Weekly Dark Web Trends/Advisory

WEEKLY REPORT | 03 June 2022

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 two 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) 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 the 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:

The Black Basta ransomware moves quickly, rarely triggering alerts to cybersecurity defenders, and by the time they realize it, the damage has already been done.

Based on its victim list, Black Basta is not targeting any specific industry, but rather organizations that collect a large number of PII data, financial information, and other sensitive information from their customers or clients.

New Victims:

Victim	Industry	Geography
BLAIR inc.	Constructions	USA
Blairex Laboratories, Inc.	Healthcare	USA
Love, Barnes & McKew Insurance Adjusters, Inc.	Insurance	USA
JBS TEXTILE GROUP	Clothing & Accessories	Denmark
Groupe J.F. Nadeau Inc	Transportation & Logistics	Canada
Cavender	Retail	USA

2) Clop Ransomware Group

Clop ransomware operates under the ransomware-as-a-service (RaaS) business model that creates and distributes its malware via affiliates. Clop ransomware belongs to CryptoMix ransomware family. Clop ransomware was first observed in February 2019. Clop ransomware encrypts the file using AES+RSA algorithms. This ransomware encrypts files and then modifies their filenames by appending the .Clop extension. After this ransomware completes encrypting a device, it drops a ransom note,

"CIopReadMe.txt" into every encrypted directory. This ransom note emphasizes that files are not only encrypted but also at risk of being published if the ransom is not duly paid.

Clop News:

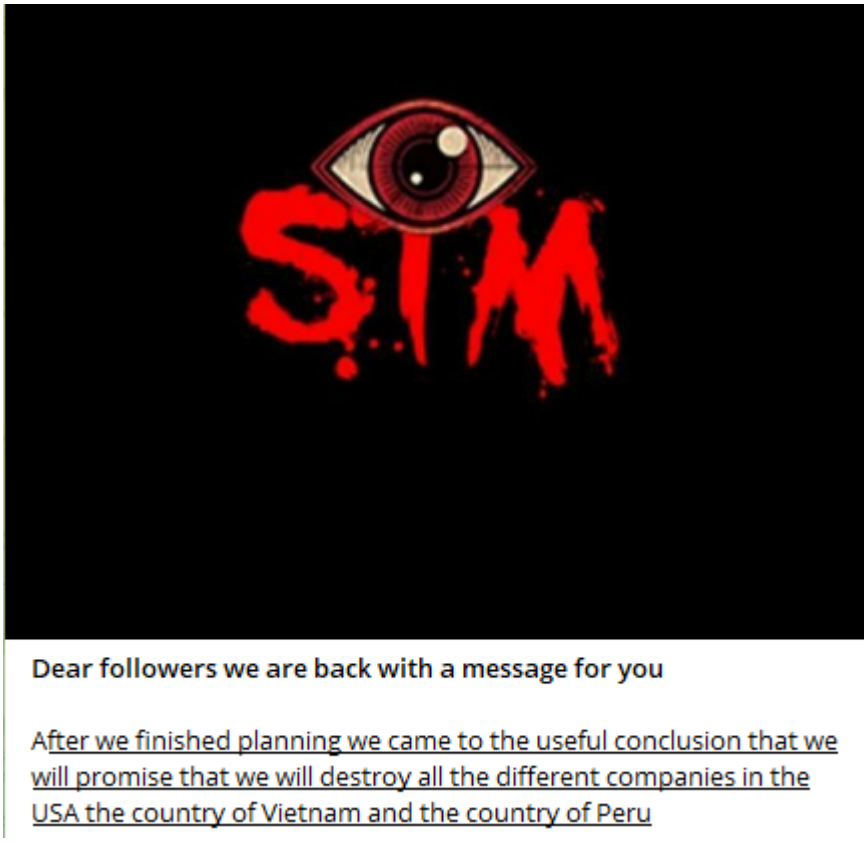
When it comes to Clop ransomware attacks, the industrial sector was the most affected, accounting for 45 percent of incidents and 27 percent of tech organizations. Industrial and tech sector organizations need to be watchful of attacks from the Clop ransomware group.

New Victims:

Victim	Industry	Geography
LATOURNERIE-WOLFROM.COM	Legal Services	France
ATAPCOPROPERTIES.COM	Real Estate	USA
FERRAN-SERVICES.COM	Electrical Components	USA
PRICEDEX.COM	Software	Canada
ENSSECURITY.COM	Software	USA

Other observations:

- STORMOUS Ransomware - STORMOUS Ransomware group announced to resume its operation, we can see some action from the group in the coming days. Group is planned to target companies in **Vietnam, Peru, and USA.** This is the same group, that claimed ransomware attack on Coca-Cola.

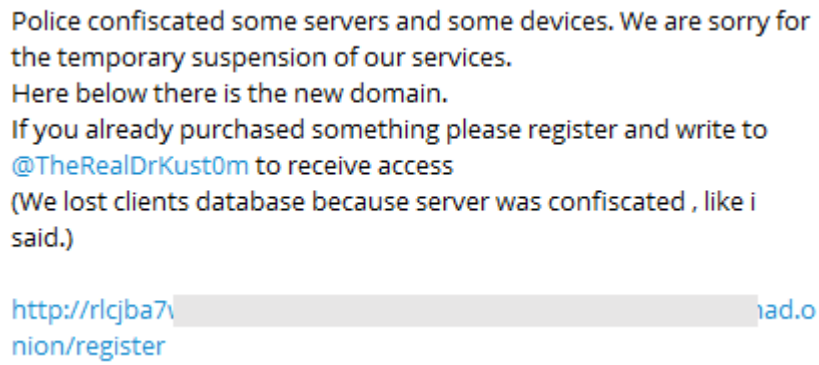


Source: Telegram channel

- Russain-based hacktivist group KillNet planned to establish its representation in other countries. They initiated a poll to gather the opinion of group members. Hacktivism picking up its pace to grow beyond boundaries, this will place government websites at the risk of DDoS attacks.

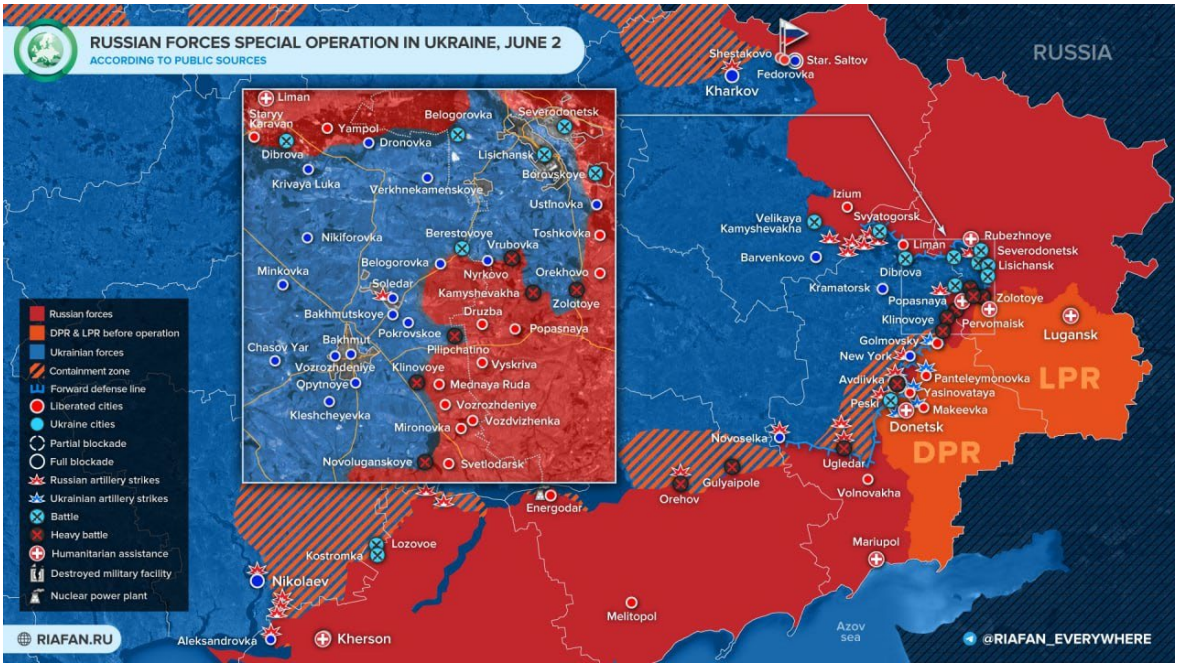
Source: Telegram channel

- Eternity' Malware-as-a-Service – Law enforcement confiscated some of the eternity servers. Earlier Tor page is inactive, but the group continued its offering and services through a new domain.



Source: Telegram channel

- The armed forces of the Russian Federation continued the special operation in Ukraine together with the troops of the Donetsk and Luhansk People's Republics.



Source: RIAFAN.RU