CISCO TALOS

OUR JOB IS YOUR DEFENSE

Joe Marshall – Sr. Security Strategist

Who am I?

Joe Marshall

@immortanjo3

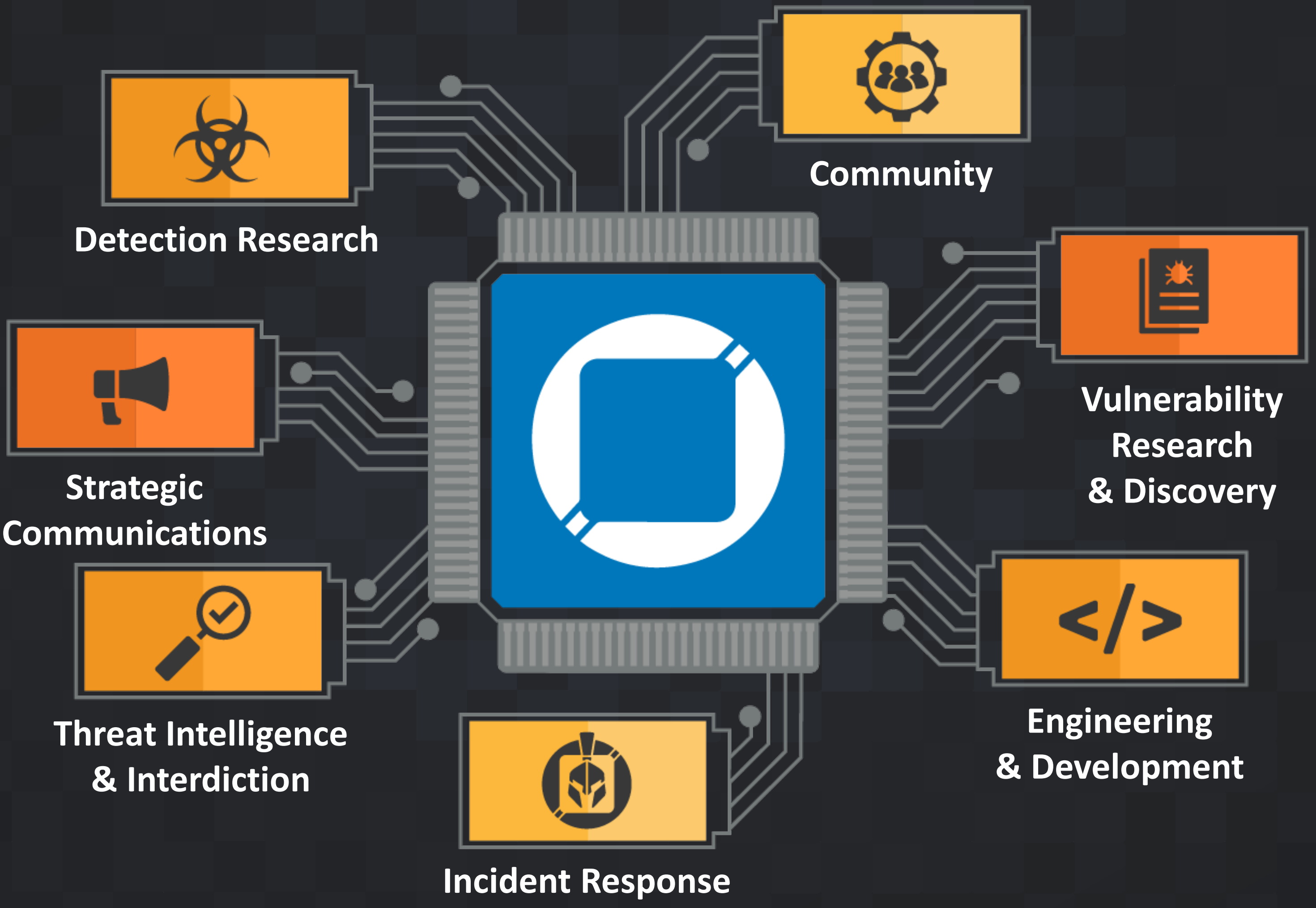
josmarsh@cisco.com

- Senior Security Strategist and threat researcher
- Hacking, IoT, and keeping the internet safe.
- Baltimore, MD

TALOS
Cisco Security Research

Our job is protecting your network

Talos is the threat intelligence group at Cisco. We are here to fight the good fight — we work to keep our customers, and users at large, safe from malicious actors.



Community
Detection Research
Vulnerability Research & Discovery
Strategic Communications
Threat Intelligence & Interdiction
Engineering & Development
Incident Response

Talos
Cisco Security Research

Unmatched visibility across the threat landscape

550B security events/**day**

~9M emails blocked/**hour**

~2,000 new samples/**minute**

~2,000 domains blocked/**second**

Let’s learn about cyber crime

And how it relates to Agriculture

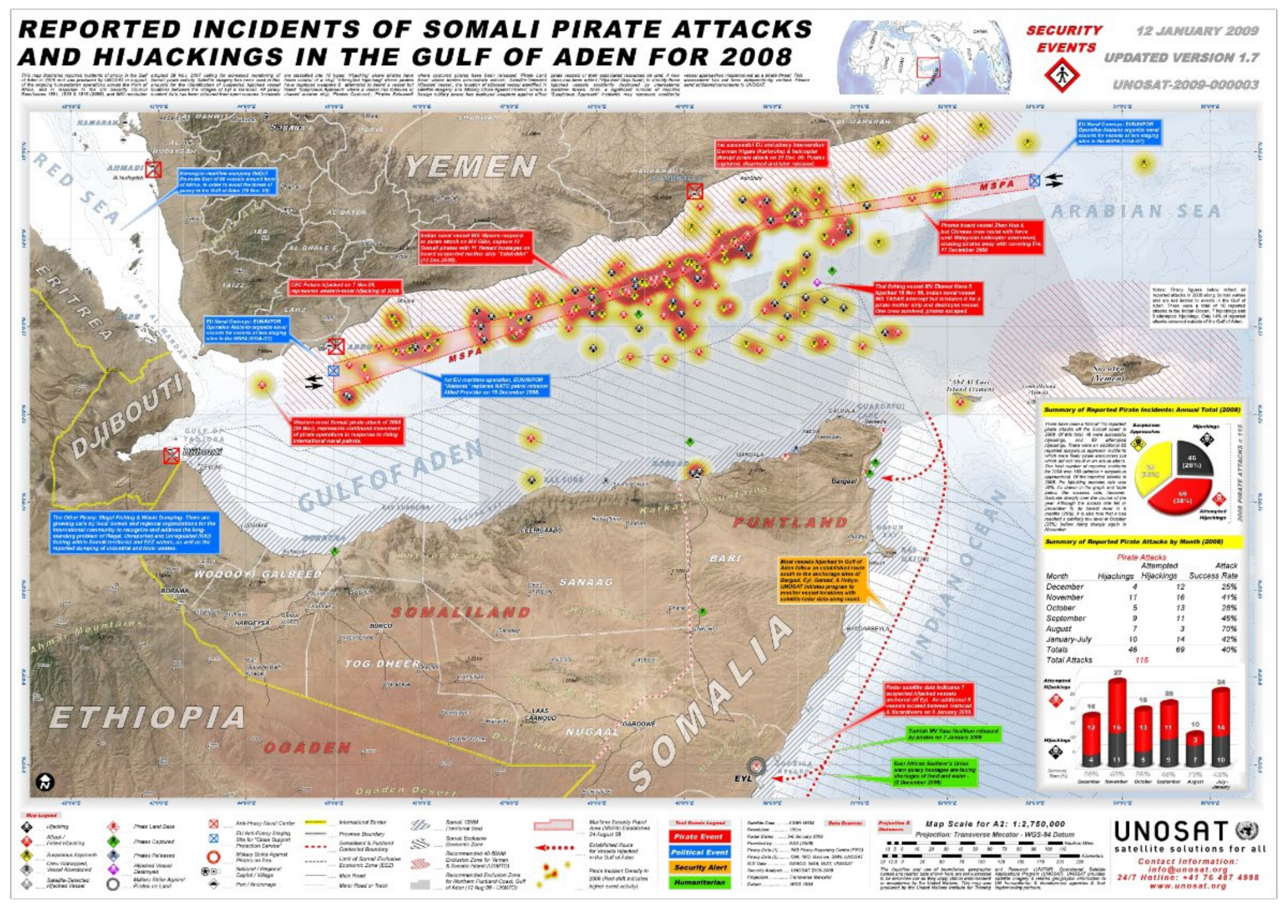
TALOS

Cisco Security Research

Pirates are cool

(not really)

What do pirates need?



REPORTED INCIDENTS OF SOMALI PIRATE ATTACKS AND HIJACKINGS IN THE GULF OF ADEN FOR 2008

SECURITY EVENTS

12 JANUARY 2009

UPDATED VERSION 1.7

UNOSAT-2009-000003

Summary of Reported Pirate Incidents: Annual Total (2008)

Summary of Reported Pirate Attacks by Month (2008)

	Pirate Attacks		
Month	Hijackings	Attempted Hijackings	Attack Success Rate
December	4	12	25%
November	11	16	41%
October	5	13	28%
September	9	11	45%
August	7	3	70%
January-July	10	14	42%
Totals	46	69	40%
Total Attacks	115		

Talos
Cisco Security Research

The word of the day?

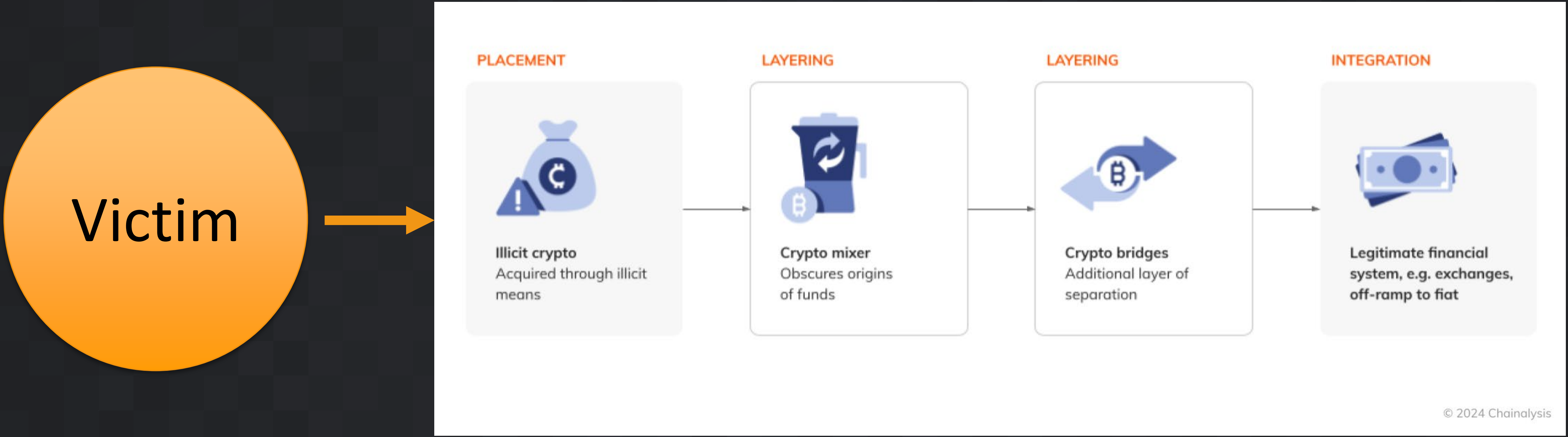
Corruption

Russia and the Cartels

Talos
Cisco Security Research

And there are rules

Understand that crypto is often linked to cyber crime



Victim

PLACEMENT

Illicit crypto
Acquired through illicit means

LAYERING

Crypto mixer
Obscures origins of funds

LAYERING

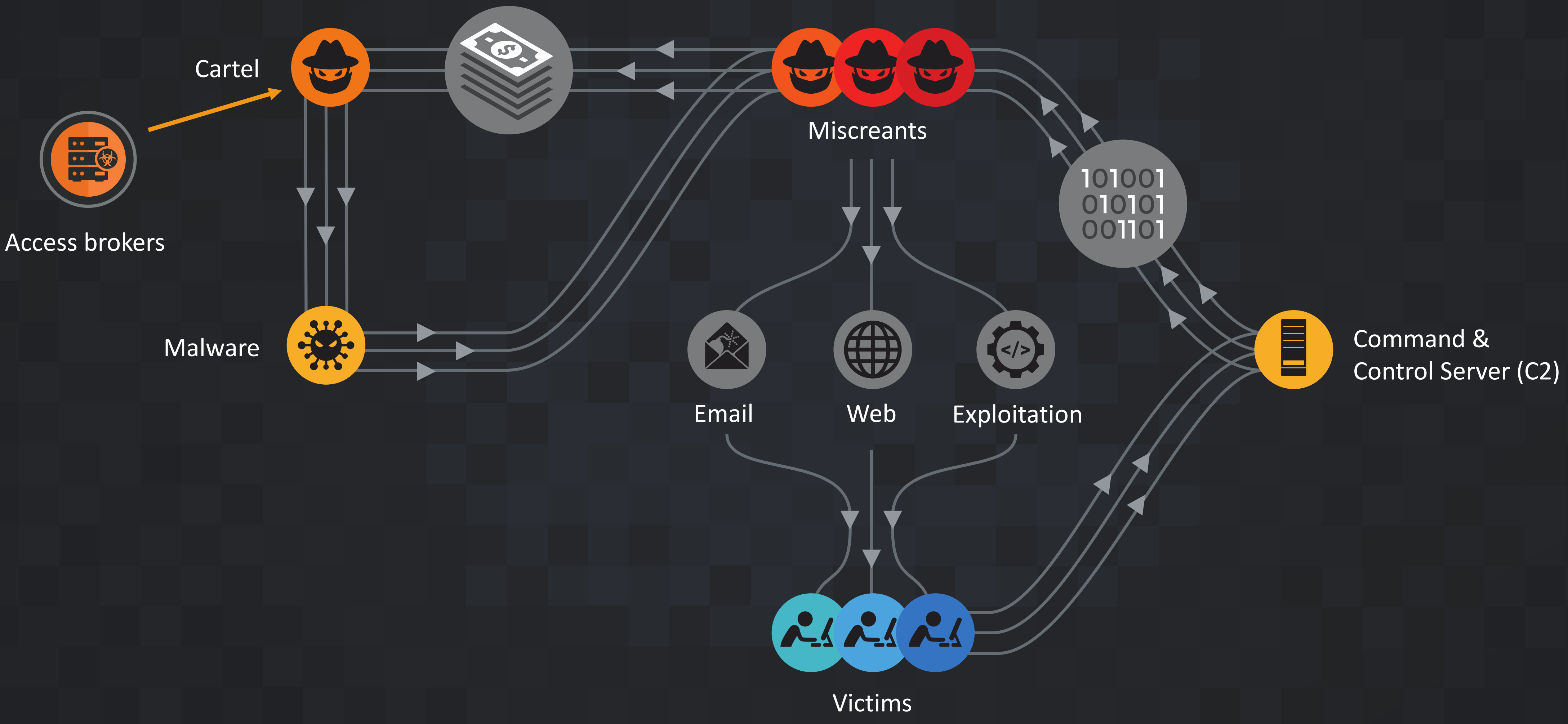
Crypto bridges
Additional layer of separation

INTEGRATION

Legitimate financial system, e.g. exchanges, off-ramp to fiat

© 2024 Chainalysis

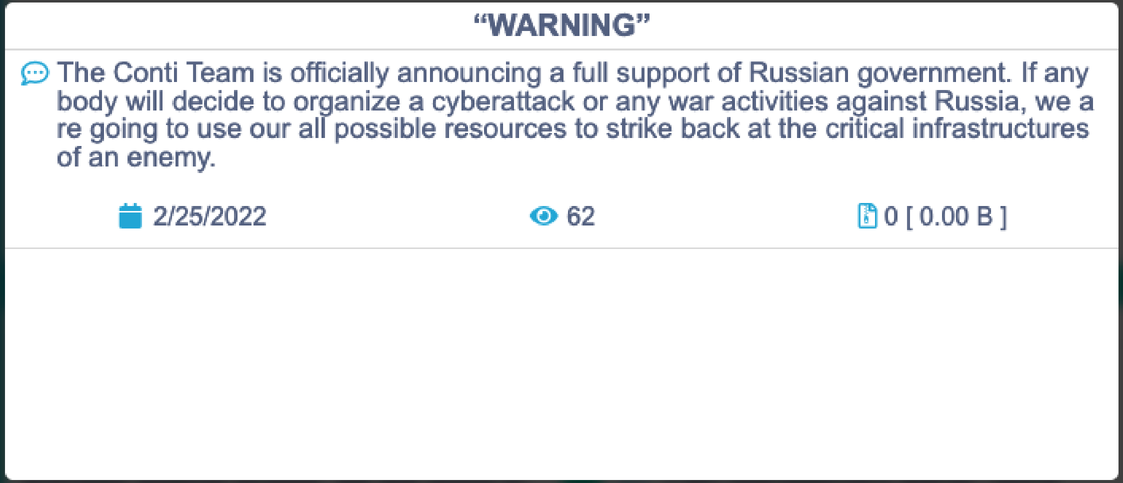
The Ransomware Business Model



Talos
Cisco Security Research

Example: Conti Cartel

(RIP)



“WARNING”

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we a re going to use our all possible resources to strike back at the critical infrastructures of an enemy.

Talos
Cisco Security Research

A look inside a cartel

Conti and Hive ransomware operations:

Leveraging victim chats for insights

WRITTEN BY
KENDALL MCKAY
with contributions from
PAUL EUBANKS and JAIME FILSON

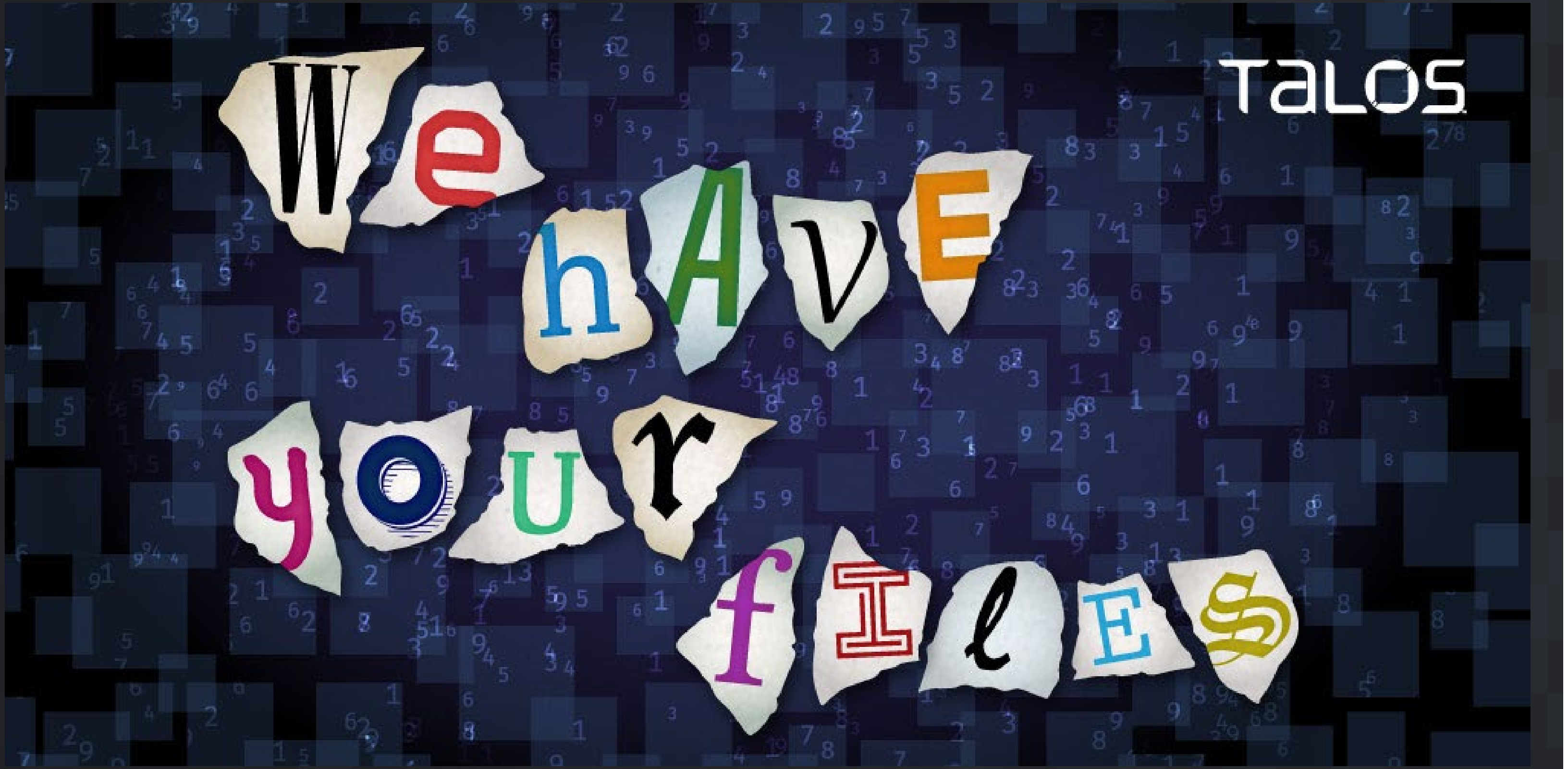
Updated May 2, 2022

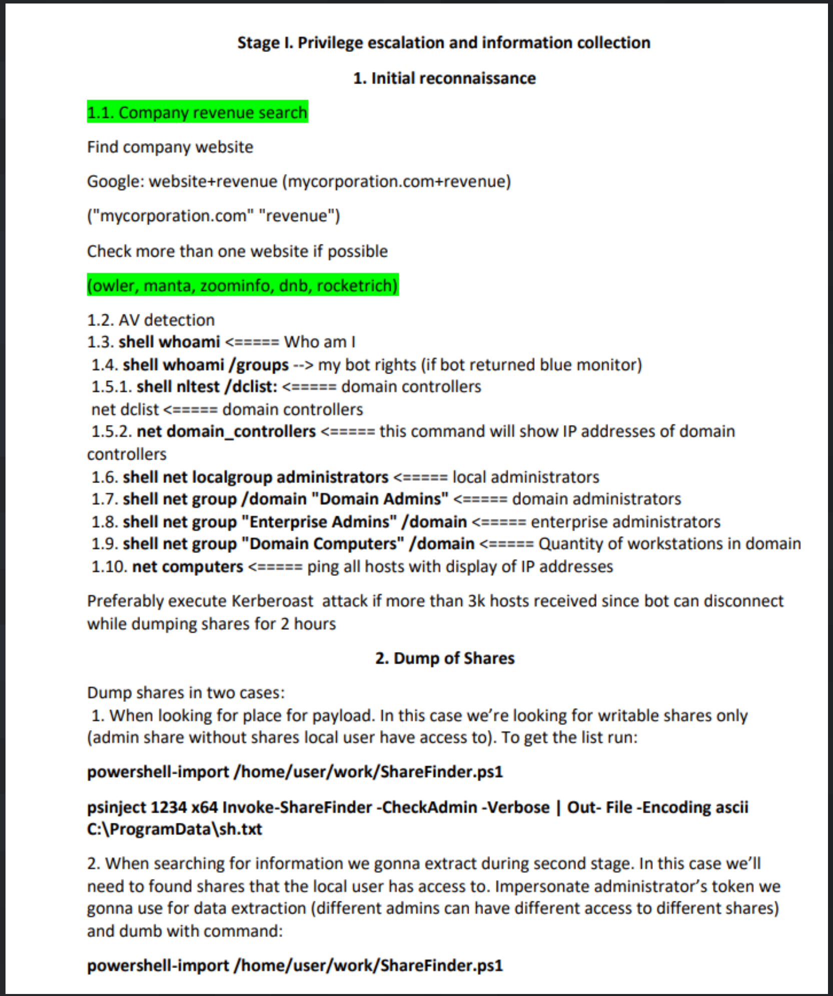
cisco | Talos

Talos
Cisco Security Research

You can even read their playbook

https://blog.talosintelligence.com/2021/09/Conti-leak-translation.html





Stage I. Privilege escalation and information collection

1. Initial reconnaissance

1.1. Company revenue search

Find company website

Google: website+revenue (mycorporation.com+revenue)

("mycorporation.com" "revenue")

Check more than one website if possible

(owler, manta, zoominfo, dnb, rocketrich)

1.2. AV detection

1.3. **shell whoami** <===== Who am I

1.4. **shell whoami /groups** --> my bot rights (if bot returned blue monitor)

1.5.1. **shell nltest /dclist:** <===== domain controllers

net dclist <===== domain controllers

1.5.2. **net domain_controllers** <===== this command will show IP addresses of domain controllers

1.6. **shell net localgroup administrators** <===== local administrators

1.7. **shell net group /domain "Domain Admins"** <===== domain administrators

1.8. **shell net group "Enterprise Admins" /domain** <===== enterprise administrators

1.9. **shell net group "Domain Computers" /domain** <===== Quantity of workstations in domain

1.10. **net computers** <===== ping all hosts with display of IP addresses

Preferably execute Kerberoast attack if more than 3k hosts received since bot can disconnect while dumping shares for 2 hours

2. Dump of Shares

Dump shares in two cases:

1. When looking for place for payload. In this case we're looking for writable shares only (admin share without shares local user have access to). To get the list run:

powershell-import /home/user/work/ShareFinder.ps1

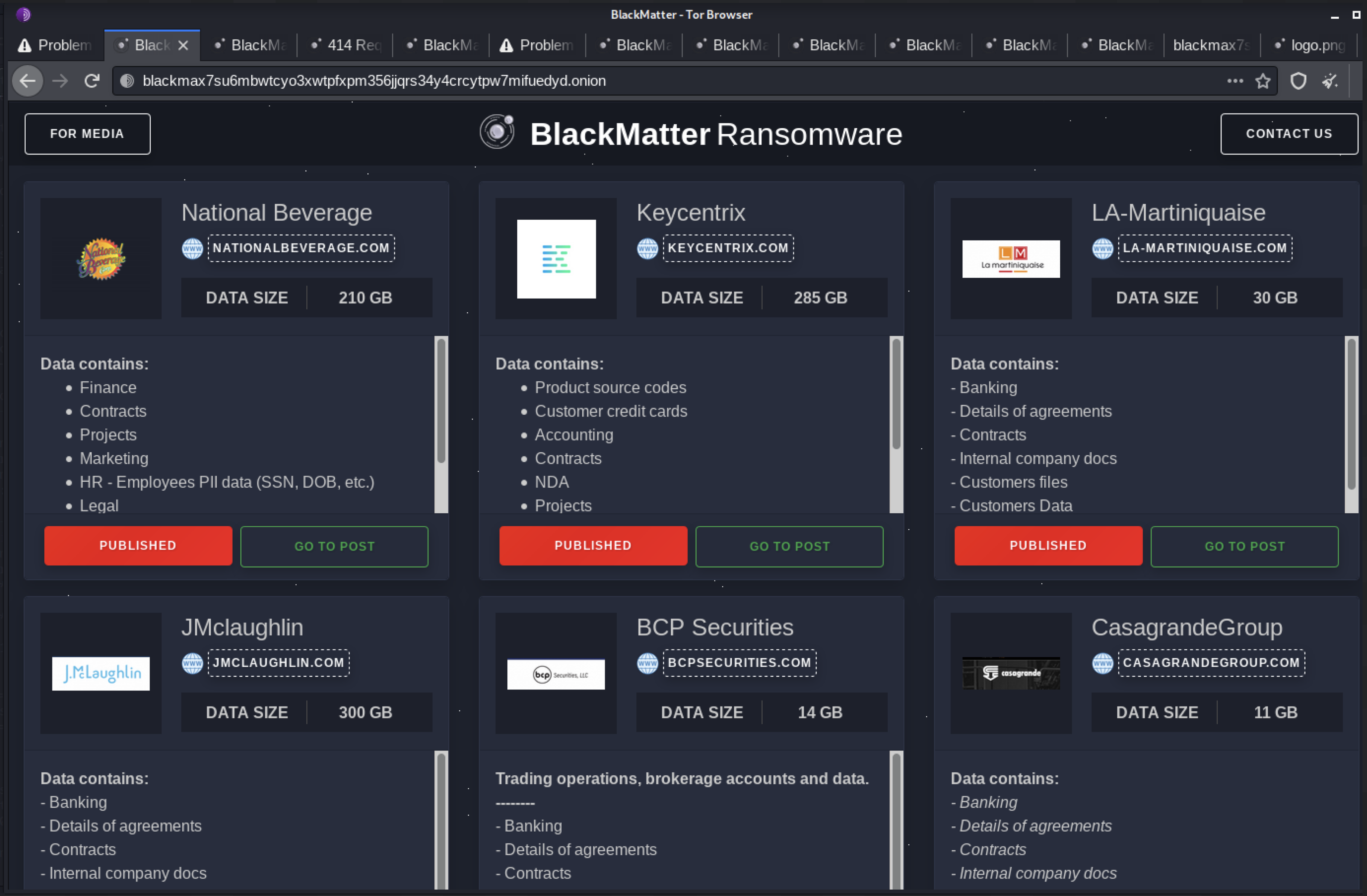
psinject 1234 x64 Invoke-ShareFinder -CheckAdmin -Verbose | Out- File -Encoding ascii C:\ProgramData\sh.txt

2. When searching for information we gonna extract during second stage. In this case we'll need to found shares that the local user has access to. Impersonate administrator's token we gonna use for data extraction (different admins can have different access to different shares) and dumb with command:

powershell-import /home/user/work/ShareFinder.ps1

Talos
Cisco Security Research

Shaming sites



BlackMatter Ransomware

National Beverage	NATIONALBEVERAGE.COM	DATA SIZE	210 GB	PUBLISHED	GO TO POST
Keycentrix	KEYCENTRIX.COM	DATA SIZE	285 GB	PUBLISHED	GO TO POST
LA-Martiniquaise	LA-MARTINIQUAISE.COM	DATA SIZE	30 GB	PUBLISHED	GO TO POST

National Beverage

Data contains:

- Finance
- Contracts
- Projects
- Marketing
- HR - Employees PII data (SSN, DOB, etc.)
- Legal

Keycentrix

Data contains:

- Product source codes
- Customer credit cards
- Accounting
- Contracts
- NDA
- Projects

LA-Martiniquaise

Data contains:
- Banking
- Details of agreements
- Contracts
- Internal company docs
- Customers files
- Customers Data

JMclaughlin	JMCLAUGHLIN.COM	DATA SIZE	300 GB
BCP Securities	BCPSECURITIES.COM	DATA SIZE	14 GB
CasagrandeGroup	CASAGRANDEGROUP.COM	DATA SIZE	11 GB

JMclaughlin

Data contains:
- Banking
- Details of agreements
- Contracts
- Internal company docs

BCP Securities

Trading operations, brokerage accounts and data.

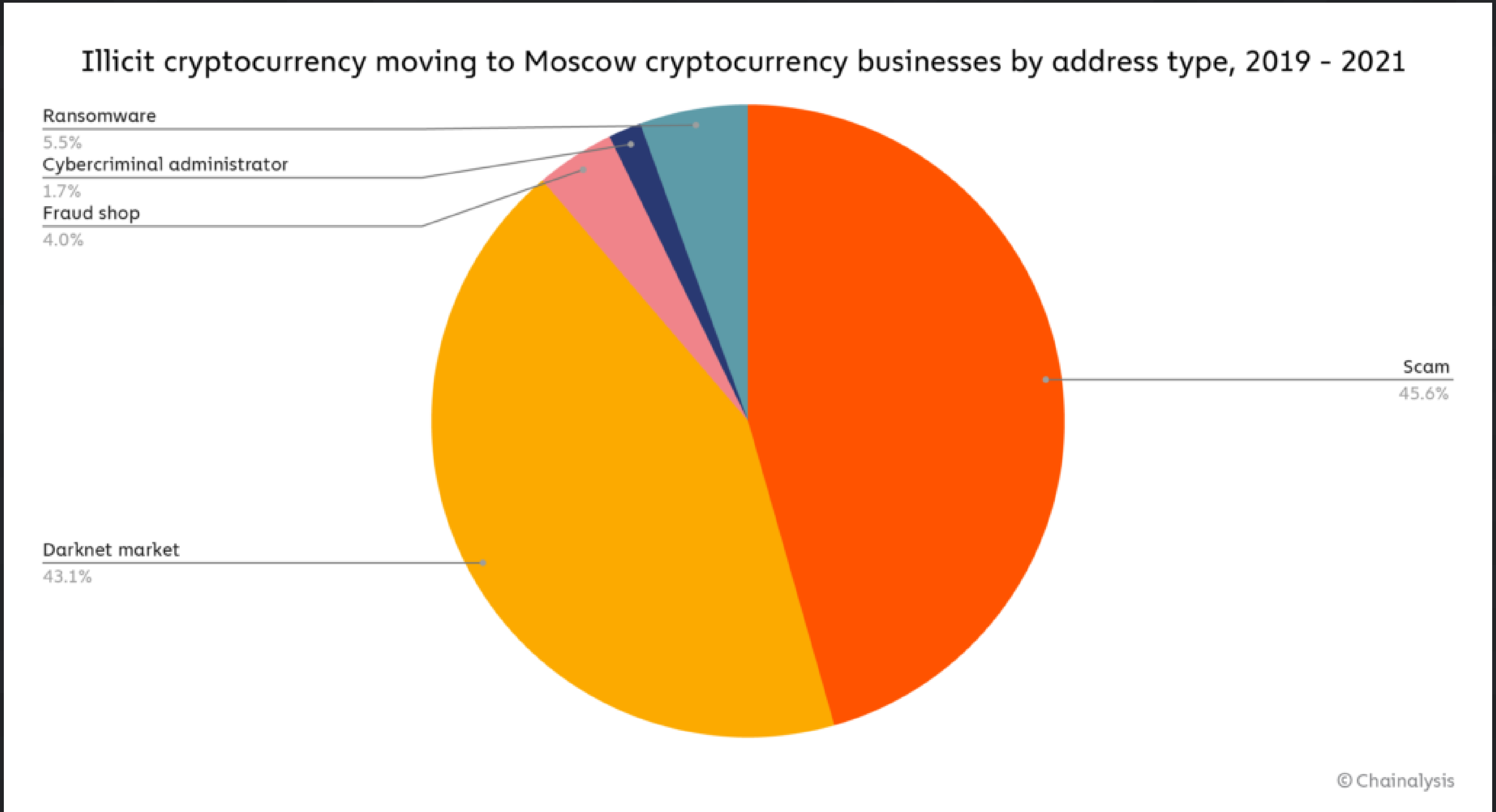
- Banking
- Details of agreements
- Contracts

CasagrandeGroup

Data contains:
- *Banking*
- *Details of agreements*
- *Contracts*
- *Internal company docs*

Talos
Cisco Security Research

Understanding the macro

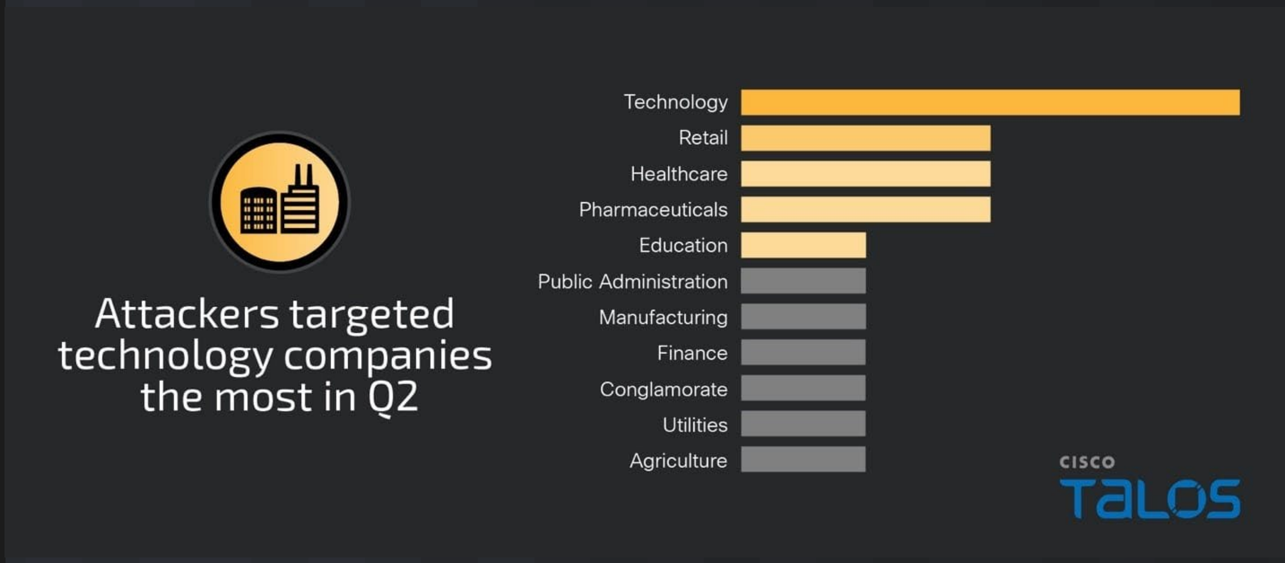


Cisco Security Research

Recent news

NCA
National Crime Agency
NPCC
National Police Chiefs' Council
Operation
DESTABILISE

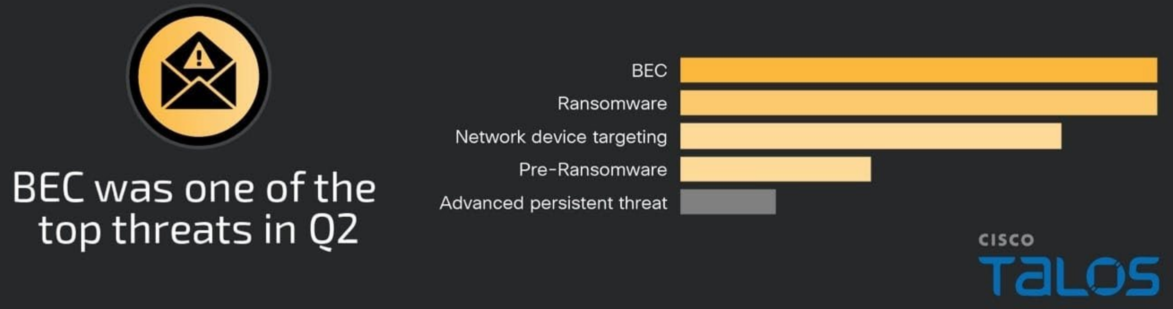
Education/MFG/FINS RV – pushing to the front!



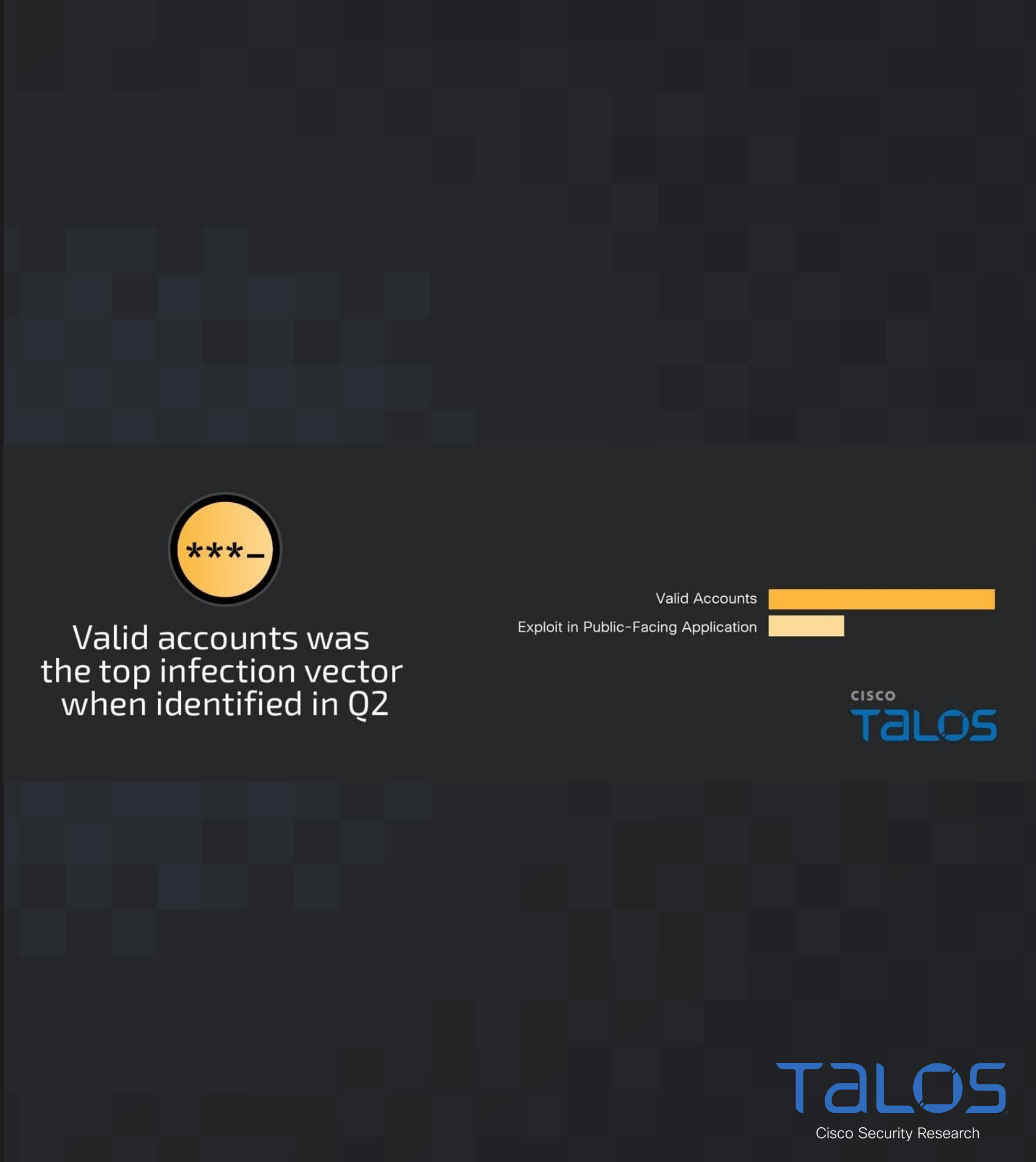
Attackers targeted technology companies the most in Q2

Cisco Security Research

BEC climbs to defeat ransomware

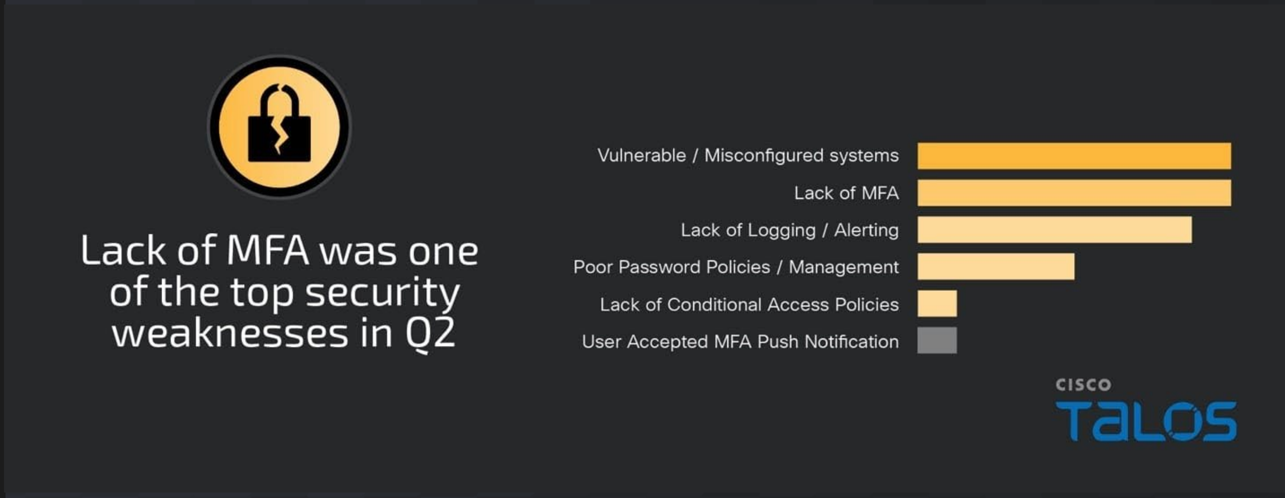


Valid accounts was the top infection vector when identified in Q2



Valid accounts was the top infection vector when identified in Q2

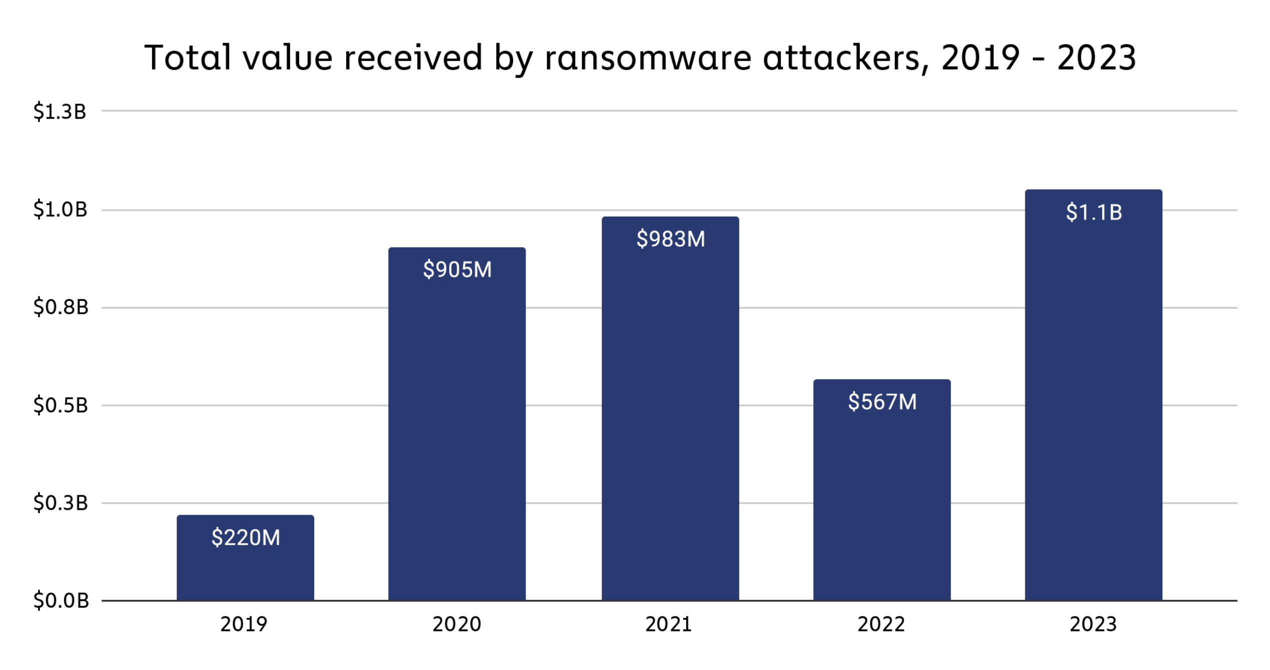
Lack of MFA is *still* the top security weakness



Lack of MFA was one of the top security weaknesses in Q2

Cisco Security Research

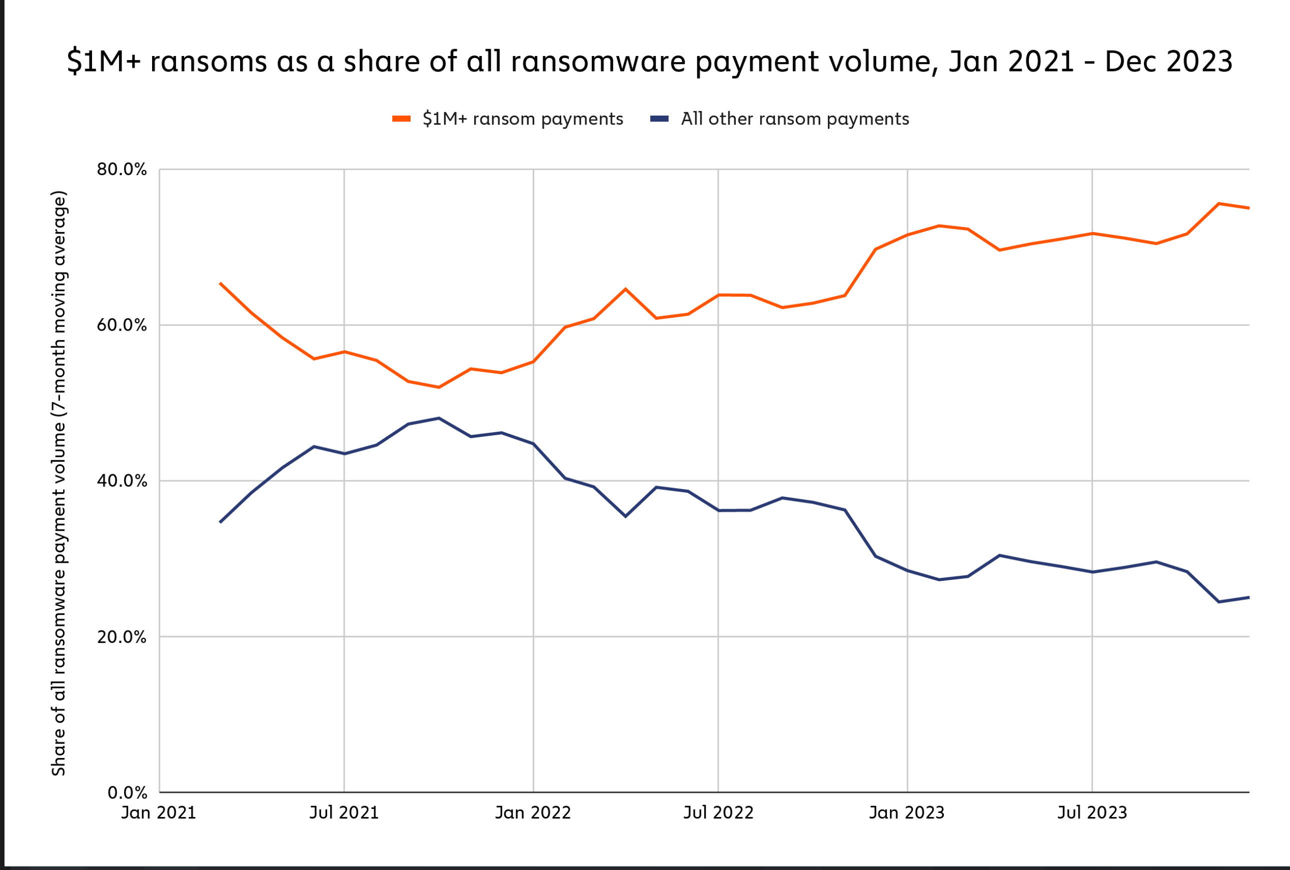
$$$$$$$$$



© Chainalysis

Talos
Cisco Security Research

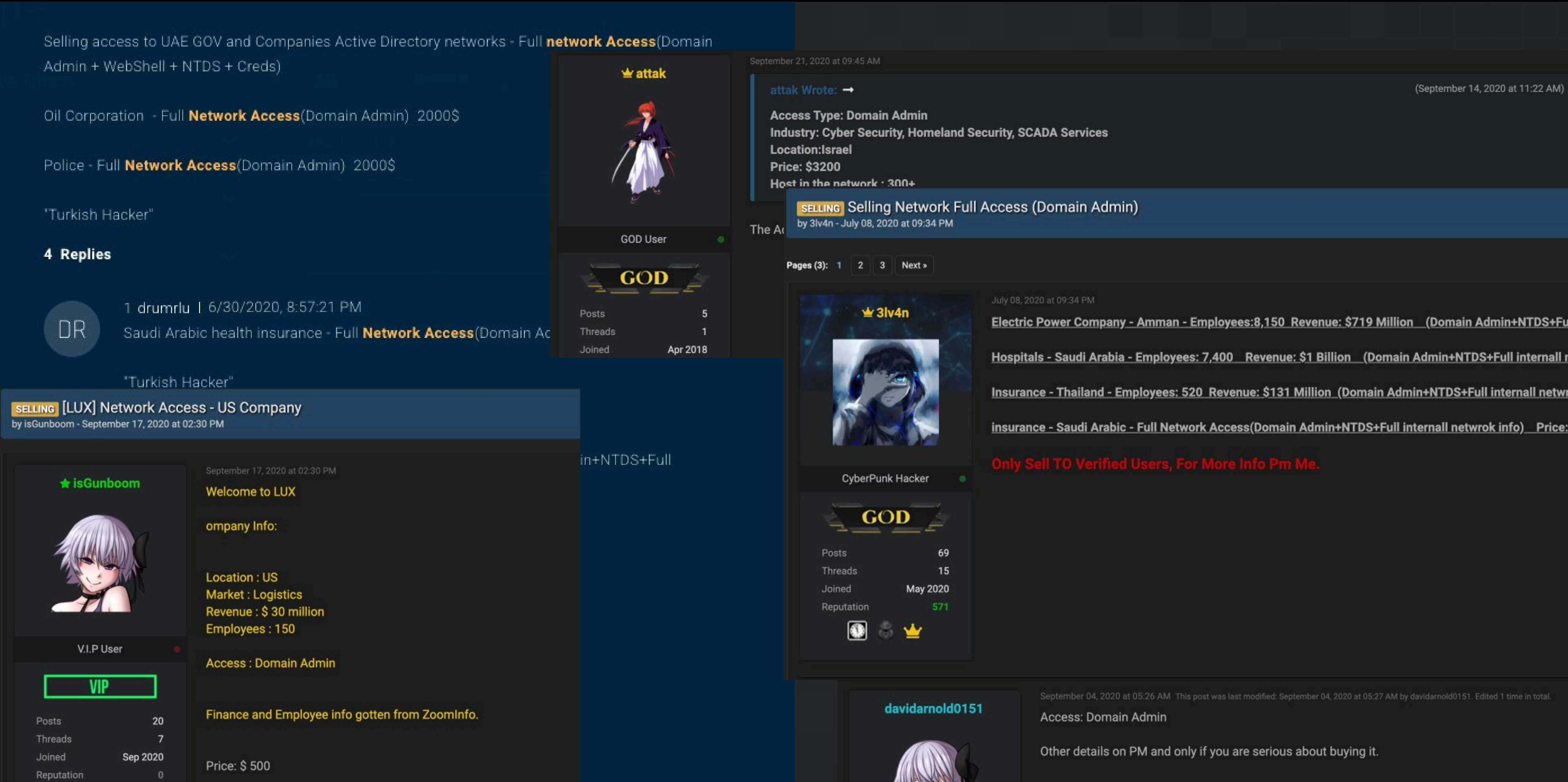
Big Game Hunting!



© Chainalysis

Cisco Security Research

Compromise as a Service



Selling access to UAE GOV and Companies Active Directory networks - Full **network Access**(Domain Admin + WebShell + NTDS + Creds)

Oil Corporation - Full **Network Access**(Domain Admin) 2000$

Police - Full **Network Access**(Domain Admin) 2000$

"Turkish Hacker"

4 Replies

DR 1 drumrlu | 6/30/2020, 8:57:21 PM

Saudi Arabic health insurance - Full **Network Access**(Domain Ac

"Turkish Hacker"

in+NTDS+Full

attak

GOD User

GOD

Posts 5
Threads 1
Joined Apr 2018

September 21, 2020 at 09:45 AM

attak Wrote: ➞ (September 14, 2020 at 11:22 AM)

Access Type: Domain Admin
Industry: Cyber Security, Homeland Security, SCADA Services
Location:Israel
Price: $3200
Host in the network : 300+

The Ac

SELLING Selling Network Full Access (Domain Admin)
by 3lv4n - July 08, 2020 at 09:34 PM

Pages (3): 1 2 3 Next »

3lv4n

CyberPunk Hacker

GOD

Posts 69
Threads 15
Joined May 2020
Reputation 571

July 08, 2020 at 09:34 PM

Electric Power Company - Amman - Employees:8,150 Revenue: $719 Million (Domain Admin+NTDS+Fu

Hospitals - Saudi Arabia - Employees: 7,400 Revenue: $1 Billion (Domain Admin+NTDS+Full internall r

Insurance - Thailand - Employees: 520 Revenue: $131 Million (Domain Admin+NTDS+Full internall netw

insurance - Saudi Arabic - Full Network Access(Domain Admin+NTDS+Full internall netwrok info) Price:

Only Sell TO Verified Users, For More Info Pm Me.

SELLING [LUX] Network Access - US Company
by isGunboom - September 17, 2020 at 02:30 PM

isGunboom

V.I.P User

VIP

Posts 20
Threads 7
Joined Sep 2020
Reputation 0

September 17, 2020 at 02:30 PM

Welcome to LUX

ompany Info:

Location : US
Market : Logistics
Revenue : $ 30 million
Employees : 150

Access : Domain Admin

Finance and Employee info gotten from ZoomInfo.

Price: $ 500

davidarnold0151

September 04, 2020 at 05:26 AM This post was last modified: September 04, 2020 at 05:27 AM by davidarnold0151. Edited 1 time in total.

Access: Domain Admin

Other details on PM and only if you are serious about buying it.

So, what’s the deal?

Well, there's this of course....

Global agriculture is all connected

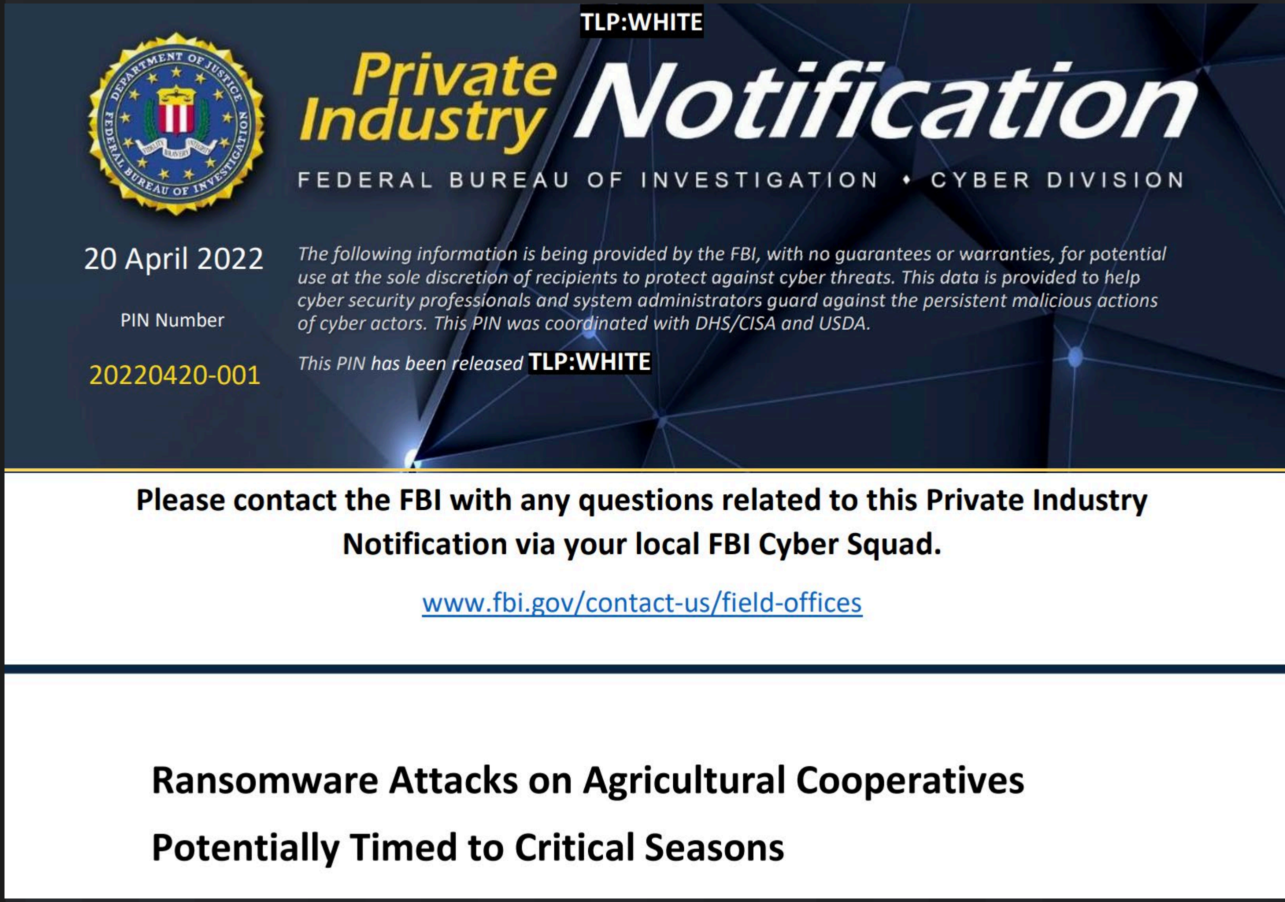
https://blog.talosintelligence.com/ukraine-and-fragility-of-agriculture/

But it goes deeper of course

What else ties into Ag? *Everything.*

FBI PIN Alert

https://www.ic3.gov/CSA/2022/220420-2.pdf



TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

20 April 2022

PIN Number

20220420-001

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS/CISA and USDA.

This PIN has been released **TLP:WHITE**

Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.

www.fbi.gov/contact-us/field-offices

Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons

Food for thought….

“The FBI noted ransomware attacks during these seasons against six grain cooperatives during the fall 2021 harvest and two attacks in early 2022 that could impact the planting season by disrupting the supply of seeds and fertilizer. Cyber actors may perceive cooperatives as lucrative targets with a willingness to pay due to the timesensitive role they play in agricultural production. Although ransomware attacks against the entire farm-to-table spectrum of the FA sector occur on a regular basis, the number of cyber attacks against agricultural cooperatives during key seasons is notable.”

Excellent work here!

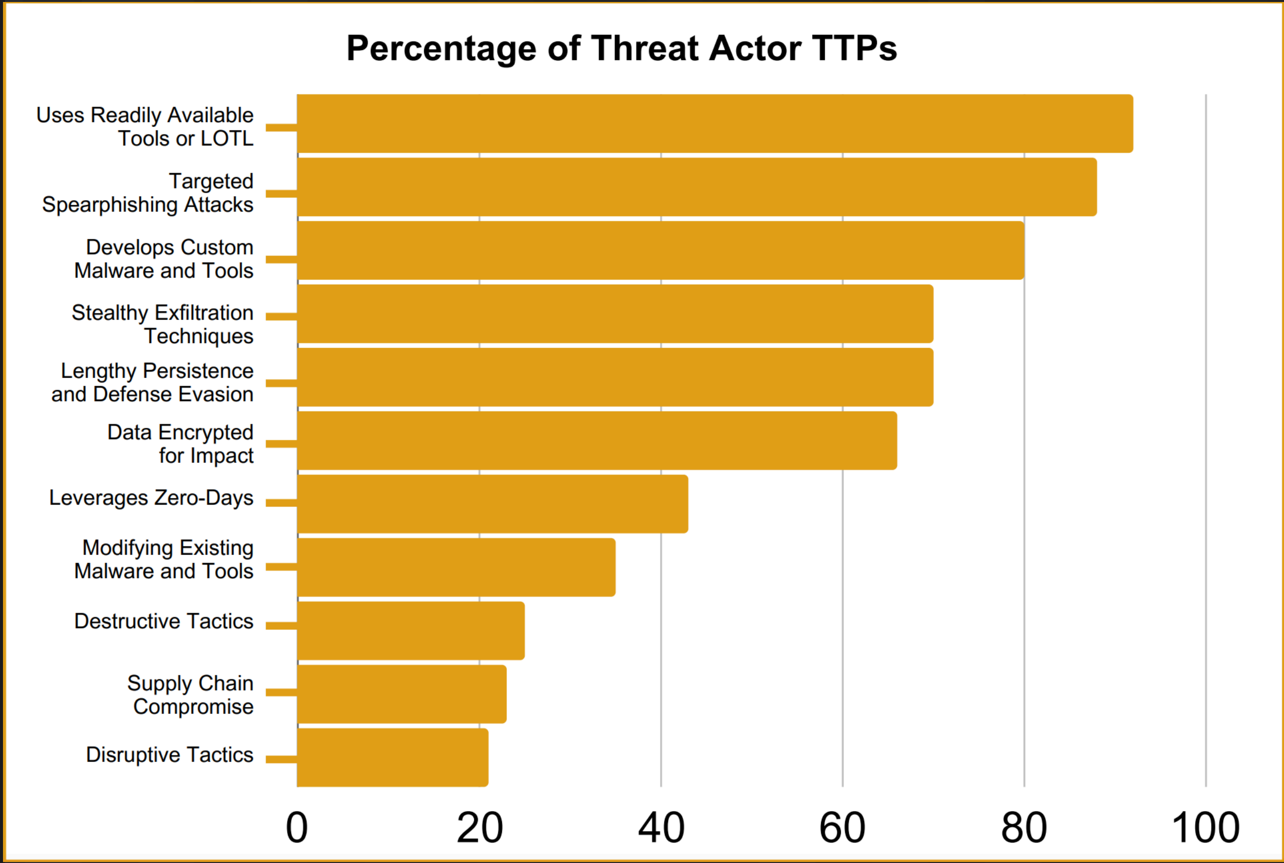
https://www.foodandag-isac.org/_files/ugd/473ff0_08416fb686f54fd7837b6e3e5df00054.pdf

Food Ag ISAC

An IT ISAC Community

FARM-TO-TABLE RANSOMWARE REALITIES

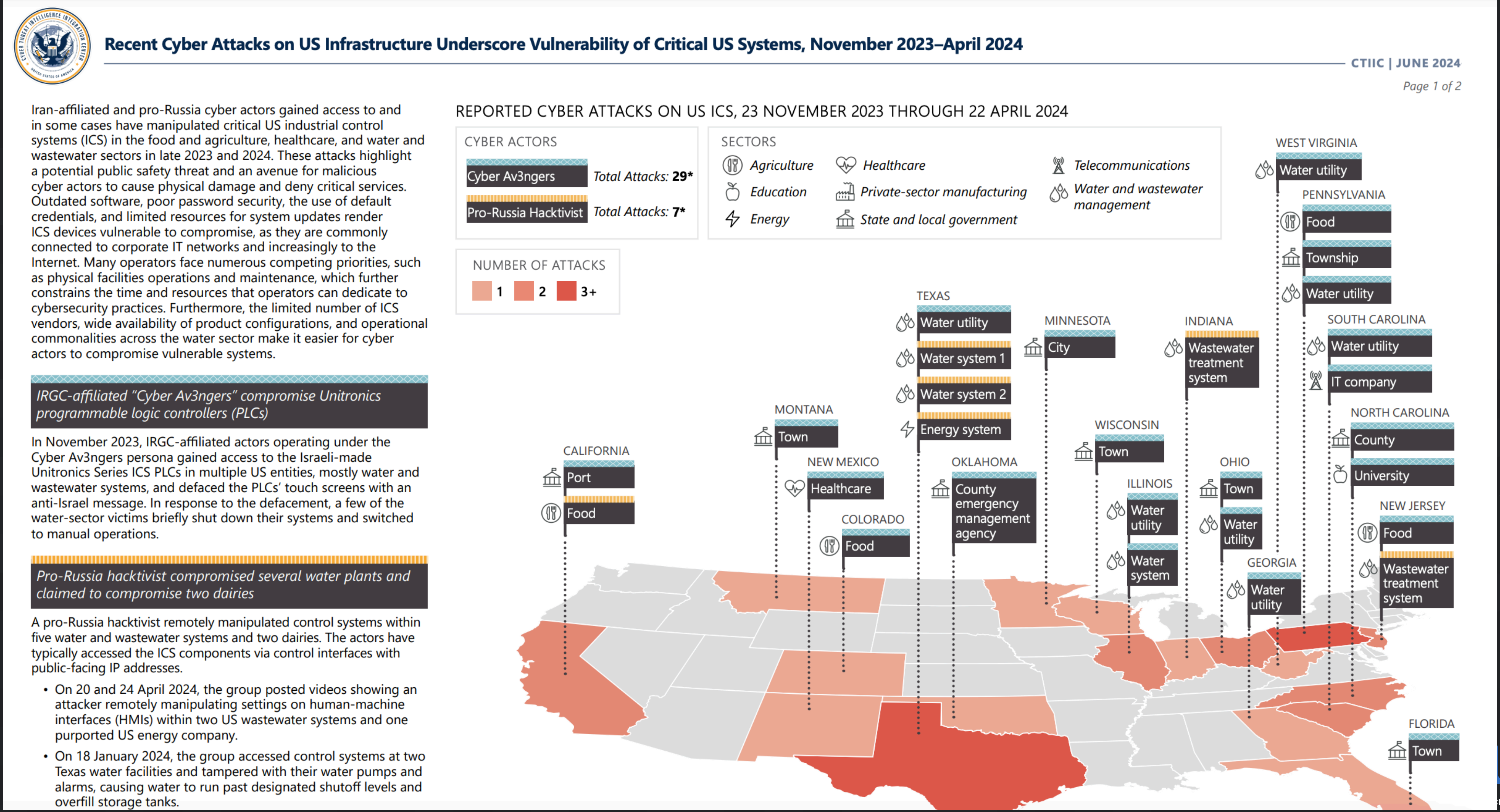
Exploring the 2023 Ransomware Landscape and Insights for 2024 https://www.foodandag-isac.org/_files/ugd/473ff0_70ffe1fe676e4adfb4c726de66864371.pdf



Cisco Security Research

Infrastructure writ large are targets

https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf



Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024

CTIIC | JUNE 2024

Page 1 of 2

Iran-affiliated and pro-Russia cyber actors gained access to and in some cases have manipulated critical US industrial control systems (ICS) in the food and agriculture, healthcare, and water and wastewater sectors in late 2023 and 2024. These attacks highlight a potential public safety threat and an avenue for malicious cyber actors to cause physical damage and deny critical services. Outdated software, poor password security, the use of default credentials, and limited resources for system updates render ICS devices vulnerable to compromise, as they are commonly connected to corporate IT networks and increasingly to the Internet. Many operators face numerous competing priorities, such as physical facilities operations and maintenance, which further constrains the time and resources that operators can dedicate to cybersecurity practices. Furthermore, the limited number of ICS vendors, wide availability of product configurations, and operational commonalities across the water sector make it easier for cyber actors to compromise vulnerable systems.

IRGC-affiliated "Cyber Av3ngers" compromise Unitronics programmable logic controllers (PLCs)

In November 2023, IRGC-affiliated actors operating under the Cyber Av3ngers persona gained access to the Israeli-made Unitronics Series ICS PLCs in multiple US entities, mostly water and wastewater systems, and defaced the PLCs' touch screens with an anti-Israel message. In response to the defacement, a few of the water-sector victims briefly shut down their systems and switched to manual operations.

Pro-Russia hacktivist compromised several water plants and claimed to compromise two dairies

A pro-Russia hacktivist remotely manipulated control systems within five water and wastewater systems and two dairies. The actors have typically accessed the ICS components via control interfaces with public-facing IP addresses.

- On 20 and 24 April 2024, the group posted videos showing an attacker remotely manipulating settings on human-machine interfaces (HMIs) within two US wastewater systems and one purported US energy company.
- On 18 January 2024, the group accessed control systems at two Texas water facilities and tampered with their water pumps and alarms, causing water to run past designated shutoff levels and overfill storage tanks.

REPORTED CYBER ATTACKS ON US ICS, 23 NOVEMBER 2023 THROUGH 22 APRIL 2024

CYBER ACTORS

Cyber Av3ngers	*Total Attacks:* **29***
Pro-Russia Hacktivist	*Total Attacks:* **7***

SECTORS

Agriculture, *Education*, *Energy*, *Healthcare*, *Private-sector manufacturing*, *State and local government*, *Telecommunications*, *Water and wastewater management*

NUMBER OF ATTACKS

🟥 1 🟥 2 🟥 3+

CALIFORNIA
- Port
- Food

MONTANA
- Town

NEW MEXICO
- Healthcare

COLORADO
- Food

TEXAS
- Water utility
- Water system 1
- Water system 2
- Energy system

OKLAHOMA
- County emergency management agency

MINNESOTA
- City

WISCONSIN
- Town

ILLINOIS
- Water utility
- Water system

INDIANA
- Wastewater treatment system

OHIO
- Town
- Water utility

GEORGIA
- Water utility

WEST VIRGINIA
- Water utility

PENNSYLVANIA
- Food
- Township
- Water utility

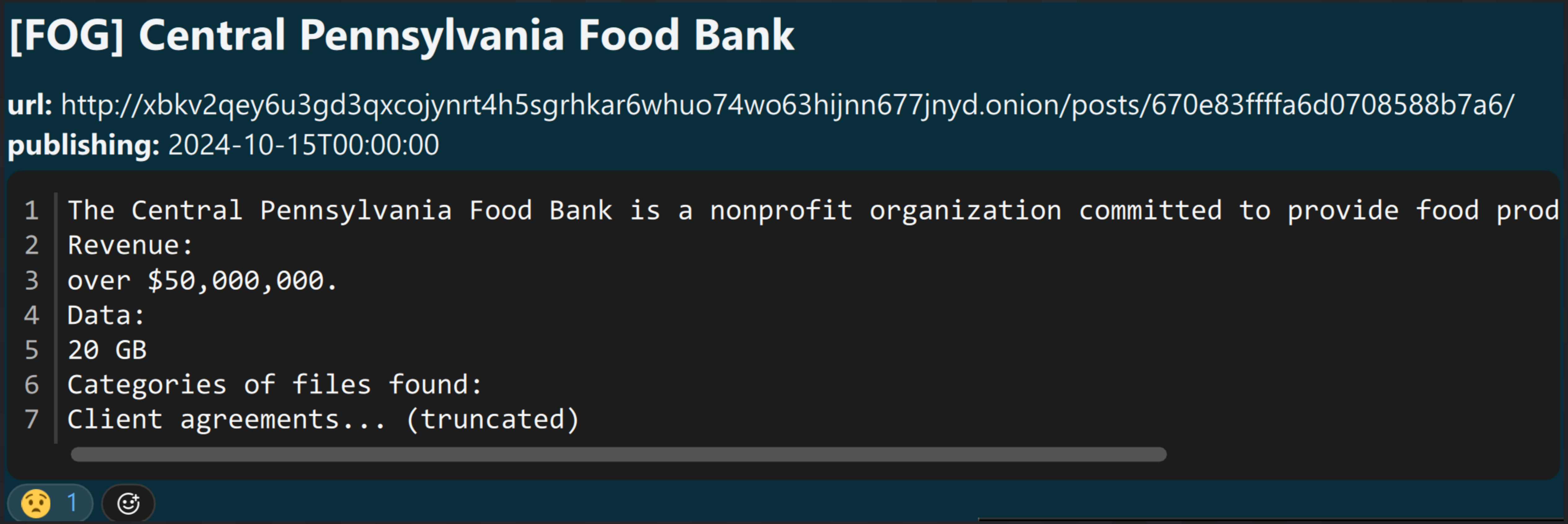
SOUTH CAROLINA
- Water utility
- IT company

NORTH CAROLINA
- County
- University

NEW JERSEY
- Food
- Wastewater treatment system

FLORIDA
- Town

Why I do what I do



[FOG] Central Pennsylvania Food Bank

url: http://xbkv2qey6u3gd3qxcojynrt4h5sgrhkar6whuo74wo63hijnn677jnyd.onion/posts/670e83ffffa6d0708588b7a6/
publishing: 2024-10-15T00:00:00

```
The Central Pennsylvania Food Bank is a nonprofit organization committed to provide food prod
Revenue:
over $50,000,000.
Data:
20 GB
Categories of files found:
Client agreements... (truncated)
```

Q&A

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity