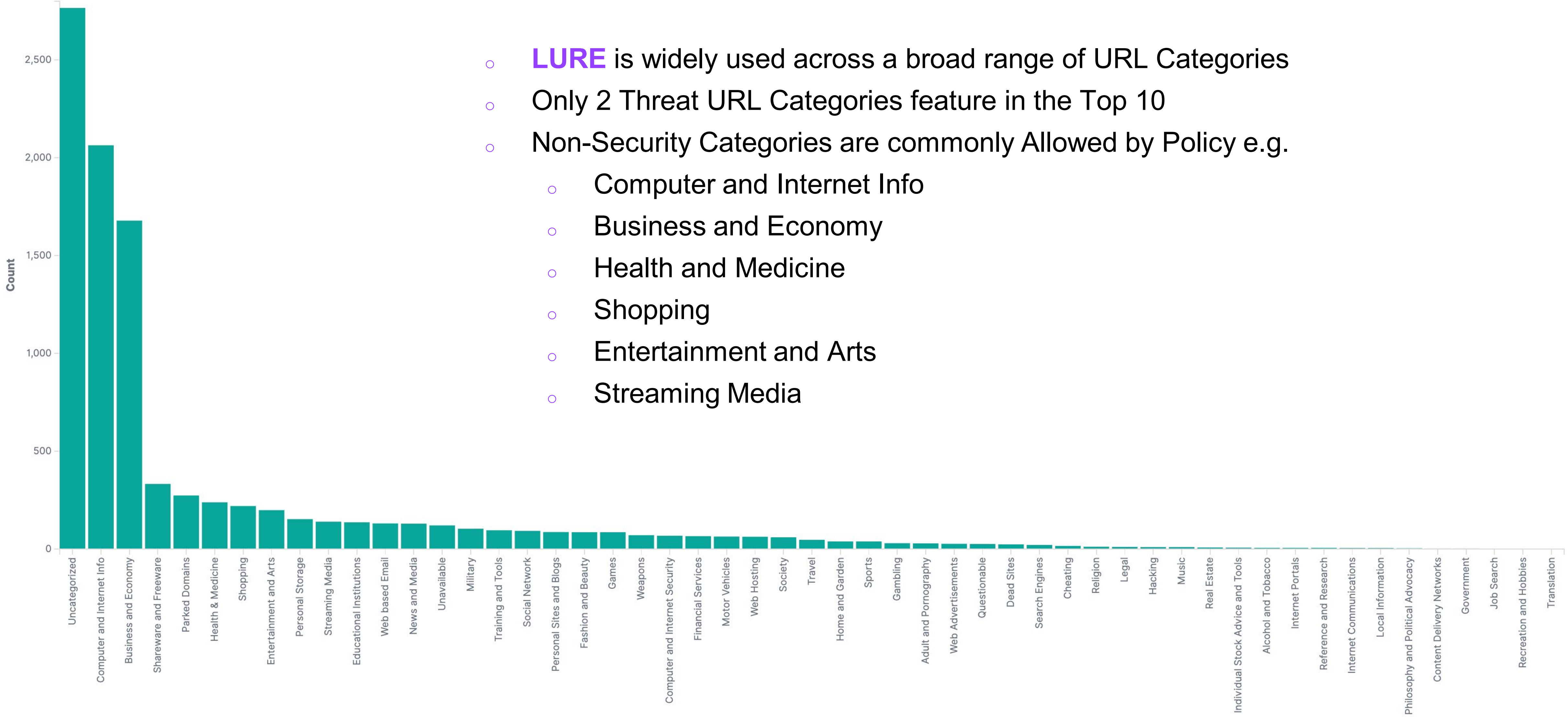
1 in 5

Infected Files of Last 90 Days is HTML Smuggling

1.5M+

PW Protected Files Detected In Last 90 Days

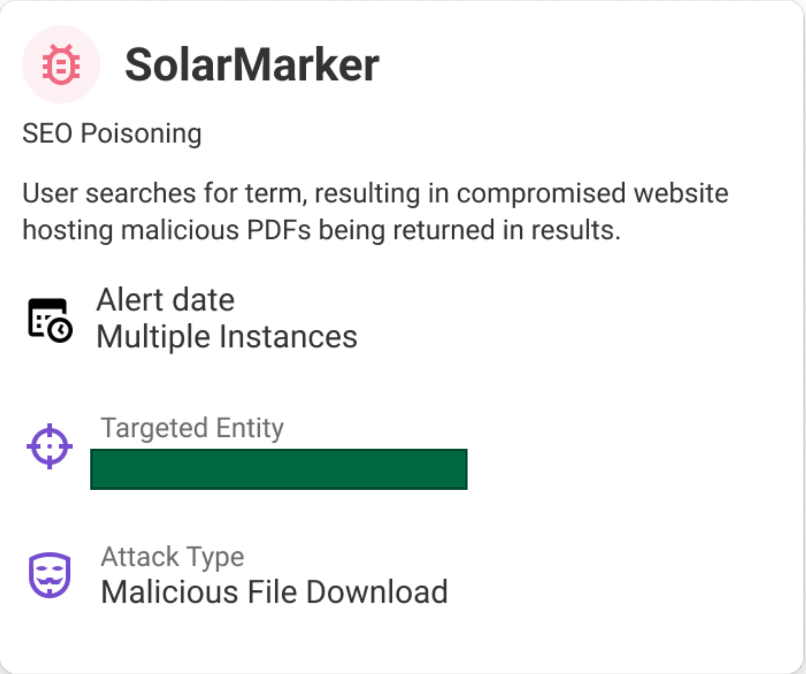
Evidence | LURE attempts via Menlo Security



- LURE is widely used across a broad range of URL Categories
- Only 2 Threat URL Categories feature in the Top 10
- Non-Security Categories are commonly Allowed by Policy e.g.
  - Computer and Internet Info
  - Business and Economy
  - Health and Medicine
  - Shopping
  - Entertainment and Arts
  - Streaming Media

Notable Attacks

90 Days



SolarMarker

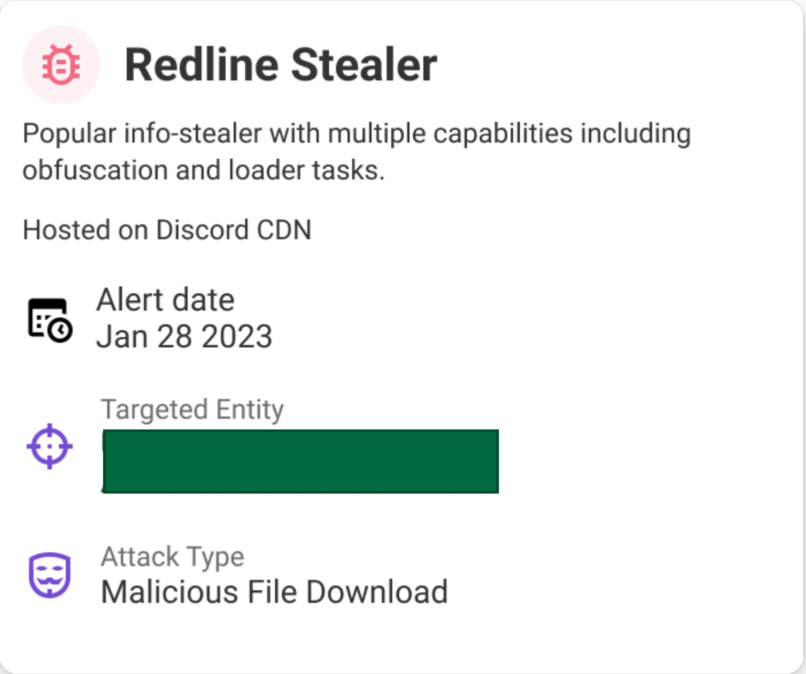
SEO Poisoning

User searches for term, resulting in compromised website hosting malicious PDFs being returned in results.

Alert date
Multiple Instances

Targeted Entity
[redacted]

Attack Type
Malicious File Download



Redline Stealer

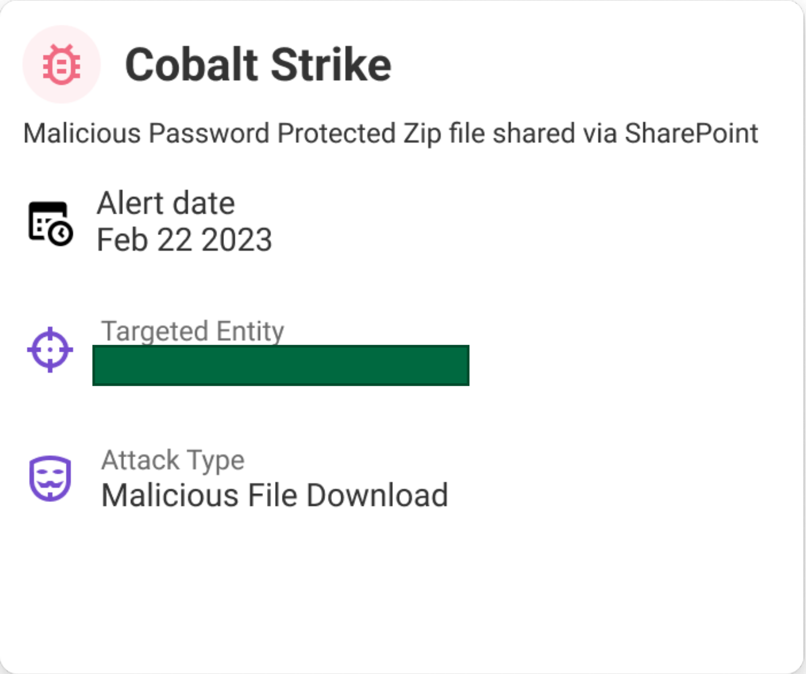
Popular info-stealer with multiple capabilities including obfuscation and loader tasks.

Hosted on Discord CDN

Alert date
Jan 28 2023

Targeted Entity
[redacted]

Attack Type
Malicious File Download



Cobalt Strike

Malicious Password Protected Zip file shared via SharePoint

Alert date
Feb 22 2023

Targeted Entity
[redacted]

Attack Type
Malicious File Download

SolarMarker

User searches for term, resulting in compromised website hosting malicious PDFs being returned in results.

Some other text.....

Alert date
Multiple instances

Targeted Entity
[redacted]

Attack Type
Malicious File Download

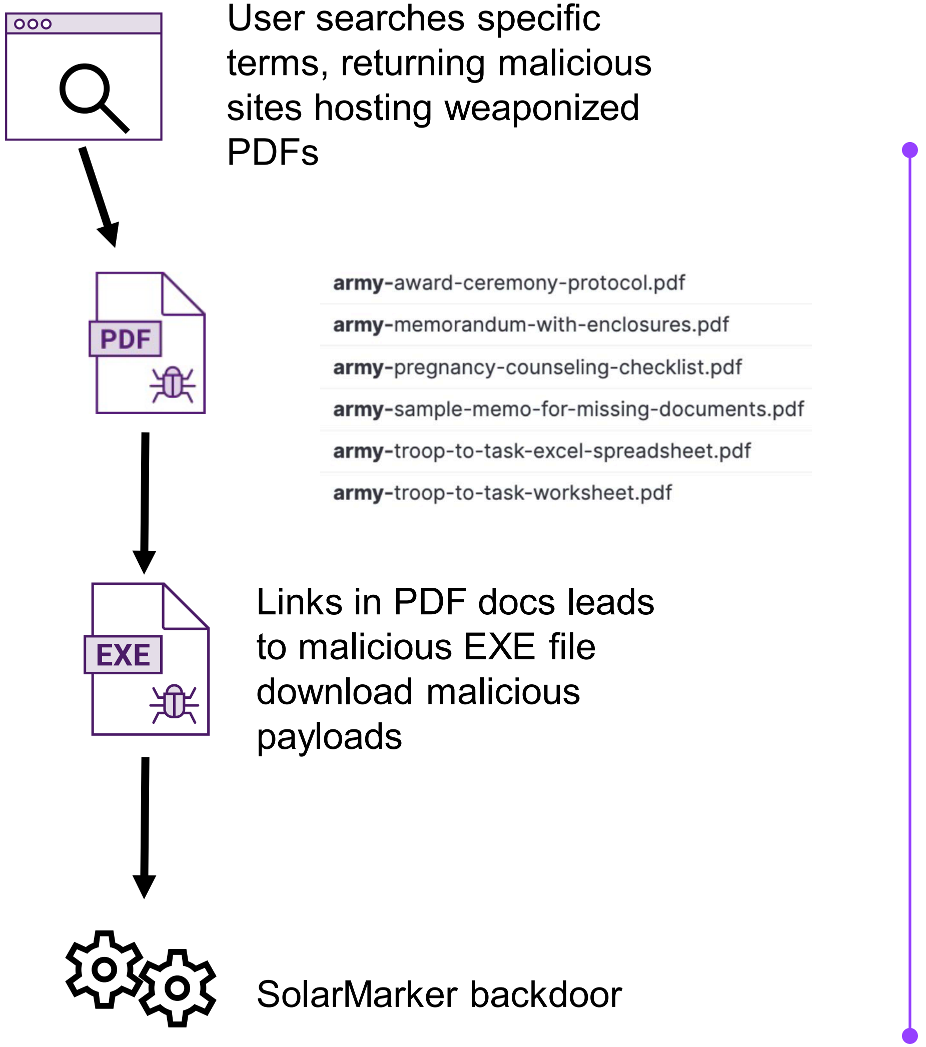
Initial Access Method
SEO Poisoning

Evasive Techniques
URL category evasion

File Details
Multiple PDF files - see image

Domain
Multiple (hosted on Wordpress sites)

Insights Query
file_type=PDF virus="Document-PDF.Phishing.PhishingX" | top(tid, limit=1000)



User searches specific terms, returning malicious sites hosting weaponized PDFs

army-award-ceremony-protocol.pdf
army-memorandum-with-enclosures.pdf
army-pregnancy-counseling-checklist.pdf
army-sample-memo-for-missing-documents.pdf
army-troop-to-task-excel-spreadsheet.pdf
army-troop-to-task-worksheet.pdf

Links in PDF docs leads to malicious EXE file download malicious payloads

SolarMarker backdoor

Cobalt Strike

Malicious Password Protected Zip file shared via SharePoint

Alert date
Feb 22 2023

Targeted Entity
[redacted]

Attack Type
Malicious File Download

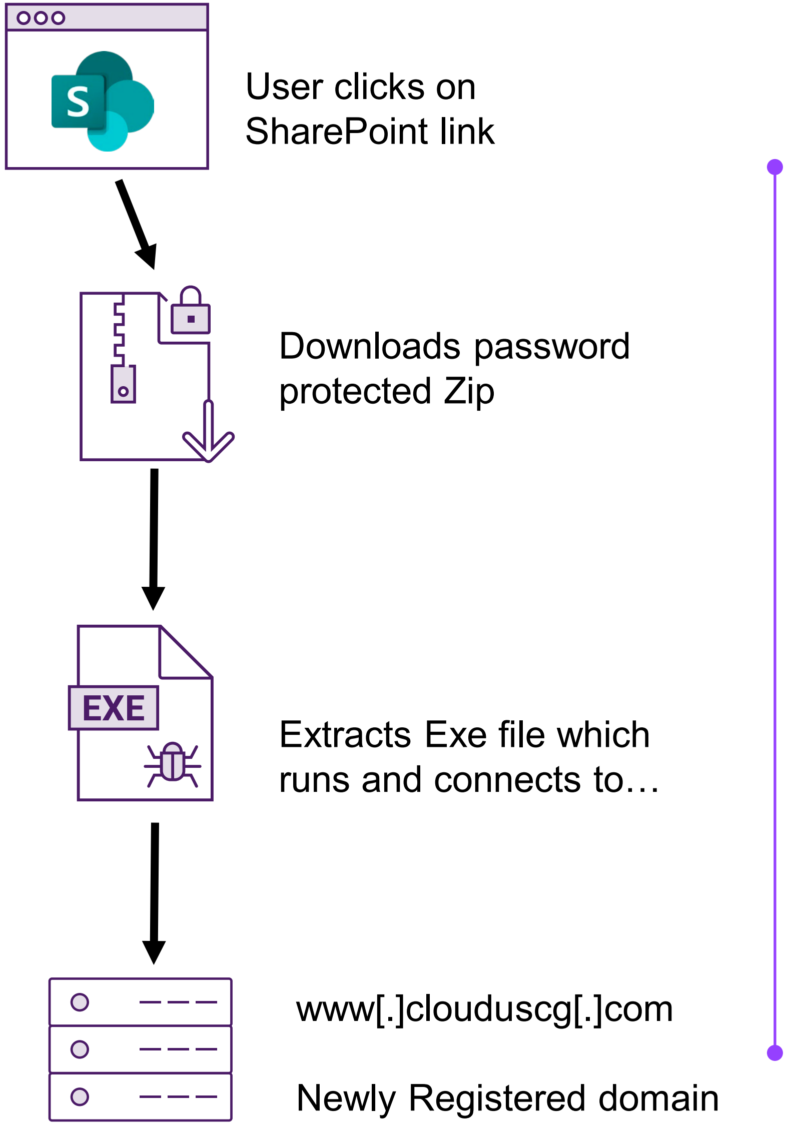
Initial Access Method
Archive shared via Sharepoint

Evasive Techniques
Pwd Protected Archive
URL category evasion

File Details
download1.zip

Domain
firstinfotech-my.sharepoint.com

Insights Query
domain='firstinfotech-my.sharepoint.com' | top(tid)



User clicks on SharePoint link

Downloads password protected Zip

Extracts Exe file which runs and connects to…

www[.]clouduscg[.]com

Newly Registered domain

Redline Stealer

Popular info-stealer with multiple capabilities including obfuscation and loader tasks.

Hosted on Discord CDN

Alert date
Jan 28 2023

Targeted Entities
[redacted]

Attack Type
Malicious File Download

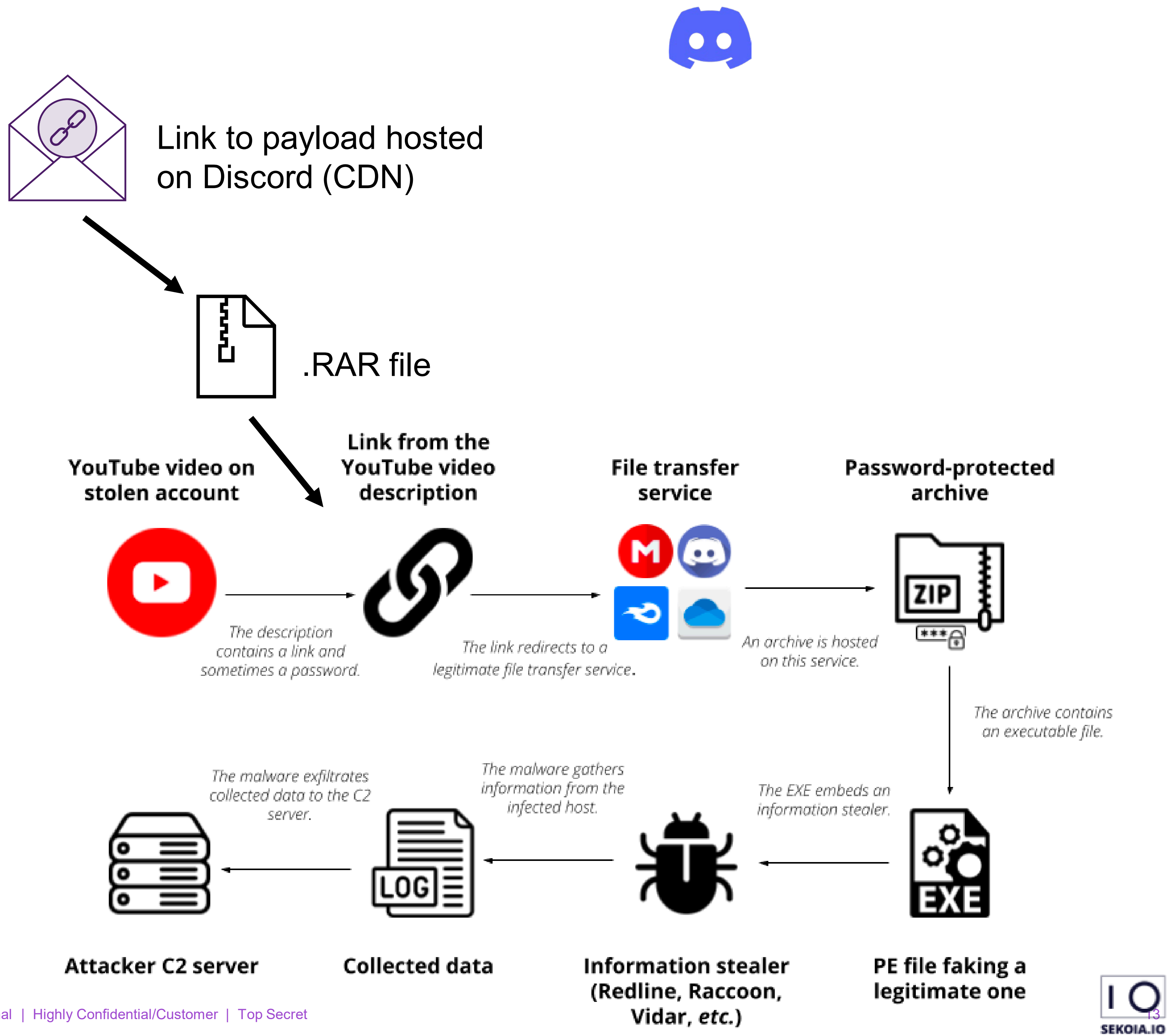
Initial Access Method
Malicious file hosted on DISCORD

Evasive Techniques
URL category evasion
RAR Archive

File Details
UpdaterBrowsers.rar

Domain
cdn.discordapp.com

Insights Query
filename=UpdaterBrowsers.rar
domain=cdn.discordapp.com



Link to payload hosted on Discord (CDN)

.RAR file

YouTube video on stolen account
Link from the YouTube video description
File transfer service
Password-protected archive
The description contains a link and sometimes a password.
The link redirects to a legitimate file transfer service.
An archive is hosted on this service.
ZIP
The archive contains an executable file.
The malware exfiltrates collected data to the C2 server.
The malware gathers information from the infected host.
The EXE embeds an information stealer.
LOG
EXE
Attacker C2 server
Collected data
Information stealer (Redline, Raccoon, Vidar, *etc.*)
PE file faking a legitimate one

HEAT DEMO

CISA Capacity Enhancement Guide

"Embraced by the Department of Defense and major corporations, browser isolation is a strategic architectural decision."

Internet browser isolation provides the following benefits:

- Isolates potential malicious code and content within the "protected" cloud platform, separating the threat from direct connections to the host operating system, eliminating ransomware attacks, and allowing users to click on any website
- Reduces the need for website allow listing and blocklisting and for web browser security user training
- Gives administrators the flexibility to set tunable policies ranging from isolating a portion of traffic to isolating every download, attachment, and link
- Diminishes significant attack avenues by substantially reducing file risk content when coupled with a file-transfer solution to permit webmail and webpage document downloads (i.e., a "save as" to local storage)
- Provides a rich source of insider threat intelligence within the virtual browser logs because it allows users to visit high-risk websites
- Neutralizes existing malware in the network by disrupting the link to the command-and-control site
- Does not increase the browser's memory usage, slow processing, or adversely impact the user's web browsing experience—unlike the site isolation capability currently offered by most web browsers

Three Common Techniques for RBI

Pixel Streaming

- Continuous sequence of images from the remote browser to the endpoint

DOM Mirroring

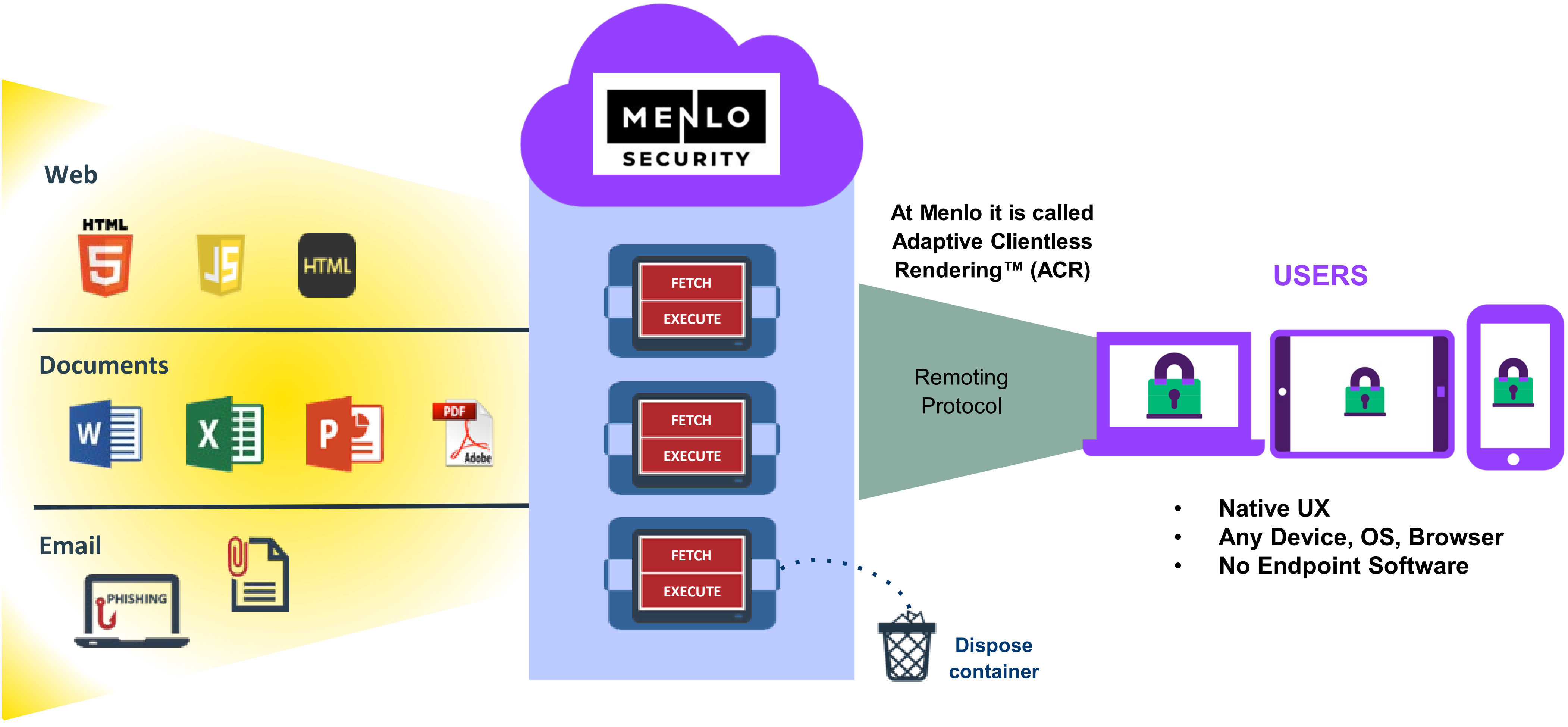
- Document Object Model (DOM) is created by the remote browser after executing all the active code
- DOM is copied from the remote browser to the user's endpoint browser

Draw Operations

- Draw operations are sent from the remote browser to the user's browser
- Some vendors calls this Vector Rendering

Menlo's RBI – Dual-Engine Isolation Platform

Menlo Security Isolation Platform uses both DOM mirroring and Draw Operations



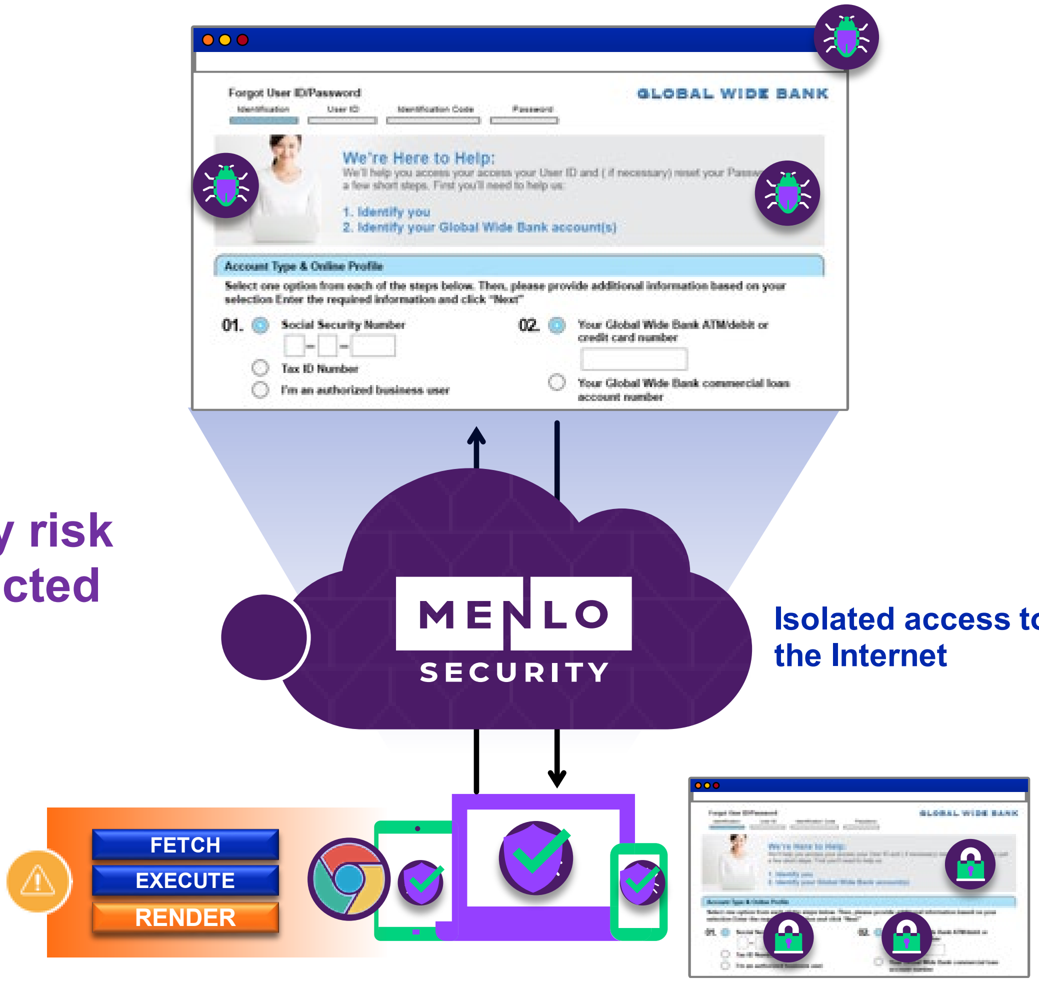
At Menlo it is called Adaptive Clientless Rendering™ (ACR)

- Native UX
- Any Device, OS, Browser
- No Endpoint Software

Zero Trust Internet Powered by Isolation

Trust Nothing, Isolate Everything

Users Isolated from any risk while allowing unrestricted Internet access.



Forgot User ID/Password

Identification | User ID | Identification Code | Password

GLOBAL WIDE BANK

We're Here to Help:

We'll help you access your access your User ID and (if necessary) reset your Passw... a few short steps. First you'll need to help us:

1. Identify you
2. Identify your Global Wide Bank account(s)

Account Type & Online Profile

Select one option from each of the steps below. Then, please provide additional information based on your selection Enter the required information and click "Next"

01. ● Social Security Number

○ Tax ID Number

○ I'm an authorized business user

02. ● Your Global Wide Bank ATM/debit or credit card number

○ Your Global Wide Bank commercial loan account number

Isolated access to the Internet

Result with Isolation:

Users isolated from any risk

HEAT Attacks Prevented by the Menlo Isolation Platform

Key characteristics of a mature RBI solution…

- No change to user experience.
  - -Support any device, any OS, any browser.
  - -No change or limitation to the functionality of the web browser. (e.g., no tab limitations, no read-only URL bars)
  - -No change to web page rendering, interaction, and collaboration.
  - -No latency or increase in bandwidth
- No limitations to URLs or web categories that can be Isolated.
- Document & archive isolation is essential.
- No agent required.
- Easy deployment.
- Low-touch management.
- Extensible & scalable.

RBI DEMO

Menlo Security for Federal Government:

US Department of Defense and 60+ Mission Partners

Challenges:

- Web browser is biggest threat vector
- Slow web experience
- Increasing costs to maintain on-prem security
- Bandwidth challenges, and growing download and backhaul costs

Results:

- Protect 3.5 million users against HEAT attacks
- Reduced VPN traffic by 44%
- Cost savings of $300M
- Improved web experience
- Complete visibility
- Remote worker protection
- Bandwidth savings

Menlo Capabilities

- Secure Web Gateway
- Cloud Access Security Broker
- Data Loss Prevention
- Remote Browser Isolation

Proven, Effective, Scalable, Mission Enabler.

“CBII has been that solution that enables mission partners to solve their bandwidth constraints, especially in response to mass telework due to COVID-19,”

“For mission partners who are operating in low-bandwidth, high-latency environments, CBII has been the solution for them to conserve bandwidth for their mission-essential functions.”

Laurel Lashley, DISA’s CBII program manager (2021)

Reference: https://fcw.com/it-modernization/2021/04/can-disas-cbii-make-dod-telework-more-secure/258194/

“Beyond improved performance or latency reduction, many users are unaware that they’re even doing something different,” she said. “All the users generally have to do is browse, except now their browsing occurs in the isolated container, and all internet-born browser code is executed outside of the DODIN. Therefore, users are protected against any recent zero-day browser vulnerabilities.”

Laurel Lashley, DISA’s CBII program manager (2021)

Reference: https://fcw.com/it-modernization/2021/04/can-disas-cbii-make-dod-telework-more-secure/258194/

“The user’s web browsing experience is greatly improved by the increased bandwidth and reduced access time for commercial websites…CBII reduces load times by up to 50%…..while providing greater security against malicious web-based code.”

“Powers said the DoD stands to save about $130 million in costs due to incident reduction through the 2024 fiscal year.”

Dale Powers, IT Specialist, Fort Knox, US Army (2021)

Reference: https://www.army.mil/article/247605/new_it_initiative_promises_safer_faster_web_browsing_experience_for_dod_employees

"CBII is proving to be a game-changing solution in our ability to protect department networks against web browser-based threats, making them more secure from the office or from home,”

Navy Vice Adm. Nancy A. Norton, DISA director (2021)

Reference: https://www.defense.gov/News/News-Stories/Article/Article/2465443/disa-director-touts-benefits-of-cloud-computing-telework/

Zero Trust + Isolation

Go together like peanut butter and jelly

- Isolation = Trust nothing
- Zero Trust = Never trust

Executive Office of the President

Zero Trust Cybersecurity Principles

"Agencies must develop a Zero Trust architecture plan that describes the agency's approach to environmental isolation in consultation with CISA"

Highlights:

- Agencies **must develop a Zero Trust architecture plan** that describes the agency's approach to environmental isolation in consultation with CISA and submit it to OMB as part of their Zero Trust implementation plan.

- In SP 800-207, NIST describes several approaches to a Zero Trust architecture (ZTA) for enterprise workflows: enhanced identity governance, logical micro-segmentation, and network-based segmentation. Each of these approaches has the same goal: **to meaningfully isolate environments**, so that an adversary that compromises one application or component cannot easily move laterally within an organization and compromise other distinct environments.

- Mature cloud platforms typically feature strong identity- and attribute-based access control and rely on identity governance and **virtualized logical isolation of environments**. As a result, they are well optimized for zero trust architectures, and agencies are expected to make robust, secure use of cloud-based infrastructure.

Zero Trust Fun Fact

John Kindervag
Founder / Creator of Zero Trust

BORN IN
NEBRASKA

UNIVERSITY OF
Nebraska
Lincoln

Summary

A mature RBI platform will deliver a native browsing experience. No URL or category limits, no special browsers, no change in UX, scalable.

Isolation is a force multiplier – users have more freedom to navigate the web with zero risk, organizations align with Zero Trust principles.

Advanced threats (HEAT) and browser zero-days cannot be stopped with legacy security tooling. Isolation is the only preventative solution.

Zero Trust and RBI go hand in hand | Default Never Trust

Isolation removes the weakest link – the user!

Let’s Connect!

Mike Rider
Solutions Architect
Menlo Security – Public Sector

Mike.Rider@menlosecurity.com