# Sep 2023 Cybercrime Update | New Ransomware Threats and the Rising Menace of Telegram

sentinelone.com/blog/sep-2023-cybercrime-update-new-ransomware-threats-and-the-rising-menace-of-telegram/

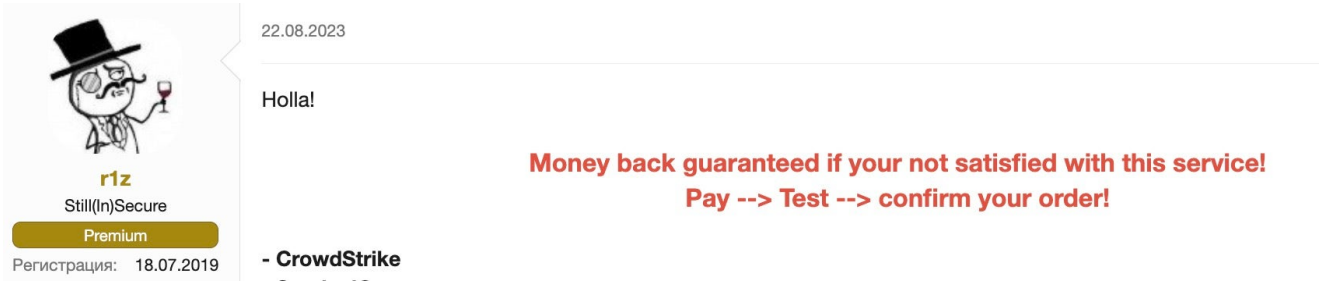
September 13, 2023

In this blog post, we delve into the notable trends that have been shaping the cyber landscape over the past month. From the burgeoning market of bypass services to the alarming criminal activities on Telegram, we provide an update on cybercriminal activity to help defenders, SOC Teams and security leaders stay abreast of the latest developments and fortify their defenses in this ever-evolving battleground.


## The AV/EDR/XDR Bypass Market

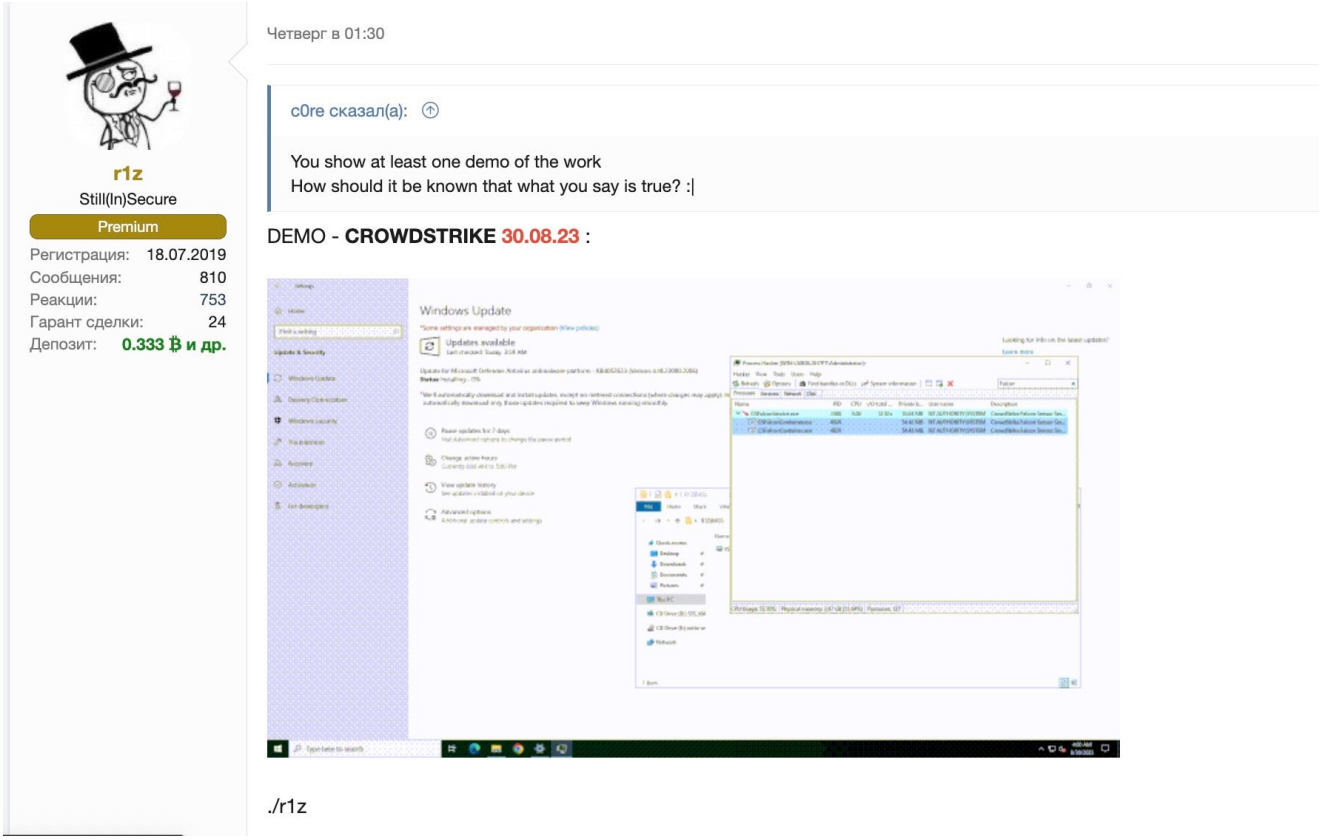
Threat actors across the cybercrime landscape are interested in anything that will help them bypass security solutions and evade detection, and this has resulted in a busy trade for tools and services which claim to answer this need.

The bypass market is not new but has witnessed an alarming growth in both the sophistication of the tools being offered and the assertiveness of the actors involved. These actors are leveraging unprecedented access to enterprise-level tools, continually testing and refining their malware against these tools, and posing a sophisticated and potent threat in targeted environments.




Advertisement for “EDR Killer”, a malware dropper and bypass service

Bypass tools and services, which are far from being budget-friendly, are becoming a staple in the arsenal of ransomware operators. The bespoke nature of these services, exemplified by vendors such as “r1z,” indicates a burgeoning market where customizations can drive the price upwards from a base of around 3000 USD.




Demo of “EDR Killer” bypassing an AV company

However, modern EDR/XDR technologies are not entirely helpless against these tools, provided they are well-maintained and appropriately configured. Threat actor tools, when successful, are usually deployed against outdated versions or ill-maintained and misconfigured setups, laying open the vulnerabilities for these AV bypass tools to exploit.

## Ransomware | New Threat Actors Ramping Up Attacks

The ransomware threat may be less in the headlines than this time last year, but known and new threat actors continue their activities, exploiting novel techniques and finding overlooked weaknesses in organizations’ security posture, as the ransomware attack on MGM Resorts

this week has shown.

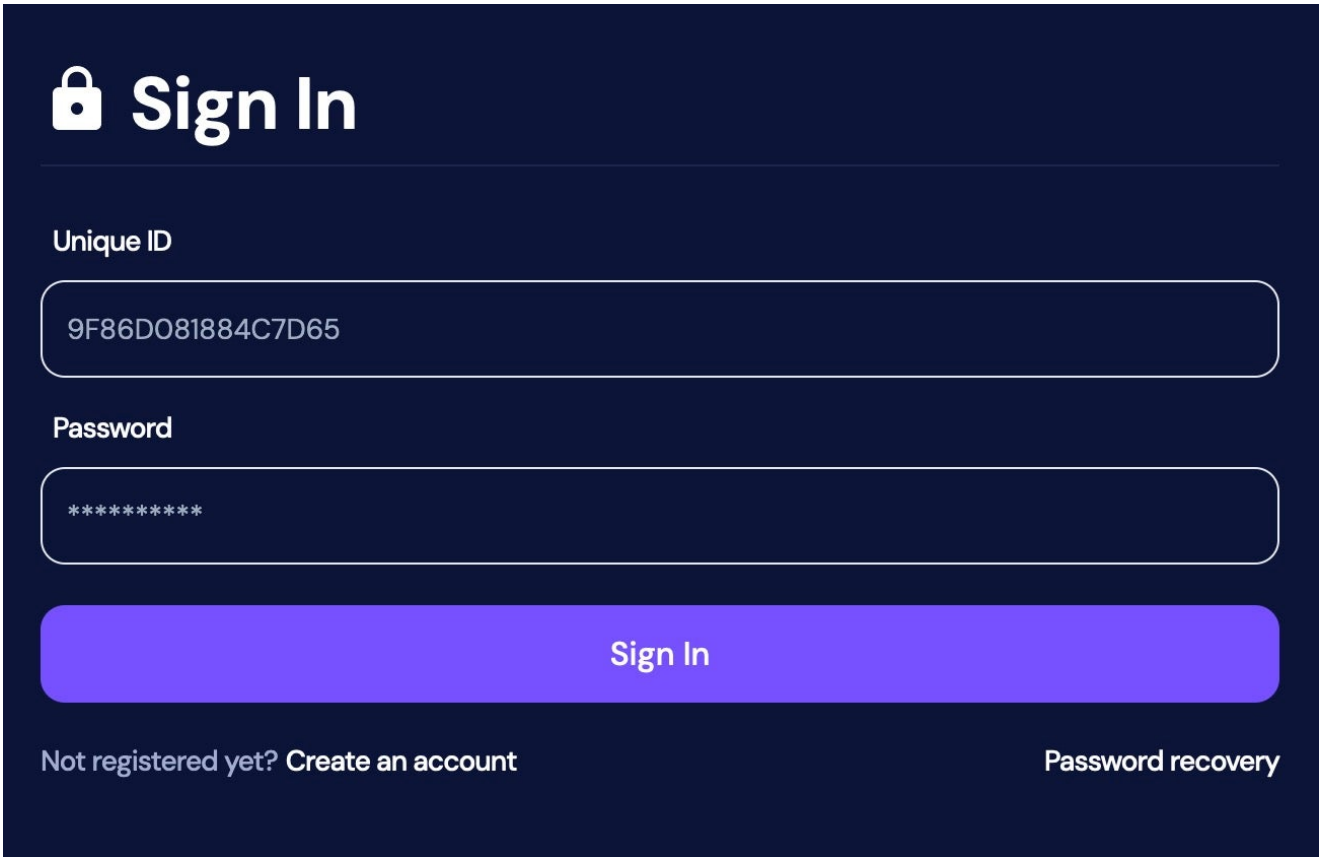
> All ALPHV ransomware group did to compromise MGM Resorts was hop on LinkedIn, find an employee, then call the Help Desk.
>
> A company valued at $33,900,000,000 was defeated by a 10-minute conversation.
>
> — vx-underground (@vxunderground) September 13, 2023

Elsewhere, new threat actors continue to appear and are ramping up operations. The coming months are expected to be a busy time for new attacks.

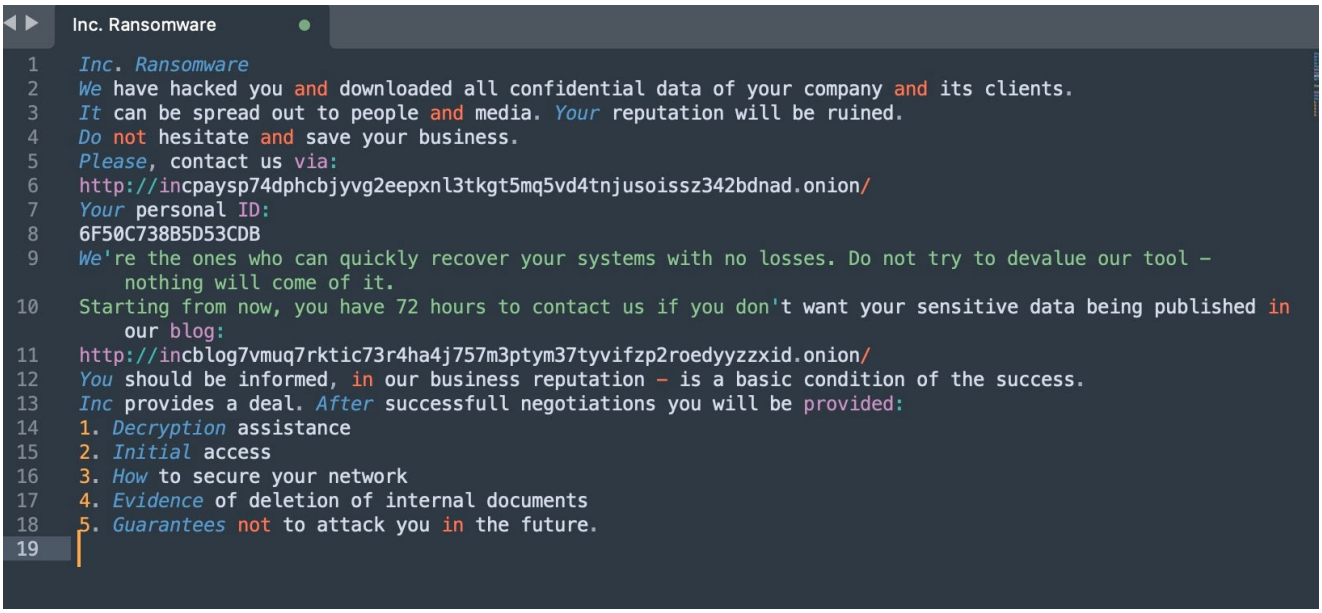
## INC Ransom

The INC Ransom group emerged on the scene in early August 2023, establishing themselves with a semi-private, affiliate-based operation. A closer look at their operation reveals a penchant for exploiting weaknesses in Remote Desktop Protocols (RDP) and utilizing purchased valid account credentials, typically acquired through Initial Access Brokers (IAB).

Their modus operandi includes leveraging living-off-the-land binaries (LOLBINs) such as `WMIC.EXE` and `MSTC.EXE`, among others, aiming to bypass detection technologies embedded in targeted environments. The victims, once infected, are ushered into a negotiation process via a TOR-based portal, with a stringent 72-hour window to comply with the payment demands before their data gets published.



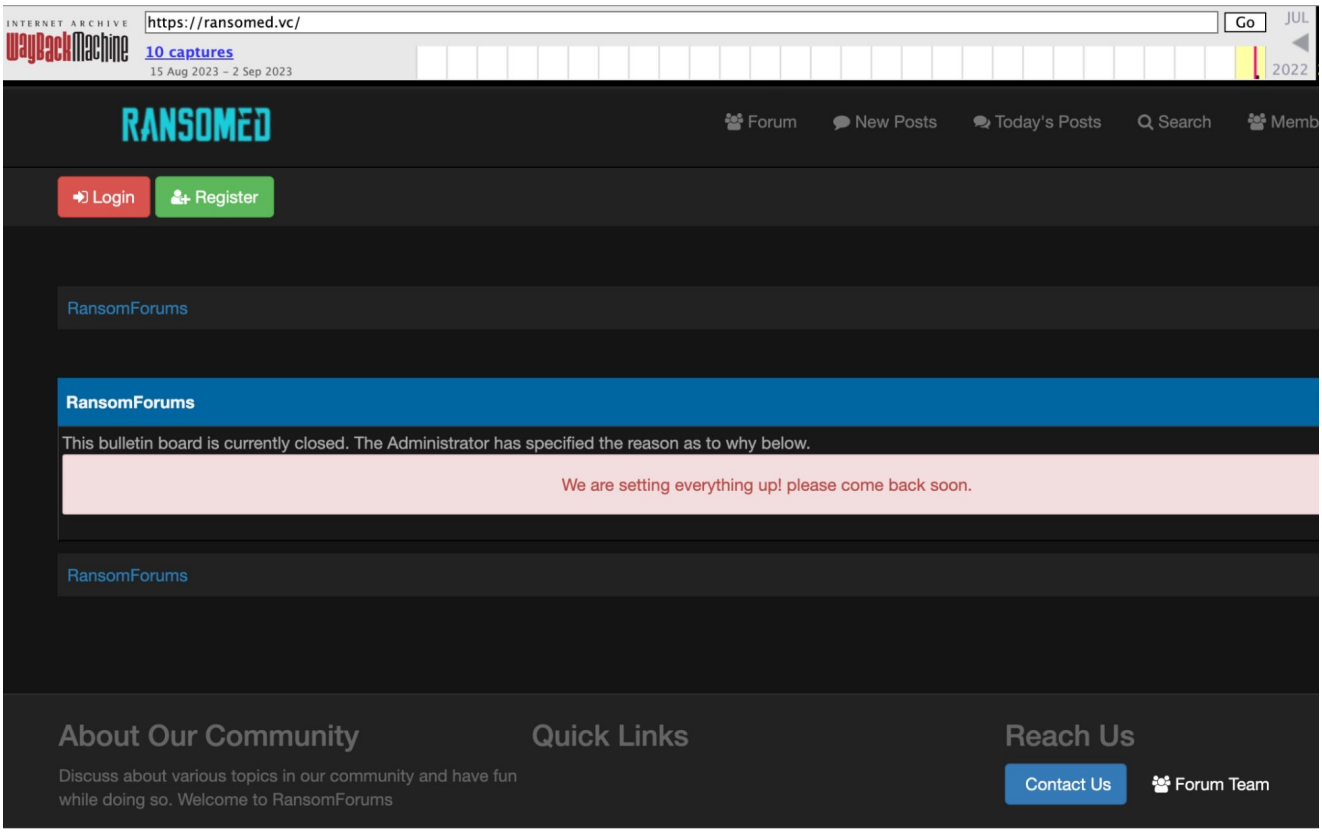

INC Ransomware victim sign-in portal




INC Ransom ransom note

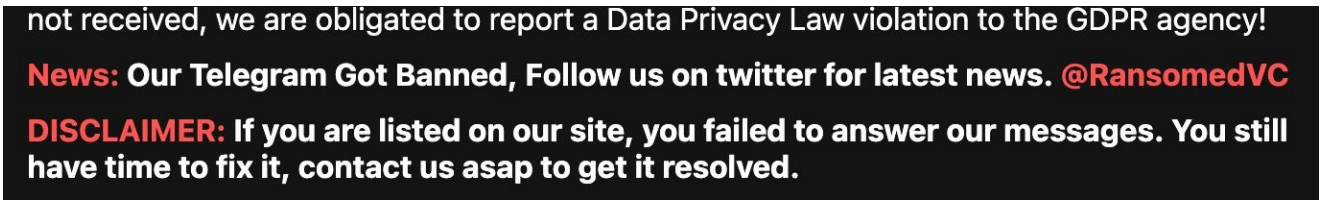
## Ransomed.VC

Ransomed.VC burst onto the scene with a well-orchestrated PR campaign, encompassing a clearnet site and multiple communication channels including Telegram and Twitter/X profiles. Their operations are heavily inclined towards exploiting GDPR penalties as a method of extortion, threatening victims with potential legal repercussions in case of data leaks.



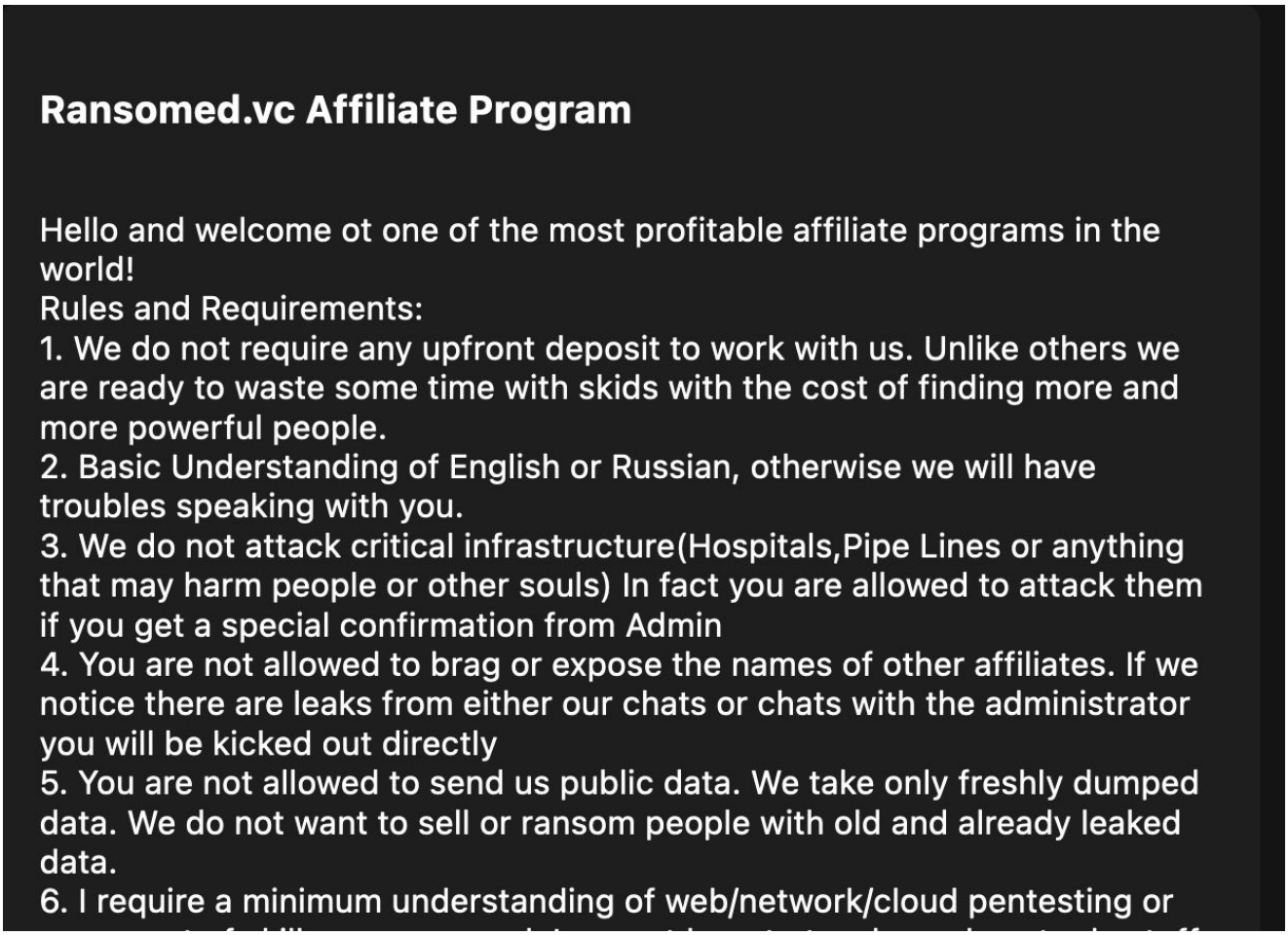
Ransomed.vc capture for August 2023 (Wayback Machine)

Their evolutionary journey can be traced back to the “RANSOMED” forums, with their website undergoing a significant transformation before a highly publicized launch in August 2023. The group has expanded its communication channels, utilizing both clearnet and dark web platforms to circulate news and updates regarding their activities.



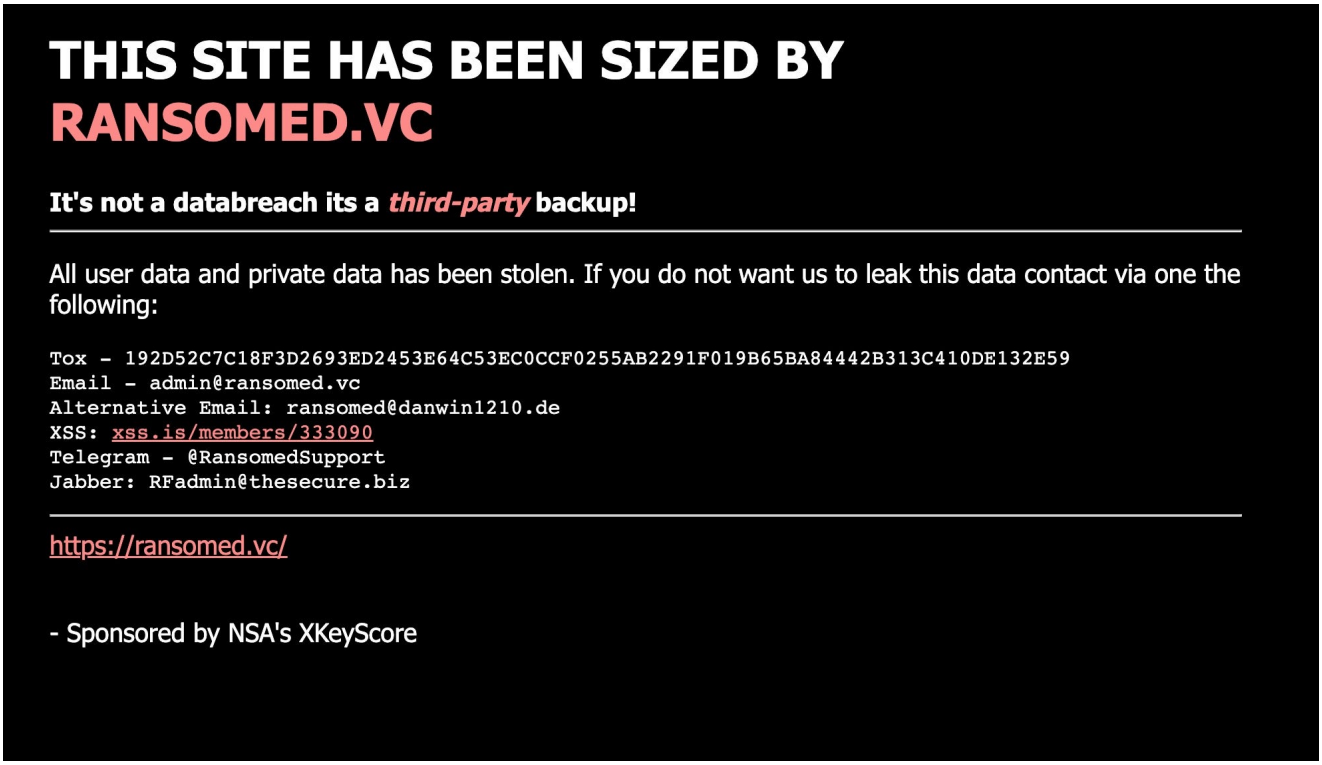
Ransomed Telegram channel is banned

Despite facing bans from various social media and communication platforms, they have adapted quickly, shifting their communication hub to other platforms including underground Russian cybercrime forums. Their approach indicates a brazen disregard for the potential humanitarian consequences of their actions, even allowing for attacks on critical infrastructure sectors, provided they get an approval from the “admin”.



Advert to join the Ransomed RaaS (Affiliate Program)

Their business model encompasses an affiliate program, providing a platform for like-minded criminals to collaborate and enhance their nefarious activities. The group has also demonstrated their ability to deface websites, including government domains, using them as a billboard to showcase their ransom demands and details of the attacks.



Ransomware message on Hawaii[.]gov website

Leveraging GDPR laws, they have positioned themselves as a pure extortion group, operating without deploying any ransomware. This approach complicates the efforts to neutralize and respond to their threats effectively.

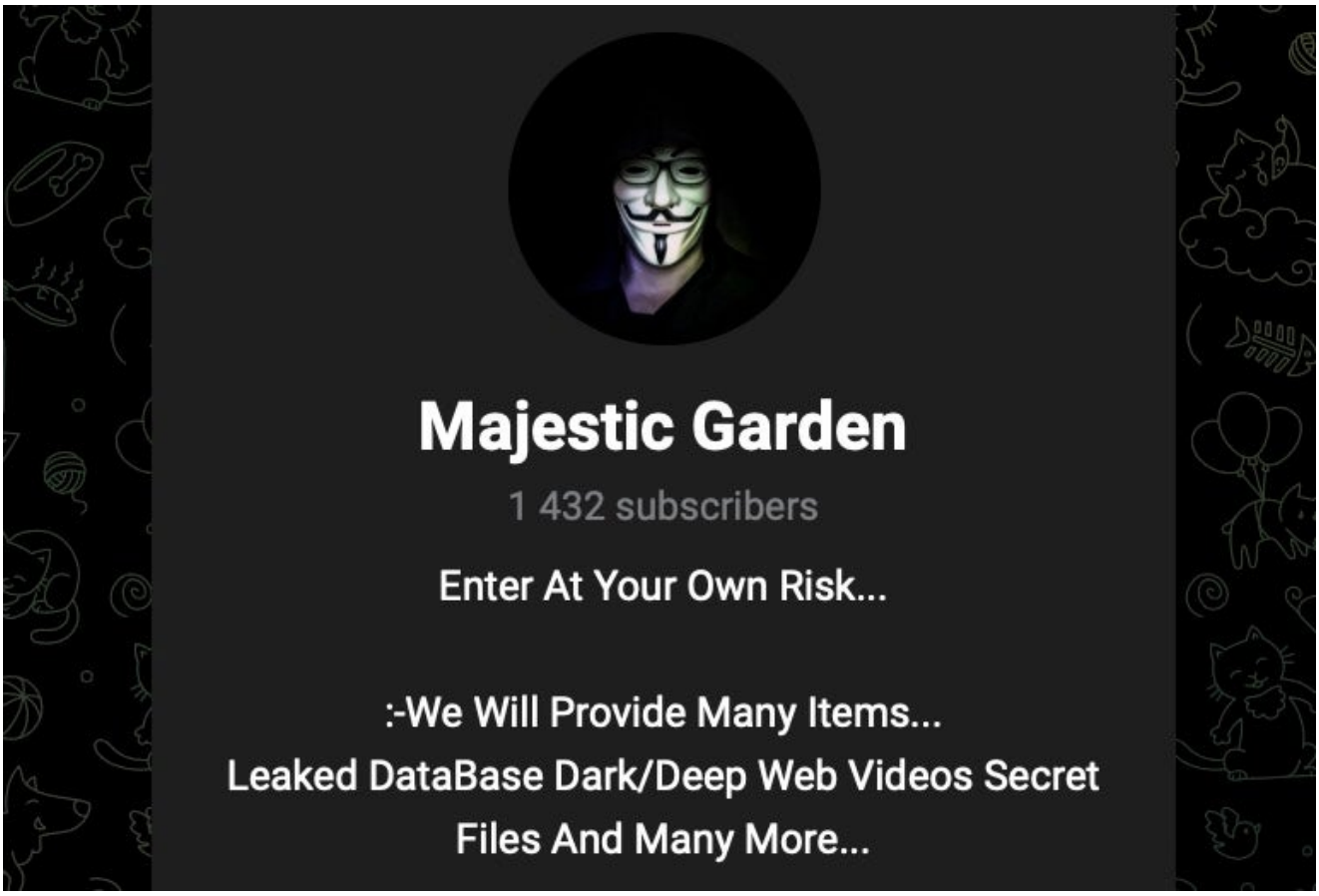
## Telegram | The “Wild Wild West” of Cybercrime

Since its inception in 2013, Telegram has gradually but steadily morphed into a hub for criminal activities, such that it now resembles the unregulated and chaotic nature of IRC channels and the early days of the internet. From malware distribution to recruitment into criminal organizations, the platform is now a hotbed for various cybercrime ventures.

One of many Telegram channels offering EDR Bypass tools, tips and tricks

Telegram's encrypted environment, coupled with the capability to host large groups and automate processes through "bots," has facilitated a significant migration of cybercriminal activities from traditional dark web markets to this more secure platform.

As of September 2023, the platform continues to teem with vendors offering custom malware tools and crypters, and it has now become the preferred platform for ransomware groups to disseminate stolen data and recruit affiliates, functioning as a versatile tool in their operations.



Telegram has become a hive for cybercriminals to share stolen data

## Conclusion

As we approach fall of 2023, with businesses returning to offices and schools and colleges opening for the new term, the cybercrime landscape continues to evolve at pace, with new entrants wielding sophisticated tools looking for any avenue of attack. Organizations must be vigilant and prepared, continuously adapting to the ever-changing threats emerging from the digital shadows.

In the face of these emerging trends, employing a comprehensive security solution like Singularity XDR, which leverages AI and automated remediation, can serve as a potent weapon in an organization's cybersecurity arsenal. It's more crucial than ever to stay ahead of the curve, adopting proactive measures that help detect and mitigate threats before they can inflict significant damage.

The cybercriminals are not resting, and neither should we. To learn more about how SentinelOne can help defend your organization's endpoint, cloud, and network assets, contact us or request a free demo.