Manufacturing Threat Landscape

Manufacturers Alliance April 2024

eSENTIRE

Threat Response Unit

Presenter

Spence

Hutchinson

Staff Threat Intelligence Researcher,
Threat Response Unit

eSENTIRE Threat Response Unit

Key Takeaways From TRU Research

THREAT INTELLIGENCE SPOTLIGHT

Increasing Cyber Resilience Against Cyber Threats Impacting the Manufacturing Industry

- IT transformation + growing attack surface.
- Ransomware remains a major concern.
- Intrusions stemmed from compromised identities or known vulnerabilities.
- Browser-based malware on the rise.

- Businesses in manufacturing were the most victimized industry sector by ransomware.
- SMBs made up the majority of all victims.
- Threat Opportunity: Manufacturing orgs had higher exposure to underground services such as credential markets.

RANSOMWARE REPORT

Ransomware Readiness: How SMBs Can Prepare for the Rising Threat of Ransomware-as-a-Service, Initial Access Brokers, and Credential Theft

January 2024

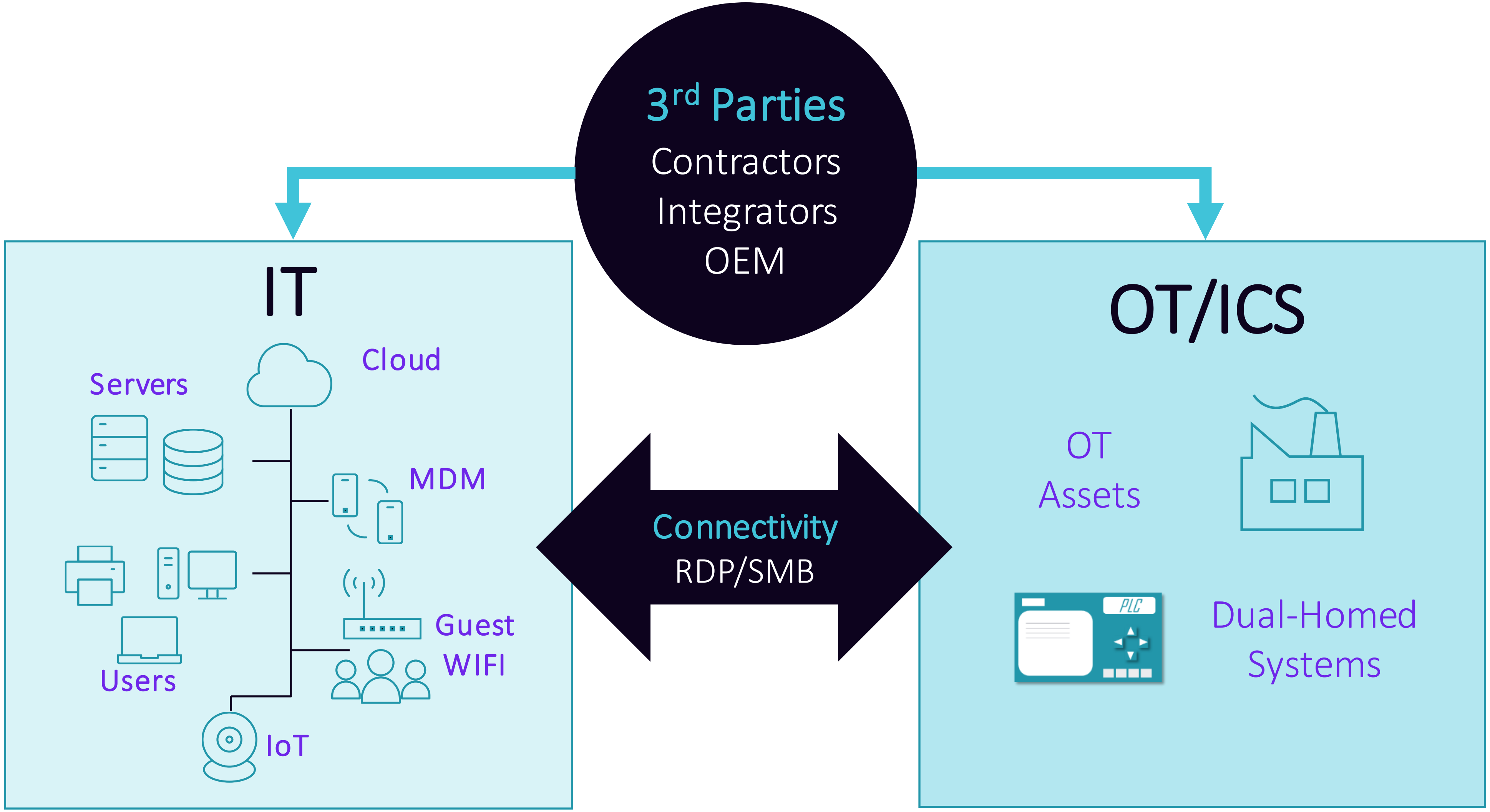
Technology Transformation Enables Efficiency But Increases Attack Surface

Cloud Migration

Edge Devices

Remote Access Services

Threat Surface Scope Creep



eSentire
Threat Response Unit

Threat Surface Scope Creep – Visibility Lagging Behind

80%

Of manufacturing organizations have limited visibility into their environments

- Dragos, ICS/OT Cybersecurity Year in Review 2022

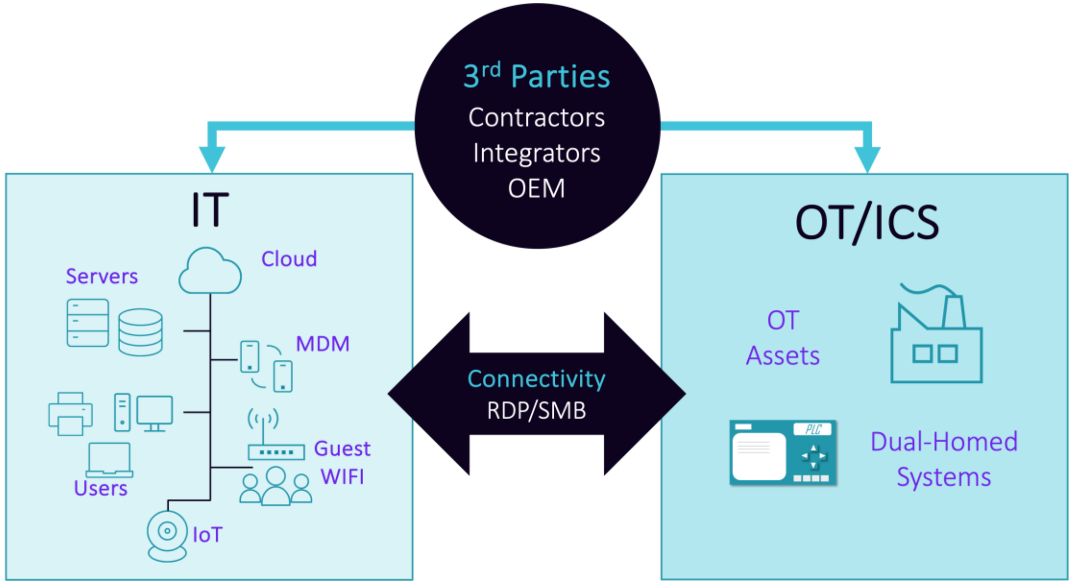
Majority of intrusions leveraged valid credentials or unpatched vulnerabilities

- eSentire Threat Intelligence Spotlight 2023

Ask Your Team

- ❑ Do we have phish-resistant MFA?
- ❑ How are we prioritizing vulns?
- ❑ Can unmanaged devices access network resources?
- ❑ How are we monitoring? North/South? East/West?

RE: Vendors. Trust, But Verify



eSENTIRE Threat Response Unit

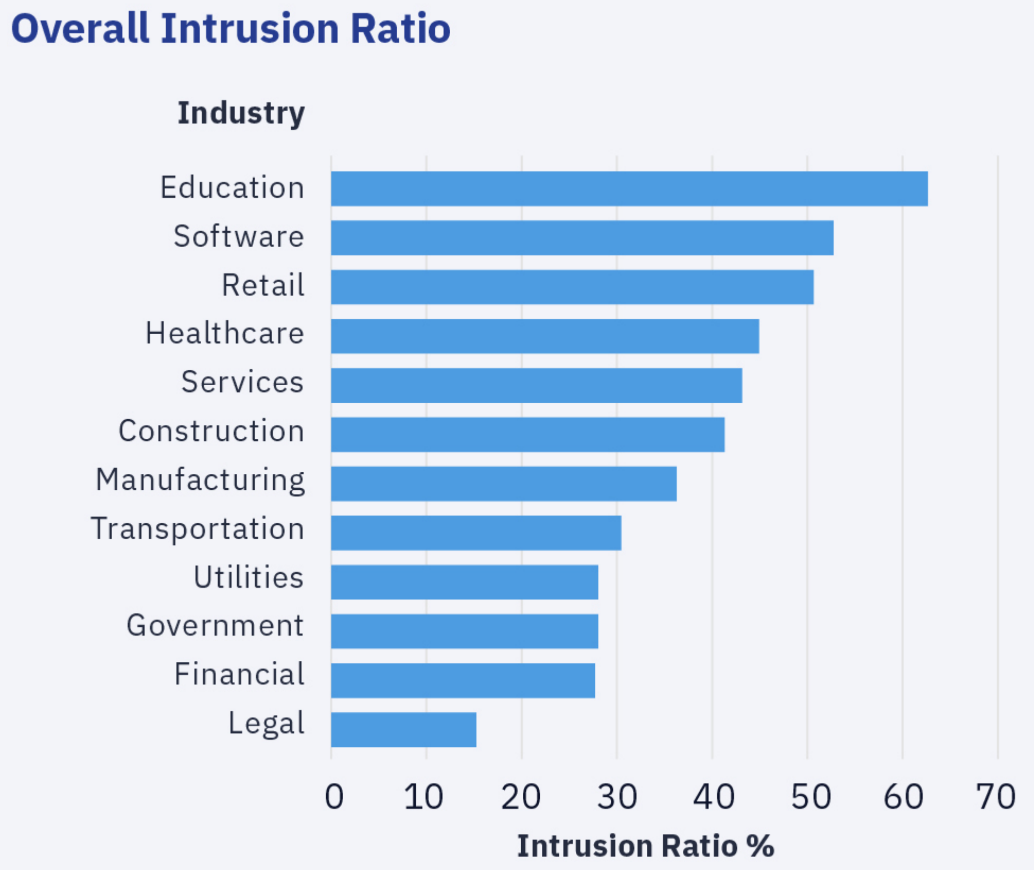
Attack Trends

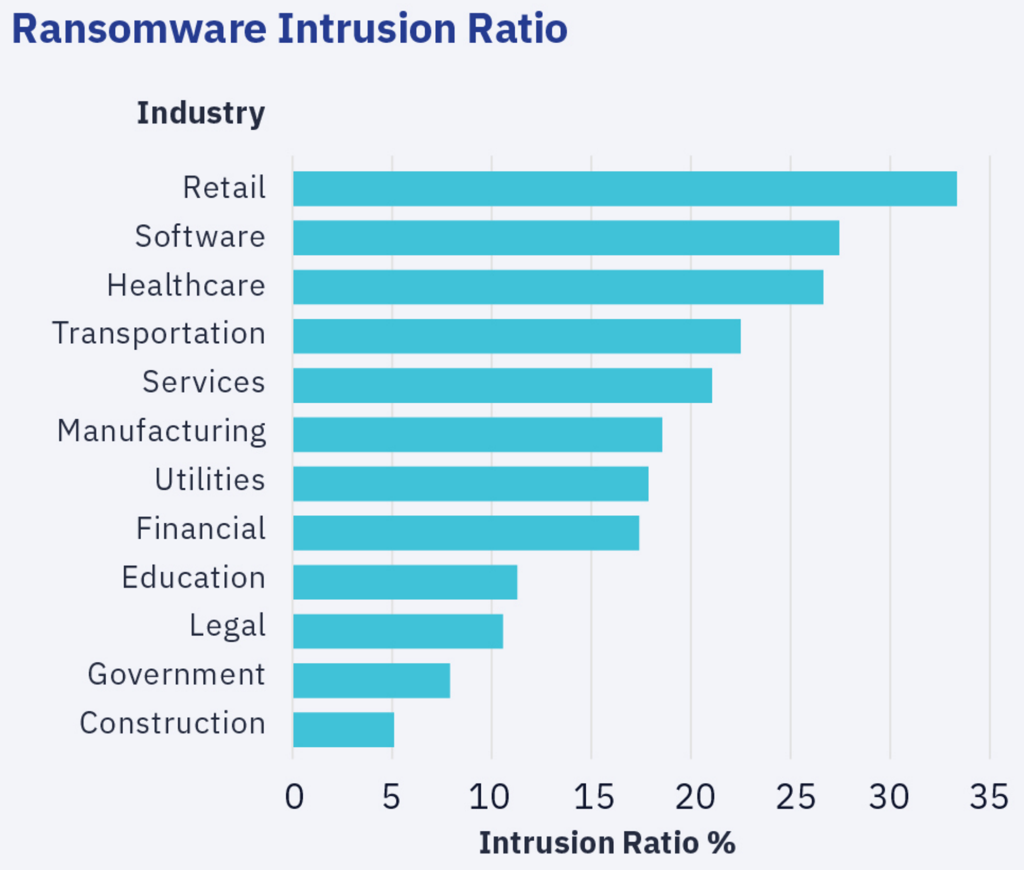
Web Browsing Threats

Email Threats

Unmanaged Devices

Industry Intrusion Ratios





Initial Access Trends

Email outpaced by browser-based attacks

Browser Attacks

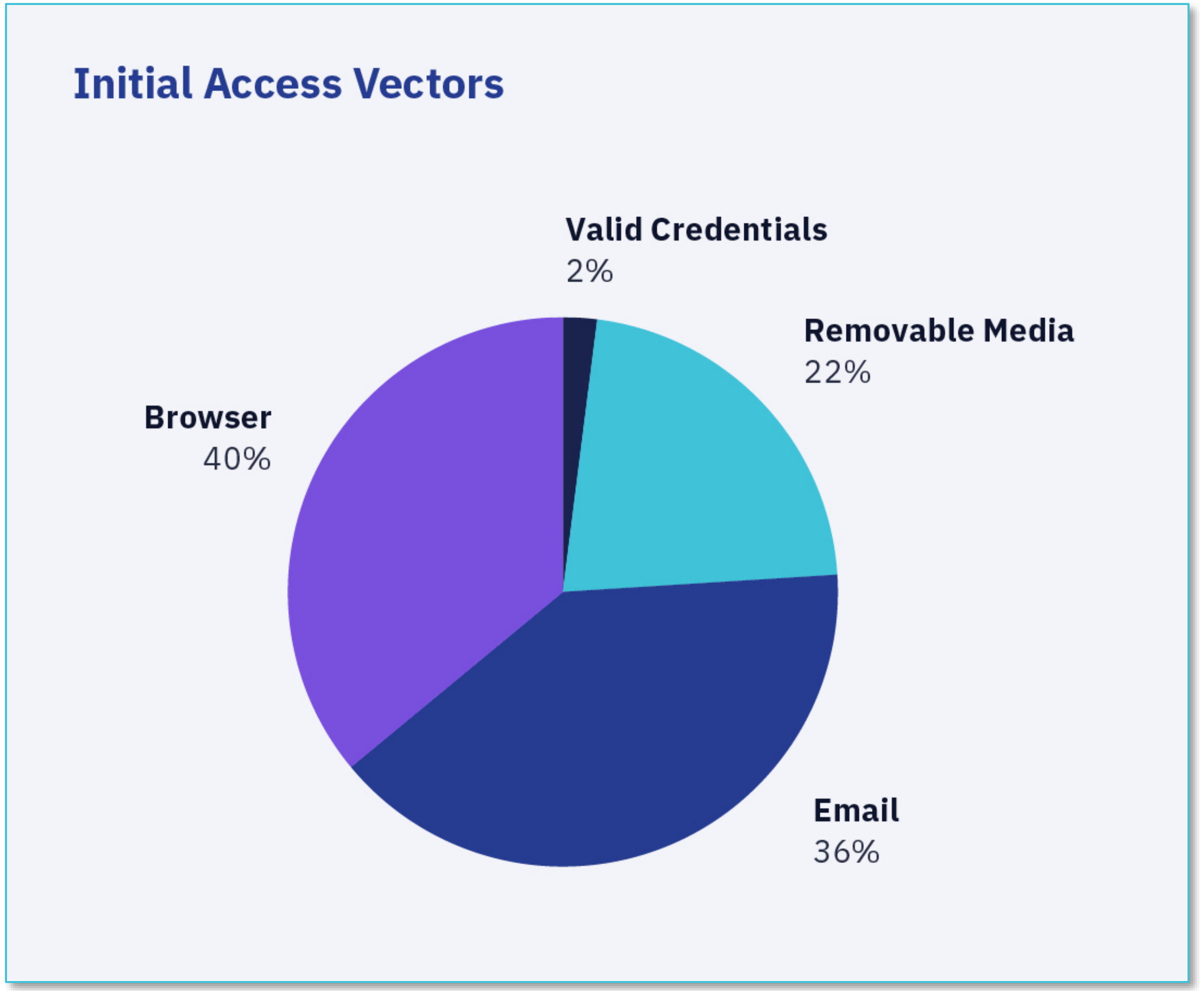
- Fake Browser Update
- Malicious Search Advertisement
- Malicious Search Result

USB Worms a concern for manufacturing

- Raspberry Robin

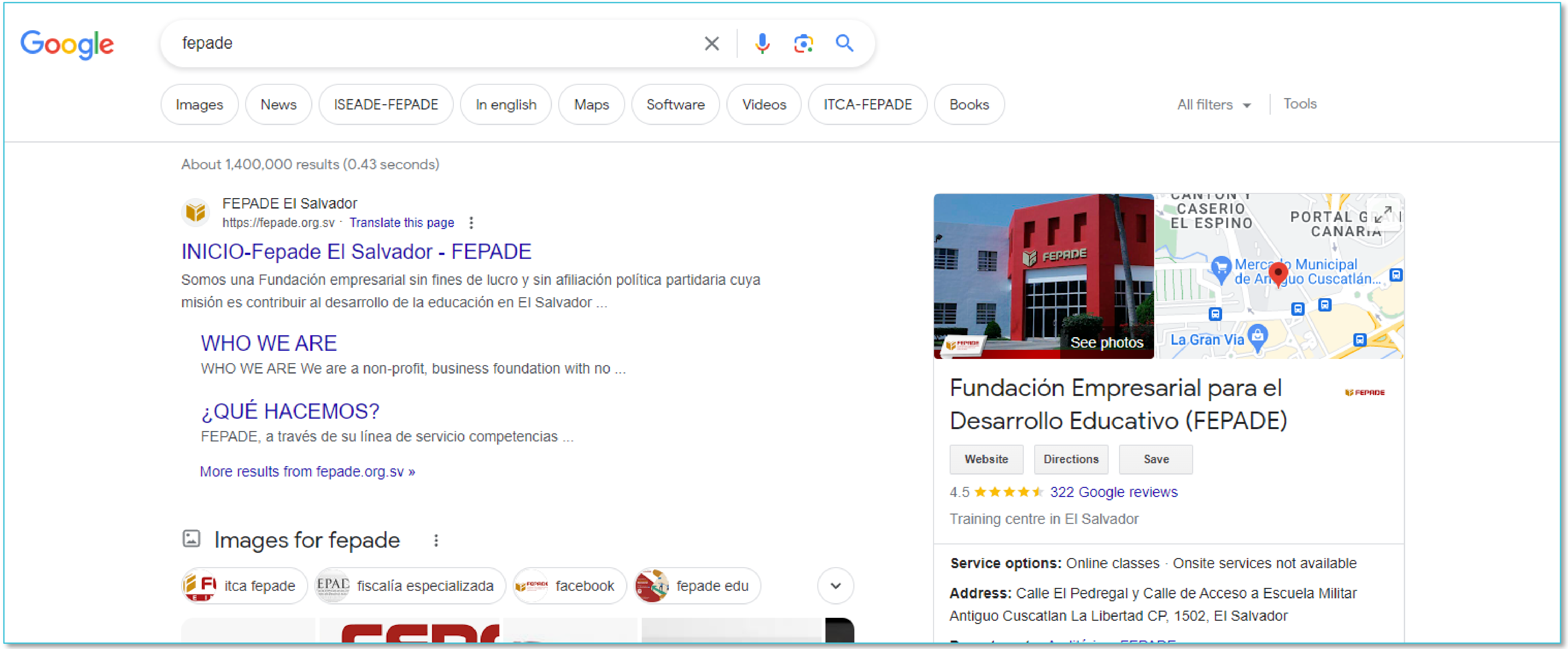
Valid Credentials

- Low volume but high impact



Initial Access Vectors

Web Threat Example – Clear Fake Campaign



fepade

Images · News · ISEADE-FEPADE · In english · Maps · Software · Videos · ITCA-FEPADE · Books · All filters · Tools

About 1,400,000 results (0.43 seconds)

FEPADE El Salvador
https://fepade.org.sv · Translate this page

INICIO-Fepade El Salvador - FEPADE

Somos una Fundación empresarial sin fines de lucro y sin afiliación política partidaria cuya misión es contribuir al desarrollo de la educación en El Salvador ...

WHO WE ARE

WHO WE ARE We are a non-profit, business foundation with no ...

¿QUÉ HACEMOS?

FEPADE, a través de su línea de servicio competencias ...

More results from fepade.org.sv »

Images for fepade

itca fepade · fiscalía especializada · facebook · fepade edu

FEPADE
See photos
CANTON Y CASERIO EL ESPINO
PORTAL GRAN CANARIA
Mercado Municipal de Antiguo Cuscatlán...
La Gran Via

Fundación Empresarial para el Desarrollo Educativo (FEPADE)

Website · Directions · Save

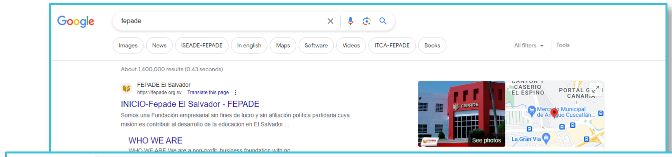
4.5 ★★★★★ 322 Google reviews

Training centre in El Salvador

Service options: Online classes · Onsite services not available

Address: Calle El Pedregal y Calle de Acceso a Escuela Militar Antiguo Cuscatlan La Libertad CP, 1502, El Salvador

Web Threat Example – Clear Fake Campaign



fepade

Images · News · ISEADE-FEPADE · In english · Maps · Software · Videos · ITCA-FEPADE · Books · All filters · Tools

About 1,400,000 results (0.43 seconds)

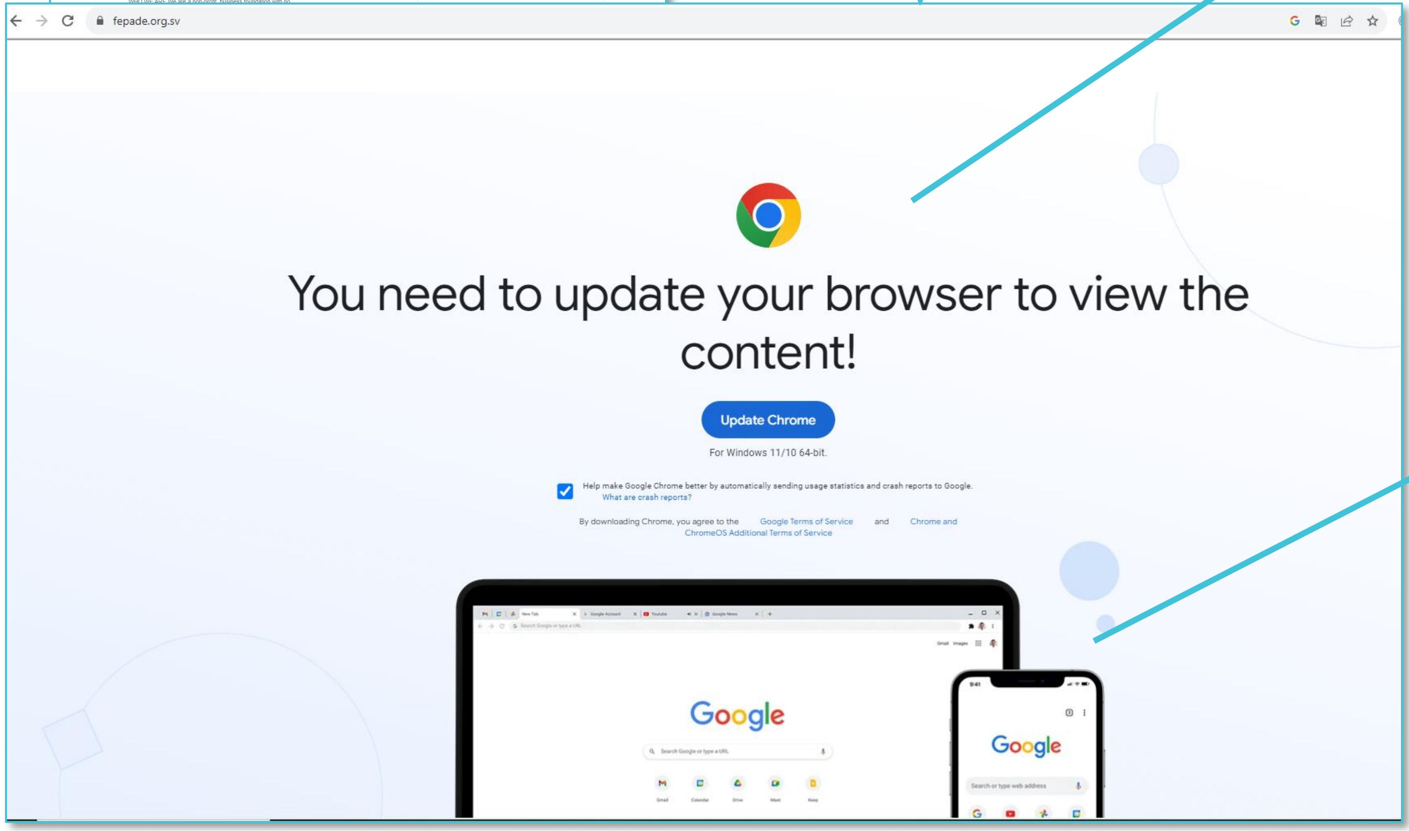
FEPADE El Salvador
https://fepade.org.sv · Translate this page

INICIO-Fepade El Salvador - FEPADE

Somos una Fundación empresarial sin fines de lucro y sin afiliación política partidaria cuya misión es contribuir al desarrollo de la educación en El Salvador ...

WHO WE ARE

iFrame Injection



fepade.org.sv

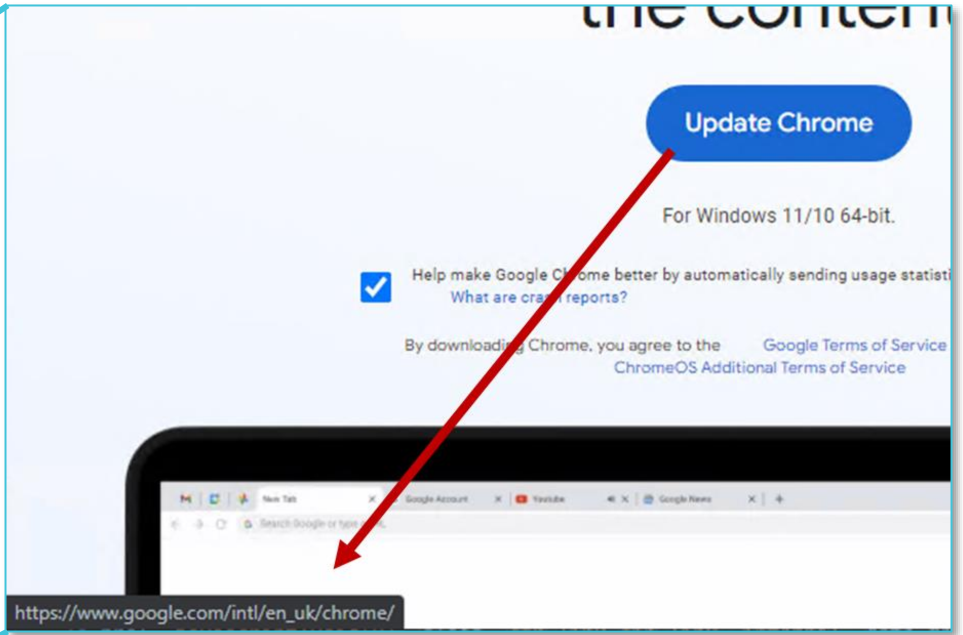
You need to update your browser to view the content!

Update Chrome

For Windows 11/10 64-bit.

☑ Help make Google Chrome better by automatically sending usage statistics and crash reports to Google. What are crash reports?

By downloading Chrome, you agree to the Google Terms of Service and Chrome and ChromeOS Additional Terms of Service



Update Chrome

For Windows 11/10 64-bit.

https://www.google.com/intl/en_uk/chrome/

Event Listener Click Hijack

↓

Keitaro TDS

↓

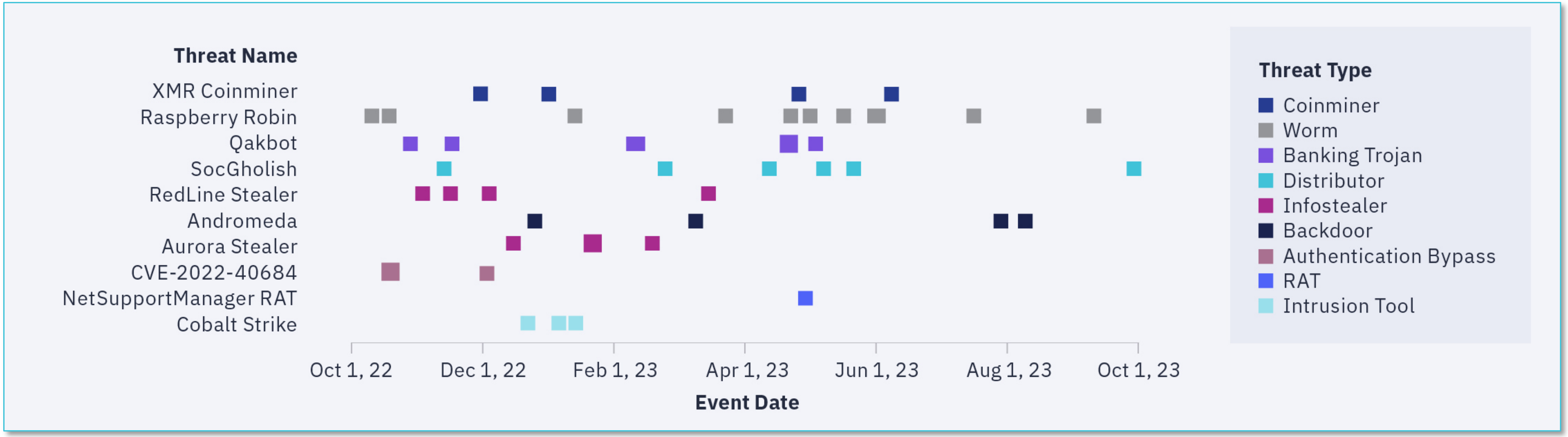
OneDrive Payload

https://www.esentire.com/blog/fake-browser-updates-distribute-lummac-stealer-amadey-and-privateloader-malware

eSENTIRE Threat Response Unit

Disrupted Threats in 2023

eSentire's Threat Response Unit (TRU) detected and responded to nearly 129 attacks against manufacturers in the 12-month period from October 2022 through September 2023, a significant increase compared to the 30 attacks recorded in the previous year from October 2021 through September 2022.



Ransomware & The Underground

Fraud Markets

Initial Access Brokers

RaaS

Microsoft Digital Defense Report 2023

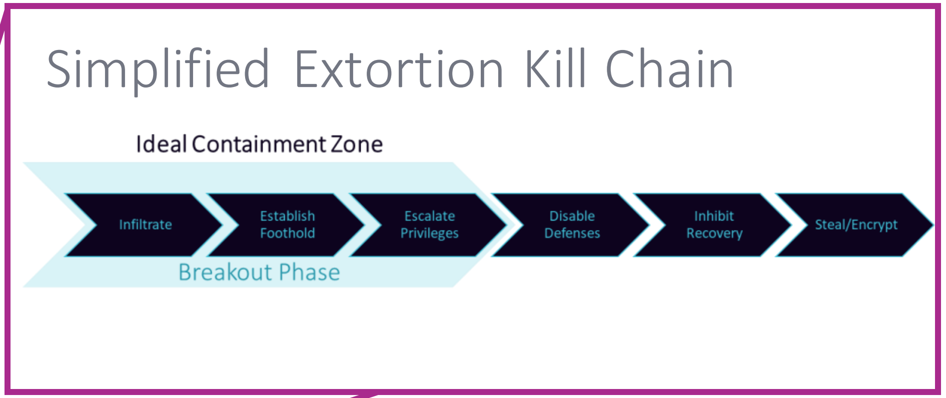
1. 80-90% of all successful ransomware compromises originate through unmanaged devices.

2. Human-operated ransomware attacks are up more than 200%.

*To keep pace with adversaries, we need to look beyond the network edge.

How do Ransomware Groups Infiltrate Networks?

Dark Web/Underground Services are Here to Help



Exploits
Auction House/Kits

Malware
As a Service

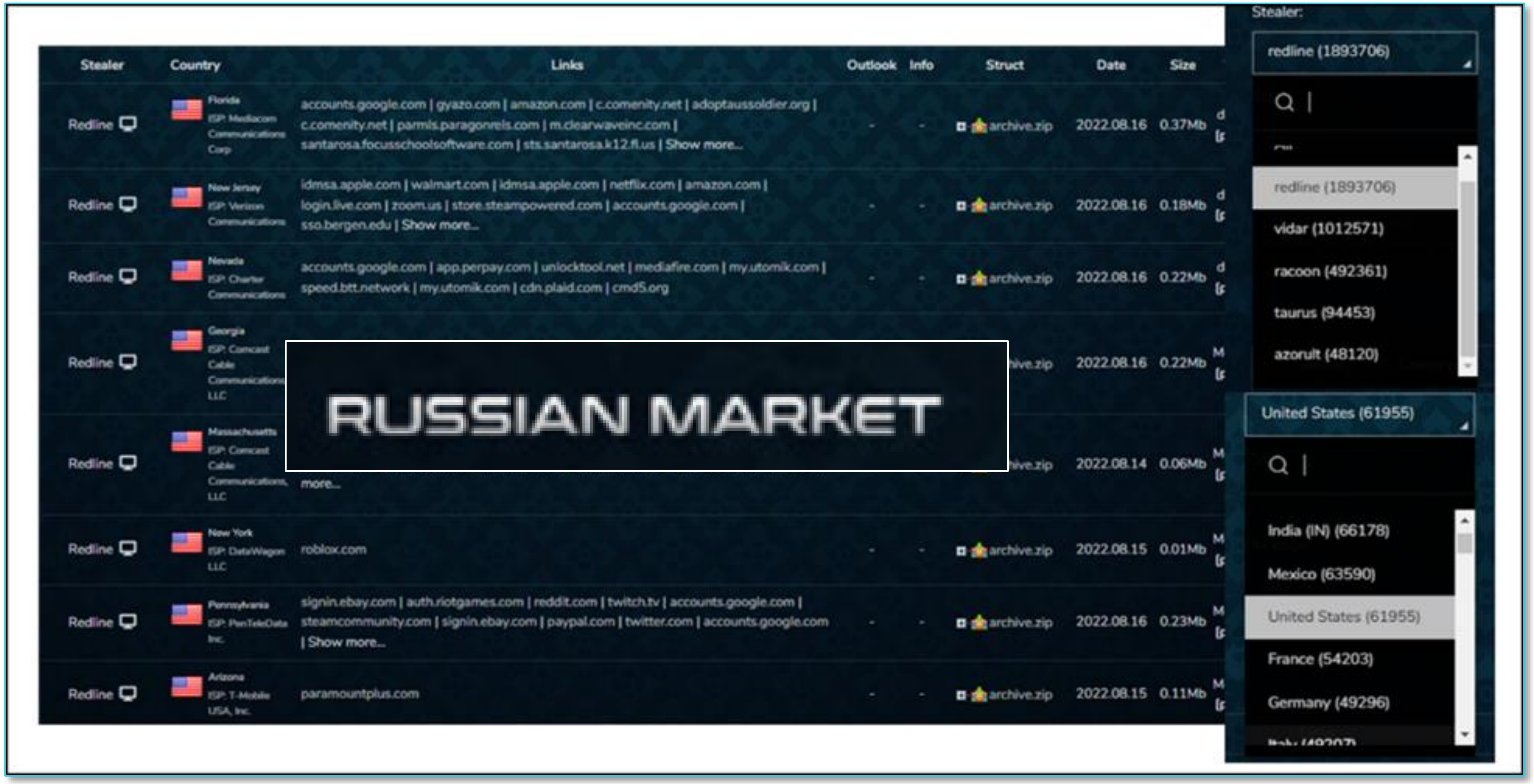
Infiltrate

Phishing
Phishing-as-a-Service

Valid Credentials
Credential Markets

Credential Markets

Russian Market & Telegram



Stealer	Country	Links	Outlook	Info	Struct	Date	Size
Redline 🖥	Florida ISP: Mediacom Communications Corp	accounts.google.com | gyazo.com | amazon.com | c.comenity.net | adoptaussoldier.org | c.comenity.net | parmis.paragonrels.com | m.clearwaveinc.com | santarosa.focusschoolsoftware.com | sts.santarosa.k12.fl.us | Show more...	-	-	⊞ archive.zip	2022.08.16	0.37Mb
Redline 🖥	New Jersey ISP: Verizon Communications	idmsa.apple.com | walmart.com | idmsa.apple.com | netflix.com | amazon.com | login.live.com | zoom.us | store.steampowered.com | accounts.google.com | sso.bergen.edu | Show more...	-	-	⊞ archive.zip	2022.08.16	0.18Mb
Redline 🖥	Nevada ISP: Charter Communications	accounts.google.com | app.perpay.com | unlocktool.net | mediafire.com | my.utomik.com | speed.btt.network | my.utomik.com | cdn.plaid.com | cmd5.org	-	-	⊞ archive.zip	2022.08.16	0.22Mb
Redline 🖥	Georgia ISP: Comcast Cable Communications LLC				hive.zip	2022.08.16	0.22Mb
Redline 🖥	Massachusetts ISP: Comcast Cable Communications, LLC	more...			hive.zip	2022.08.14	0.06Mb
Redline 🖥	New York ISP: DataWagon LLC	roblox.com	-	-	⊞ archive.zip	2022.08.15	0.01Mb
Redline 🖥	Pennsylvania ISP: PenTeleData Inc.	signin.ebay.com | auth.riotgames.com | reddit.com | twitch.tv | accounts.google.com | steamcommunity.com | signin.ebay.com | paypal.com | twitter.com | accounts.google.com | Show more...	-	-	⊞ archive.zip	2022.08.16	0.23Mb
Redline 🖥	Arizona ISP: T-Mobile USA, Inc.	paramountplus.com	-	-	⊞ archive.zip	2022.08.15	0.11Mb

RUSSIAN MARKET

Stealer:

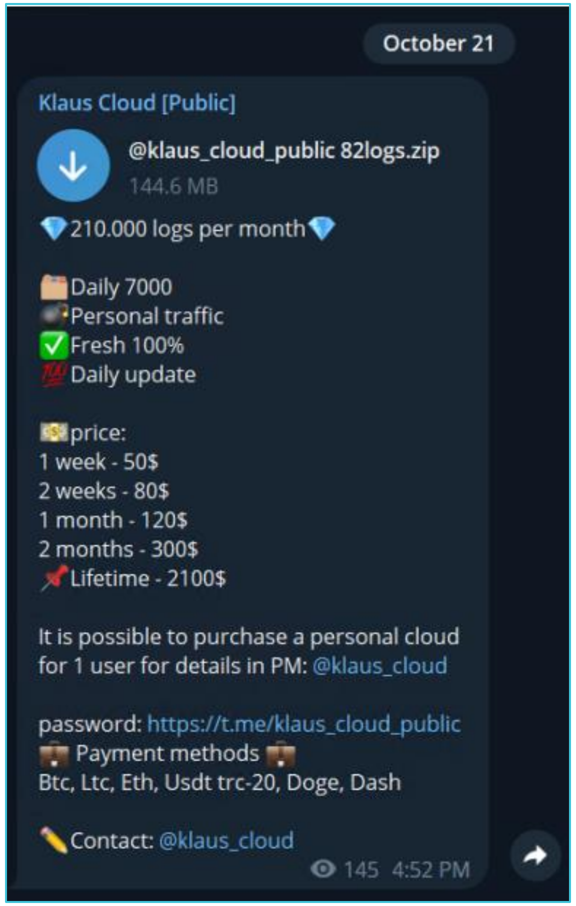
redline (1893706)

- redline (1893706)
- vidar (1012571)
- racoon (492361)
- taurus (94453)
- azorult (48120)

United States (61955)

- India (IN) (66178)
- Mexico (63590)
- United States (61955)
- France (54203)
- Germany (49296)
- Italy (49207)

Russian Market Fraud Shop



October 21

Klaus Cloud [Public]

@klaus_cloud_public 82logs.zip
144.6 MB

💎210.000 logs per month💎

📁Daily 7000
Personal traffic
✅Fresh 100%
💯Daily update

💵price:
1 week - 50$
2 weeks - 80$
1 month - 120$
2 months - 300$
📌Lifetime - 2100$

It is possible to purchase a personal cloud for 1 user for details in PM: @klaus_cloud

password: https://t.me/klaus_cloud_public
💼 Payment methods 💼
Btc, Ltc, Eth, Usdt trc-20, Doge, Dash

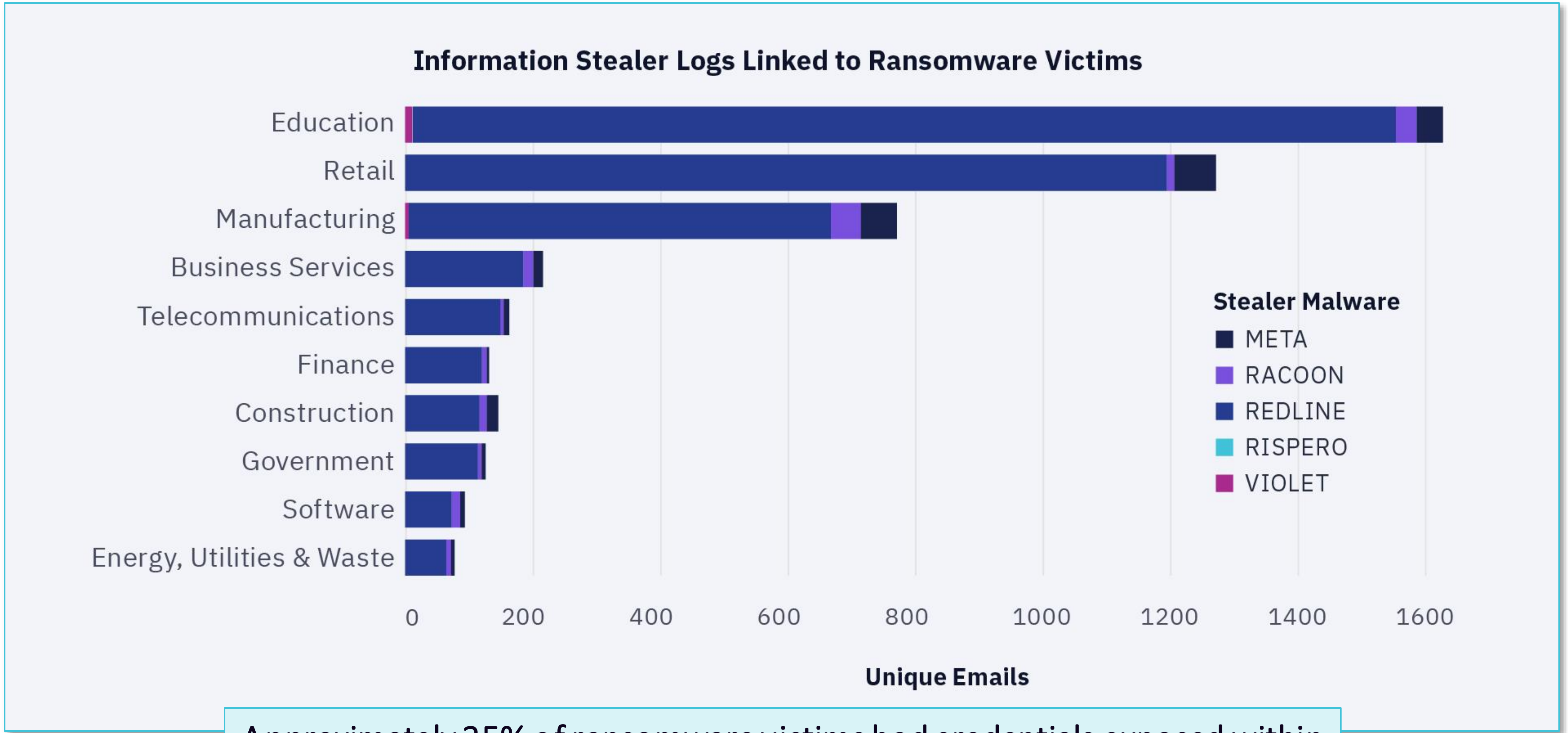
✏️Contact: @klaus_cloud

👁 145 4:52 PM

Klaus Cloud Telegram Shop

Credential Exposure

Stealer Logs Linked to Ransomware Victims



Approximately 25% of ransomware victims had credentials exposed within 30 days of their identity disclosure on ransomware leak sites.

eSENTIRE
Threat Response Unit

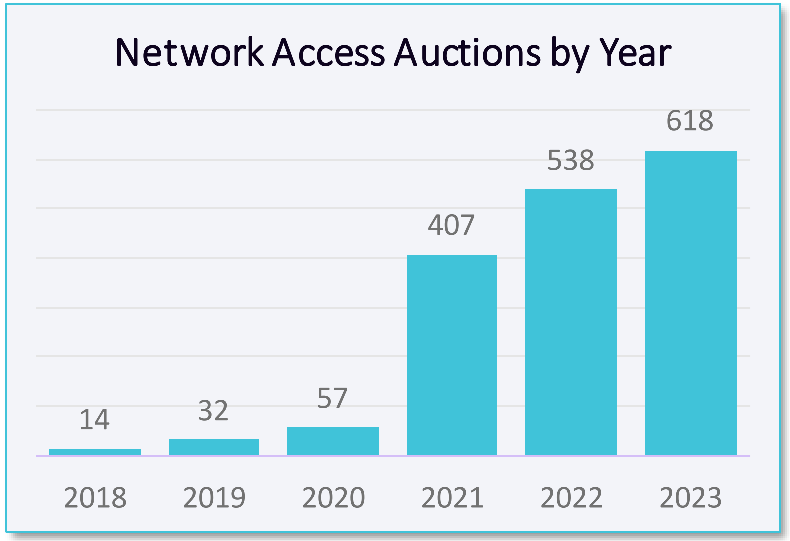
Initial Access Auctions

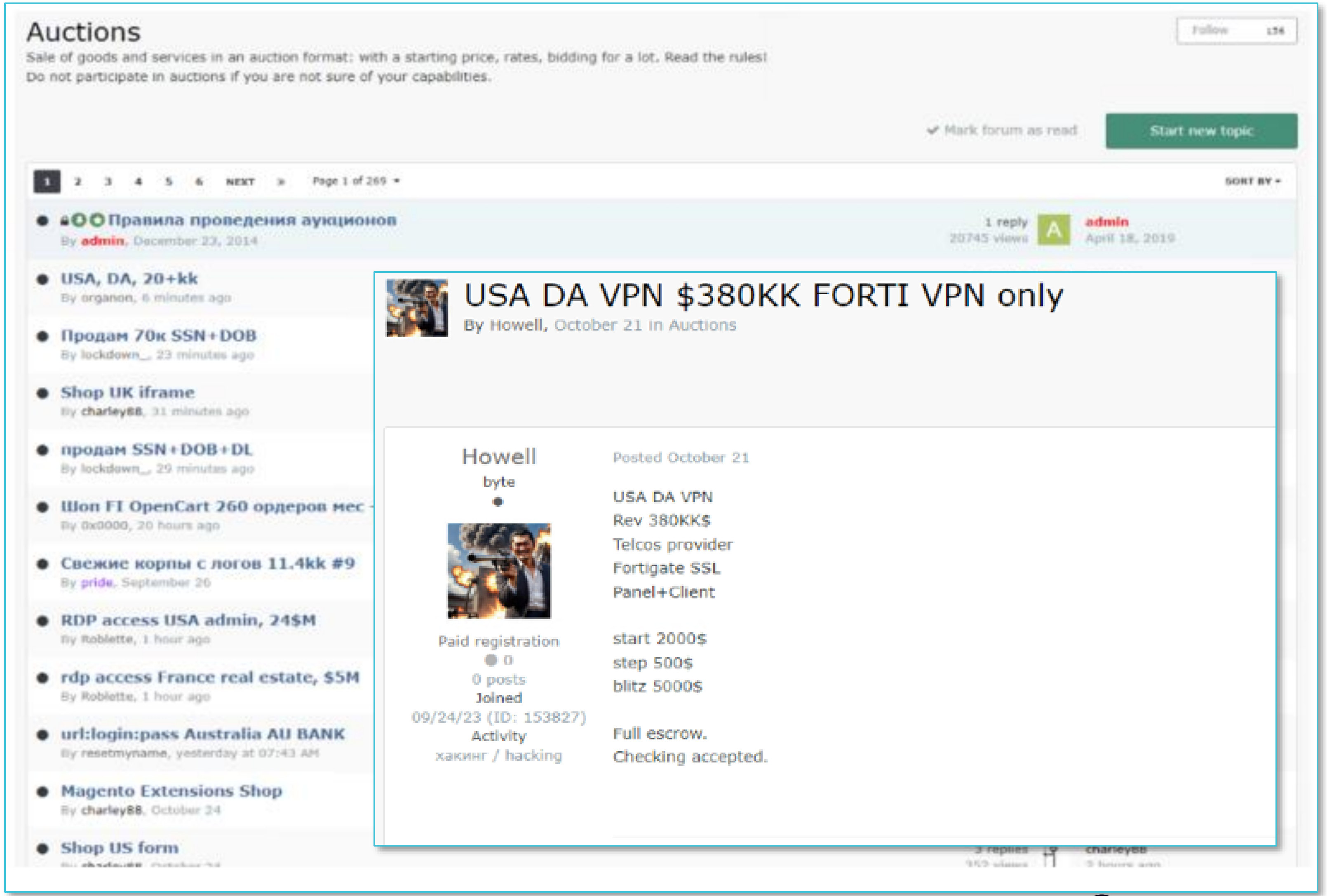
Auctions Held on Criminal Forums

Footholds Valued by Revenue, Industry

Increasing Auctions

Extortion Likely Driving Demand





Auctions

Sale of goods and services in an auction format: with a starting price, rates, bidding for a lot. Read the rules!
Do not participate in auctions if you are not sure of your capabilities.

- Правила проведения аукционов
  By admin, December 23, 2014 — 1 reply, 20745 views — admin, April 18, 2019
- USA, DA, 20+kk
  By organon, 6 minutes ago
- Продам 70к SSN+DOB
  By lockdown_, 23 minutes ago
- Shop UK iframe
  By charley88, 31 minutes ago
- продам SSN+DOB+DL
  By lockdown_, 29 minutes ago
- Шоп FI OpenCart 260 ордеров мес
  By 0x0000, 20 hours ago
- Свежие корпы с логов 11.4kk #9
  By pride, September 26
- RDP access USA admin, 24$M
  By Roblette, 1 hour ago
- rdp access France real estate, $5M
  By Roblette, 1 hour ago
- url:login:pass Australia AU BANK
  By resetmyname, yesterday at 07:43 AM
- Magento Extensions Shop
  By charley88, October 24
- Shop US form

USA DA VPN $380KK FORTI VPN only

By Howell, October 21 in Auctions

Howell
byte

Paid registration
0
0 posts
Joined
09/24/23 (ID: 153827)
Activity
хакинг / hacking

Posted October 21

USA DA VPN
Rev 380KK$
Telcos provider
Fortigate SSL
Panel+Client

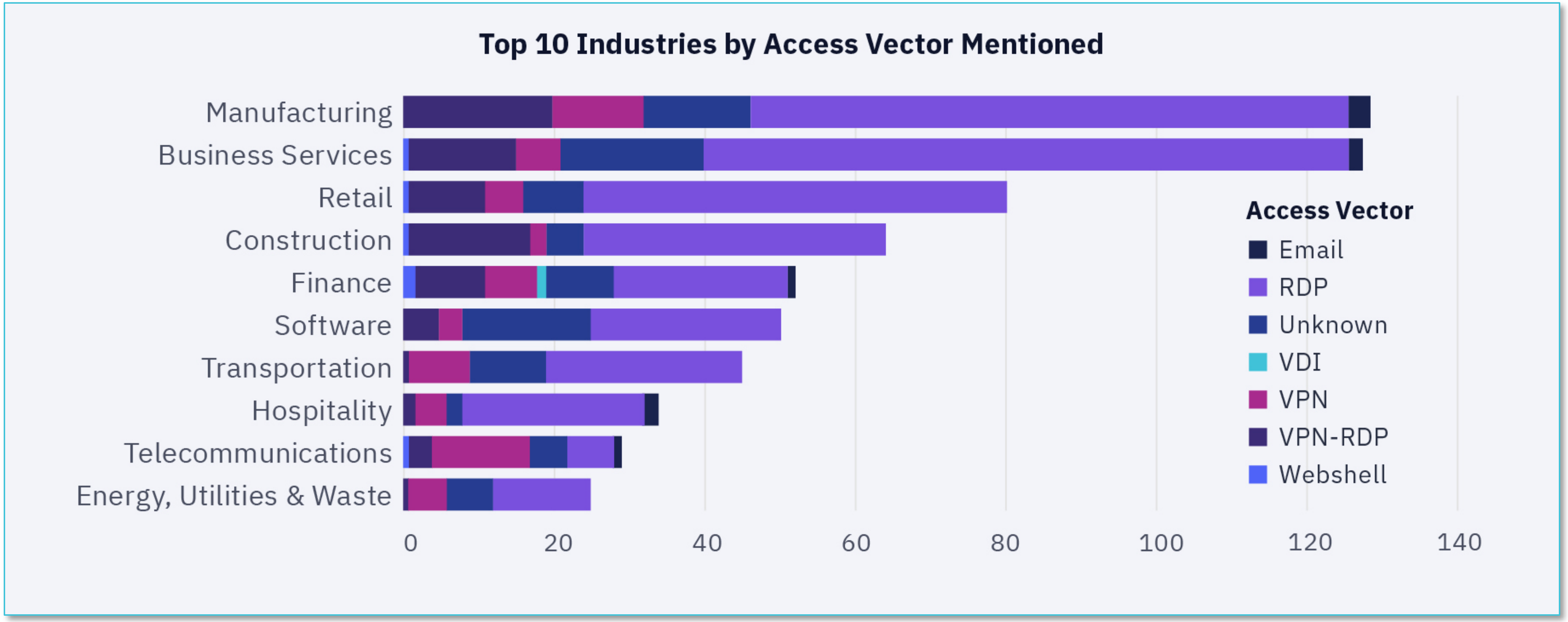
start 2000$
step 500$
blitz 5000$

Full escrow.
Checking accepted.

eSENTIRE Threat Response Unit

Industry Exposure in Initial Access Auctions

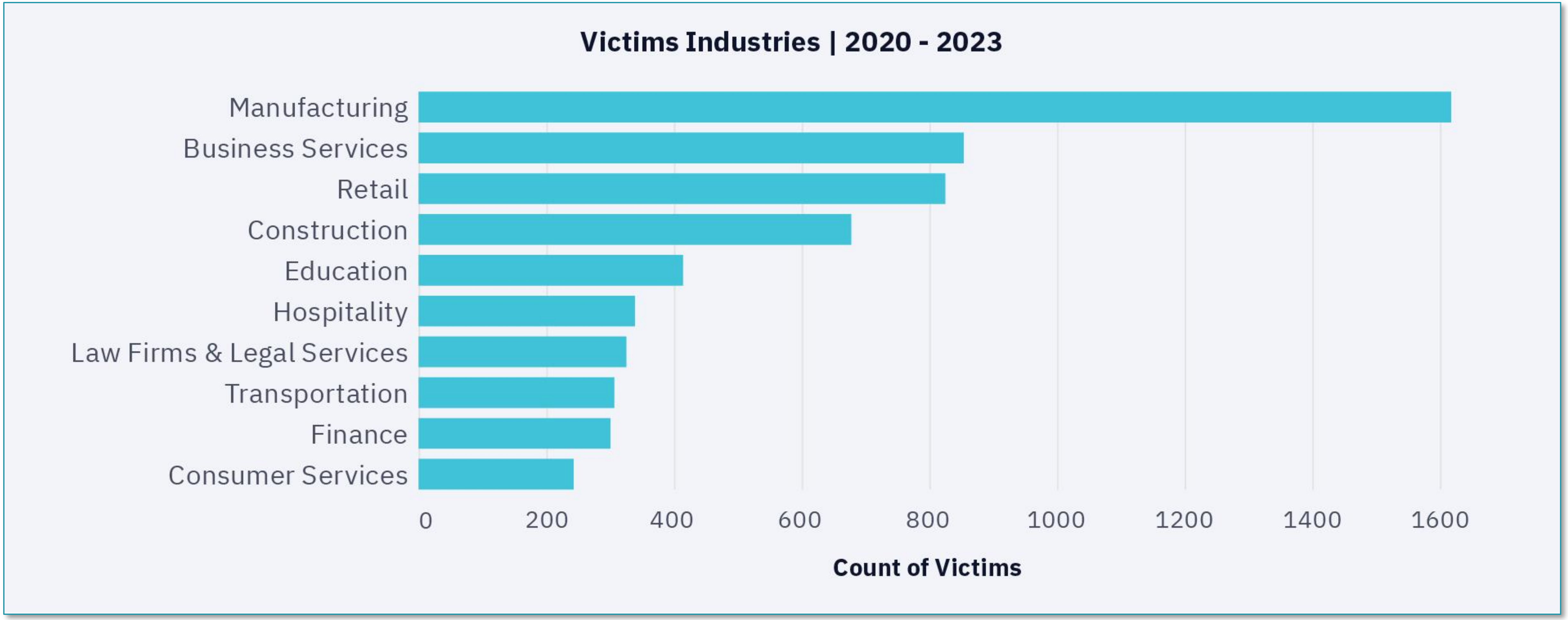
Manufacturing at Increased Exposure, Remote Desktop Protocol Preferred



- RDP and VPN command the highest prices and are most common.
- Manufacturing, Business Services and Retail makeup top auctions.

eSENTIRE Threat Response Unit

Industry Exposure in Ransomware Leak Sites



eSENTIRE Threat Response Unit

Recommendations

Understand, Prepare, and Predict Cyber Threats

- Ensure your phishing and security awareness training program covers both **email** and **browser-based** threats
- Secure your edge devices and services
- Reduce the impact of compromised credentials
  - See -> MFA
- Consider dark web/underground monitoring capability

Detect, Investigate, Disrupt, and Contain Cyberattacks

- Centralize logging for all edge devices
- Monitor log-on activity for **remote access services**, such as VPN/RDP
- Remediate malware infections **as quickly as possible**

Eradicate Threats and Return to Standard Operations

- Identify the type of ransomware and/or the threat actors behind the attack, if possible, to determine if there is a possible decryption key already available
- Create, maintain, and exercise a strong cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident

TRU’s Latest Research Reports

DOWNLOAD NOW >

RANSOMWARE REPORT

Ransomware Readiness:
How SMBs Can Prepare for the Rising Threat of Ransomware-as-a-Service, Initial Access Brokers, and Credential Theft

January 2024

DOWNLOAD NOW >

THREAT INTELLIGENCE SPOTLIGHT

Increasing Cyber Resilience Against Cyber Threats Impacting the Manufacturing Industry