CSO COUNCIL

Elitarna przestrzeń wymiany doświadczeń
dyrektorów bezpieczeństwa informacji


# Komunikacja C2

## W ransomware i w atakach APT

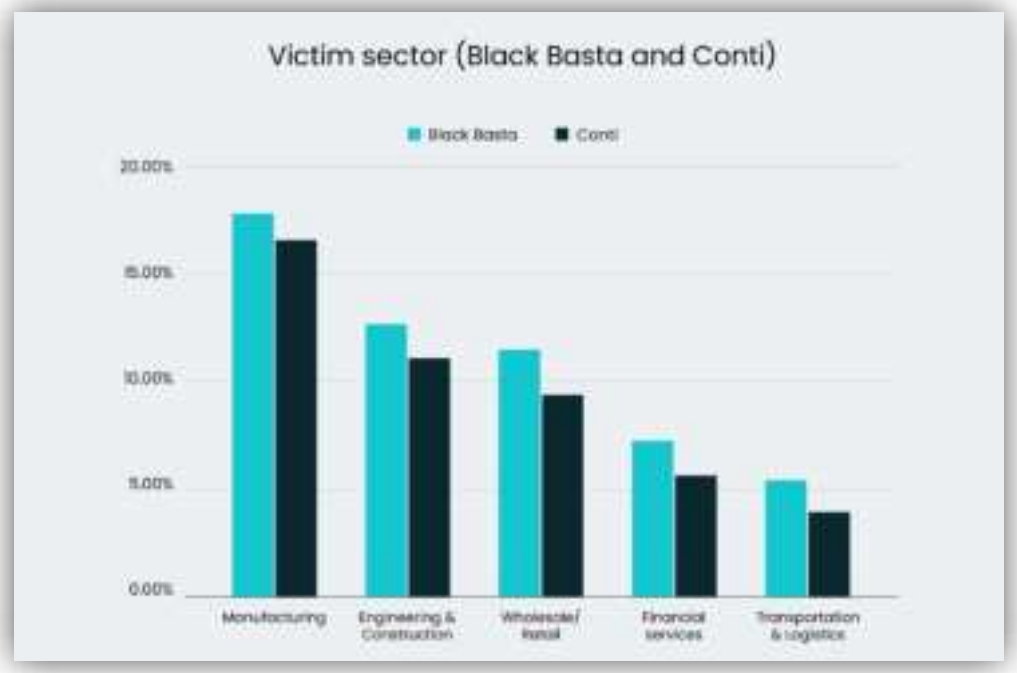
Piotr Głaska
Principal Solutions Architect

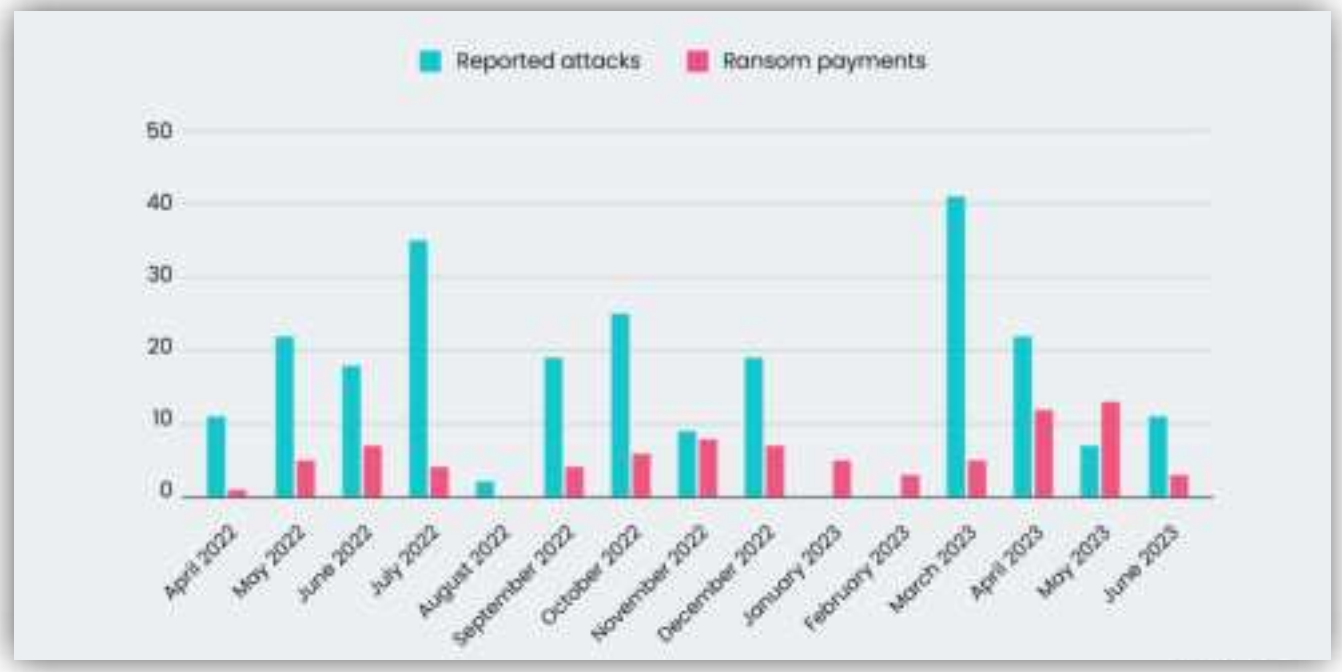
# Ransomware Black Basta

- Rosyjska grupa przestępcza, aktywna od 2022
- ~500 ofiar w 2 lata
- $107M+ okupu od 90+ ofiar (dane do XI.2023)*
- Największy zapłacony okup $9M oraz co najmniej 18 okupów powyżej $1M*
- Podwójny szantaż (zaszyfrowanie oraz wyciek danych)

* Źródło: https://www.elliptic.co/blog/black-basta-ransomware-victims-have-paid-over-100-million

# Black Basta – statystyka




Źródło: https://www.elliptic.co/blog/black-basta-ransomware-victims-have-paid-over-100-million

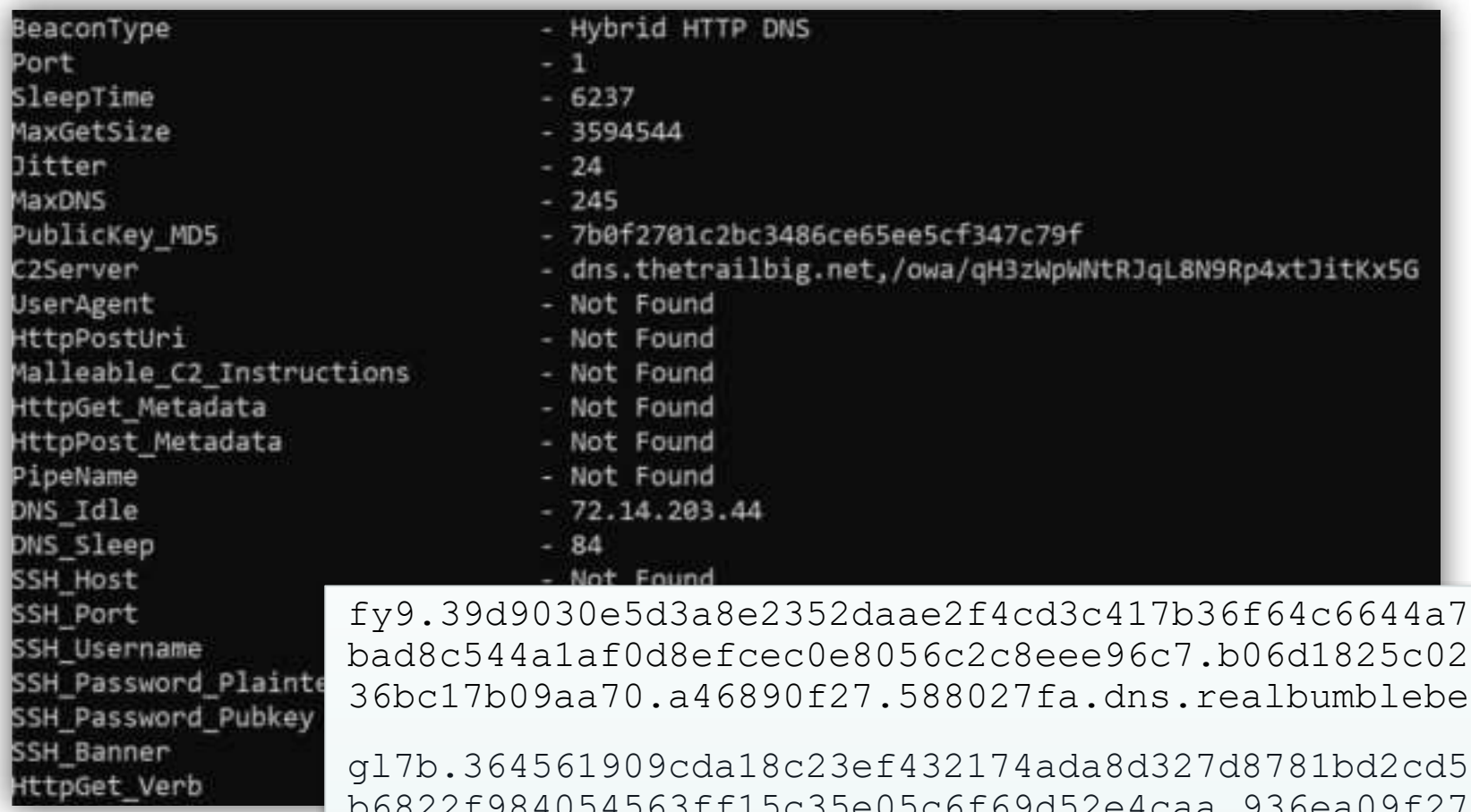
infoblox

# Black Basta – ofiary z ostatnich tygodni

| OFIARA | ZARAPORTOWANA | KRAJ | WŁAMANIE | UWAGI |
|---|---|---|---|---|
| **trugreen.com** | **21.05.2024** | **USA** | | **6000 employees, $1.5B revenue, newest Automated Moving Target Defense (AMTD) protection** |
| atlasoil.com | 21.05.2024 | USA | | |
| grupocadarso.com | 21.05.2024 | Spain | | |
| mfgroup.it | 21.05.2024 | Italy | | |
| **lactanet.ca** | **20.05.2024** | **Canada** | **mid-April 2024** | **450 employees, $88M revenue, Big4 consulting cyber-risk assessments, MDR, simulated fake phishing campaigns** |
| levian.com | 20.05.2024 | USA | | |
| gai-it.com | 4.05.2024 | Italy | | |
| active-pcb.com | 4.05.2024 | UK | | |
| synlab.com | 4.05.2024 | Italy | April 18, 2024 | |
| ayesa.com | 4.05.2024 | Spain | April 25, 2024 | |
| teaspa.it | 4.05.2024 | Italy | | |
| olsonsteel.com | 4.05.2024 | USA | | |
| swisspro.ch | 4.05.2024 | Switzerland | April 25, 2024 | |
| provencherroy.ca | 4.05.2024 | Canada | | |
| ids-michigan.com | 4.05.2024 | USA | | |
| cmactrans.com | 4.05.2024 | USA | | |
| thelawrencegroup.com | 3.05.2024 | USA | | |
| bdcm.com | 30.04.2024 | USA | | |
| thelawrencegroup.com_privat | 26.04.2024 | USA | | |
| true.co.uk | 24.04.2024 | UK | | |
| fluenthome.com | 19.04.2024 | Canada | | |
| macphie.com | 19.04.2024 | UK | | |
| cavotec.com | 19.04.2024 | Switzerland | | |
| hymer-alu.de | 19.04.2024 | Germany | | |
| azdel.com | 19.04.2024 | USA | | |
| doyon.com \| | | | | |

infoblox

# Black Basta - C2 over DNS (Cobalt Strike)




fy9.39d9030e5d3a8e2352daae2f4cd3c417b36f64c6644a783b9629147a1.afd8b8a4615358e0313bad8c544a1af0d8efcec0e8056c2c8eee96c7.b06d1825c0247387e38851b06be0272b0bd619b7c9636bc17b09aa70.a46890f27.588027fa.dns.realbumblebee[.]net

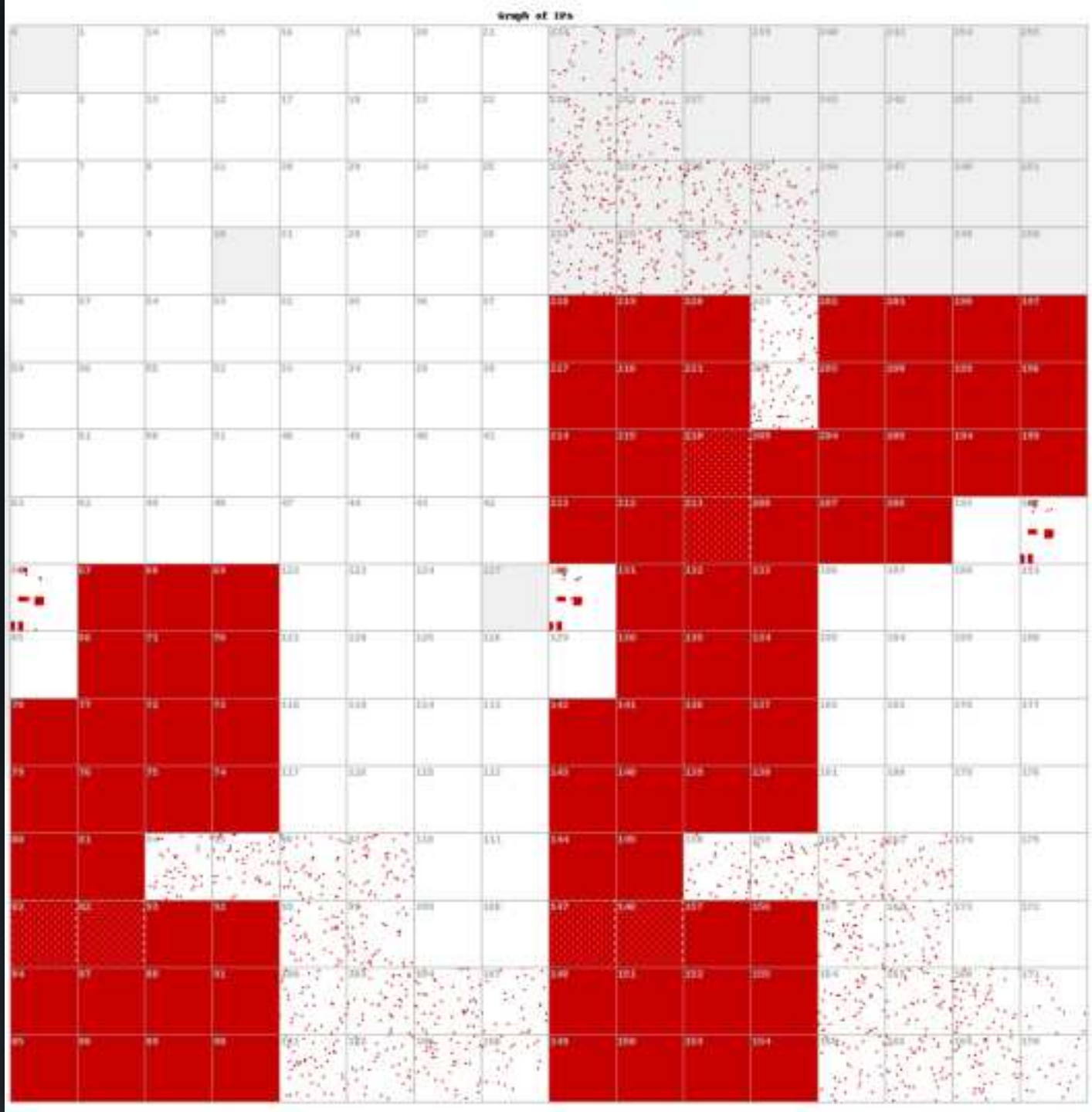
gl7b.364561909cda18c23ef432174ada8d327d8781bd2cd57ec208833be8a.54674ead8fcf4124a7b6822f984054563ff15c35e05c6f69d52e4caa.936ea09f27af2e1b2f2005629812e6785acd69d6199d7893aed9a6f1.1371d3a6c.190dbdb6.dns.thetrailbig[.]net

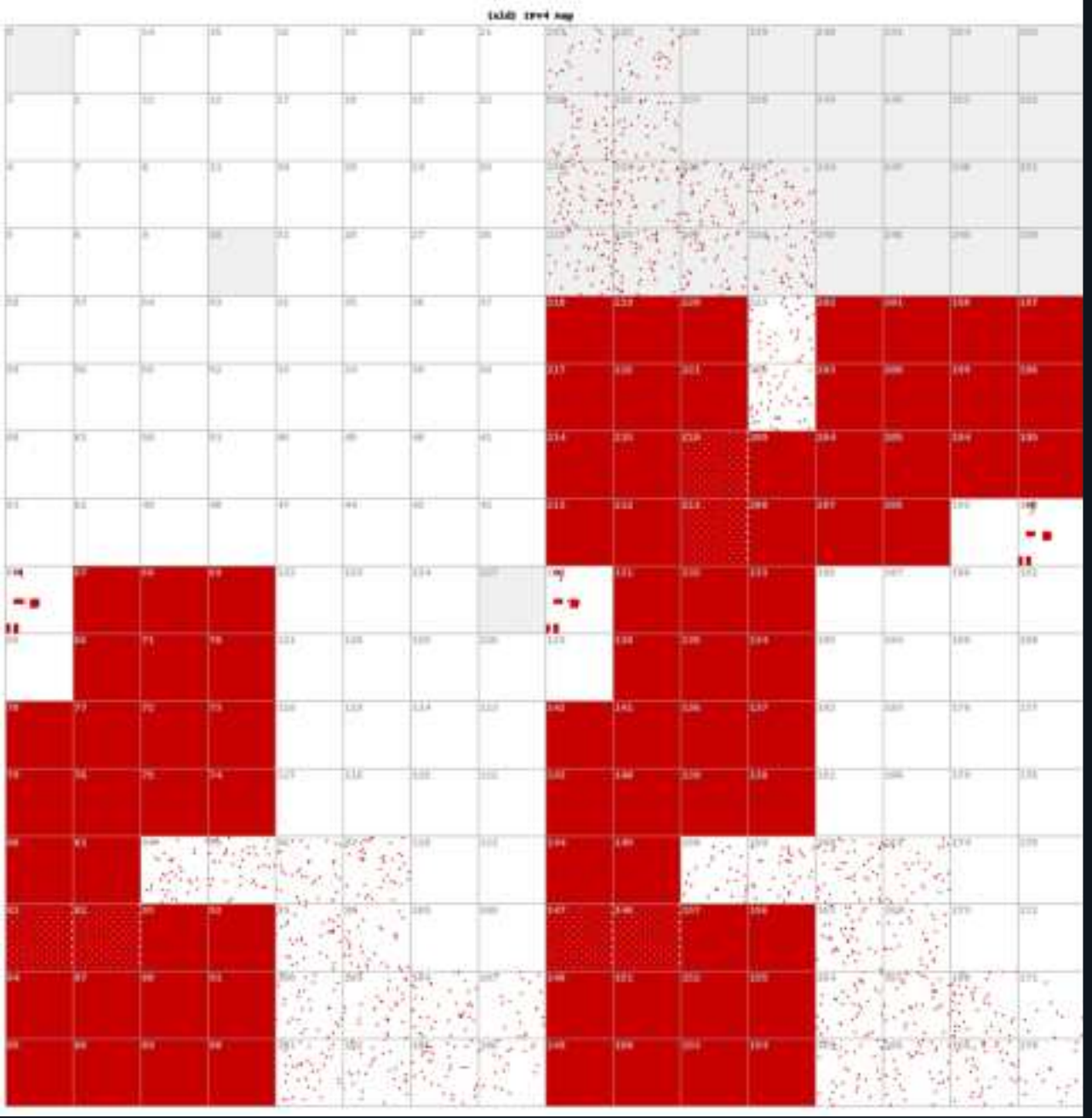
# Decoy Dog

Grupa APT Hellhounds

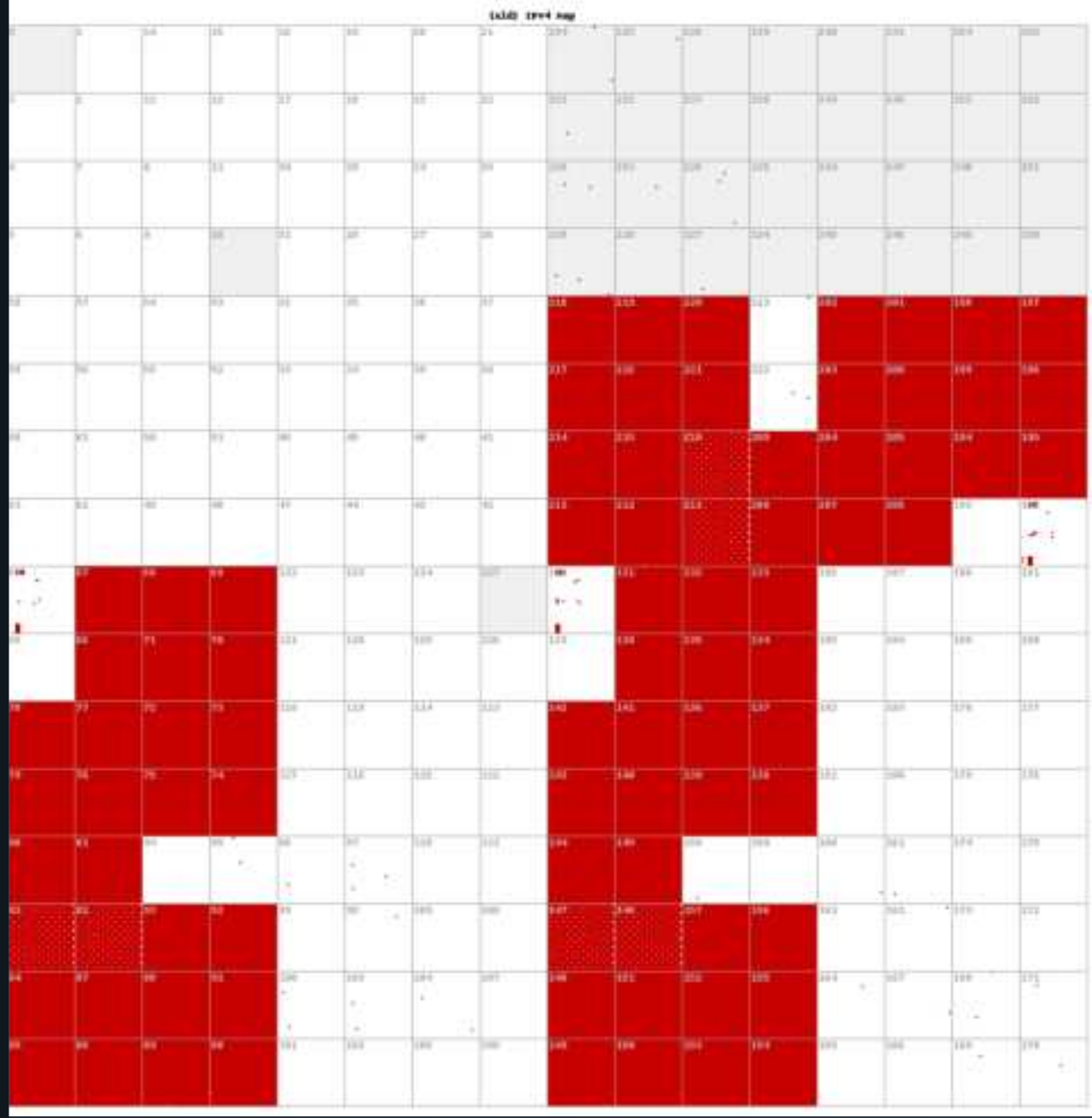
# Decoy Dog C2 over DNS

| IP | LAST REPORT | SOURCE | HOST |
|---|---|---|---|
| 64.89.13.254 | 04/06/2023 | PDNS | e12e5m1f1i1zcmze2d22p532dn3a9999.113cjofolvozr3veumtlrvq9.allowlisted.net. |
| 67.54.147.254 | 04/06/2023 | PDNS | ledk3gi9.e12e5m1f1i1zcmze2d22p532dn3a9999.113cjofolvozr3veumtlrvq9.allowlisted.net. |
| 6:9fb4:9b49:ffbb:32e9:67ad:f909:4731 | 04/06/2023 | PDNS | ledk3gi9.e12e5m1f1i1zcmze2d22p532dn3a9999.113cjofolvozr3veumtlrvq9.allowlisted.net. |
| 64.88.120.74 | 04/06/2023 | PDNS | rymw16ecygl6syu4wykgmnyyvgia9999.113iay5iokhtmmezzveyqiq9.allowlisted.net. |
| 131.240.72.50 | 04/06/2023 | PDNS | t3unzli9.rymw16ecygl6syu4wykgmnyyvgia9999.113iay5iokhtmmezzveyqiq9.allowlisted.net. |
| 6:9efa:f824:1906:5e19:44f2:b341:672d | 04/06/2023 | PDNS | t3unzli9.rymw16ecygl6syu4wykgmnyyvgia9999.113iay5iokhtmmezzveyqiq9.allowlisted.net. |
| 64.88.213.108 | 04/06/2023 | PDNS | dxm1hfwzgssl4kbor6pukgh6uc5q9999.11e1m5wphc23xgydaa1afwa9.allowlisted.net. |
| 68.82.98.98 | 04/06/2023 | PDNS | z4yyfly9.dxm1hfwzgssl4kbor6pukgh6uc5q9999.11e1m5wphc23xgydaa1afwa9.allowlisted.net. |
| 6:9166:ad31:a529:38ca:2231:2bde:8172 | 04/06/2023 | PDNS | z4yyfly9.dxm1hfwzgssl4kbor6pukgh6uc5q9999.11e1m5wphc23xgydaa1afwa9.allowlisted.net. |
| 71.244.165.58 | 04/06/2023 | PDNS | kesjxrdcedpe3vahbgpacbw1smhq9999.11hcffk1mti1o2xutzqdcsy9.allowlisted.net. |
| 67.42.102.180 | 04/06/2023 | PDNS | 6qjw4ky9.kesjxrdcedpe3vahbgpacbw1smhq9999.11hcffk1mti1o2xutzqdcsy9.allowlisted.net. |
| 68.95.103.102 | 04/06/2023 | PDNS | 6qjw4ky9.kesjxrdcedpe3vahbgpacbw1smhq9999.11hcffk1mti1o2xutzqdcsy9.allowlisted.net. |
| 6:ce1f:9533:5a2f:dfdb:562c:5df1:6d96 | 04/06/2023 | PDNS | 6qjw4ky9.kesjxrdcedpe3vahbgpacbw1smhq9999.11hcffk1mti1o2xutzqdcsy9.allowlisted.net. |
| 64.89.182.166 | 04/06/2023 | PDNS | kesku2jdbofoxrwxhyjghyh4erna9999.11hqnn1r1l6xhy6qw5xzq1i9.allowlisted.net. |
| 130.84.238.10 | 04/06/2023 | PDNS | 6qjw4ky9.kesku2jdbofoxrwxhyjghyh4erna9999.11hqnn1r1l6xhy6qw5xzq1i9.allowlisted.net. |
| 6:a5d5:2a77:536:3c1b:e0f7:e6a6:eb55 | 04/06/2023 | PDNS | 6qjw4ky9.kesku2jdbofoxrwxhyjghyh4erna9999.11hqnn1r1l6xhy6qw5xzq1i9.allowlisted.net. |


Graph of IPs



Domain: cbox4.ignorelist[.]com



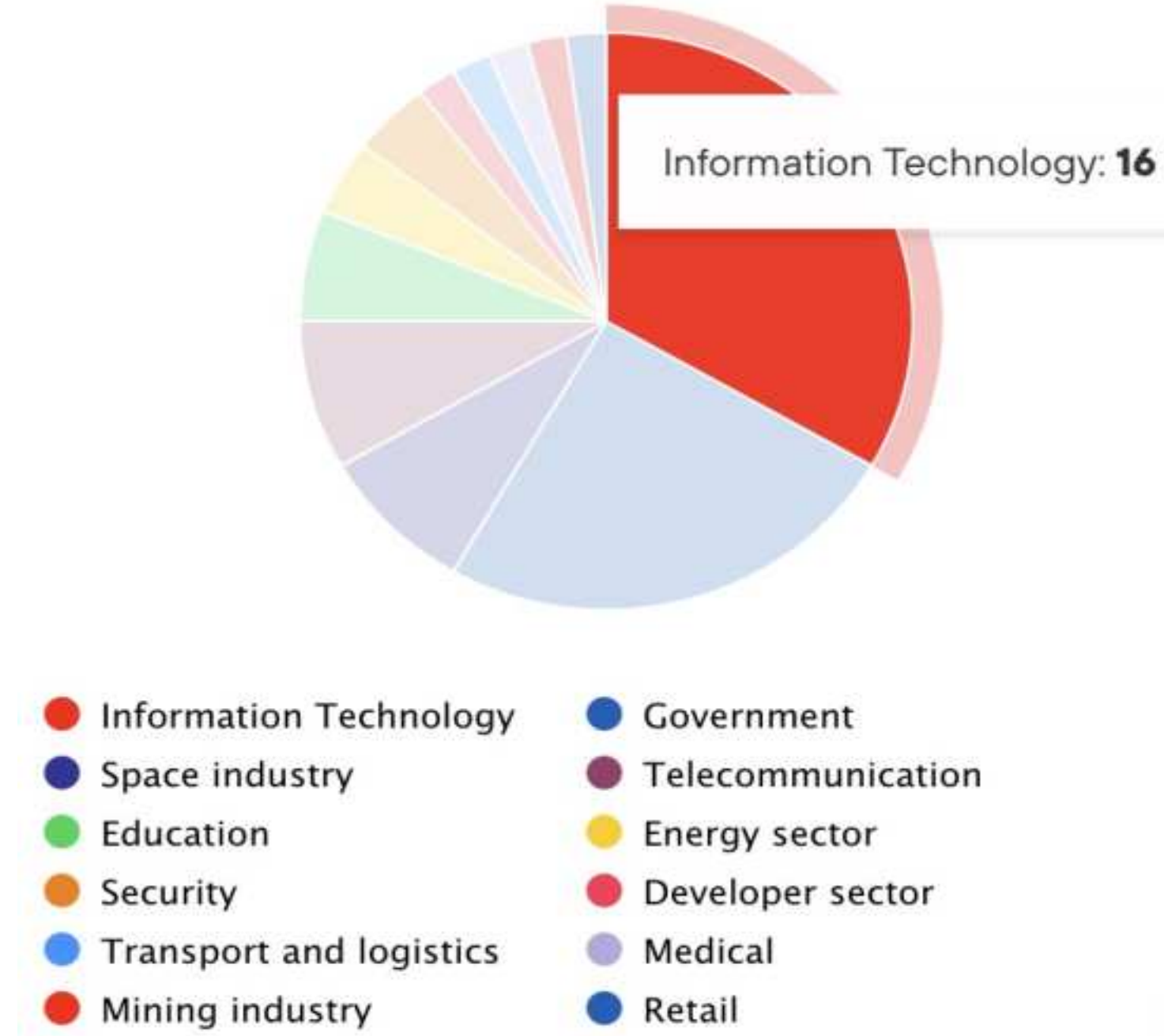
Domain: cbox4.ignorelist[.]net

# Decoy Dog

- 6 kwietnia 2023 – wstępne wykrycie ruchu C2 over DNS w globalnym systemie passive DNS
- 20 kwietnia 2023 – Infoblox publikuje wyniki badania wraz z listą IoC
- Listopad 2023 –RT Solar prezentuje na konferencji SOC Forum
  - 22 kwietnia 2023 – RT Solar wykrył komunikację do ww. IoC w ruchu z sensorów w Rostelecom

# Victims

Wg artykułu PT Security z maja 2024 co najmniej 48 rosyjskich firm było ofiarami Decoy Doga od co najmniej 2021 roku.




Source: https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/hellhounds-operation-lahat/

# Decoy Dog w sieci rosyjskiego operatora telco

- **Wykradanie danych niewykryte przez 9 miesięcy.** Nie zidentyfikowano sposobu włamania.
- 12 zainfekowanych serwerów *nixowych w kilka różnych segmentach sieci
- **Finalne działanie – data wiper**:
  wykasowane VMki, zablokowany dostęp do Tacacs, wykasowana konfiguracja switchy MPLS, wyczyszczone macierze Huawei
- Wynik:
  - Przez 9 miesięcy włamywacze mieli dostęp do poczty, gitlab, confluence, haseł i innych danych.
  - Następnie klienci nie mieli usług telekomunikacyjnych przez prawie 24 godziny.
  - Zniszczono całkowicie system billingowy – po przywróceniu działania sieci usługi świadczono za darmo
  - Niektóre bazy klientów zostały nieodwracalnie utracone
  - W kanałach IP TV puszczono niepożądane wideo (prawdopodobnie w czerwcu 2023)
    (specjalna wersja Decoy Doga dla Linuxa ARM została wgrana na mały, zapomniany NAS Synology w segmencie IP TV)

Source: Solar 4RAYS https://forumsoc.ru/upload/iblock/f7c/6ncp0iit9pxcth1taxfku9varczadc5b.pdf

# Porównanie C2 over DNS

## Ransomware vs APT

- BlackBasta

Narzędzie: **Cobalt Strike**

Celowane platformy: **Windows**

Dane domeny C2: **podejrzane**

Długość zapytań DNS: **~200 znaków + domena**

Odstęp zapytań DNS: **~60 sekund**

Kodowanie danych w zapytaniach: **HEX**

Wykrycie: **relatywnie łatwe, a jeżeli się nie uda to atakujący sami się szybko ujawniają**

**Korzystają nadal z tego samego narzędzia i techniki długo po wykryciu**

- DecoyDog

**Zmodyfikowany Pupy RAT**

**Linux x64, Linux ARM, Windows**

**podejrzane**

**40-60 znaków + domena**

**Minuty / godziny**

**Base32**

**Trudne, atakujący nie wykryci przez 9-24 m-cy**

**Korzystają nadal z tego samego narzędzia i techniki długo po wykryciu**


Piotrek zrobi prezentację na Infoblox Exchange.
infoblox
Exchange
11 czerwca 2024
No i fajnie, to swój chłop.
• Tak się tylko mówi, to oczywiście mój chłop •

infoblox

CSO COUNCIL

SPOŁECZNOŚĆ SZEFÓW
BEZPIECZEŃSTWA
I CYBERBEZPIECZEŃSTWA

11 CZERWCA 2024

# WCZESNE WYKRYWANIE ZAGROŻEŃ

## - zero false positives czy low regret

infoblox