Dark Peep #2: War and a Piece of Hilarity

socradar.io/dark-peep-2-war-and-a-piece-of-hilarity/

October 17, 2023

The Dark Web is not standing still, with the Israel-Palestine Conflict, the cyber world has become even more active, and we can say that interesting behaviors that attract our attention are on the rise. As the SOCRadar team, we continue to keep up to date on this issue, and in this blog post, we have brought you the news that attracted our attention in the last two weeks.

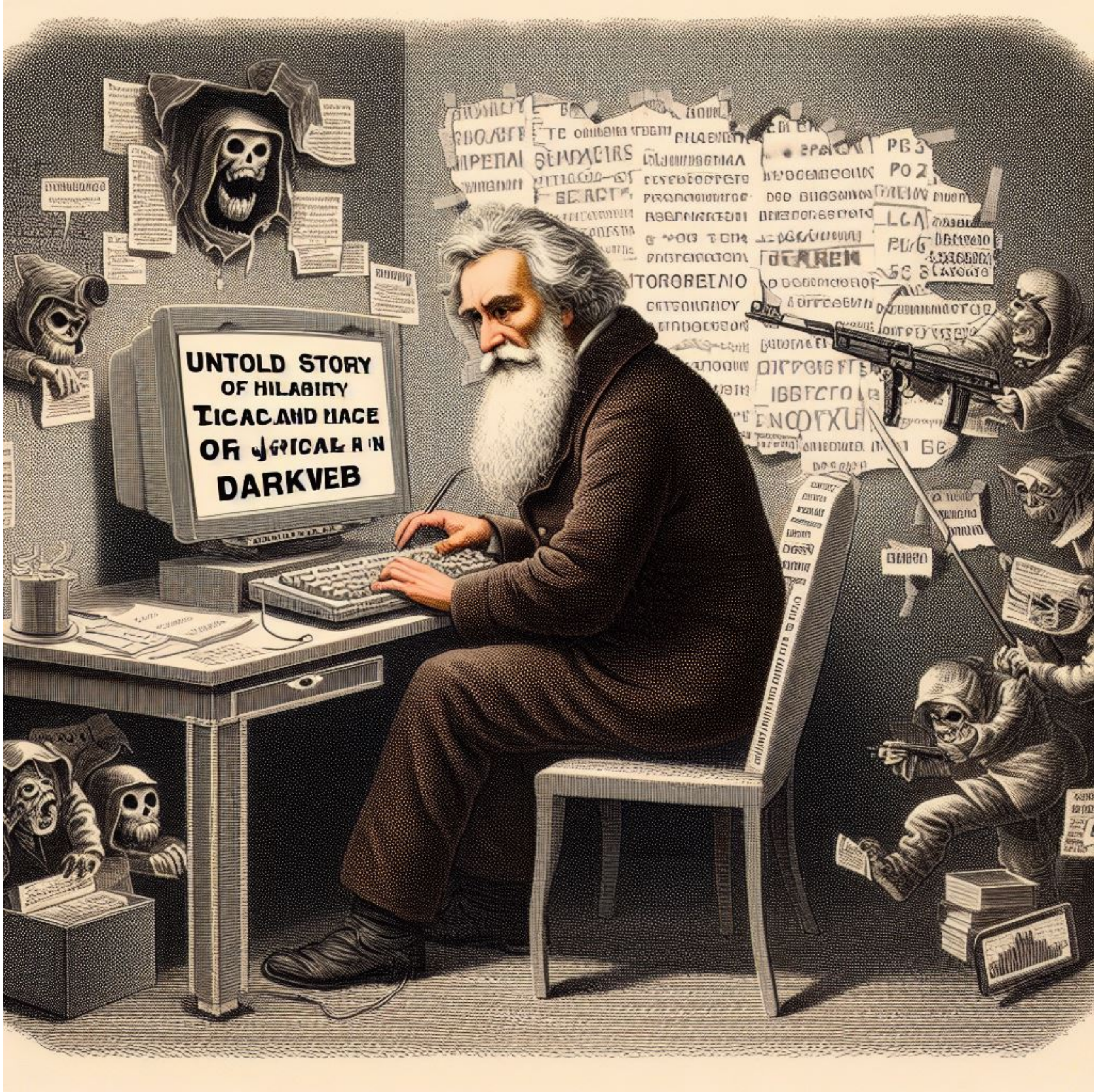
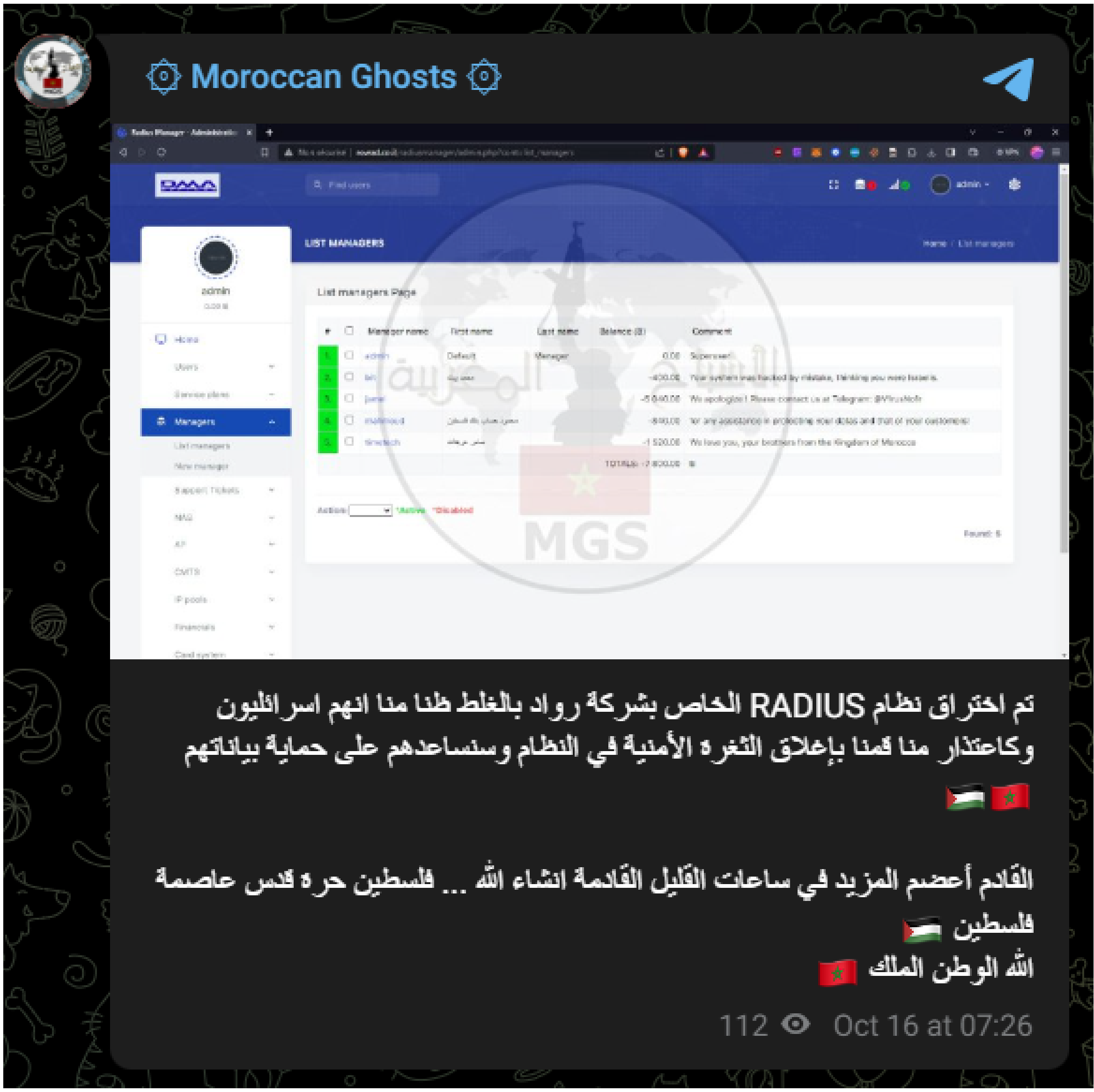


Fig. 1. Illustration of Tolstoy writing the “War and a Piece of Hilarity” Story of Dark Peep

(generated using OpenAI's DALL-E 3)

RADIUS Riddled: Moroccan Ghosts Unmask System Weakness!

In a turn of events that might make tech companies re-evaluate their security measures, the group **'Moroccan Ghosts'** claimed responsibility for penetrating the RADIUS system. With no sophisticated hacking tools in their arsenal, these digital phantoms relied solely on mental prowess and coding acumen.



List managers Page

#	☐	Manager name	First name	Last name	Balance (﷼)	Comment
1.	☐	admin	Default	Manager	0.00	Supervisor
2.	☐	bri	[illegible]		-400.00	Your system was hacked by mistake, thinking you were Israelis.
3.	☐	jamal			-5 640.00	We apologize! Please contact us at Telegram: @VirusNofr
4.	☐	mahmoud	[illegible]		-840.00	for any assistance in protecting your datas and that of your customers!
5.	☐	timetech	[illegible]		-1 520.00	We love you, your brothers from the Kingdom of Morocco
					TOTALS: -7 800.00	﷼

Action: *Active *Disabled

Found: 5

تم اختراق نظام RADIUS الخاص بشركة رواد بالغلط ظنا منا انهم اسرائليون
وكاعتذار منا قمنا بإغلاق الثغرة الأمنية في النظام وسنساعدهم على حماية بياناتهم
🇵🇸🇲🇦

القادم أعضم المزيد في ساعات القليل القادمة انشاء الله ... فلسطين حره قدس عاصمة
فلسطين 🇵🇸
الله الوطن الملك 🇲🇦

112 👁 Oct 16 at 07:26

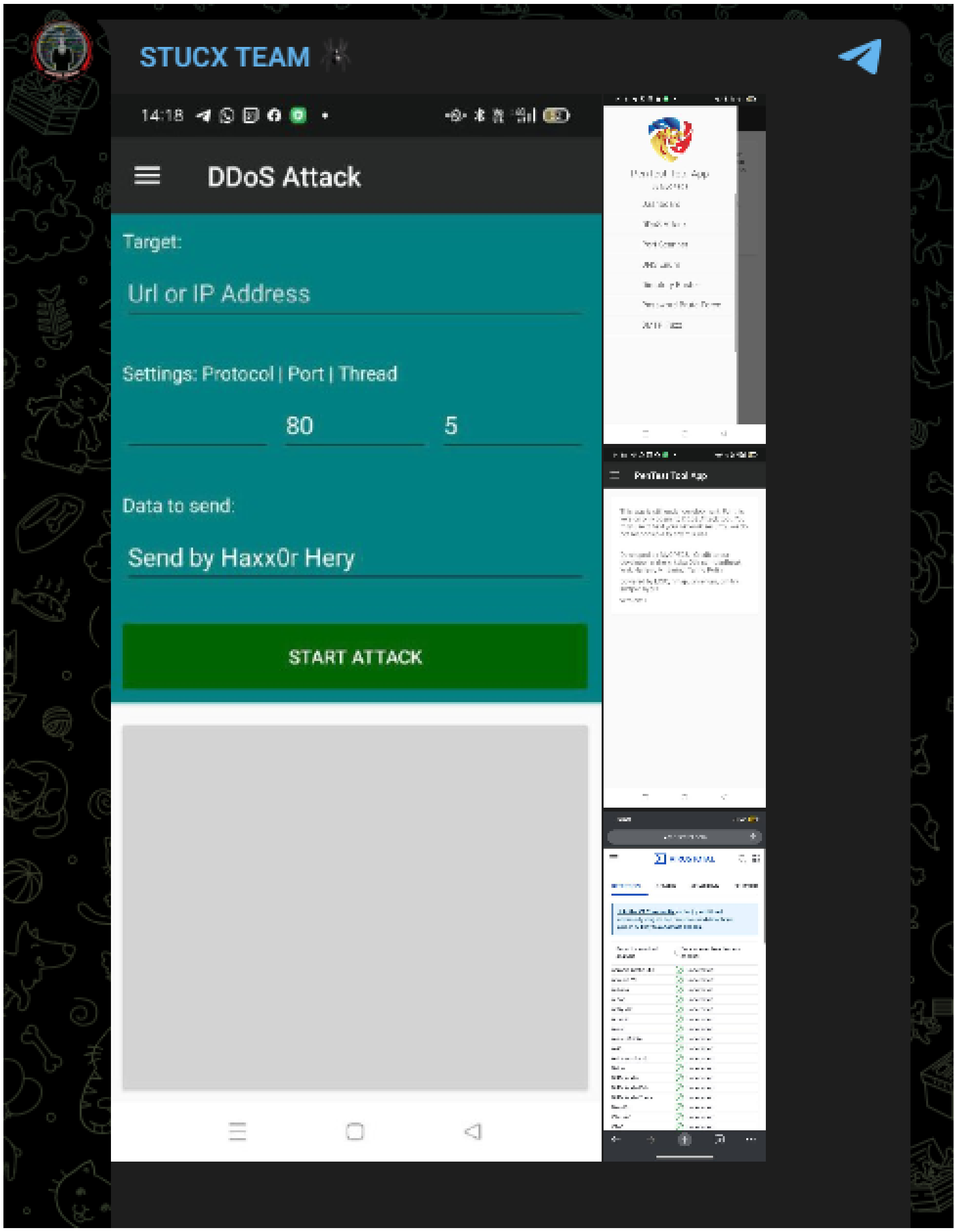
Fig.2.

Moroccan Ghosts Telegram post about RADIUS

This spectral breach serves as a reminder: In the digital realm, sometimes the most significant threats aren't invisible; they're right before our eyes. The "ghosts" have issued a chilling warning: beef up your defenses, or prepare for more unexpected "visitations" in the future.

Stucx Team Endorses MyOPECS' Mobile Magic: PenTest Tool App

MyOPECS has just heralded its grand entry into the world of **mobile penetration testing**. With the showing off of their new application and the sharing of the APK file of the first version on their Telegram channel, smartphone users will soon be able to access it via both Google Play Store and Apple App Store.



DDoS Attack

Target:

Url or IP Address

Settings: Protocol | Port | Thread

80 5

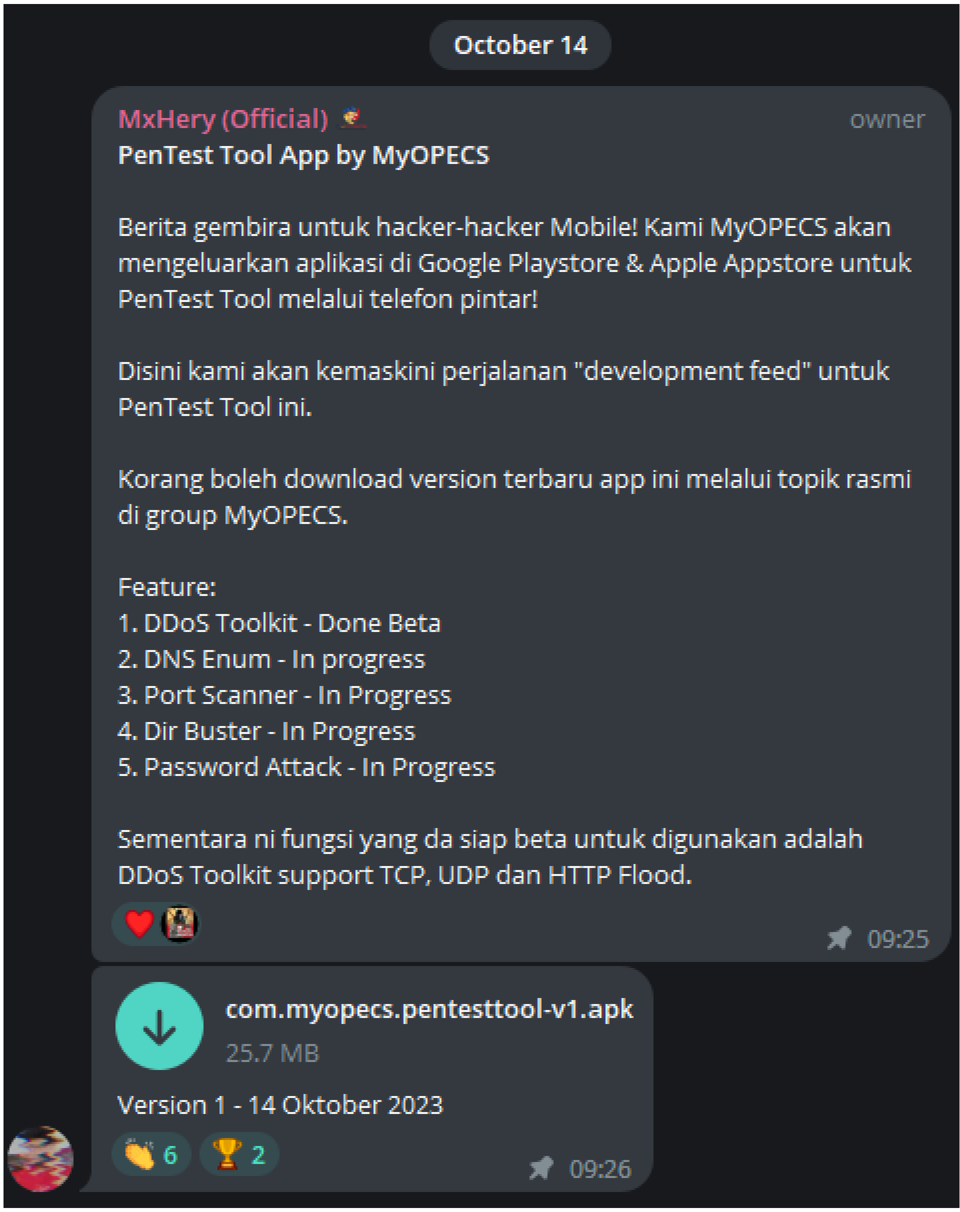
Data to send:

Send by Haxx0r Hery

START ATTACK

Fig. 3. STUCX Team shared the screenshots of PenTest Tool App developed by MyOPECS

Stay tuned to their “development feed” journey, as MyOPECS promises real-time updates for this groundbreaking PenTest Tool. And for those eager to get ahead of the curve, the latest version of the app is available for download in the official MyOPECS group.



October 14

MxHery (Official)

owner

PenTest Tool App by MyOPECS

Berita gembira untuk hacker-hacker Mobile! Kami MyOPECS akan mengeluarkan aplikasi di Google Playstore & Apple Appstore untuk PenTest Tool melalui telefon pintar!

Disini kami akan kemaskini perjalanan "development feed" untuk PenTest Tool ini.

Korang boleh download version terbaru app ini melalui topik rasmi di group MyOPECS.

Feature:
1. DDoS Toolkit - Done Beta
2. DNS Enum - In progress
3. Port Scanner - In Progress
4. Dir Buster - In Progress
5. Password Attack - In Progress

Sementara ni fungsi yang da siap beta untuk digunakan adalah DDoS Toolkit support TCP, UDP dan HTTP Flood.

09:25

com.myopecs.pentesttool-v1.apk

25.7 MB

Version 1 - 14 Oktober 2023

09:26

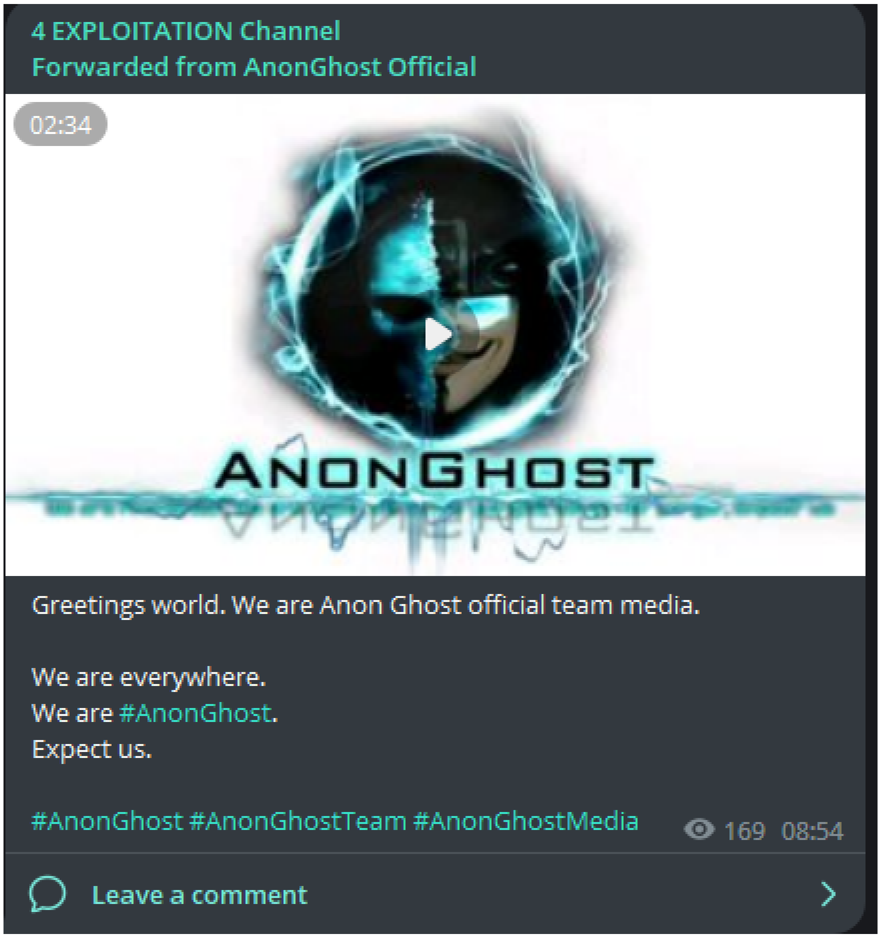
Fig. 4. MyOPECS' Telegram post of describing its PenTest Tool App and sharing the App's APK file

Under development key features of this app are:

- DDoS Toolkit
- DNS Enum
- Port Scanner
- Dir Buster
- Password Attack

Threat Actors Are Now Sharing Videos, Like Influencers

The Indonesian hacktivist group AnonGhost posted a video of themselves using their own video to show that they have followers who identify themselves as AnonGhost and that their real account is the one that posted the video.


4 EXPLOITATION Channel
Forwarded from AnonGhost Official

Greetings world. We are Anon Ghost official team media.

We are everywhere.
We are #AnonGhost.
Expect us.

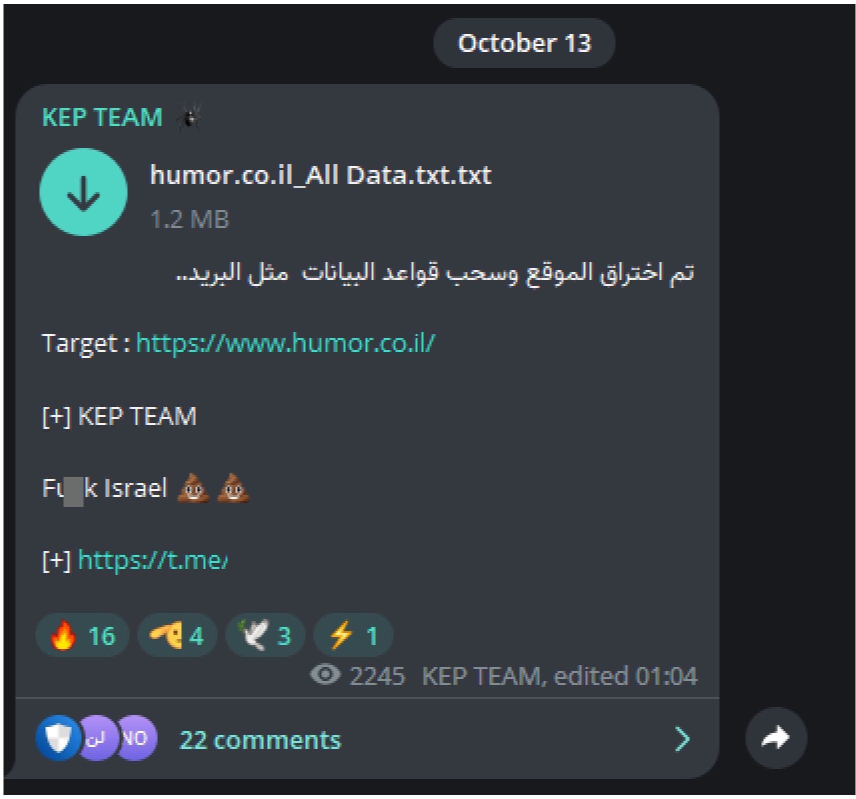
#AnonGhost #AnonGhostTeam #AnonGhostMedia

Fig. 5. AnonGhost's Telegram post contains the group's video

Threat actors have reached such a stage that people have started to operate under the names of known groups, interesting…

War Spilled Over Into "Humor"

In a turn of events showcasing the profound effects of the ongoing Israel-Palestine conflict on the digital front, the website "Humor.co.il" recently faced a cyberattack. The **KEP TEAM** claimed responsibility for the breach, indicating the intersection of political tensions and cyber warfare. As real-world disputes intensify, it appears no domain, not even those meant for levity and laughter, is immune from the reach of hackers. The incident serves as a stark reminder of the blurred lines between online platforms and geopolitical disputes, emphasizing the need for heightened cyber vigilance.



October 13

KEP TEAM

humor.co.il_All Data.txt.txt

1.2 MB

تم اختراق الموقع وسحب قواعد البيانات مثل البريد..

Target : https://www.humor.co.il/

[+] KEP TEAM

Fu[redacted]k Israel 💩 💩

[+] https://t.me/

🔥 16 🤙 4 🕊 3 ⚡ 1

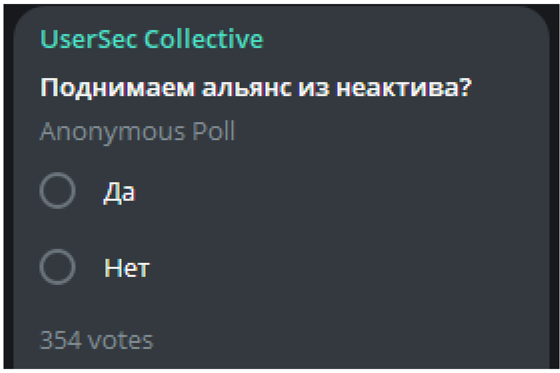
2245 KEP TEAM, edited 01:04

22 comments

Fig. 6. KEP TEAM's Telegram post about leaked data of humor.co.il

It is Important to Take the Decision From the Followers

The **UserSec Collective** recently conducted an anonymous poll. The question at hand? Whether to breathe new life into an alliance that's been dormant. With two straightforward options, "Yes" and "No", members were prompted to voice their opinions on the proposed resurgence. It's a testament to the fact that even in the digital realm, collective decisions hinge on the perspectives of individual members. The number of votes already pouring in showcases the engagement and investment of the community in the UserSec's future decisions.



UserSec Collective

Поднимаем альянс из неактива?

Anonymous Poll

○ Да

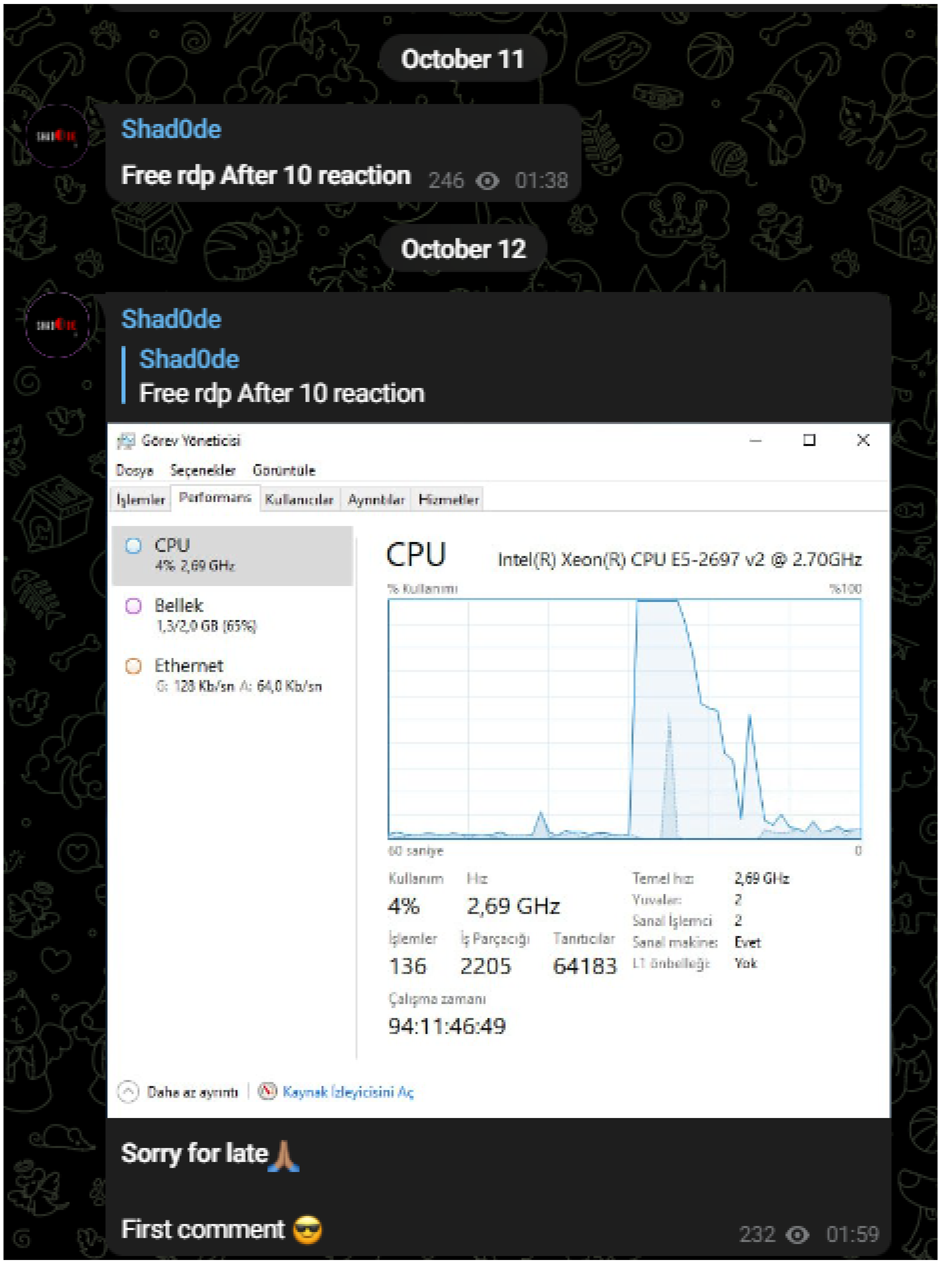
○ Нет

354 votes

Fig. 7. UserSec's anonymous poll post on Telegram

It is Possible to Become a Threat Actor by Participating in a Giveaway!

The threat actor **Shad0de** is known for distributing RDP access via Telegram, and his latest post is about RDP access to a Turkish language operating system server with an Intel Xeon processor. Good luck to the participants of the giveaway!


October 11

Shad0de
Free rdp After 10 reaction 246 01:38

October 12

Shad0de
Shad0de
Free rdp After 10 reaction

Görev Yöneticisi

CPU
4% 2,69 GHz

Bellek
1,3/2,0 GB (65%)

Ethernet
G: 128 Kb/sn A: 64,0 Kb/sn

CPU Intel(R) Xeon(R) CPU E5-2697 v2 @ 2.70GHz

Kullanım 4%
Hız 2,69 GHz
İşlemler 136
İş Parçacığı 2205
Tanıtıcılar 64183
Çalışma zamanı 94:11:46:49

Temel hız: 2,69 GHz
Yuvalar: 2
Sanal İşlemci 2
Sanal makine: Evet
L1 önbelleği: Yok

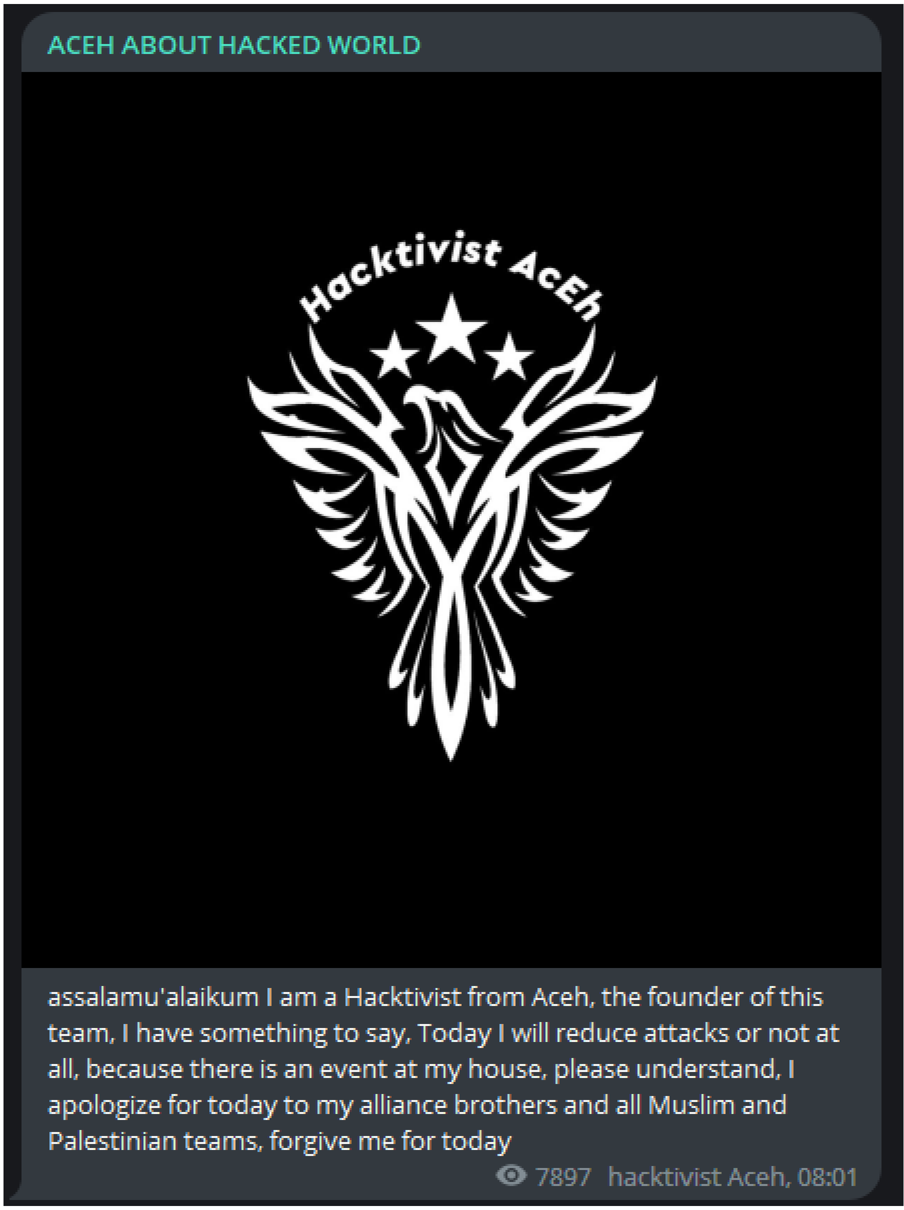
Sorry for late🙏

First comment 😎 232 01:59

Fig. 8. Shad0de's free RDP access giveaway post on Telegram

Hacktivist Takes a Day Off

Hacktivist **Aceh**, the founder of a renowned hacking group, took to the digital realm to make a personal announcement. Despite the often depersonalized nature of cyber-activities, this message brings a touch of everyday humanity to the forefront. Citing a personal event at home, the hacktivist made a candid request for understanding, emphasizing the need for a break from their usual activities. The announcement serves as a quirky reminder that behind every digital persona, there lies an individual navigating the complexities of daily life. Sometimes, even the most dedicated hacktivists need a day off for family events.



ACEH ABOUT HACKED WORLD

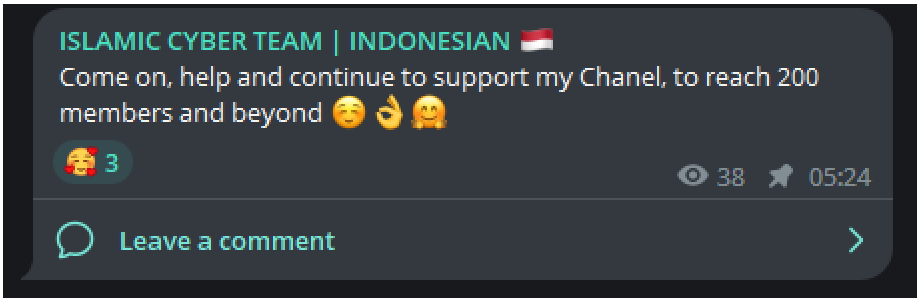
assalamu'alaikum I am a Hacktivist from Aceh, the founder of this team, I have something to say, Today I will reduce attacks or not at all, because there is an event at my house, please understand, I apologize for today to my alliance brothers and all Muslim and Palestinian teams, forgive me for today

7897 hacktivist Aceh, 08:01

Fig. 9. Aceh's Telegram post about Aceh's day off

Participate in the War, but If No One Sees It, There's No Point, Right?

The Islamic Cyber Team, a hacktivist group known for executing DDoS attacks and leaking data targeting Israel, has limited followers. Recognizing this shortfall, the group is actively seeking more supporters to ensure the impact of their activities isn't wasted.

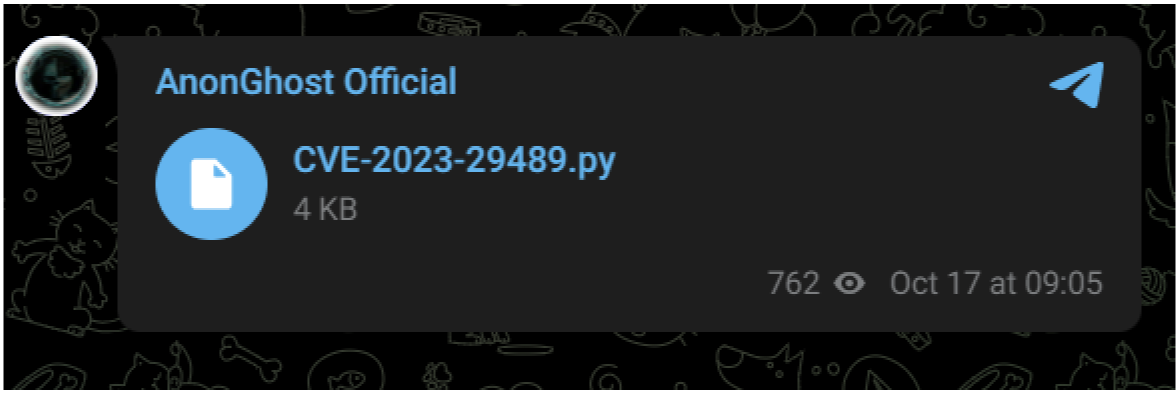


ISLAMIC CYBER TEAM | INDONESIAN 🇮🇩
Come on, help and continue to support my Chanel, to reach 200 members and beyond ☺️ 👌 🤗

Fig. 10. Islamic Cyber Team's Telegram post of seeking more supporters

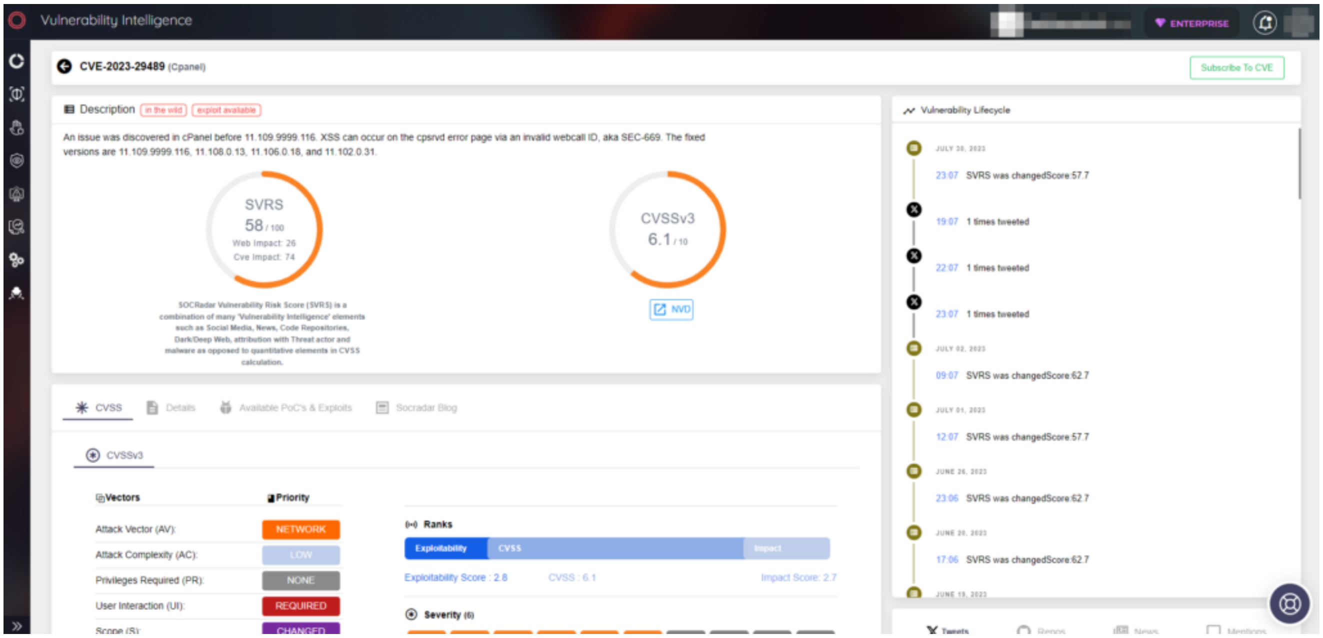
CVEs Are Floating on the Dark Web

The AnonGhost group shared the PoC of CVE-2023-29489 in the form of a Python script on its Telegram channel. We assume this is intended to encourage its followers to exploit the cPanel's Cross-site Scripting (XSS) vulnerability discovered in April.



AnonGhost Official
CVE-2023-29489.py
4 KB

Fig. 11. AnonGhost's Telegram post of CVE-2023-29489's PoC



CVE-2023-29489 (Cpanel)

Description (in the wild) (exploit available)

An issue was discovered in cPanel before 11.109.9999.116. XSS can occur on the cpsrvd error page via an invalid webcall ID, aka SEC-669. The fixed versions are 11.109.9999.116, 11.108.0.13, 11.106.0.18, and 11.102.0.31.

SVRS 58 / 100
Web Impact: 26
Cve Impact: 74

SOCRadar Vulnerability Risk Score (SVRS) is a combination of many 'Vulnerability Intelligence' elements such as Social Media, News, Code Repositories, Dark/Deep Web, attribution with Threat actor and malware as opposed to quantitative elements in CVSS calculation.

CVSSv3 6.1 / 10

Vectors	Priority
Attack Vector (AV):	NETWORK
Attack Complexity (AC):	LOW
Privileges Required (PR):	NONE
User Interaction (UI):	REQUIRED
Scope (S):	CHANGED

Ranks

Exploitability Score : 2.8 CVSS : 6.1 Impact Score: 2.7

Severity (6)

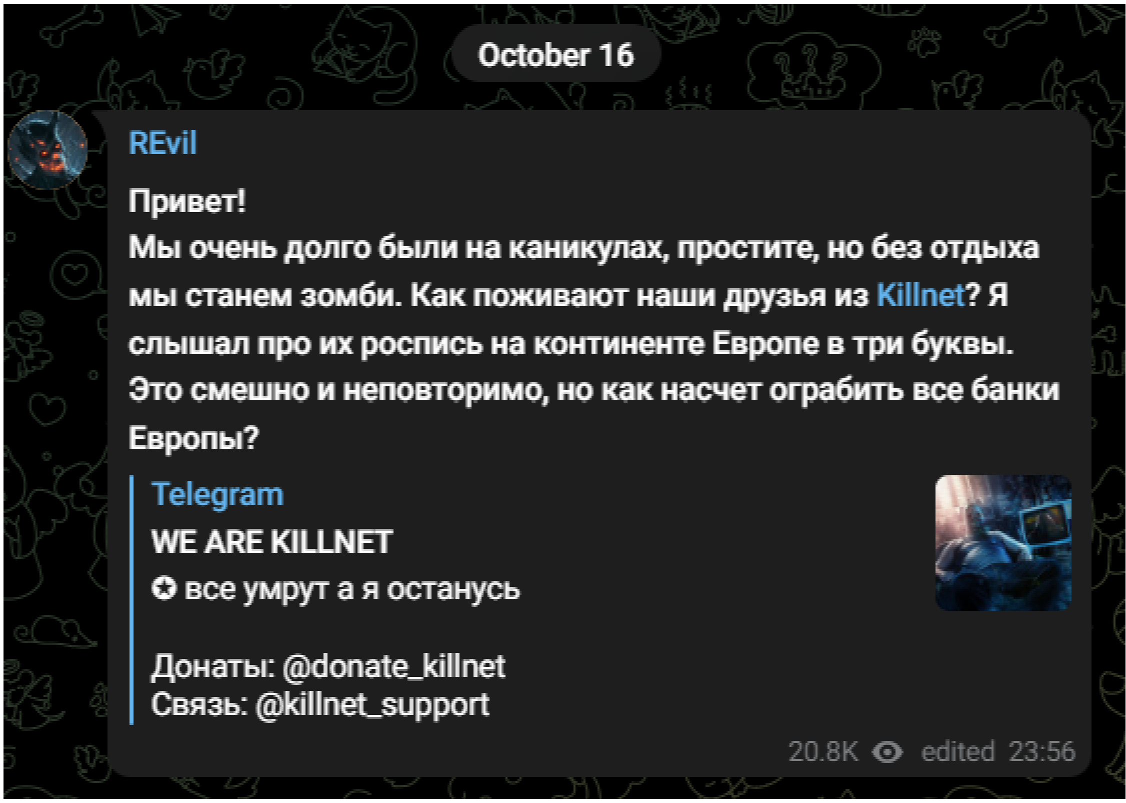
Vulnerability Lifecycle

JULY 30, 2023
23:07 SVRS was changedScore:57.7
19:07 1 times tweeted
22:07 1 times tweeted
23:07 1 times tweeted
JULY 02, 2023
09:07 SVRS was changedScore:62.7
JULY 01, 2023
12:07 SVRS was changedScore:57.7
JUNE 26, 2023
23:06 SVRS was changedScore:62.7
JUNE 20, 2023
17:06 SVRS was changedScore:62.7
JUNE 19, 2023

Fig. 12. CVE-2023-29489's information page of SOCRadar XTI's Vulnerability Intelligence Page of CTI Module (Source: SOCRadar)

REvil Resurfaces or Just a Shadow's Trick?

A recent Telegram post that looks like from REvil, we are not sure, has left the cybersecurity community in a dilemma: Is this the real deal Ransomware Evil “REvil” making a return, or is it the work of a **copycat**, trying to ride on the infamous group’s fame? The message suggests a possible alliance with Killnet and even jests about robbing banks across Europe. While it’s laced with REvil’s characteristic audacity, only time will tell if this is genuinely their work or an imitation act hoping to gain fame in the world of the Dark Web.



October 16

REvil

Привет!
Мы очень долго были на каникулах, простите, но без отдыха мы станем зомби. Как поживают наши друзья из Killnet? Я слышал про их роспись на континенте Европе в три буквы. Это смешно и неповторимо, но как насчет ограбить все банки Европы?

Telegram
WE ARE KILLNET
✪ все умрут а я останусь

Донаты: @donate_killnet
Связь: @killnet_support

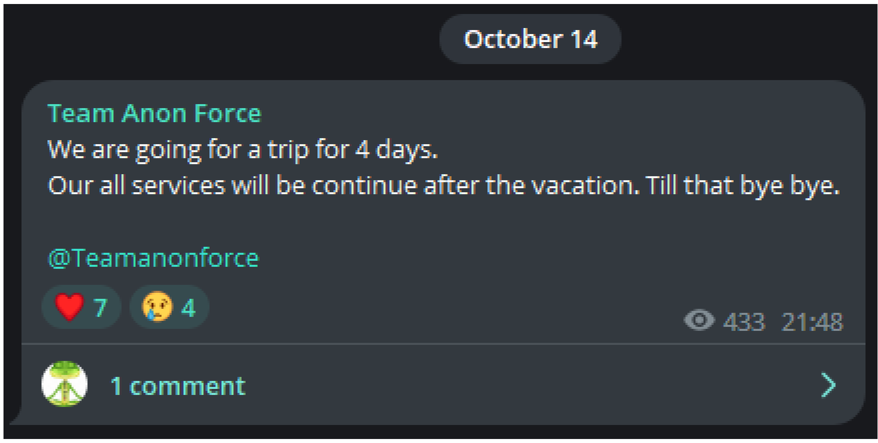
20.8K edited 23:56

Fig. 13.

REvil’s Telegram post about their come back and targeting European banks

Like Everyone Else, Hacktivists Also Need a Digital Detox

In a world that’s always online, even the most dedicated of teams need a moment to disconnect and reboot. **Team Anon Force**, known for their hacktivist activities, recently dropped on their Telegram group a status update that’s less binary and more human. They’re “powering down” for a brief 4-day getaway.



October 14

Team Anon Force
We are going for a trip for 4 days.
Our all services will be continue after the vacation. Till that bye bye.

@Teamanonforce

❤️ 7 😢 4

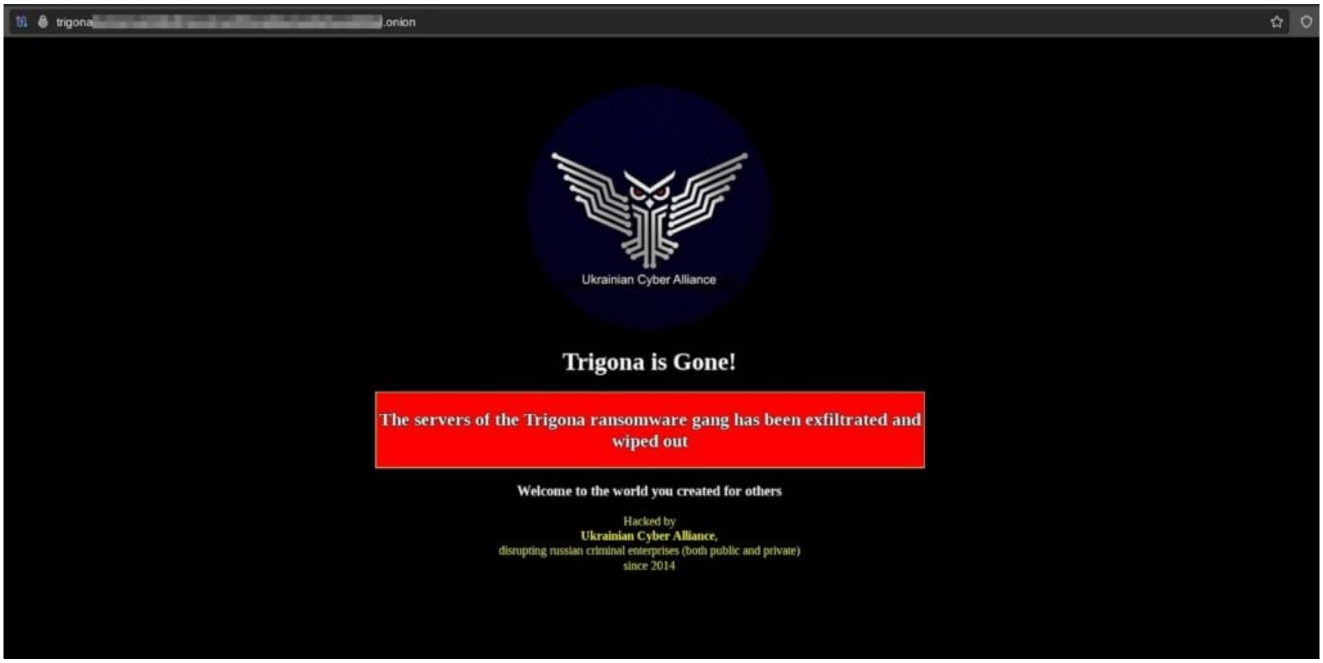
433 21:48

1 comment

Fig. 14. Team Anon Force's Telegram post about the group's vacation

Even Ransomware Groups Aren't Safe in Cyberwarfare

The **Ukrainian Cyber Alliance**, a group of cyber activists, successfully breached the servers of the **Trigona ransomware gang**. Utilizing a public exploit tied to a critical vulnerability, they accessed the gang's infrastructure, copied all essential data, and subsequently wiped the servers.



trigona[redacted].onion

Trigona is Gone!

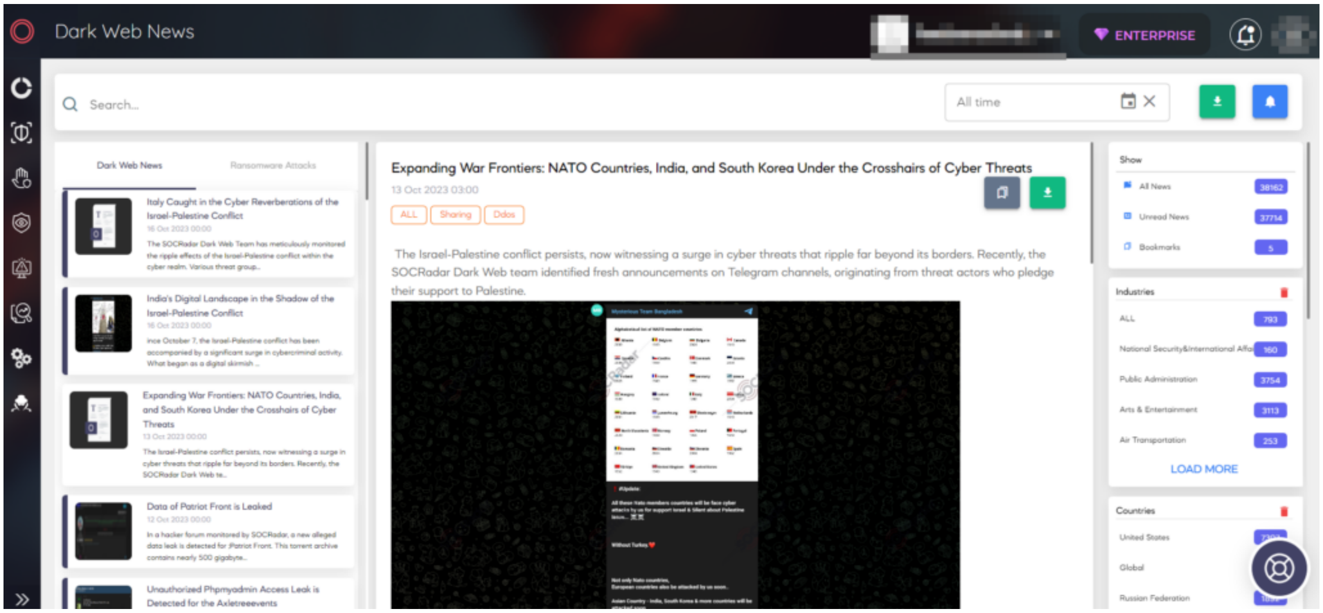
The servers of the Trigona ransomware gang has been exfiltrated and wiped out

Welcome to the world you created for others

Hacked by
Ukrainian Cyber Alliance,
disrupting russian criminal enterprises (both public and private)
since 2014

Fig. 15. Trigona Ransomware's TOR site defaced by Ukrainian Cyber Alliance (Source: bleepingcomputer)

The Dark Web is not at rest and we don't expect it to become slower. You can use Dark Web News in SOCRadar XTI's Cyber Threat Intelligence module to keep up to date with developments on the Dark Web:



Italy Caught in the Cyber Reverberations of the Israel-Palestine Conflict
16 Oct 2023 00:00
The SOCRadar Dark Web Team has meticulously monitored the ripple effects of the Israel-Palestine conflict within the cyber realm. Various threat group...

India's Digital Landscape in the Shadow of the Israel-Palestine Conflict
16 Oct 2023 00:00
ince October 7, the Israel-Palestine conflict has been accompanied by a significant surge in cybercriminal activity. What began as a digital skirmish ...

Expanding War Frontiers: NATO Countries, India, and South Korea Under the Crosshairs of Cyber Threats
13 Oct 2023 00:00
The Israel-Palestine conflict persists, now witnessing a surge in cyber threats that ripple far beyond its borders. Recently, the SOCRadar Dark Web te...

Data of Patriot Front is Leaked
12 Oct 2023 00:00
In a hacker forum monitored by SOCRadar, a new alleged data leak is detected for Patriot Front. This torrent archive contains nearly 500 gigabyte...

Unauthorized Phpmyadmin Access Leak is Detected for the Axletreeevents

Expanding War Frontiers: NATO Countries, India, and South Korea Under the Crosshairs of Cyber Threats
13 Oct 2023 03:00
ALL Sharing Ddos

The Israel-Palestine conflict persists, now witnessing a surge in cyber threats that ripple far beyond its borders. Recently, the SOCRadar Dark Web team identified fresh announcements on Telegram channels, originating from threat actors who pledge their support to Palestine.

Show	
All News	38162
Unread News	37714
Bookmarks	5

Industries	
ALL	793
National Security&International Affai	160
Public Administration	3754
Arts & Entertainment	3113
Air Transportation	253

Countries	
United States	[illegible]
Global	
Russian Federation	[illegible]

Fig. 14. SOCRadar XTI’s Dark Web News page under the CTI Panel (Source: SOCRadar)