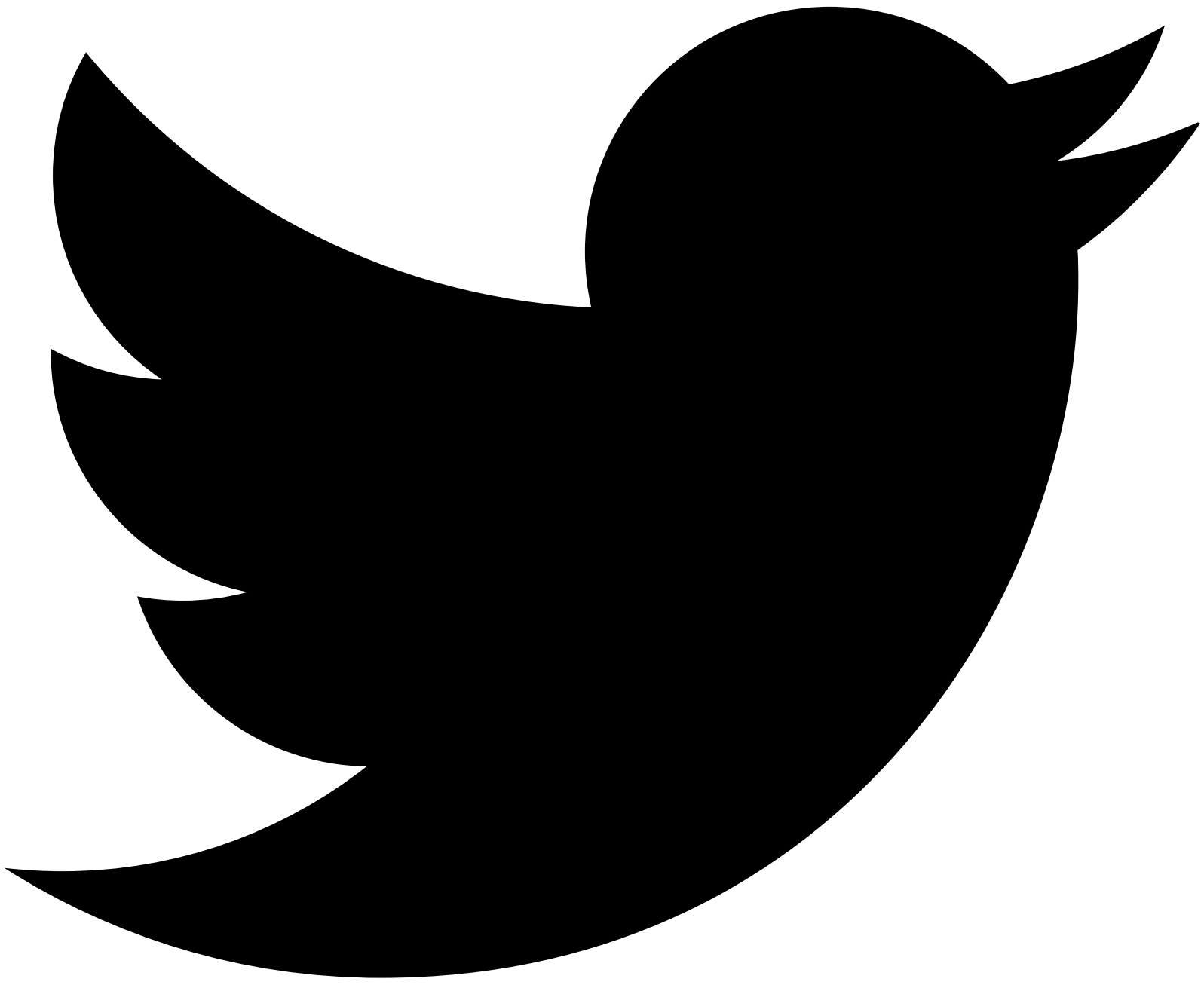
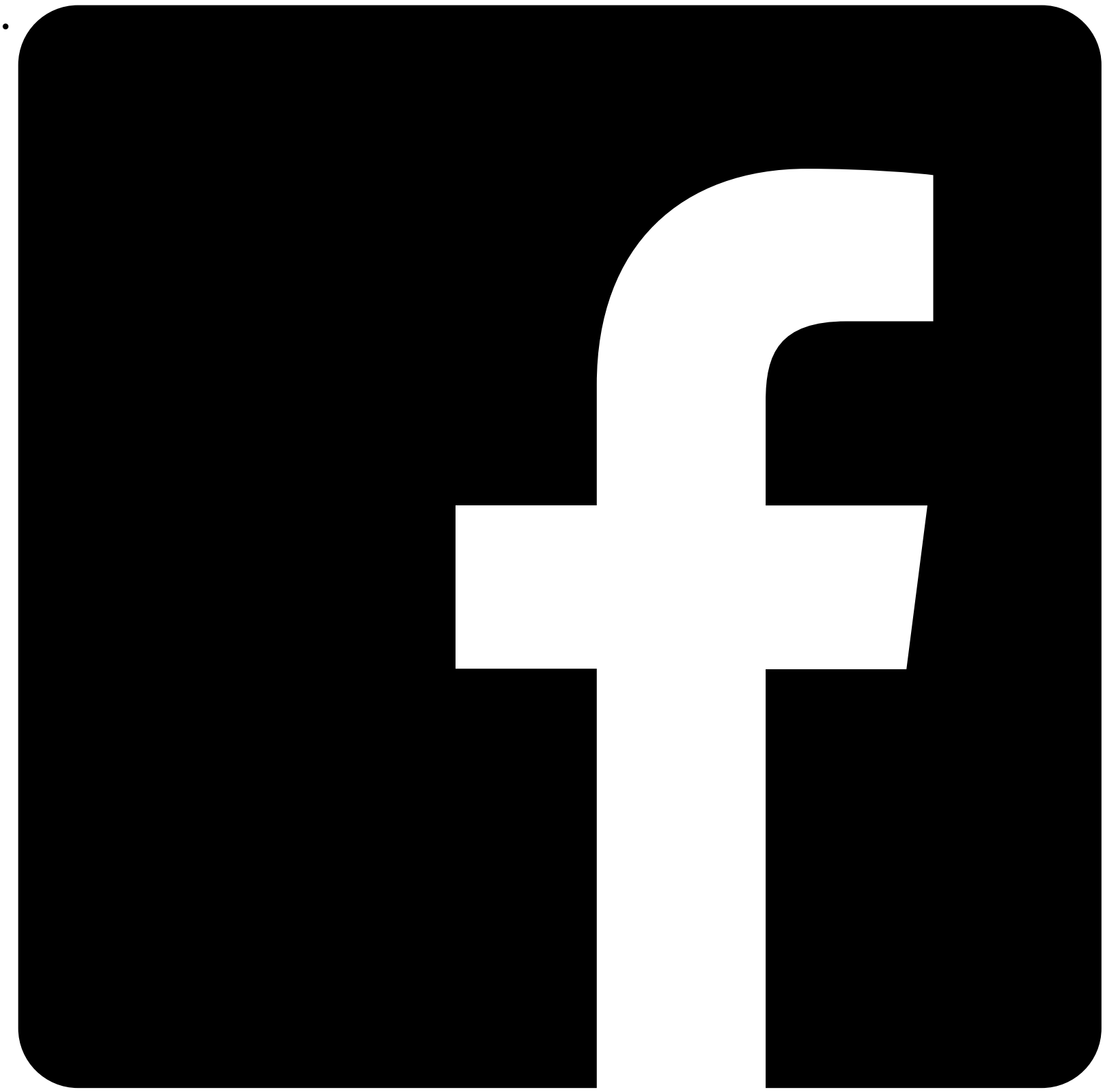
Stormous: The Pro-Russian, Clout Hungry Ransomware Gang Targets the US and Ukraine

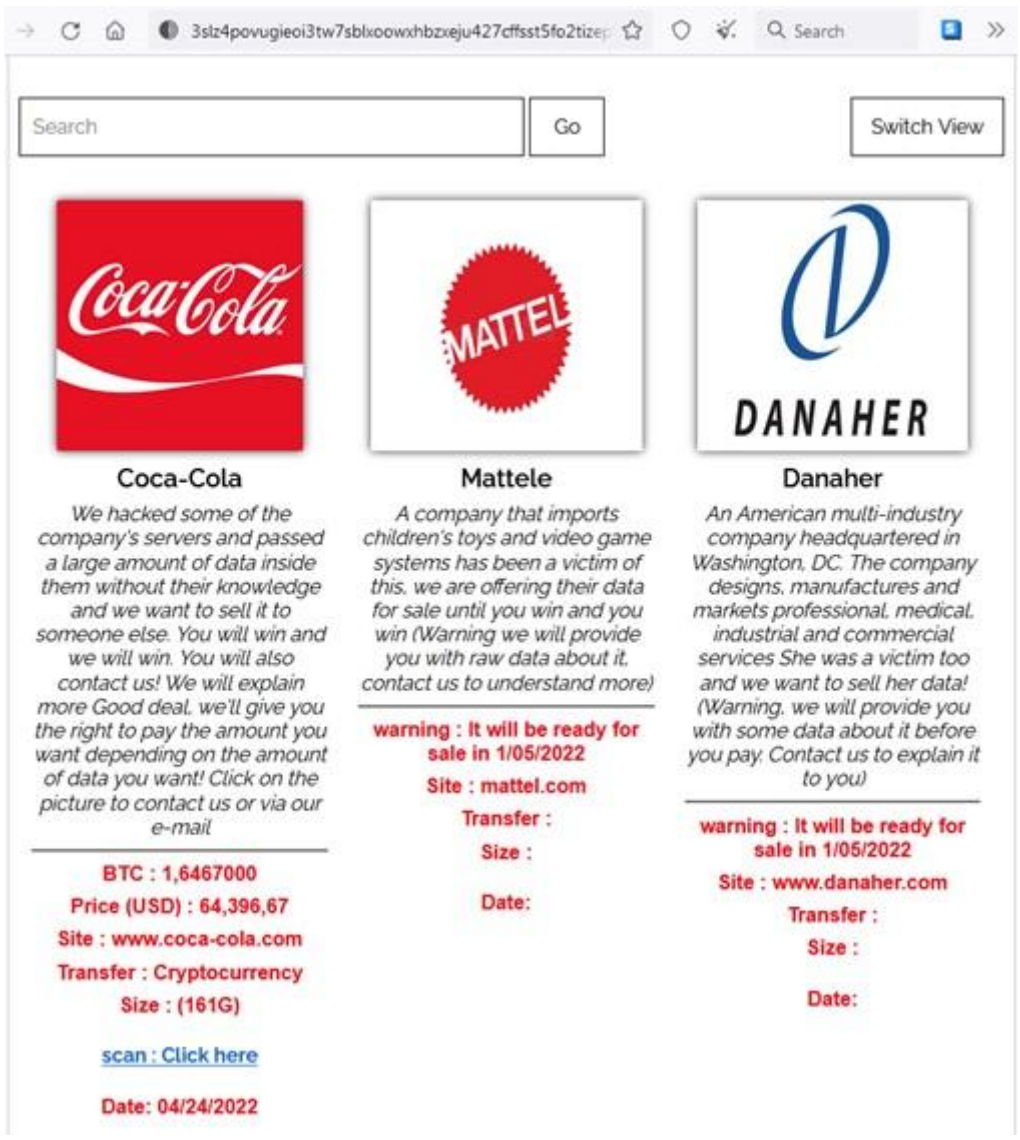
access_timeApril 29, 2022 person_outlineTrustwave SpiderLabs share





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.

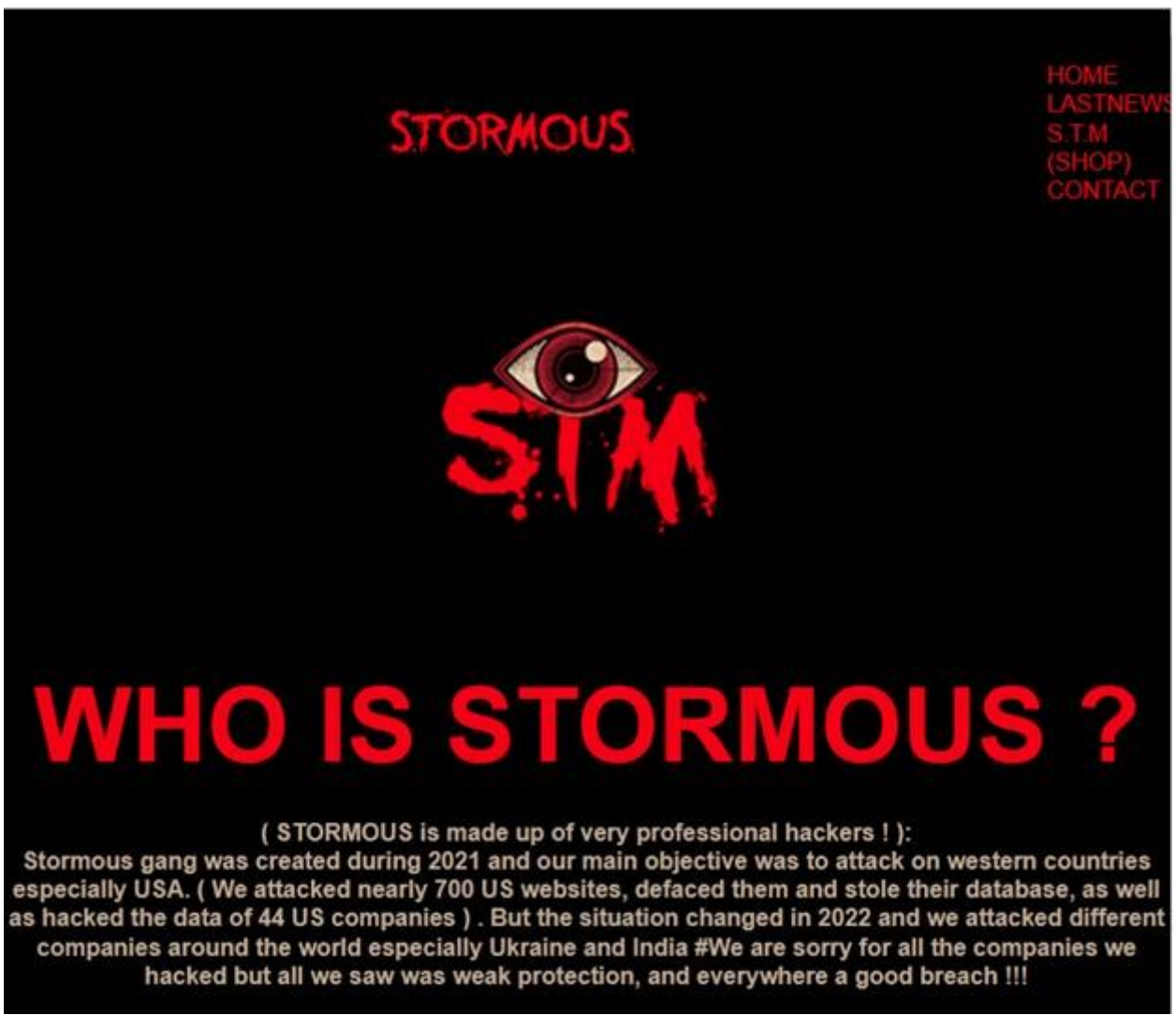
As of April 29, the group has listed the Coca-Cola data for sale on its Dark Web site. At the time of publishing, Coca-Cola has neither confirmed nor denied whether the data listed is legitimate. Most recently, the gang has promised to release additional stolen information from multinational toy manufacturer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



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.

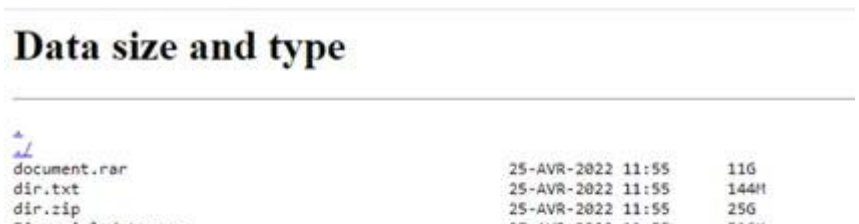
The group communicates through a Telegram channel and an .onion website on Tor. There is little chatter on the Telegram channel, with the conversation mainly comprised of the group's proclamations. While the group identifies itself as a ransomware group, it is not operating as a Ransomware-as-a-Service (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-AVR-2022 11:55	11G
dir.txt	25-AVR-2022 11:55	144M
dir.zip	25-AVR-2022 11:55	25G
Financial data.rar	25-AVR-2022 11:55	516K
Network.rar	25-AVR-2022 11:55	22G
a.Hardware.zip	25-AVR-2022 11:55	900M
admin.txt	25-AVR-2022 11:55	2G
media.zip	25-AVR-2022 11:55	24M
accounts.zip	25-AVR-2022 11:55	44G
Payments.zip	25-AVR-2022 11:55	5G
email.txt	25-AVR-2022 11:55	500M
passwords.txt	25-AVR-2022 11:55	3G
Pictures.rar	25-AVR-2022 11:55	44M

./aasdcat/HR_part3/
./aasdcat/HR_part3/Financial data.rar
./aasdcat/HR_part3/
./aasdcat/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-colaHR_part3/
./coca-cola/HR_part3/Financial/Financial data 4
./coca-colaHR_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
./acoca-cola/HR_part3/
./coca-cola/HR_part3/Financial/Financial data 14
./coca-colat/HR_part3/

Screenshot purporting to be stolen data from Coca-Cola

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 Security Week.

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.

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.

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.