

Dark Peep #2: War and a Piece of Hilarity

Published: 2023-10-17 · Archived: 2026-04-02 12:37:40 UTC

1. [Home](#)
2. [Blog](#)
3. [Dark Web](#)
4. Dark Peep #2: War and a Piece of Hilarity

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.

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.

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.

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.

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.

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.

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!

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

Hactivist Takes a Day Off

Hactivist **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 hactivist 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 hactivists need a day off for family events.

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 hactivist 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.

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.

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

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](#).

Fig. 13. REvil's Telegram post about their come back and targeting European banks

Like Everyone Else, Hactivists 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 hactivist 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.

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.

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:

Fig. 14. SOCRadar XTI's Dark Web News page under the CTI Panel (Source: [SOCRadar](#))

Source: <https://socradar.io/dark-peep-2-war-and-a-piece-of-hilarity/>