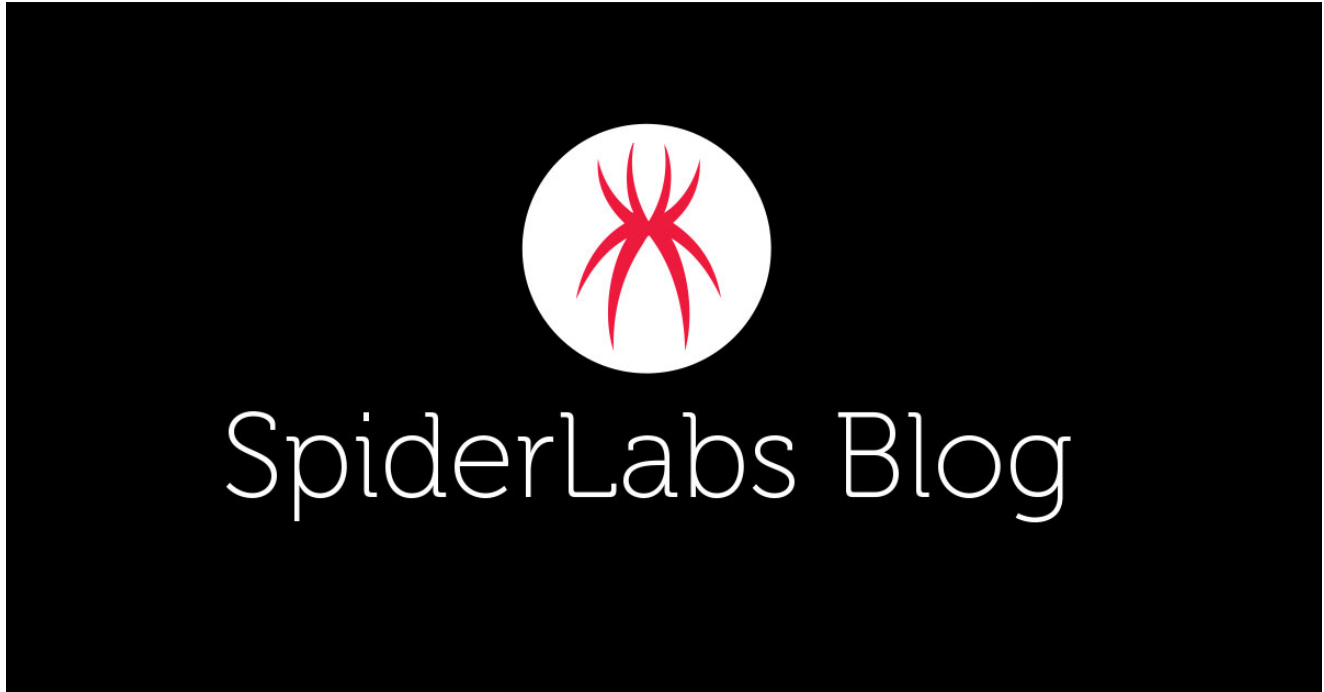


Stormous: The Pro-Russian, Clout Hungry Ransomware Gang Targets the US and Ukraine

 trustwave.com/en-us/resources/blogs/spiderlabs-blog/stormous-the-pro-russian-clout-hungry-ransomware-gang-targets-the-us-and-ukraine



May 2 Stormous update: The Trustwave SpiderLabs team has noted Stormous' underground website became inaccessible on April 29. At this time it is not known why the site is down. We will continue to monitor for additional threat intelligence.



Browser



Network



Onionsite

Onionsite Has Disconnected

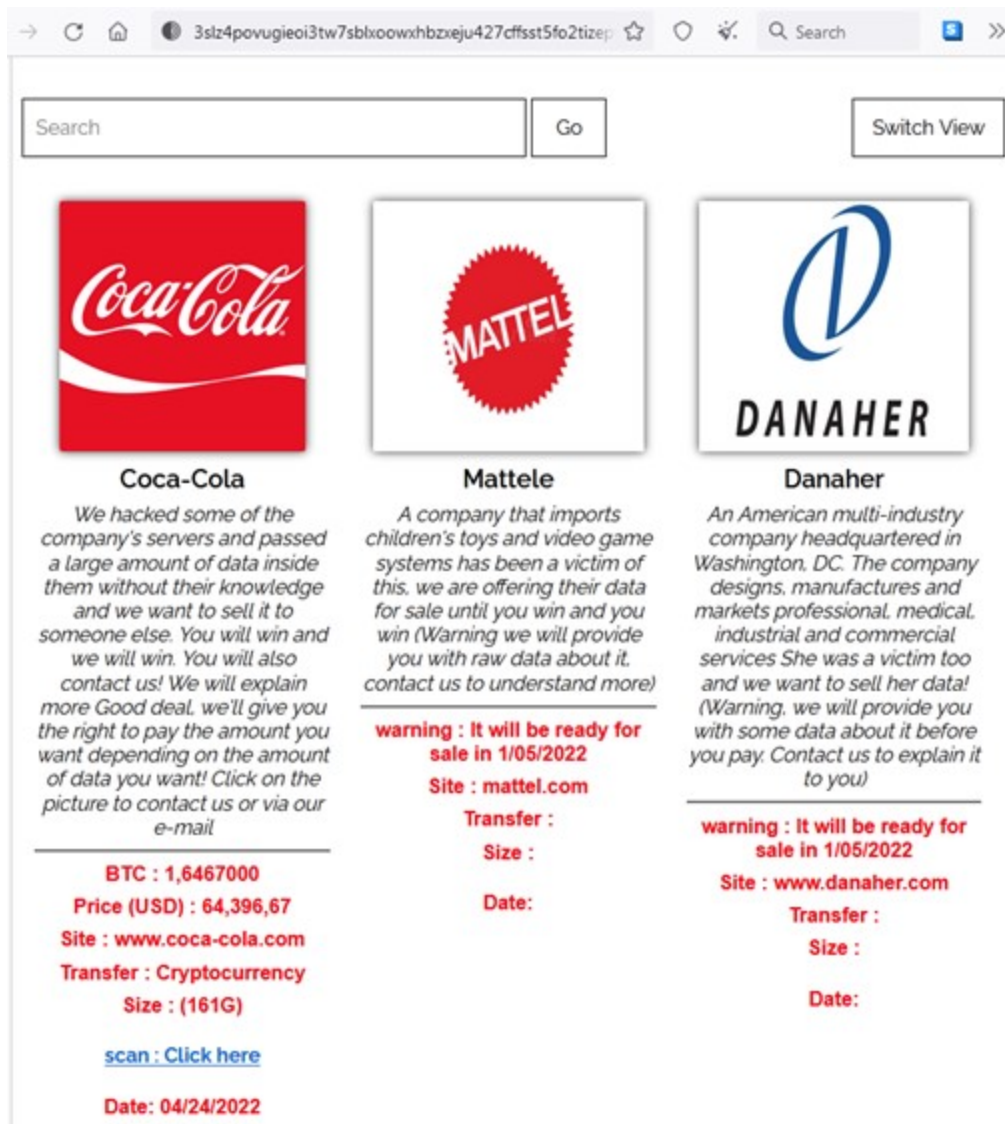
The most likely cause is that the onionsite is offline. Contact the onionsite administrator.

Details: 0xF2 — Introduction failed, which means that the descriptor was found but the service is no longer connected to the introduction point. It is likely that the service has changed its descriptor or that it is not running.

Try Again

As part of our regular Dark Web and cybercriminal research, Trustwave SpiderLabs has uncovered and analyzed postings from a politically motivated, pro-Russian ransomware group named Stormous. The group has recently proclaimed support for Russia in its war with Ukraine, attacking the Ukraine Ministry of Foreign Affairs and allegedly obtaining and making public phone numbers, email addresses, and national identity cards. But the group also claims to have a successful ransomware operation and has taken responsibility for cyber attacks on major American brands Coca-Cola, Mattel and Danaher. In total, Stormous claims to have already accessed and defaced 700 U.S. websites and attacked 44 American companies.

As of April 29, the group has listed the Coca-Cola data for sale on its Dark Web site. At the time of publishing, Coca-Cola has neither confirmed nor denied whether the data listed is legitimate. Most recently, the gang has promised to release additional stolen information from multinational toy manufacturer Mattel and medical diagnostics and healthcare technology company Danaher on May 1.



The screenshot shows a web browser window with a search bar and a 'Switch View' button. Below the search bar are three listings for stolen data. Each listing includes a logo, a title, a description, a warning, a site URL, transfer details, and a date.

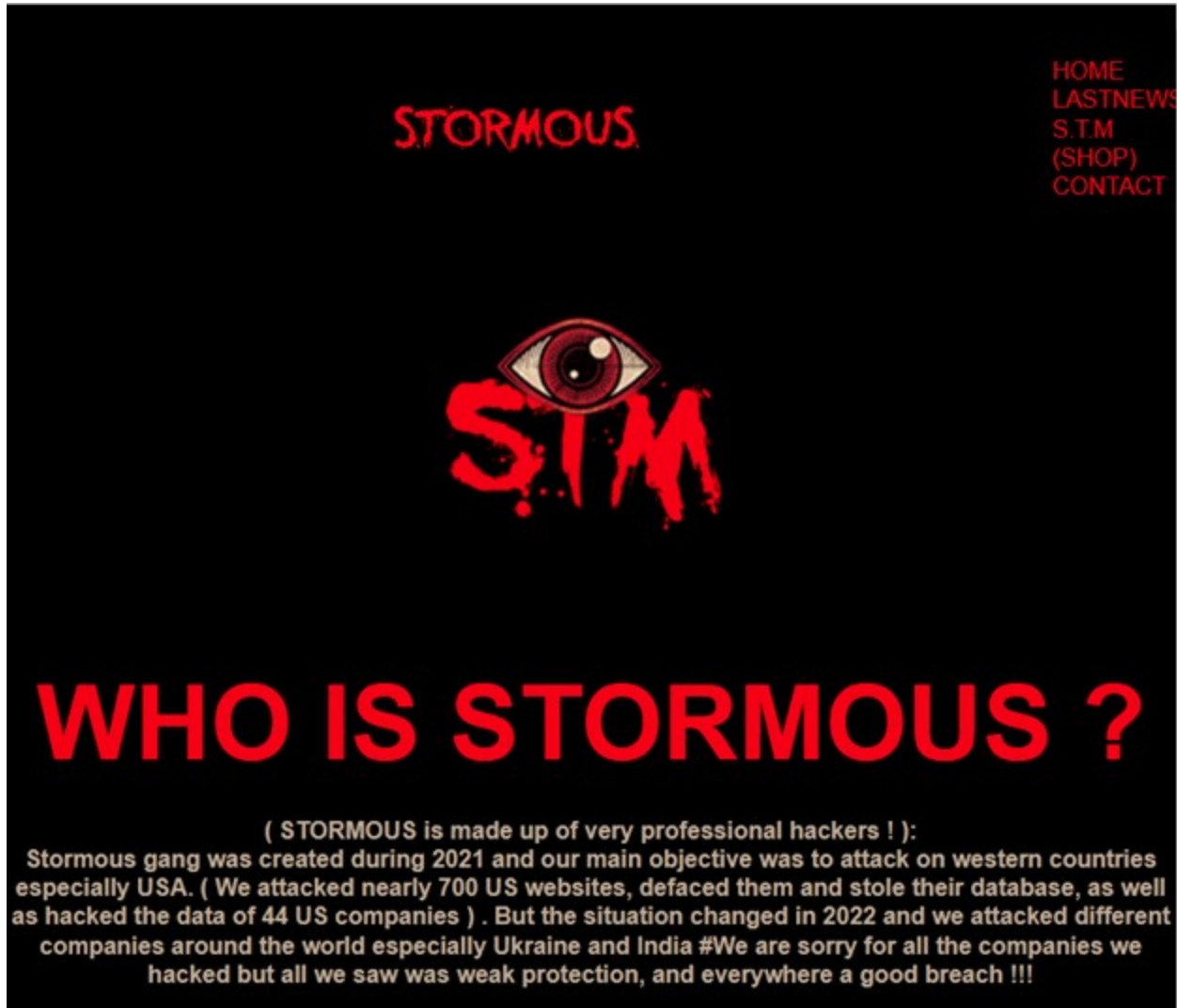
Company	Description	Warning	Site	Transfer	Size	Date
Coca-Cola	We hacked some of the company's servers and passed a large amount of data inside them without their knowledge and we want to sell it to someone else. You will win and we will win. You will also contact us! We will explain more Good deal. we'll give you the right to pay the amount you want depending on the amount of data you want! Click on the picture to contact us or via our e-mail					
Mattele	A company that imports children's toys and video game systems has been a victim of this. we are offering their data for sale until you win and you win (Warning we will provide you with raw data about it. contact us to understand more)	warning : It will be ready for sale in 1/05/2022	Site : mattel.com	Transfer :	Size :	Date:
Danaher	An American multi-industry company headquartered in Washington, DC. The company designs, manufactures and markets professional, medical, industrial and commercial services She was a victim too and we want to sell her data! (Warning, we will provide you with some data about it before you pay. Contact us to explain it to you)	warning : It will be ready for sale in 1/05/2022	Site : www.danaher.com	Transfer :	Size :	Date:

Coca-Cola
BTC : 1,6467000
Price (USD) : 64,396,67
Site : www.coca-cola.com
Transfer : Cryptocurrency
Size : (161G)
[scan : Click here](#)
Date: 04/24/2022

Stormous' announcement of the Coca-Cola data for sale and teasing new data dumps from other US companies

Who Is Stormous and Where Does Its Allegiance Lie?

Stormous, which may have begun operating as early as mid-2021, has posted a mission statement stating its objective is to attack targets in the U.S. and other western nations. This goal shifted in 2022, adding Ukraine and India to its target list. The way they discuss countries as their targets as opposed to specific businesses or industries suggests that politics more influence these shifts in targets than financial gain.



Screenshot from the Stormous Dark Web page

Our initial analysis of Stormous indicates the gang likely has members located in Mid-Eastern countries and Russia. Some of the group's postings are written in Arabic along with its public pro-Russian stance, which is consistent with the region. Moreover, two of the group's members that were arrested were from mid-eastern countries.

The group communicates through a Telegram channel and an .onion website on Tor. There is little chatter on the Telegram channel, with the conversation mainly comprised of the group's proclamations. While the group identifies itself as a ransomware group, it is not operating as a Ransomware-as-a-Service (RaaS), and it's not known what type of ransomware it may be using in their campaigns

The group's motivating principles and behavior somewhat resemble the Lapsus\$ hacker group, which targets entities mainly in the Western hemisphere. Like Lapsus\$, Stormous is quite "loud" online and looks to attract attention to itself, making splashy proclamations on the Dark Web and utilizing Telegram to communicate with its audience and organize to determine who to hack next.

Click-Bait or Serious Business?

Stormous has stated that on May 1, it will put up for sale data allegedly exfiltrated from toy manufacturer Mattel and Danaher, a global science and technology innovator. However, the group did not define the type or amount of data it had taken, and neither Mattel nor Danaher reported suffering a related cyber incident.

Stormous has already claimed responsibility for an alleged attack on the Coca-Cola Corp that it claims garnered 161GB of data. The group began selling the data on April 24 for 1.6 BTC, or about \$64,000.

Data size and type

document.rar	25-APR-2022 11:55	11G
dir.txt	25-APR-2022 11:55	144M
dir.zip	25-APR-2022 11:55	25G
Financial data.rar	25-APR-2022 11:55	516K
Network.rar	25-APR-2022 11:55	22G
a.Hardware.zip	25-APR-2022 11:55	900M
admin.txt	25-APR-2022 11:55	2G
media.zip	25-APR-2022 11:55	24M
accounts.zip	25-APR-2022 11:55	44G
Payments.zip	25-APR-2022 11:55	5G
email.txt	25-APR-2022 11:55	500M
passwords.txt	25-APR-2022 11:55	3G
Pictures.rar	25-APR-2022 11:55	44M

```
/aasdcac/HR_part3/  
/aasdcac/HR_part3/Financial data.rar  
/aasdcac/HR_part3/  
/aasdcac/HR_part3/Financial/Financial data  
/coca-cola/HR_part3/  
/coca-cola/HR_part3/Financial/Financial data 2  
/coca-cola/HR_part3/  
/coca-cola/HR_part3/Financial/Financial data 3  
/coca-cola/HR_part3/  
/coca-cola/HR_part3/Financial/Financial data 4  
/coca-cola/HR_part3/  
/coca-cola/HR_part3/Financial/Financial data 5  
/coca-cola/HR_part3/  
/coca-cola/HR_part3/Financial/Financial data 6  
/coca-cola/HR_part3/  
/coca-cola/HR_part3/Financial/Financial data 7  
/coca-cola/HR_part3/  
/coca-cola/HR_part3/Financial/Financial data 8  
/coca-cola/HR_part3/  
/coca-cola/HR_part3/Financial/Financial data 8  
/coca-cola/HR_part3/  
/coca-cola/HR_part3/Financial/Financial data 9  
/coca-cola/HR_part3/  
/coca-cola/HR_part3/Financial/Financial data 10  
/coca-cola/HR_part3/  
/coca-cola/HR_part3/Financial/Financial data 11  
/coca-cola/HR_part3/  
/coca-cola/HR_part3/Financial/Financial data  
/coca-cola/HR_part3/  
/coca-cola/HR_part3/Financial/Financial data 13  
/coca-cola/HR_part3/  
/coca-cola/HR_part3/Financial/Financial data 14  
/coca-cola/HR_part3/
```

Screenshot purporting to be stolen data from Coca-Cola, which shows passwords and name accounts.

The soft drink giant has confirmed that it has contacted law enforcement and is investigating a cyber incident but has so far offered no details on what might have transpired, according to [SecurityWeek](#).

The screenshot from Stormous site shows that the data it sells includes files with names such as accounts.zip and passwords.txt. If those files indeed contain the content that their names imply, then that content can be used by hackers for exploring additional ways to connect to Coca Cola's networks in an unauthorized way.

There is some debate within the cybersecurity community on the validity of Stormous' claims, specifically in relation to the Coca-Cola hack. The community questions whether or not the group has truly breached the companies named and exfiltrated data or if it's merely scavenging previously stolen or public information. For example, Mattel announced in November 2020, that it had been successfully hit by a ransomware attack earlier that year. The Stormous attackers could be simply compiling this already stolen data and packaging it as a 'new' breach in an attempt to earn quick money.

Stormous has also claimed to have successfully attacked several targets in India and Saudi Arabia and possibly a Chinese government site.

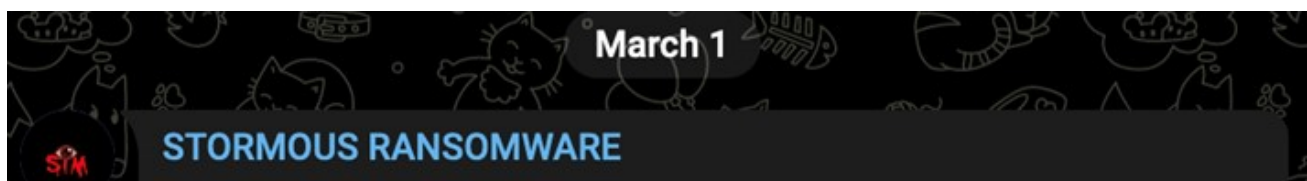


Stormous' logo wall of alleged victims

Stormous is also representative of another recent trend that sees threat actors creating a "corporate-like" structure and business model. In this case, perhaps because Stormous is relatively new to the scene, its postings and communications appear to be a brand-building exercise. Also, by pre-announcing the availability of supposedly stolen data, the group is trying to hype demand as any company might do with a new product. Finally, by taking a political stance, it likely hopes to attract supporters with similar viewpoints.

Politically Motivated Targeted Attacks

Stormous has posted its support for Russia and is claiming to have attacked the Ukraine Ministry of Foreign Affairs, obtaining and making public phone numbers, email addresses, and national identity cards. However, this attack, like the others, has not been corroborated.





يعلن فريق STORMOUS رسميًا دعمه للحكومات الروسية. وإذا قرر أي طرف في أجزاء مختلفة من العالم تنظيم هجوم إلكتروني أو هجمات إلكترونية ضد روسيا وغيرها ، فسنكون في الاتجاه الصحيح وسنبذل كل جهودنا للتخلي عن دعاء الغرب ، وخاصة البنية التحتية. ربما كانت عملية القرصنة التي نفذها فريقنا لحكومة أوكرانيا وشركة طيران أوكرانية مجرد عملية بسيطة ولكن ما هو قادم سيكون أكبر !!

The STORMOUS team has officially announced its support for the Russian governments. And if any party in different parts of the world decides to organize a cyber-attack or cyber-attacks against Russia, we will be in the right direction and will make all our efforts to abandon the supplication of the West, especially the infrastructure. Perhaps the hacking operation that our team carried out for the government of Ukraine and a Ukrainian airline was just a !!!simple operation but what is coming will be bigger

[Ukraine_and_its_allies_are_i_danger#](#)
[Strom_2022#](#)

1.1K 👁 , edited 14:57

Stormous' official statement on its support for Russia

Stormous' actions are not unique. Since the Russia-Ukraine war started on Feb. 14, threat groups have been lining up to support each side. Trustwave SpiderLabs reported on this activity soon after hostilities broke out.

Multiple sources have used Facebook and other social media outlets to try and gather a force to conduct these attacks. Most notably, Yegor Aushev, co-founder of a cybersecurity company in Kyiv, told Reuters he wrote a post calling for underground cyber defenders at the request of a senior Ukrainian Defense Ministry official who contacted him.

Trustwave SpiderLabs has observed similar calls to cyber arms on the Dark Web. These include links to groups organizing to attack Russian entities, sites containing instructions on how to conduct a DDoS attack, and a recommended DDoS attack target list.



STORMOUS RANSOMWARE



STORMOUS :

[#Ministry_of_Foreign_Affairs_\(Ukraine\)](#)

وزارة الشؤون الخارجية (أوكرانيا) هي وزارة في حكومة أوكرانيا مهمة الوزارة هي الاعتراف على علاقات أوكرانيا الخارجية .

شبكةهم حسنة تمت سرقة بياناتهم المختلفة وتوزيع حسب أرقام هواتفهم وبياناتهم الإلكترونية وحساباتهم وأرقام بطاقاتهم الوطنية الخاصة ، مع اختراق شبكة داخلية والوصول إلى معظم الملفات الأساسية هنا مع وضع هجمات الإنترنت على موقعهم الرئيسي

The Ministry of Foreign Affairs (Ukraine) is a Ministry of the Government of Ukraine whose task is to supervise the foreign relations of Ukraine.

Their network is fragile - their various data has been stolen and distributed according to their phone numbers, email, accounts and national card numbers with an internal network hacked and access to most essential files.

This is with placing denial attacks on their main site !

web : <http://mfa.gov.ua/>

Phones :

Fax:

e-mail:

pay - 

time:

00.00.00.00

contact :

stormous@protonmail.com

970  , edited 23:41

A message in Arabic from the Stormous Telegram channel stating it had attacked the Ukraine Ministry of Foreign Affairs

The Stormous group has also signaled that it won't stand by and allow other entities, such as ransomware groups, to attack Russia. Stormous has declared it will respond to any attack against Russia, noting that if the attacks on Russia stop then, Stormous will halt its efforts.



A note from the Stormous Telegram channel

A New Age of Cybercriminal

The new style of threat group Stormous represents, being unafraid of -- and in fact seeking public adulation -- can make its members more susceptible to being found and arrested.

While there may be an upside from a clout and branding perspective to making hacking activities public, law enforcement can use communications information to bring cybercriminals more swiftly to justice.

Trustwave SpiderLabs will continue to track the threat of Stormous and group's activities as more information becomes available.