12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island

EYES WIDE OPEN

What Are the Challenges Most States and Local Government Face Today?

Joe Marshall

Sr. Strategist ICS/Threat Research, CISCO Talos

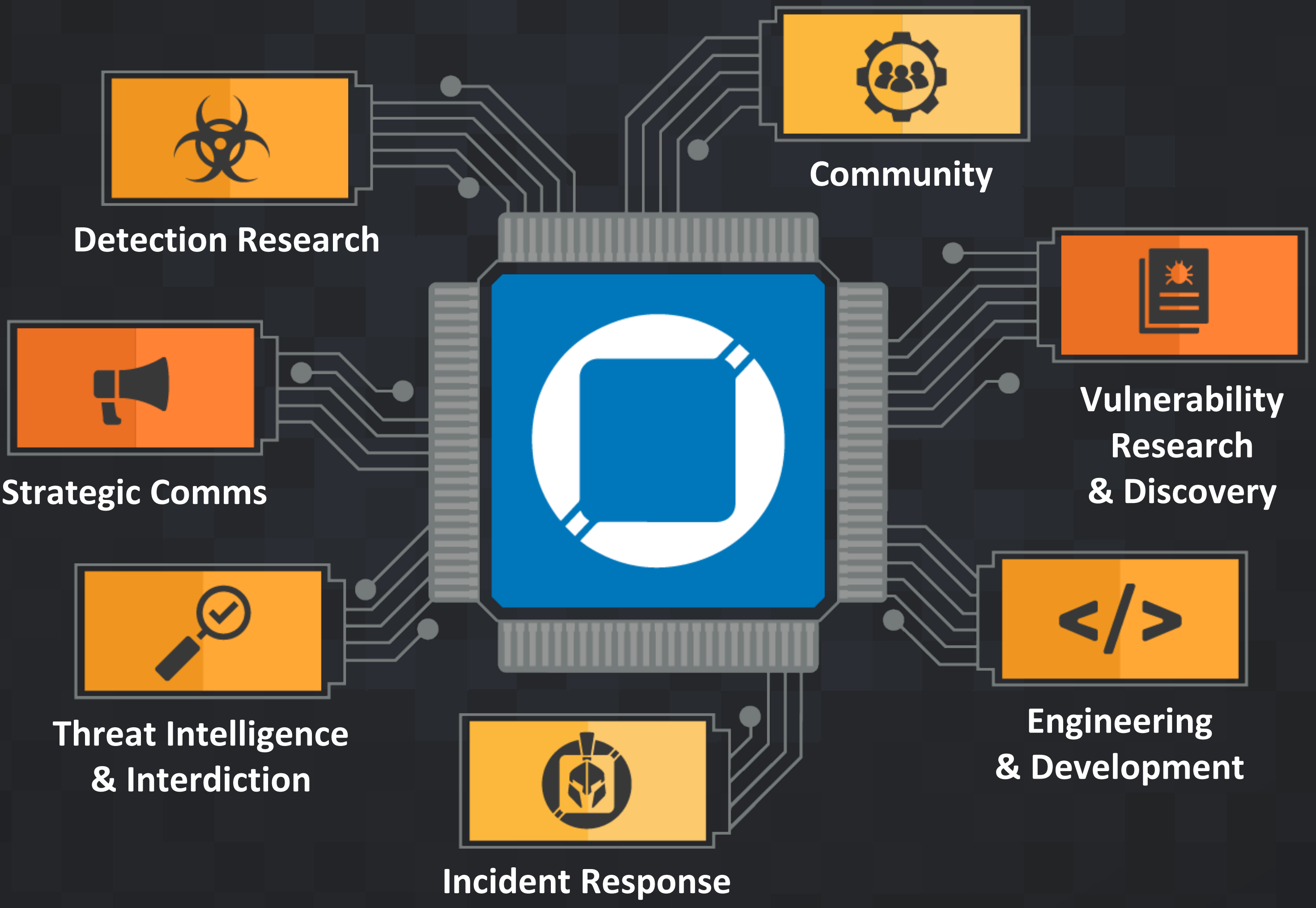
TALOS

Cisco Security Research

Fighting the Good Fight

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.


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

Talos
Cisco Security Research

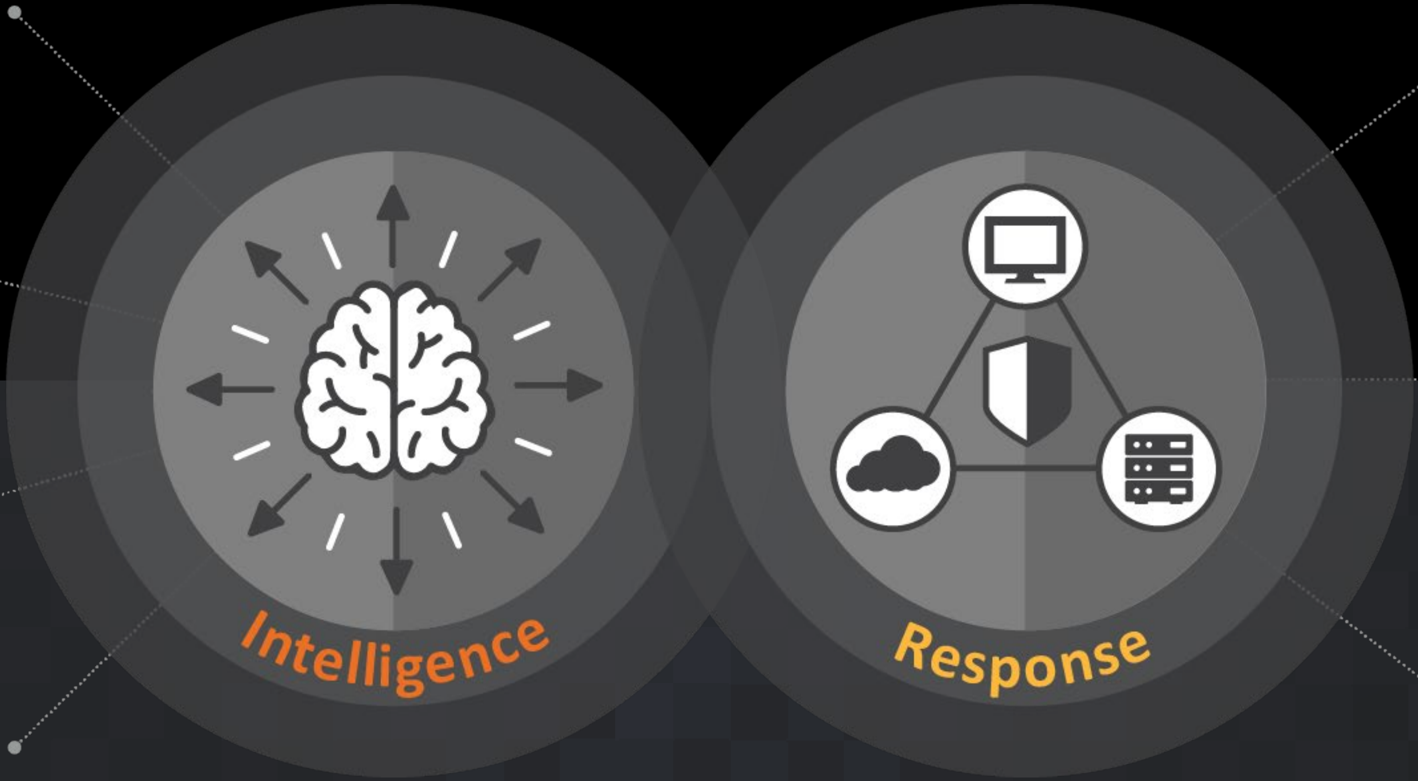
Talos tracks numerous threats

625B
web requests per day

200+
vulnerabilities discovered per year

1.4M+
new malware samples per day

30B
endpoint events per day



840K
networks protected

67M
mailboxes protected

87M
endpoints protected

Talos
Cisco Security Research

Cyber attacks in Ukraine

Seven plus months into the invasion

Talos

Cisco Security Research

NotPetya: The Costliest Cyber Attack in History

Unmatched Visibility

- AMP
- Ukraine Cyber Police
- Snort rules

Actionable Intelligence

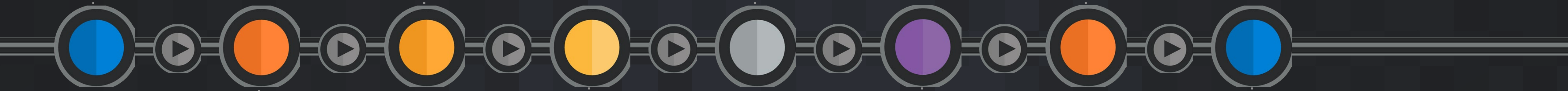
- Gathering IOCs
- Highly destructive supply chain attack
- Cyber weapon targeting the general public
- One of the costliest cyber attacks in history

Collective Response

- Field engagement
- Shipped protection
- Snort rules
- Blogs
- Consumable IOCs
- Product maturation

Talos
Cisco Security Research

A refresher of cyber attacks in Ukraine



February 2014

Russia invades Ukraine, taking the Crimea Peninsula and Donbas region

December 2015

Russia launches cyber attack, Black Energy 2, disrupting power

December 2016

Industroyer attack disrupts power again

2017 NotPetya

Supply Chain attack – costliest attack in history

February 2022

Russia invades Ukraine. Talos forms Task Force SU to assist defenders in UA

April 2022

Industroyer2 attempts to disrupt power

Feb-June 2022

WhisperGate, BGP hijack, Caddy Wiper ,Viasat, etc

June-OCT 2022

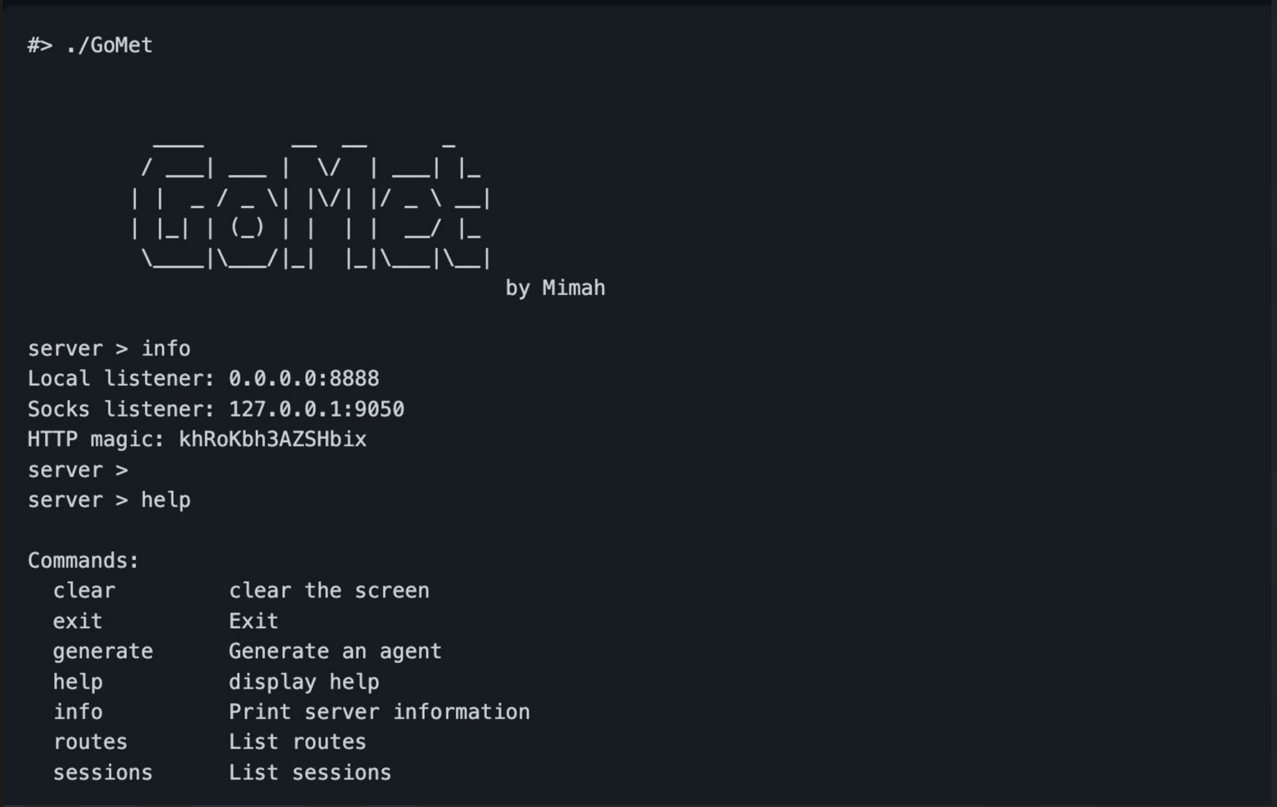
Pivot to deeper espionage and supply chain disruption

What’s new?

- Objectives have shifted - rebuilding infrastructure for new attacks
- Evidence that additional supply chain-based attacks are being planned
- Strong pivot into espionage – Baltic states, and Eastern Europe, along with other NATO countries
- Adversary OPTEMPO remains strong

Supply Chain and GoMet in Ukraine

- Targeted a massive supplier in Ukraine
- Absolute viability in unconnected systems
- Few, if any, look for or know about it
- Sounds a little familiar….

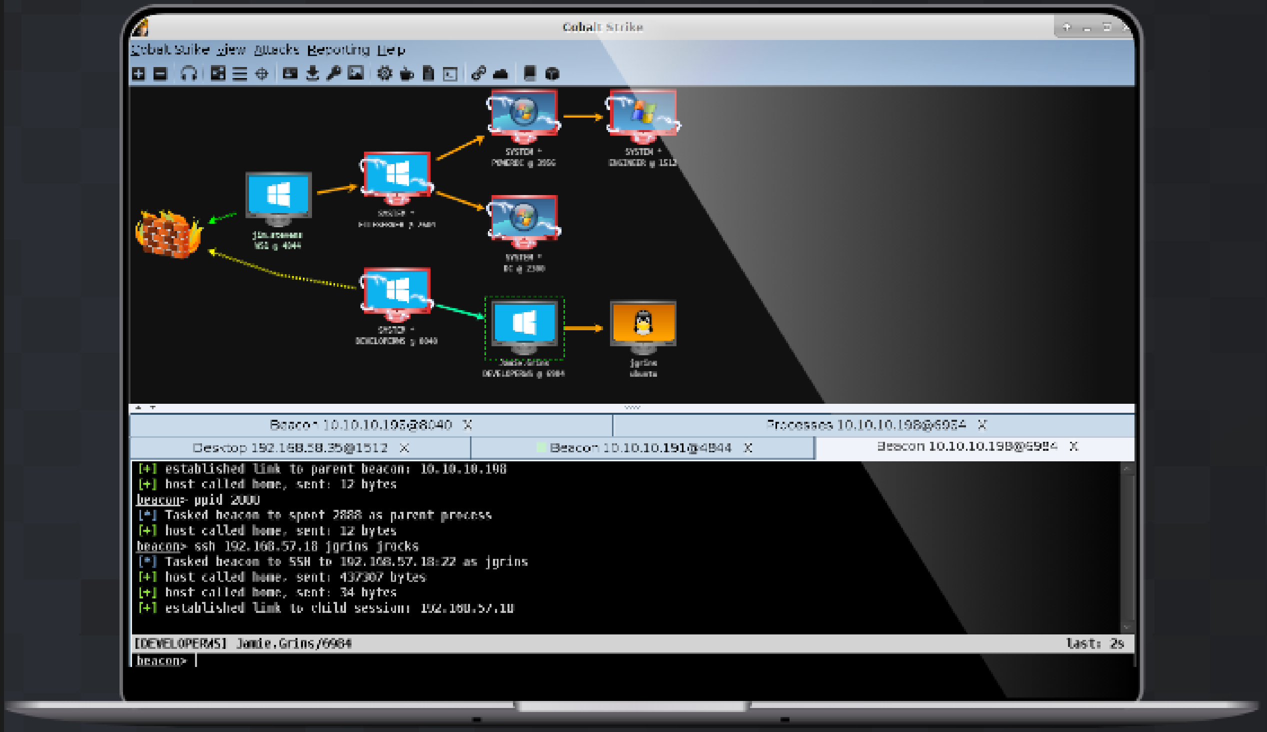


```
#> ./GoMet


          ____       __  __      _
         / ___| ___ |  \/  | ___| |_
        | |  _ / _ \| |\/| |/ _ \ __|
        | |_| | (_) | |  | |  __/ |_
         \____|\___/|_|  |_|\___|\__|
                                      by Mimah

server > info
Local listener: 0.0.0.0:8888
Socks listener: 127.0.0.1:9050
HTTP magic: khRoKbh3AZSHbix
server >
server > help

Commands:
  clear          clear the screen
  exit           Exit
  generate       Generate an agent
  help           display help
  info           Print server information
  routes         List routes
  sessions       List sessions
```

Cobalt Strike Beacon Chain?

(GoMet is better I think)

https://blog.talosintelligence.com/2022/07/attackers-target-ukraine-using-gomet.html

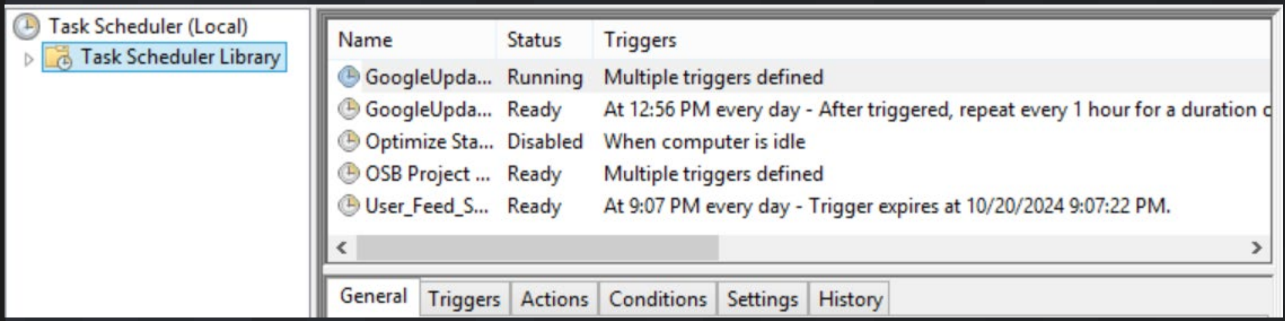

Cobalt Strike
Cobalt Strike View Attacks Reporting Help
SYSTEM * POWERDC @ 2956
SYSTEM * ENGINEER @ 1512
SYSTEM * DC @ 2380
SYSTEM * DEVELOPER45 @ 8040
Jamie.Grins DEVELOPER45 @ 6984
jgrins ubuntu
Beacon 10.10.10.195@8040 X
Processes 10.10.10.198@6984 X
Desktop 192.168.58.35@1512 X
Beacon 10.10.10.191@4844 X
Beacon 10.10.10.198@6984 X

```
[+] established link to parent beacon: 10.10.10.198
[+] host called home, sent: 12 bytes
beacon> ppid 2000
[*] Tasked beacon to spoof 2888 as parent process
[+] host called home, sent: 12 bytes
beacon> ssh 192.168.57.18 jgrins jrocks
[*] Tasked beacon to SSH to 192.168.57.18:22 as jgrins
[+] host called home, sent: 437307 bytes
[+] host called home, sent: 34 bytes
[+] established link to child session: 192.168.57.18
[DEVELOPER45] Jamie.Grins/6984                                   last: 2s
beacon>
```

Talos
Cisco Security Research

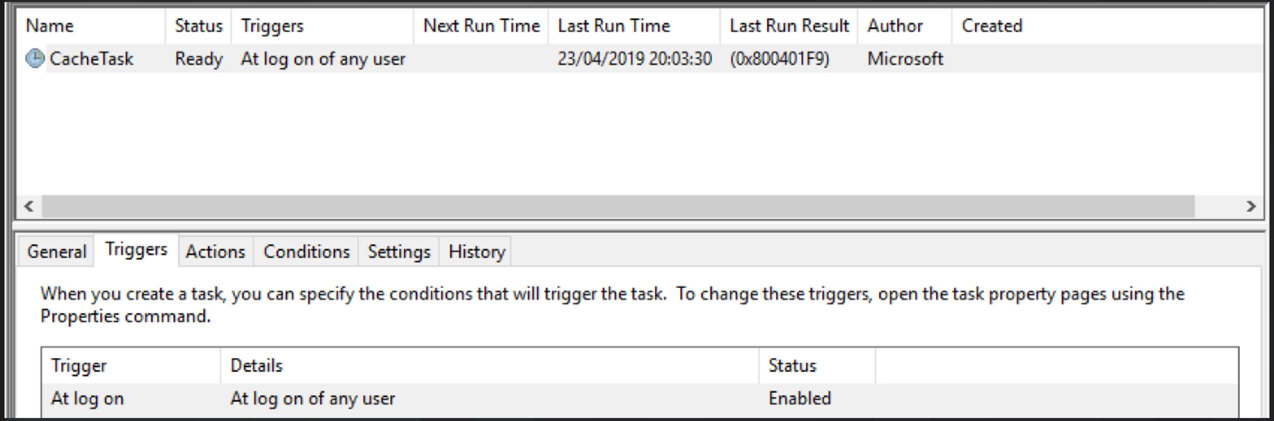
Super slick persistence

- Old tactic with a twist
- Task PE replacement!
- Good ‘ol MITRE ATT&CK T053



Name	Status	Triggers
GoogleUpda...	Running	Multiple triggers defined
GoogleUpda...	Ready	At 12:56 PM every day - After triggered, repeat every 1 hour for a duration
Optimize Sta...	Disabled	When computer is idle
OSB Project ...	Ready	Multiple triggers defined
User_Feed_S...	Ready	At 9:07 PM every day - Trigger expires at 10/20/2024 9:07:22 PM.

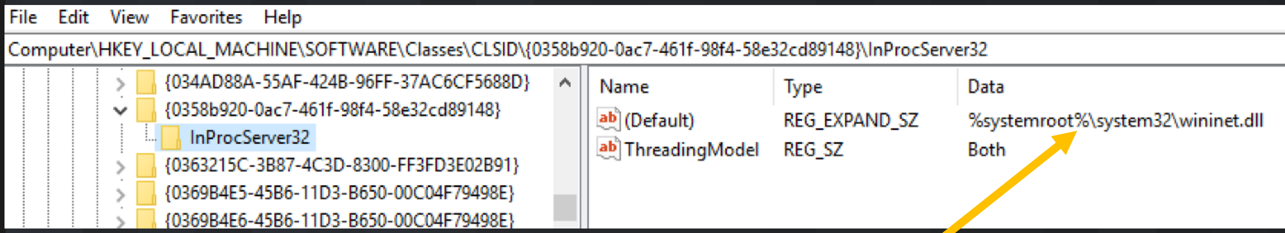
Like COM hijacking (but simpler)



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author	Created
CacheTask	Ready	At log on of any user		23/04/2019 20:03:30	(0x800401F9)	Microsoft	

When you create a task, you can specify the conditions that will trigger the task. To change these triggers, open the task property pages using the Properties command.

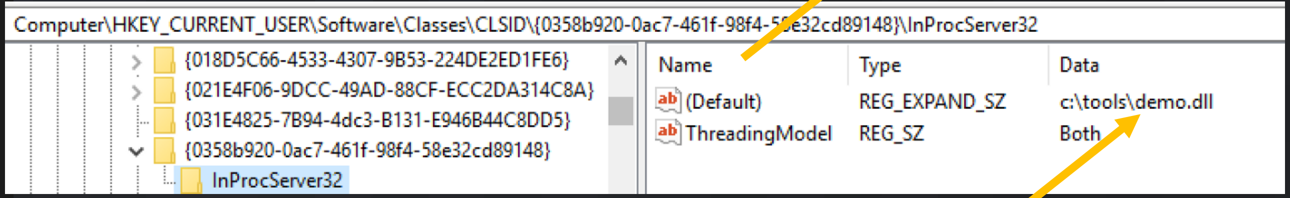
Trigger	Details	Status
At log on	At log on of any user	Enabled



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{0358b920-0ac7-461f-98f4-58e32cd89148}\InProcServer32

{034AD88A-55AF-424B-96FF-37AC6CF5688D}
{0358b920-0ac7-461f-98f4-58e32cd89148}
InProcServer32
{0363215C-3B87-4C3D-8300-FF3FD3E02B91}
{0369B4E5-45B6-11D3-B650-00C04F79498E}
{0369B4E6-45B6-11D3-B650-00C04F79498E}

Name	Type	Data
(Default)	REG_EXPAND_SZ	%systemroot%\system32\wininet.dll
ThreadingModel	REG_SZ	Both



Computer\HKEY_CURRENT_USER\Software\Classes\CLSID\{0358b920-0ac7-461f-98f4-58e32cd89148}\InProcServer32

{018D5C66-4533-4307-9B53-224DE2ED1FE6}
{021E4F06-9DCC-49AD-88CF-ECC2DA314C8A}
{031E4825-7B94-4dc3-B131-E946B44C8DD5}
{0358b920-0ac7-461f-98f4-58e32cd89148}
InProcServer32

Name	Type	Data
(Default)	REG_EXPAND_SZ	c:\tools\demo.dll
ThreadingModel	REG_SZ	Both

Talos continues to support Ukraine cyber

Additional threat hunters added

- Over 650 threat hunters across Cisco supporting Ukraine
- Active collaboration with threat hunters and incident response teams in Ukrainian private and public industry

Deep telemetry into Ukraine cyber space

- Over 30 critical industries being actively monitored
- 22,000+ endpoints being actively monitored
- Actively monitoring new behaviors and tactics Russian APT’s are utilizing real time

What can you do?

✓ Nothing we have seen in Ukraine changes our recommendations

✓ Everything that you know you're supposed to be doing is what you should do

✓ You know where you have "accepted risk"

- Revisit that decision
- Harden that environment
- Isolate and monitor aggressively

✓ Focus intelligence activities to understand current Russian and unattributed activities and react quickly

Talos
Cisco Security Research

Understanding ransomware & Russia & you

Financial crimes and geopolitics

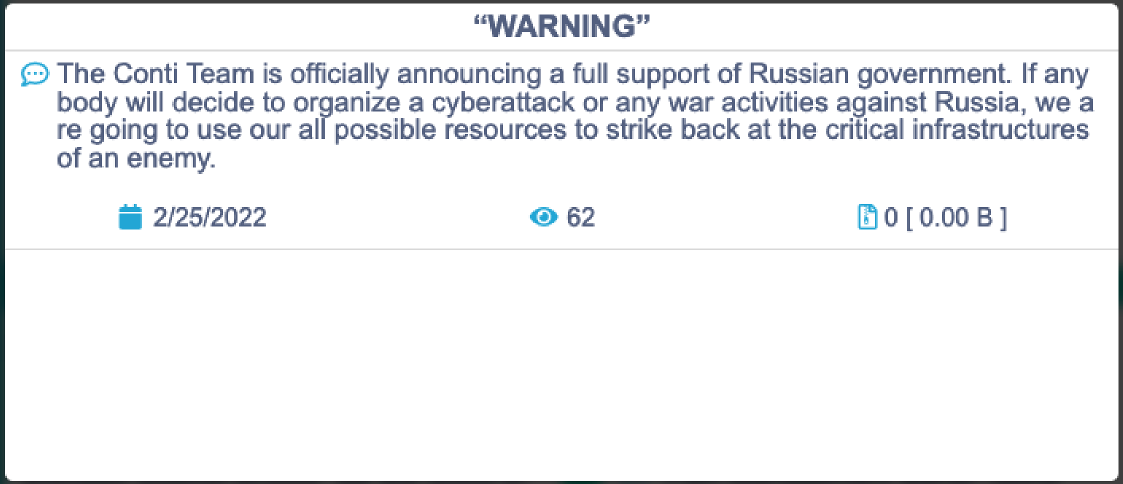
TALOS

Cisco Security Research

A preface on cartels

Russia and the Cartels

Example: Conti Cartel (RIP)



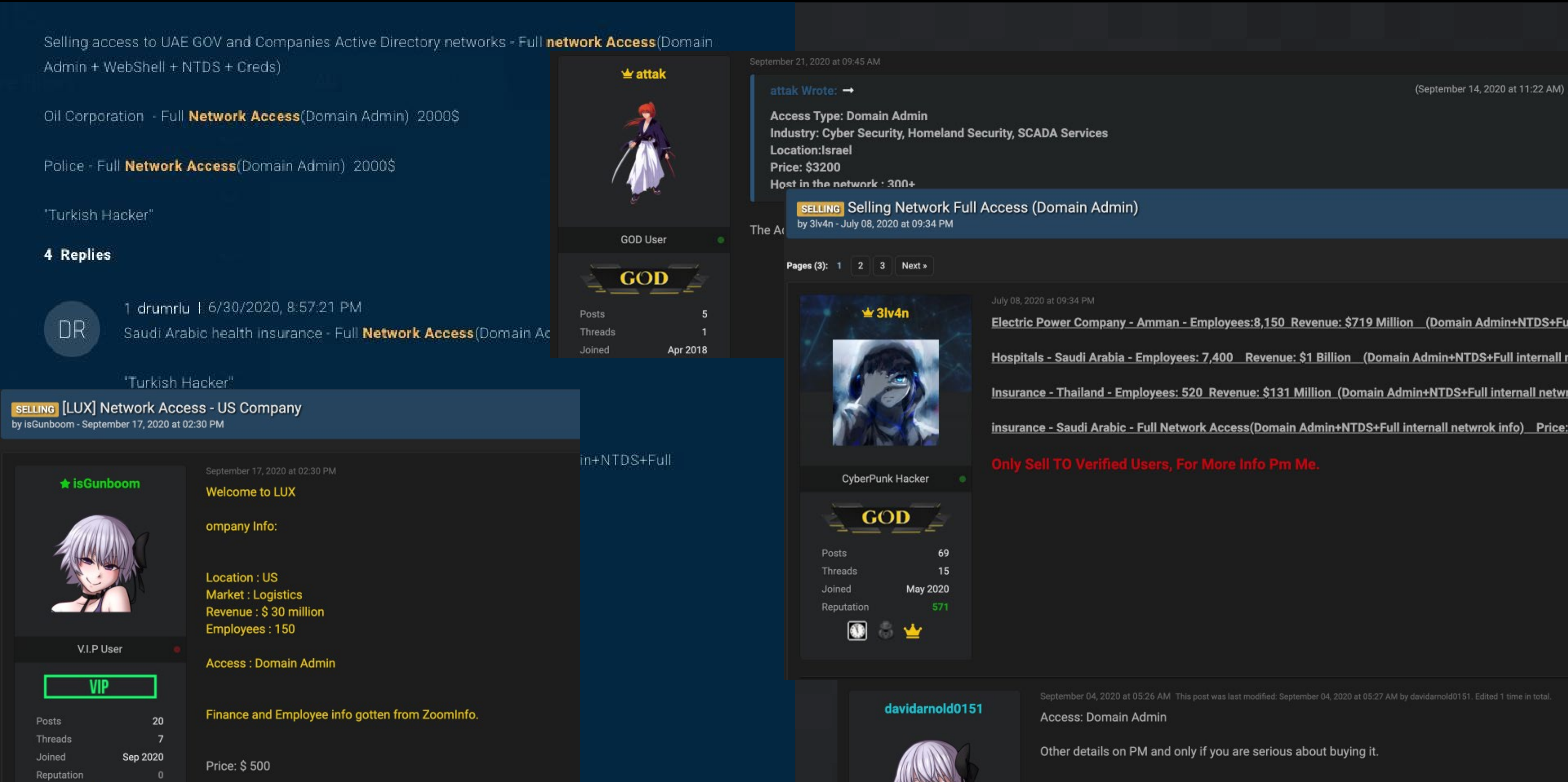
“WARNING”

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.

2/25/2022 62 0 [0.00 B]

Talos
Cisco Security Research

Admin Access for Sale



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 n

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

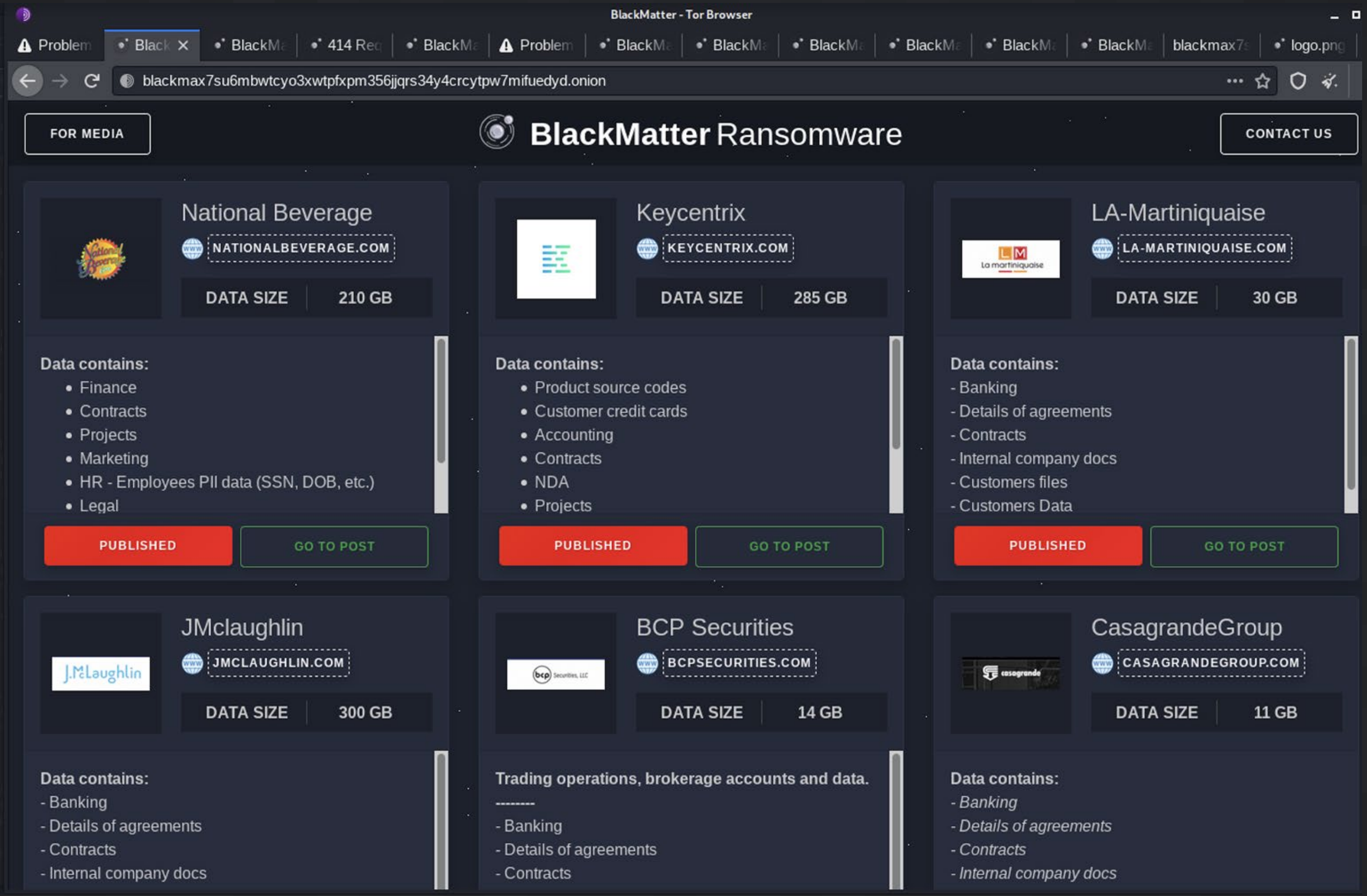
davidarnold0151

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.

2022: Data Exfiltration



blackmax7su6mbwtcyo3xwtpfxpm356jjqrs34y4crcytpw7mifuedyd.onion

BlackMatter Ransomware

National Beverage

NATIONALBEVERAGE.COM

DATA SIZE	210 GB

Data contains:

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

PUBLISHED | GO TO POST

Keycentrix

KEYCENTRIX.COM

DATA SIZE	285 GB

Data contains:

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

PUBLISHED | GO TO POST

LA-Martiniquaise

LA-MARTINIQUAISE.COM

DATA SIZE	30 GB

Data contains:

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

PUBLISHED | GO TO POST

JMclaughlin

JMCLAUGHLIN.COM

DATA SIZE	300 GB

Data contains:

- Banking
- Details of agreements
- Contracts
- Internal company docs

BCP Securities

BCPSECURITIES.COM

DATA SIZE	14 GB

Trading operations, brokerage accounts and data.

- Banking
- Details of agreements
- Contracts

CasagrandeGroup

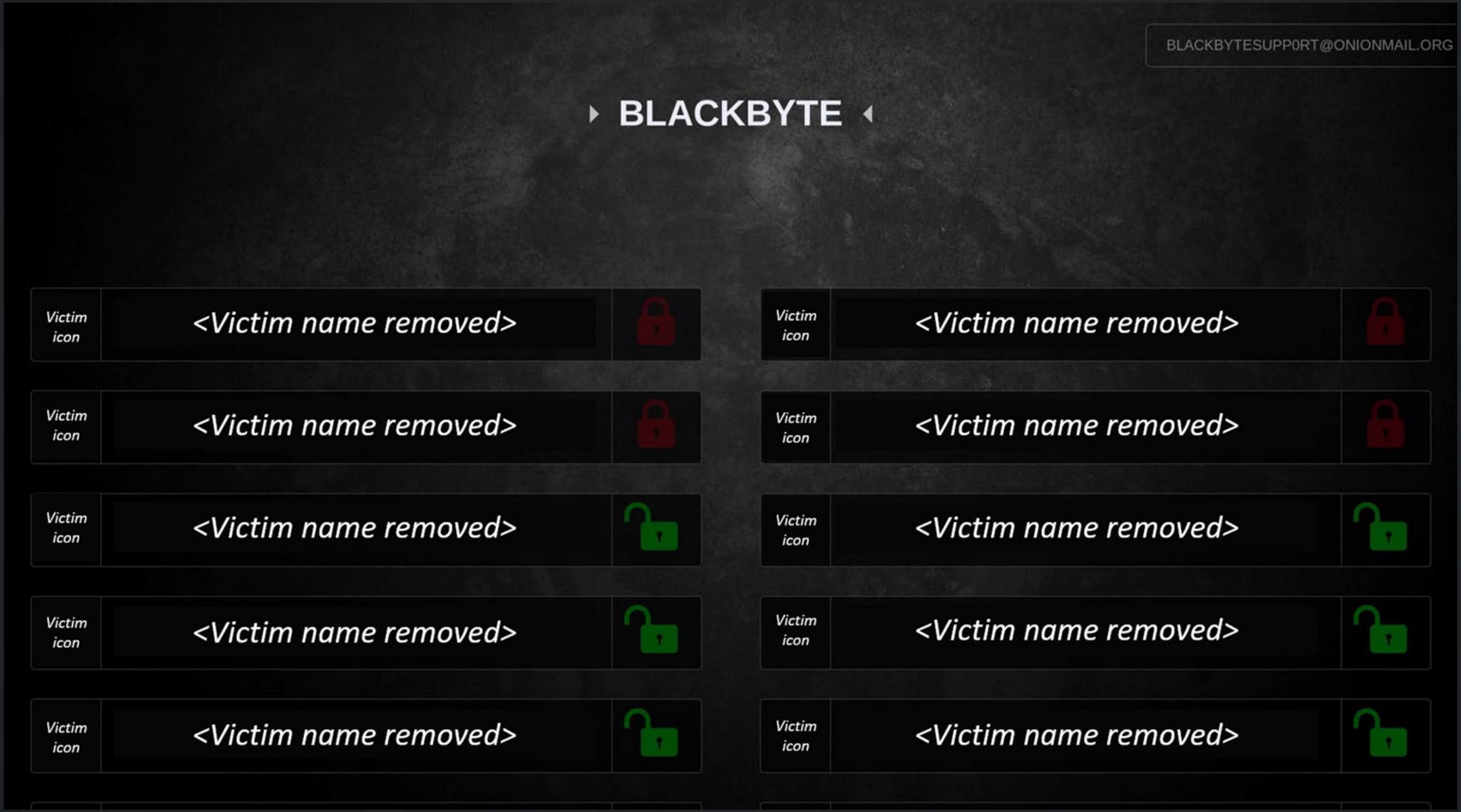
CASAGRANDEGROUP.COM

DATA SIZE	11 GB

Data contains:

- *Banking*
- *Details of agreements*
- *Contracts*
- *Internal company docs*

Blackbyte

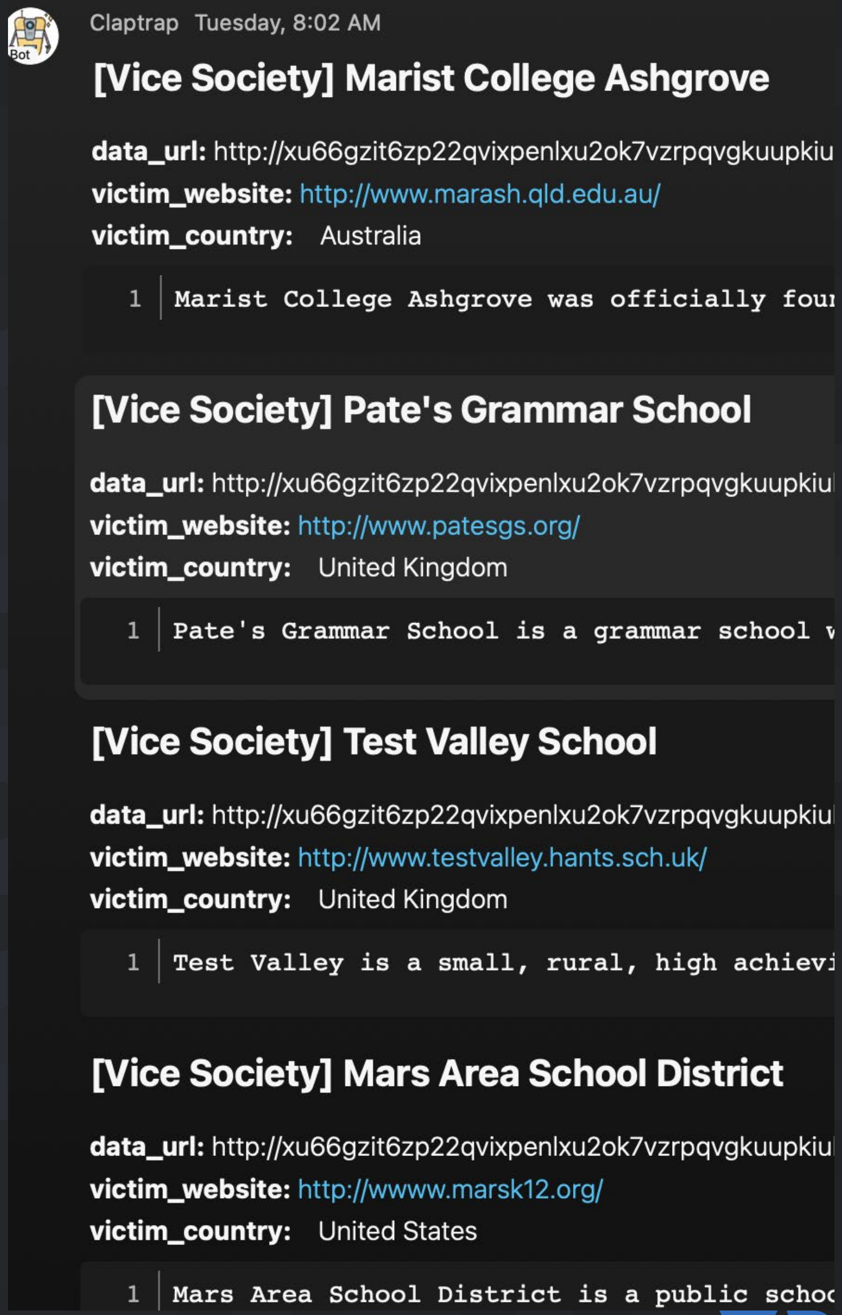


BLACKBYTESUPP0RT@ONIONMAIL.ORG

BLACKBYTE

Victim icon	<Victim name removed>	🔒
Victim icon	<Victim name removed>	🔒
Victim icon	<Victim name removed>	🔓
Victim icon	<Victim name removed>	🔓
Victim icon	<Victim name removed>	🔓
Victim icon	<Victim name removed>	🔒
Victim icon	<Victim name removed>	🔒
Victim icon	<Victim name removed>	🔓
Victim icon	<Victim name removed>	🔓
Victim icon	<Victim name removed>	🔓

Example



Claptrap Tuesday, 8:02 AM

[Vice Society] Marist College Ashgrove

data_url: http://xu66gzit6zp22qvixpenlxu2ok7vzrpqvgkuupkiu

victim_website: http://www.marash.qld.edu.au/

victim_country: Australia

```
Marist College Ashgrove was officially fou
```

[Vice Society] Pate's Grammar School

data_url: http://xu66gzit6zp22qvixpenlxu2ok7vzrpqvgkuupkiu

victim_website: http://www.patesgs.org/

victim_country: United Kingdom

```
Pate's Grammar School is a grammar school w
```

[Vice Society] Test Valley School

data_url: http://xu66gzit6zp22qvixpenlxu2ok7vzrpqvgkuupkiu

victim_website: http://www.testvalley.hants.sch.uk/

victim_country: United Kingdom

```
Test Valley is a small, rural, high achievi
```

[Vice Society] Mars Area School District

data_url: http://xu66gzit6zp22qvixpenlxu2ok7vzrpqvgkuupkiu

victim_website: http://wwww.marsk12.org/

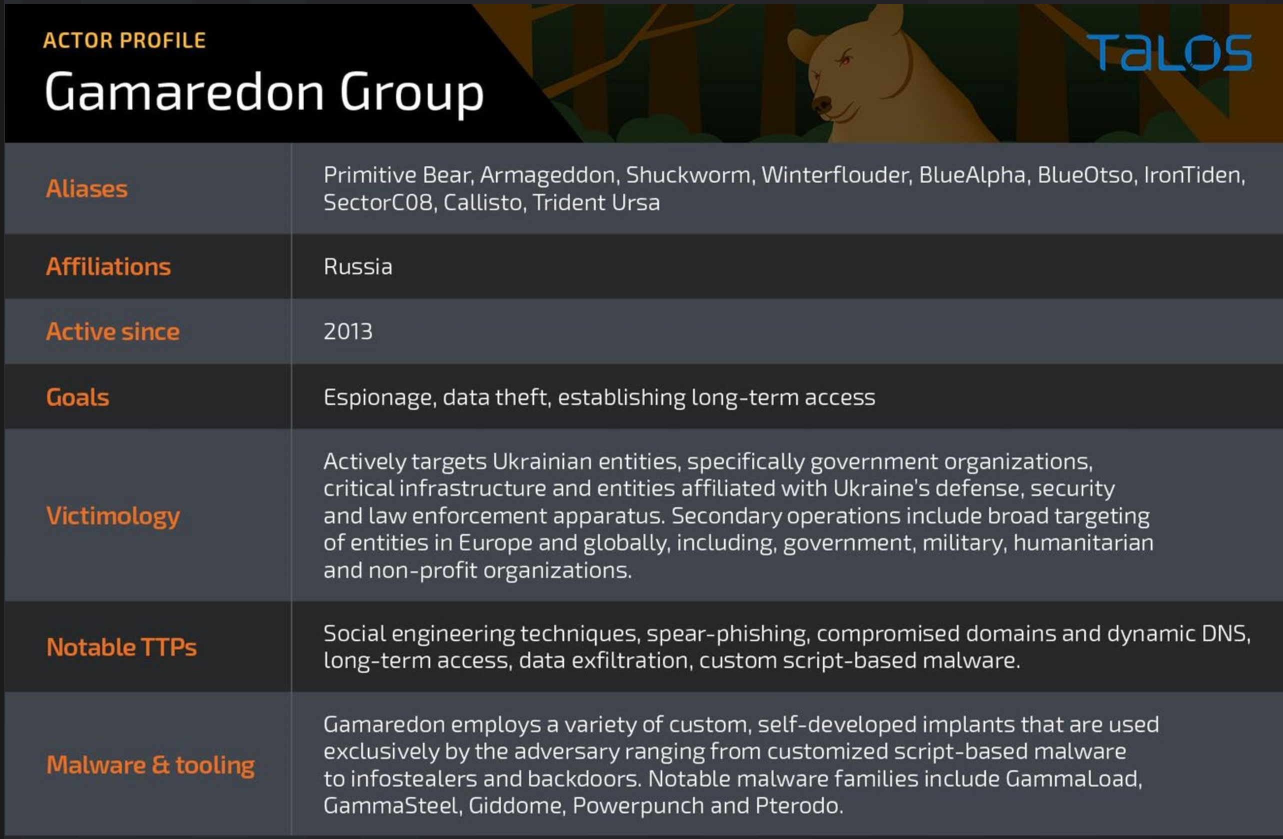
victim_country: United States

```
Mars Area School District is a public schoo
```

Case Study: Gamaredon

Cisco Security Research

Who is Gamaredon?



ACTOR PROFILE

Gamaredon Group

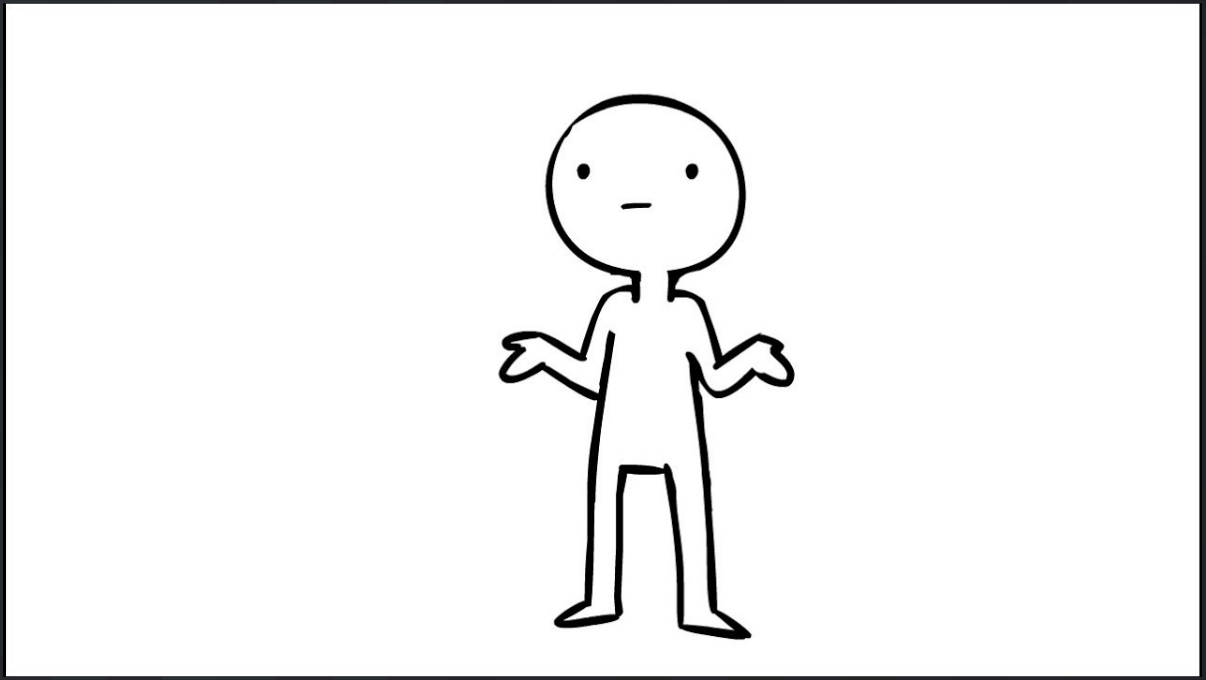
TALOS

Aliases	Primitive Bear, Armageddon, Shuckworm, Winterflouder, BlueAlpha, BlueOtso, IronTiden, SectorC08, Callisto, Trident Ursa
Affiliations	Russia
Active since	2013
Goals	Espionage, data theft, establishing long-term access
Victimology	Actively targets Ukrainian entities, specifically government organizations, critical infrastructure and entities affiliated with Ukraine's defense, security and law enforcement apparatus. Secondary operations include broad targeting of entities in Europe and globally, including, government, military, humanitarian and non-profit organizations.
Notable TTPs	Social engineering techniques, spear-phishing, compromised domains and dynamic DNS, long-term access, data exfiltration, custom script-based malware.
Malware & tooling	Gamaredon employs a variety of custom, self-developed implants that are used exclusively by the adversary ranging from customized script-based malware to infostealers and backdoors. Notable malware families include GammaLoad, GammaSteel, Giddome, Powerpunch and Pterodo.

TALOS
Cisco Security Research

Sophisticated APT?
Well. Kinda.

- Very capable
- Also very loud
- Suggestive of tradecraft that is effective but inelegant.
- Yeah, it’s kinda weird
- Pre-War: Unfocused.
- War: Ukraine



Talos
Cisco Security Research

What do we take away from this?

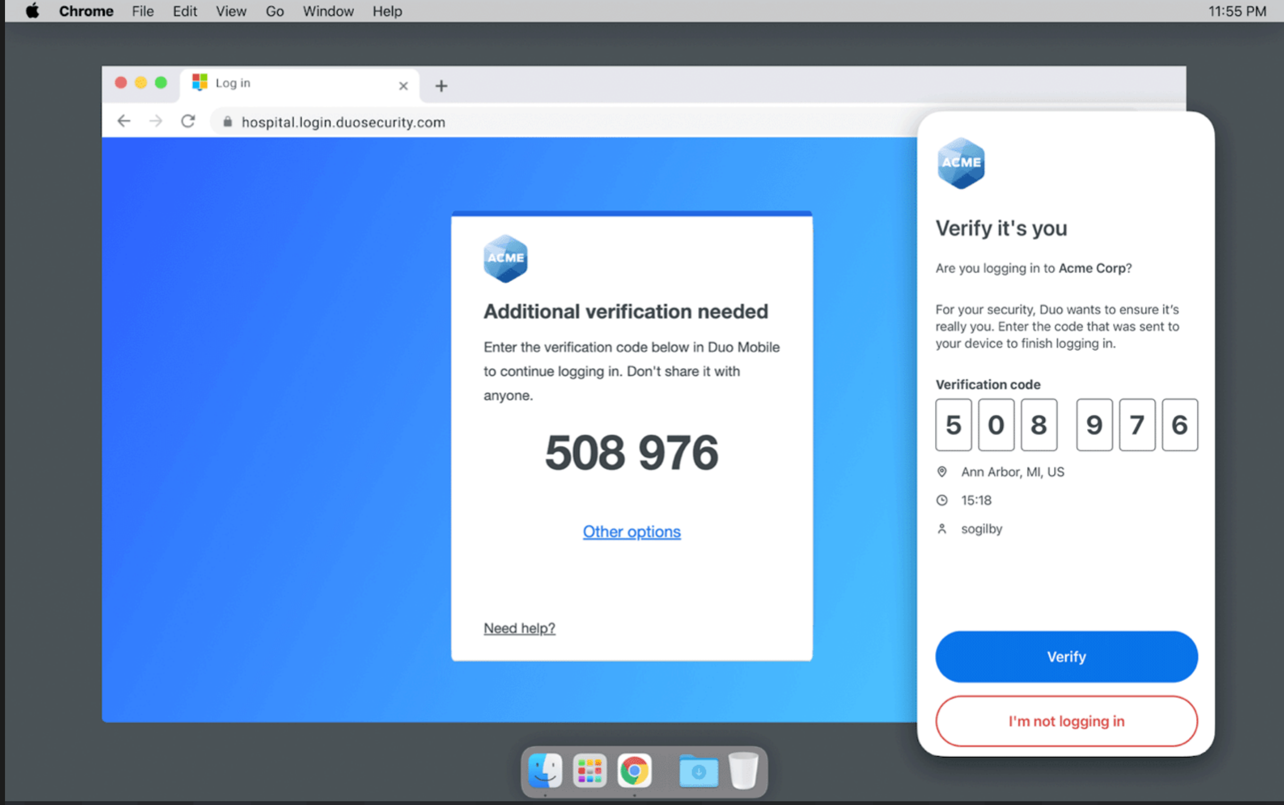
Tactics, strategy, resilience

Cisco Security Research

Knowledge is power

Strategic: MFA Fatigue

Tactical: Embrace Verified Push



Additional verification needed

Enter the verification code below in Duo Mobile to continue logging in. Don't share it with anyone.

508 976

Other options

Need help?

Verify it's you

Are you logging in to **Acme Corp**?

For your security, Duo wants to ensure it's really you. Enter the code that was sent to your device to finish logging in.

Verification code

5 0 8 9 7 6

Ann Arbor, MI, US

15:18

sogilby

Verify

I'm not logging in

Strategic: War is hell

Tactical: Visibility has saved pain in Ukraine

The fundamentals are CRITICAL

- Asset & Inventory
- Monitoring
- Baselines
- Segmentation

Prevention is where you start ……

- …**resiliency** is where you want to be
- Visibility, monitoring, and your security fundamentals are incredibly important
- Again – fundamentals. It’s a journey, not a destination.
- Learn to bend but not break

Train. Learn.

- “Everyone has a plan until they get punched in the mouth.” – Mike Tyson
- Know your risk appetite.
- Understand cyber insurance!
- Be proactive – train hard! Use 3rd party evals
  - Intelligence on demand!
  - Tabletop Exercise!
  - Threat hunts!
  - Playbooks!

Q&A

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity