Weekly Dark Web Trends/Advisory

Every week, CYFIRMA Intelligence and Research Team will highlight additional high-level information gathered while monitoring various dark web forums. This information encompasses various industries across multiple countries which could be directly/indirectly related and relevant to your organization.

Ransomware

Detailed below are the three most prolific ransomware. Additional information as to victims has been obtained from the Data Leak Sites (DLS) of each ransomware strain.

(hxxps://github.com/fastfire/deepdarkCTI/blob/main/ransomware_gang.md) – List of Data Leak Sites

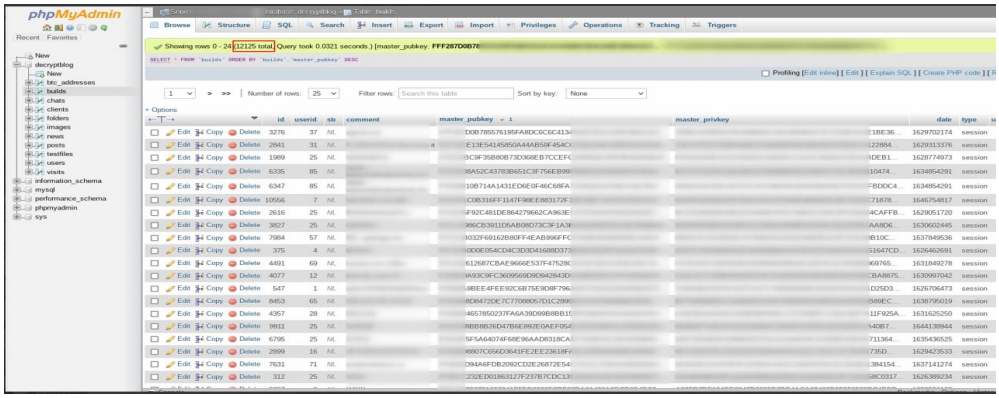
RANSOMWARE UPDATE

1) LockBit Ransomware Group

LockBit first appeared as the ABCD ransomware in September 2019 and has since evolved into one of the most prolific ransomware family. LockBit uses a ransomware-as-a-service (RaaS) model and consistently conceived new ways to stay ahead of its competitors. Its double extortion methods also add more pressure to victims, raising the stakes of their campaigns. We observed that they had the highest number of recorded victims among active ransomware groups for the month of April 2022 at 103, followed by Conti at 33.

Lockbit News:

Latest news learned from a screen shared between the gang and vx-underground, reports that the group has received the payment of the ransom from 12,125 organizations, even if on its data-leak-site (DLS) there are approximately 850 of them. As we know, publishing the data on the darkweb is the conclusion of a ransomware attack, and that only companies that have refused to pay a ransom will get this treatment. Doing a quick calculation as reported by vx-underground, 12,125 x a minimum ransom like $ 100,000, makes the figure of $ 1,212,500,000 (one billion +).



New Victims:

- https://www.hydromaxusa.com/
    - Utility field service provider based in USA
- John Burns Real Estate Consulting, LLC
    - Independent research and consulting services related to the US housing industry based in USA.
- https://sportco.com/
    - Warehouse style sporting goods store based in USA

2) Mindware Ransomware Group

Mindware is a new ransomware gang that started apperaring in the cybercrime panorama in the middle of last month. It has been denounced by the cybersecurity researcher MalwareHunterTeam. Their malicious code belongs the the SFile family, most likely SFile2. However, according the expert, today is not possible to understand if this is a new gang or a rebrand of a previous one. What is certain is that it exploits the Double Extortion scheme to increase pressure on victims and force them to pay the ransoms.

Mindware News:

Based on leak site, group is focused on tageting english speaking countries along with Germany, Italy and France.

New Victims:

- http://www.mediuscorp.com
    - Supply Chain Logistics based in USA.
- https://www.acorentacar.com
    - Car rental compant in Venezuela.
- http://www.carillonassistedliving.com
    - Provider of assisted living homes for seniors in USA

3) Black Basta Ransomware Group

The group's first known attack using the Black Basta ransomware occurred in the second week of April 2022. Like other enterprise-focused ransomware operations, Black Basta employs a double extortion scheme that involves exfiltrating confidential data before encryption to threaten victims with public release of the stolen data. According to the ransomware message, victims are given seven days to pay else the stolen content will be publicized.

Black Basta News:

Security researchers exchanged speculations on Twitter that Black Basta is possibly a rebranding of the Conti ransomware operation. MalwareHunterTeam pointed out similarities in its leak site, payment site, and negotiation style to those of Conti's. However, in another telegram channel post Conti declined speculation made by

researchers. Black Basta may be rebranded version of Conti ransomware or separated group from Conti, time will answer this question.

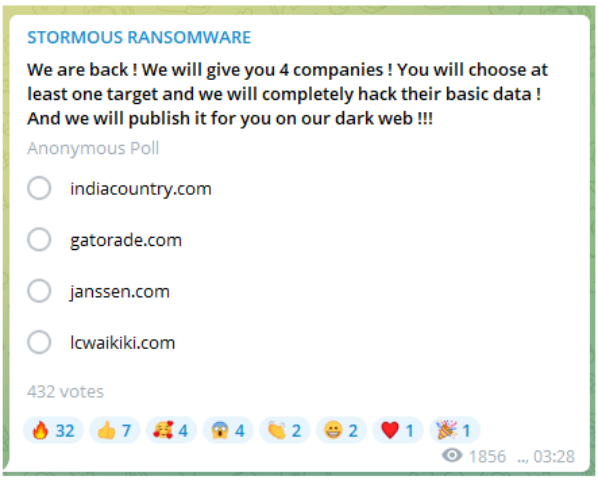
Interestingly Black Basta victim list is larger than Conti ransomware for the month of May 2022, this is another point to strengthen researcher hypothesis on Black Bastas' origin from Conti.

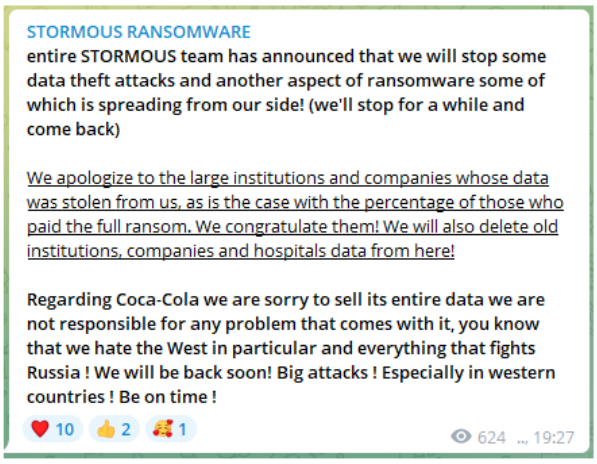
New Victims:

- Ragle Incorporated
  - Highway and bridge construction company based in USA.
- PRGX Global Inc.
  - IT service management company based in USA.
- Grohmann Aluworks GmbH & Co
  - Producers cast aluminium parts based in Germany.

Other obsevations

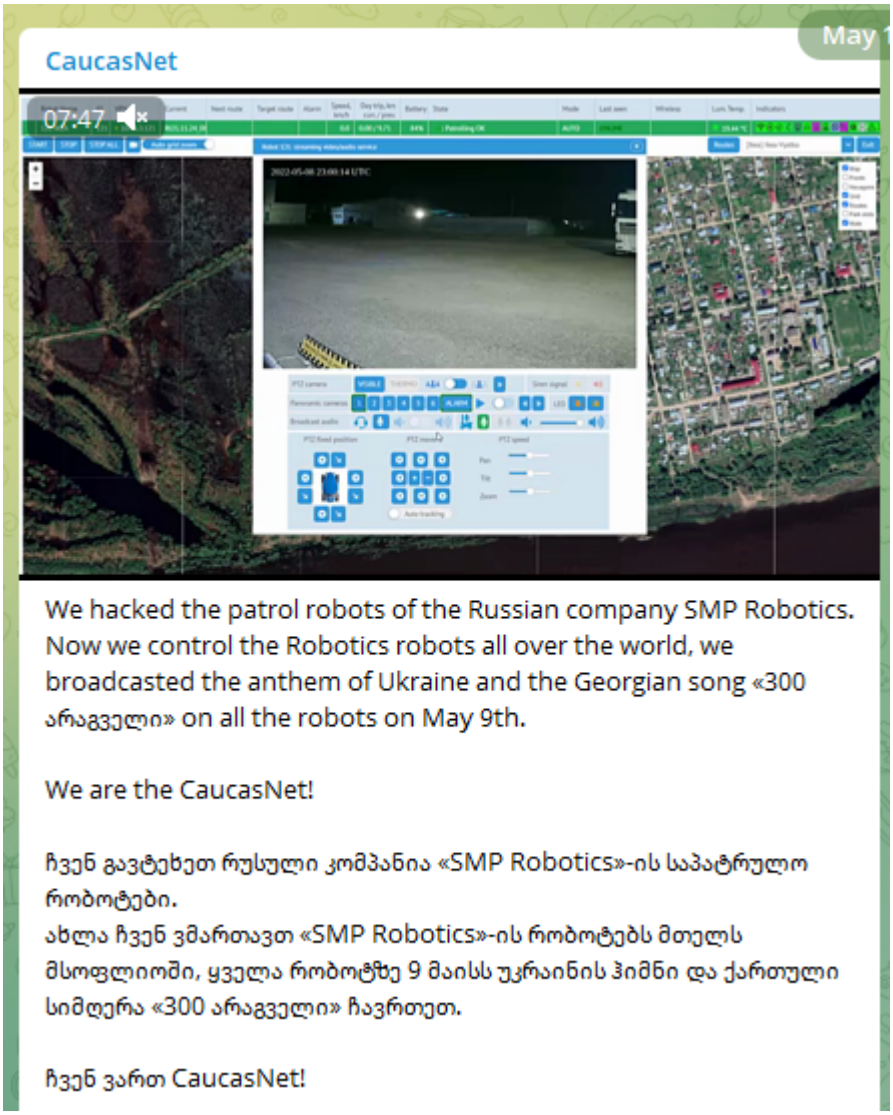
- Stormous ransomware: Poll on whom to attack next, later announced that they will take a break from data theft attacks for some time.
  The Stormous ransomware, who posted poll on whom to attack next, announced that it will stop data theft attacks for some time. Also, ironically apologised large institutions and companies whose data was stolen by them.





- A new Pro-Ukraine group know as CaucasNet has posted of their first campaign.

  The CaucasNet group claimed that, they have hacked Russian company SMP Robotics and control the Robotics robots all over the world. Based on language used in the telegram post, group is possibly pro Ukraine Georgians. Since their independence from the Soviet Union, Georgia and Ukraine consider each other strategic partners and have forged close political and cultural relations. Georgia and Russia have had no formal diplomatic relations since August 2008, largely due to the Russo-Georgian War and Russian recognition of separatist regions.


CaucasNet
May
07:47
We hacked the patrol robots of the Russian company SMP Robotics. Now we control the Robotics robots all over the world, we broadcasted the anthem of Ukraine and the Georgian song «300 არაგველი» on all the robots on May 9th.
We are the CaucasNet!
ჩვენ გავტეხეთ რუსული კომპანია «SMP Robotics»-ის საპატრულო რობოტები.
ახლა ჩვენ ვმართავთ «SMP Robotics»-ის რობოტებს მთელს მსოფლიოში, ყველა რობოტზე 9 მაისს უკრაინის ჰიმნი და ქართული სიმღერა «300 არაგველი» ჩავრთეთ.
ჩვენ ვართ CaucasNet!

END