Dark Peep #16: Play Ransomware & LockBit's Alliance, BreachForums Leak, and CyberNiggers' Revival

Published: 2024-08-08 · Archived: 2026-04-05 17:13:17 UTC

1. Home
2. Blog
3. Dark Web
4. Dark Peep #16: Play Ransomware & LockBit’s Alliance, BreachForums Leak, and CyberNiggers’ Revival

Welcome to Dark Peep #16, where we unravel the freshest and most daring cyber capers. Rumors swirl about a potential collaboration between Play Ransomware and LockBit, with Play reportedly paying $35,000 for LockBit’s tricks. Meanwhile, AzzaSec found itself ambushed, their Telegram channels hijacked, and backup channels were compromised.

A new hacktivist collective, **Holy League**, has emerged, targeting NATO, Europe, Ukraine, and Israel with alleged DDoS and defacement attacks. Brain Cipher ransomware, after causing chaos in Indonesia, unexpectedly released a decryption key, raising questions about their motives. SiegedSec announced their disbandment due to mental health and FBI pressure, and the BreachForums database leak by Emo threat actor exposed personal data of over 200,000 members

The visual representation of ‘Threat actor tries to re-awaken the threat group.’ (Generated by OpenAI’s DALL-E)

Potential Collaboration Between Play Ransomware and LockBit

In a twist straight out of a cybercrime comic book, a Telegram channel allegedly linked to Play Ransomware hints at an unlikely partnership with LockBit. Picture this: Play Ransomware and LockBit joining forces like the Joker and Harley Quinn of the digital underworld. The deal? Play Ransomware pays $35,000 for LockBit's bag of tricks.

A Telegram channel, allegedly operated by Play Ransomware, has announced a new partnership with LockBit (DailyDarkWeb)

But the fun doesn't stop there! LockBit is also offering its expertise to make Play Ransomware's operations even more chaotic. It's like a villainous mentorship, ensuring their mischievous escapades reach new heights.

For additional intelligence information, you can read our blog post about LockBit.

As this dynamic duo gears up to unleash their digital mayhem, the rest of us are left to brace for impact. But fear not, because just as Gotham has Batman, the cyber world has SOCRadar. With real-time intelligence and cutting-edge insights, SOCRadar is here to help you thwart these cybercriminals' plans and keep your digital city safe.

The Hacktivist Group Hit by Its Weapon

While documenting **AzzaSec**'s showdowns with other threat groups and their daring takeover of a rival's Telegram channel, an unexpected plot twist occurred. In a classic case of the hunter becoming the hunted, a cheeky threat actor hijacked AzzaSec's own Telegram channel. Not only did they shut it down, but they also grabbed control of their backup channels.

On AzzaSec's new Telegram channel, a threat actor claimed that AzzaSec had hijacked and shut down its Telegram channels.

This bold move, announced right on AzzaSec's platform, turned the tables and left AzzaSec looking like they'd slipped on a banana peel in the middle of their grand heist.

Once Again, Another New Collective Emerges

Turning our attention to hacktivist groups and their activities on Telegram, a significant development has surfaced. Pro-Russian and pro-Palestinian hacktivist threat groups on Telegram have announced the formation of a new collective called the Holy League.

This collective includes **over 70 threat groups**. While it is common for threat groups on Telegram to form collectives, a partnership involving this many pro-Palestinian and pro-Russian groups is unusual. These groups have claimed cyber attacks primarily targeting NATO, Europe, Ukraine and Israel, involving Distributed Denial-of-Service (DDoS) and website defacement operations.

Brain Cipher's Mysterious Decryption Key Release

Brain Cipher ransomware burst onto the cyber scene like a bolt of lightning, making headlines with their alleged attack on Indonesia's National Data Center (Pusat Data Nasional – PDN). The ransomware group quickly became infamous for supposedly disrupting essential public services, leaving government servers encrypted and citizens in a state of disarray.

Brain Cipher's post, which claims to offer a decryptor

But just as quickly as they rose to notoriety, Brain Cipher's resolve seemed to waver. In an unexpected move, the group shared an onion link that they claimed contained the decryption key along with detailed instructions on how to use it. This act left many in the cyber community scratching their heads. Was this a genuine act of contrition, or just another layer of their deceit?

The decision to release the decryption key seemed almost out of character for a group that had caused so much chaos. It hinted at a possible internal conflict or a strategic pivot, perhaps driven by fear of reprisal or a calculated attempt to curry favor.

Has the SiegedSec Threat Group Disbanded?

SiegedSec announced their sudden disbandment on their Telegram channel.

Picture it: the threat actors gather for one last mission, only to realize the heat is too intense. For the sake of their mental health, to escape the relentless stress of public notoriety, and to dodge the all-seeing eye of the FBI, they've decided to pull a Mission: Impossible disappearing act.

Their announcement read like a dramatic final scene, as if they were saying, "This tape will self-destruct in 5 seconds." SiegedSec's unexpected exit is a reminder that even in the wild world of cyber escapades, every threat actor has their breaking point.

Explore comprehensive insights and the latest updates on SiegedSec.

BreachForums Breach: Your OPsec Guide to Avoid Starring in the Next Data Drama!

The notorious Pompompurin era of BreachForums had its database leaked, courtesy of the threat actor known as Emo. Following some internal strife, Emo decided to make this treasure trove public on a Telegram channel. This data, potentially a goldmine for **OPsec (Operational Security)**, revealed personal information of 212,414 members from BreachForums 1.0.

A sample of leaked data from BreachForums

According to Emo, the data originated directly from Fitzpatrick (aka Pompompurin), who allegedly tried to sell it for $4,000 while out on bail in June 2023. Emo claims the data was eventually purchased by three threat actors. The leaked database includes user IDs, login names, email addresses, registration IPs, and the last IP address used on the site, among other details.

To add a touch of drama, let's not forget that the first major data breach forum, RaidForums, was seized by the FBI in 2022. In its aftermath, Pompompurin launched BreachForums (aka Breached) to fill the void. Fitzpatrick's arrest in early 2023 led to the original BreachForums shutting down, only for the notorious ShinyHunters to resurrect it later.

For anyone looking to tighten their OPsec, this leak is a stark reminder: in the digital wild west, it's always high noon somewhere. And remember, even Iron Man had to learn the hard way that keeping your identity secret is sometimes the best way to avoid the villains.

IntelBroker Attempts to Revive CyberNiggers

In a move sparking outrage, notorious threat actor IntelBroker has announced plans to revive the infamous and racist group CyberNiggers. Known for its harmful and offensive activities, this group is attempting to rebuild, led by IntelBroker.

IntelBroker's announcement

The recruitment process, as outlined by IntelBroker, is steeped in hate and bigotry. The criteria include being white and racist, showing disdain for law enforcement, and providing evidence of past breaches and leaks. This dangerous group also emphasizes maintaining operational security and a 'GOD Rank.'

IntelBroker admits that the group has always been under attack, facing law enforcement actions and arrests.

For more detailed information about CyberNiggers check out our Dark Web Profile.

Conclusion

With all these cyber drama unfolding, you might be wondering how to keep your digital fortresses safe. Enter SOCRadar: whether it's detecting the latest ransomware tactics, monitoring hijacked communication channels, or identifying new threat collectives, SOCRadar offers **real-time intelligence** and cutting-edge insights.

With SOCRadar on your side, you can stay a step ahead of cybercriminals, ensuring your digital defenses are always fortified. Stay vigilant, stay informed, and let SOCRadar help you navigate the ever-evolving cyber landscape.
