
INTEL471
Growing Threats of Cybercrime in the Alps
SIGS 2024 - Intel Briefing

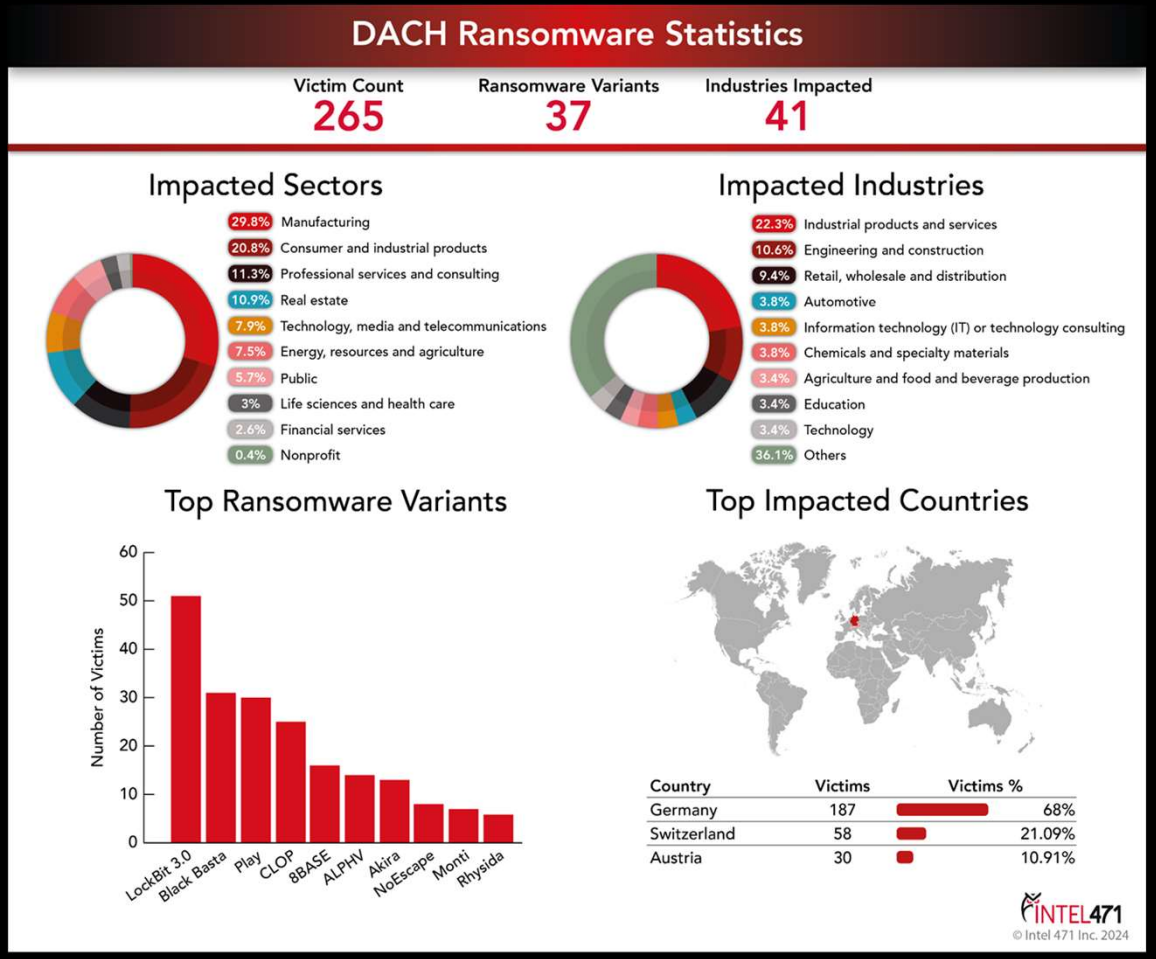
Agenda - TLP AMBER+STRICT

- Ransomware
- Initial Access Brokers / Merchants
- Malware Campaigns
- Hacktivism

ICOD: Statistical data only shows information between April 2023 - April 2024.

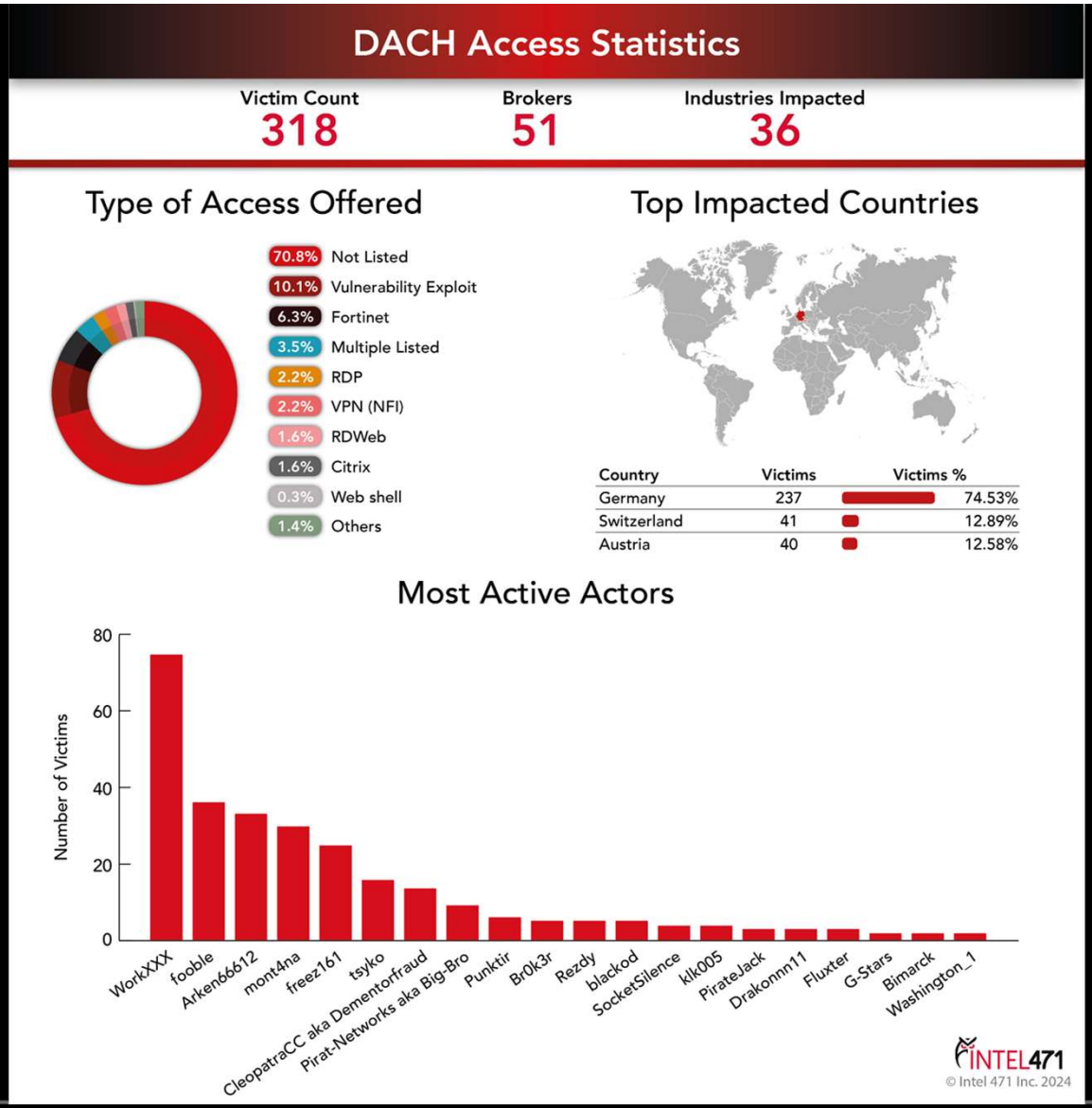
2023-2024 RaaS Incidents

- DACH region represents 21% of all RaaS incidents in **Europe**
- **179** RaaS incidents in previous YTD, representing a **49%** increase in 23/24.
- **LockBit 3.0**, **Black Basta** and **Play** RaaS Groups most impactful to region.
- **LockBit** activity likely to dissipate with recent LE activity even after **LBS** vowed to continue.



2023-2024 Initial Access Brokers

- **57%** increase in IAB offers targeting **Switzerland** compared to 2022.
- **Germany** remains a major target, ranking as the third most targeted country after the **USA** and **Brazil** in 2023. Memories of MediaMarkt?
- **IAB's** modus operandi primarily focuses on mining and harvesting info-stealer logs for valuable endpoint credentials then monetising them in Cybercriminal Forums such as XSS, Exploit or to trusted private contacts.



ACTOR PROFILE

WorkXXX

The actor **WorkXXX** joined the Exploit forum July 21, 2023, and auctioned hundreds of compromised access credentials throughout the year. In September 2023, we released several reports on a newcomer to the XSS forum, the actor **CoreLab**, whose contact information revealed the same Tox public key and alias we previously associated with **WorkXXX**. Therefore,

TTPs

- Offering to sell cor
  credentials for corp
- Suggesting the use
  "at all times"

BREACH ALERT

Furtwangen University

Published: 29 S

CONFIDENCE L

Medium

ACTOR / GROU

ALPHV aka /

SECTOR / INDU

Public secto

BREACH ALERT

Johnson Controls International PLC

Published: 27 Sep 2023 09:51:11 UTC

CONFIDENCE LEVEL

High

ACTOR / GROUP

Dark Angels aka Dark Angels Team

SECTOR / INDUSTRY

Manufacturing sector, Industrial products and services industry
Real estate sector, Engineering and construction industry
Technology, media and telecommunications sector, Technology industry

VICTIM URL

https://www.johnsoncontrols.com/

REVENUE

US $25.3 Billion

REGION / COUNTRY

Europe,
Ireland

- In Septembe
  compromise
  Furtwangen
  the ALPHV aka BlackCa
  between the actor and t

Malware Campaign

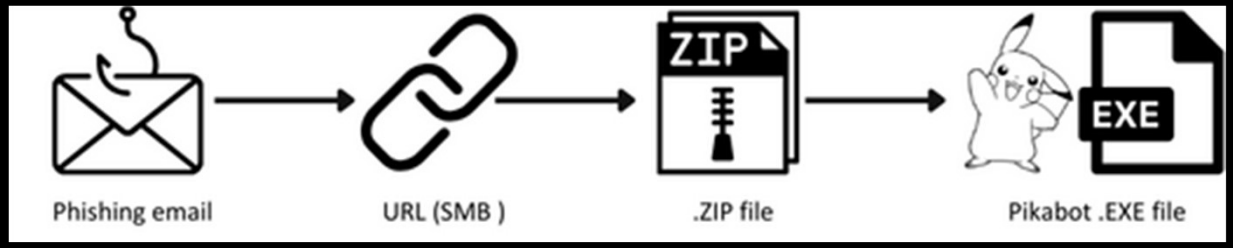
TA577 exploits CVE-2023-35311 to deliver Pikabot Loader

- On Feb. 8, 2024, Intel 471 Malware Intelligence analysts observed the onset of a series of campaigns designed to distribute a new version of the **Pikabot** malware loader, all from the same spam source.

- The latest version, leveraged the Windows server message block (SMB) protocol. Therefore it is highly likely the actor exploited the CVE-2023-35311 Microsoft Outlook security feature bypass vulnerability patched in July 2023.

- The campaign specifically targeted several European countries, including **Germany**, Italy, the Netherlands and **Switzerland.**

- In the aftermath of the 2023 Qbot disruption, the actor[s] have been experimenting with alternative families to determine the most effective infection vector.



Changes to C2 communication protocol

- The adoption of C2 routes that mimic the Slack business messaging application with application programming interface (API) requests, making malicious traffic resemble legitimate API traffic. Examples include:

```
"api/admin.inviteRequests.deny"
"api/admin.emoji.addAlias"
"api/admin.apps.requests.list."
```

Malware Campaign

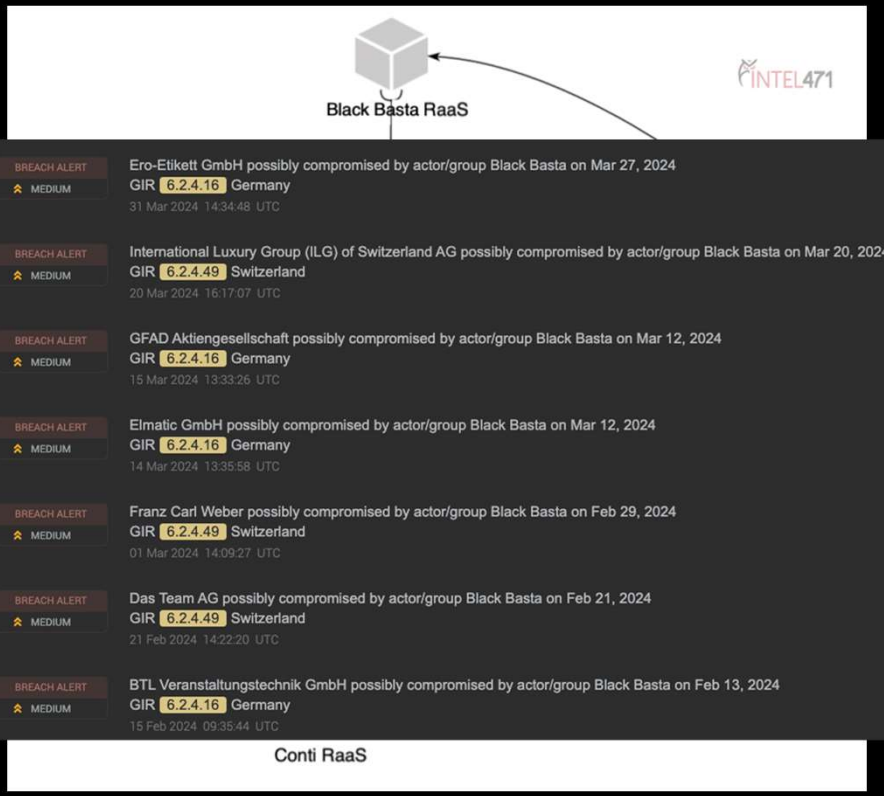
TA577 links to Black Basta Ransomware

- Intel 471 has reported extensively on the connection between the **Black Basta** RaaS groups connection with the actor operating the TR-distribution botnet.

- It is likely the Russian-speaking actor **kurva** aka **tramp** runs the **Black Basta** RaaS. The actor, previously leveraged the **Conti** and **REvil** ransomware and possibly operated Qbot aka Qakbot, QuakBot banking trojan malware. It also is possible **kurva** is an alternate persona of the actor **BlackBasta,** a public representative of the Black Basta affiliate program.

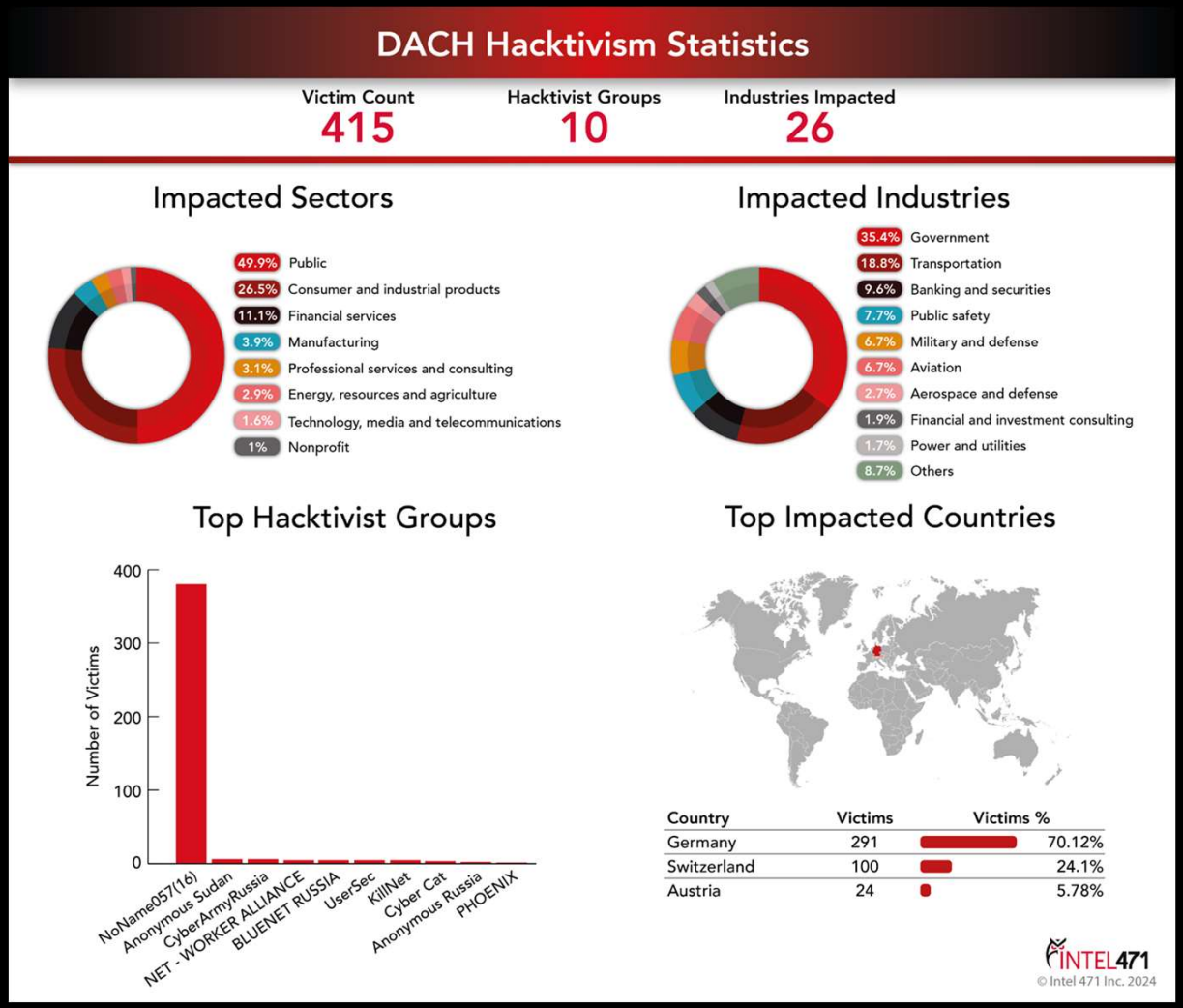
- Since the identification of the recent **Pikabot** campaign, there have been **57** new **Black Basta** Victims.

- DACH region represents 12% of those victims.



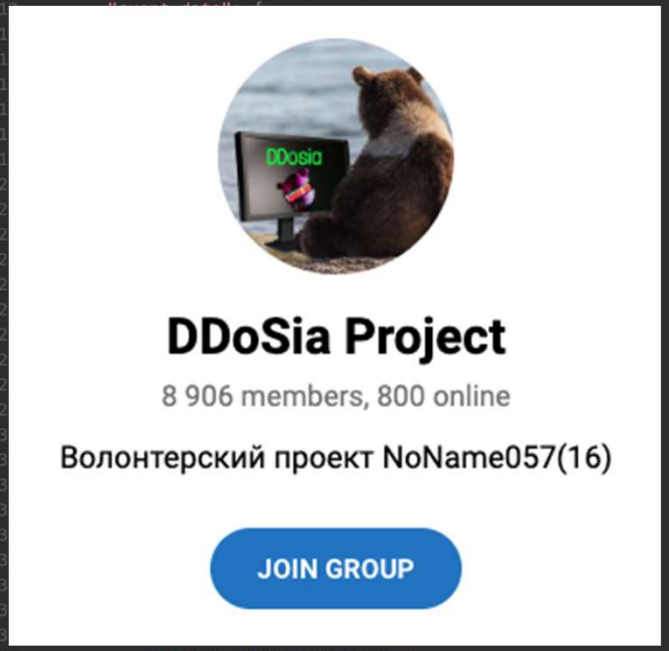
Pro -Russian Hacktivism

- Countries that have provided aid to Ukraine, imposed sanctions on Russia or were deemed detrimental to Russia typically found themselves on the receiving end of hacktivism attacks.
- **Noname057(16)** represented 91% of all attacks, predominantly in the form of DDoS attacks leveraging **DDoSia.**
- These attacks are primarily targeted towards Public Entities.
- **DE** has pledged the most military aid in DACH hence why they are primary target.



EVENT SOURCE


```
{
  "data": {
    "event": {
      "threat": { ... }
      "uid": "06618680fba45670af38204a332439fb",
      "source_id": "21e59c059a1664364b5be654c5ec11113629f107",
      "event_type": "start_ddos",
      "ipv4": "185.108.181.128",
      "host": "gov.md"
    },
    {
      "ipv4": "185.108.181.128",
      "host": "stisc.gov.md"
```

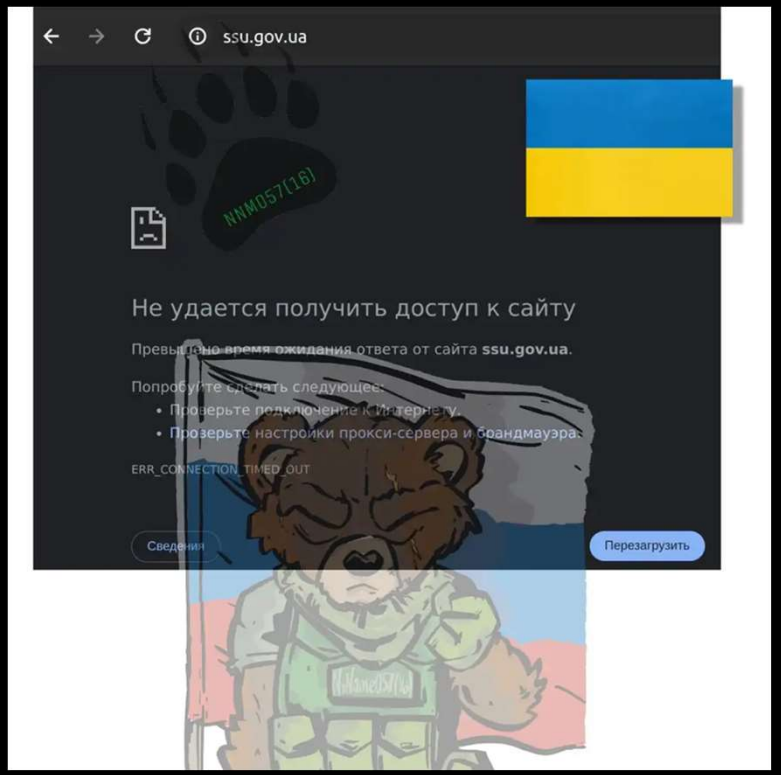



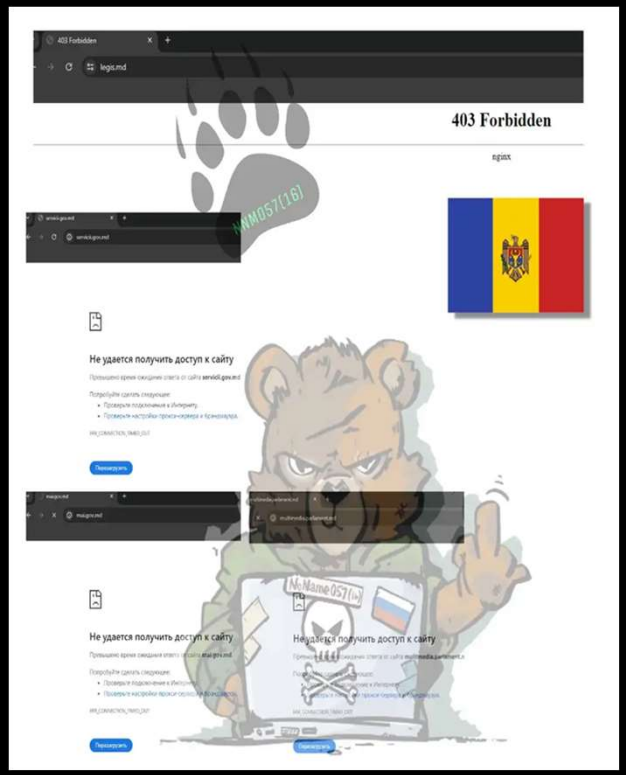
Start DDoS Attack
Malware family ddosia
CONTROLLER URL: http://45.82.13.121

IP V4: 45.82.13.121

Provided by Global Internet Solutions, AS207713 Global Internet Solutions LLC, 45.82.13.0/24
Located in Stockholm, Stockholm County, Sweden

IP V4: 193.29.204.56 IP V4: 193.109.8.163 IP V4: 185.108.181.128 IP V4: 185.108.181.116 IP V4: 185.108.181.19 IP V4: 185.108.181.128 IP V4: 185.108.181.128 IP V4: 185.108.181.128 IP V4: 185.108.181.39 IP V4: 185.108.181.128 IP V4: 185.108.181.116 IP V4: 213.150.2.164 IP V4: 46.229.154.97
Activity: Today 08:35:04 — Today 10:34:48






THANK YOU
INTEL471