Dark Web Profile: CyberNiggers

Published: 2024-02-05 · Archived: 2026-04-02 10:35:44 UTC

[Update] August 9, 2024: "Revival and Recruitment of CyberNiggers Group"

The cybersecurity landscape is in a state of flux, marked by flow of illicit activities within hacker forums. Not so recent events surrounding the shutdown and subsequent revival of Breach Forums have brought forth a wave of speculation, with some viewing it as an **FBI HoneyPot**, while others see it as an opportune space for continued illegal pursuits. At the center of this virtual tumult stands a racist threat group that has re-emerged with heightened potency—CyberNiggers.

CyberNiggers' Banner on Breach Forums

Amidst the chaos of forum dynamics and the arrest of forum administrators, the once-dormant CyberNiggers has seized the spotlight. A dominant force in the revamped Breach Forums, this threat group has taken on a renewed and ominous demeanor. While their recruitment efforts have taken a backseat, a key member named **IntelBroker** has assumed a prominent role, shouldering the group's cyber activities.

This resurgence of CyberNiggers raises alarm bells across the cybersecurity community. Their return to the forefront, coupled with a fresh wave of cyber attacks, underscores the persistent and evolving nature of digital threats. In a global landscape where organizations grapple with increasingly sophisticated cyber adversaries, the activities of CyberNiggers warrant close scrutiny.

Who is CyberNiggers ?

In the aftermath of the pompompurin's arrestment, Cyber Niggers, has emerged as a formidable threat group within the revived Breach Forums. While the forum's status as a potential HoneyPot remains a topic of debate, the activities of CyberNiggers have transcended speculation. The threat group, which is very active both in the forum and in cyber threat activities, made a name for itself with the General Electrics data they allegedly offered for sale towards the end of 2023.

The racist threat group appears to be a small group, all of whom are currently members of Breach Forums. Still, they are pursuing critical targets, especially in the US, and according to a claim by vx-underground, they are also under the surveillance of Five-Eyes.

Amidst the group's activities, a Serbian hacker, IntelBroker, a prominent member, has taken center stage. Tasked with shouldering a significant lead within the group, IntelBroker's solo endeavors have become a focal point.

IntelBroker, One of the members of CyberNiggers

CyberNiggers: Recent Breach Activities

Once dormant CyberNiggerss have resurfaced, leaving a trail of compromised entities in their wake. The threat group claimed many responsibility for infiltrating prominent organizations, showcasing their ability to exploit vulnerabilities and compromise sensitive data. Although CyberNiggers, as a parent umbrella, did not resonate in the media as much as the name IntelBroker, either the group or IntelBroker's name was mentioned in the biggest events of 2023. This section explores CyberNiggers' recent breach activities, shedding light on the specific **organizations targeted** and the potential consequences of their exploits.

Prominent targets were:

- **General Electric (GE):** CyberNiggers, seems to be led by the prominent member IntelBroker, for this attack, asserting that they have successfully breached General Electric, a multinational tech giant with a significant presence in various industries. The compromised data allegedly includes sensitive military files belonging to the US government's Defense Advanced Research Projects Agency (DARPA).

A later post about General Electric

- **Weee Grocery Service:** CyberNiggers claimed responsibility for stealing sensitive information from Weee Grocery Service, a popular online grocery platform. The data breach impacted approximately **11 million** users, raising concerns about the exposure of personal and financial information.
- **Colonial Pipeline**: CyberNiggers was also reportedly behind a significant cybersecurity breach targeting the Colonial Pipeline. A group member, identified as "comradbinski," associated with this breach, also had a history of involvement in various cyber intrusions and joined the platform on August 8, 2023.

Revelations on the dark web suggest that premium access to Colonial Pipeline, offered by comradbinski, included critical information such as billing details, private and public keys, passwords, emails, source code, PDFs, and database files. The compromised access extends to Blobs, SMTP, Bitbucket, MSSQL, and AWS S3 Buckets.

Alleged Data Leaks and Access Sales for Colonial Pipeline and other Pipeline companies

And many other victims like **Accenture**, **KitchenPal**, **UsDoT**, **Vauxhall Motors** are posted on the forum as well.

CyberNiggers are publishing many posts on the forums continuously

CyberNiggers' leaks may pose severe consequences for the targeted organizations and the individuals whose data has been compromised. These consequences may include reputational damage, financial losses, and legal ramifications. Moreover, the exposure of sensitive military files, as claimed in the GE breach, raises national security concerns, highlighting the broader implications of CyberNiggers' activities.

As organizations grapple with the aftermath of these breaches, understanding the tactics employed by CyberNiggers becomes paramount. The next section delves into the historical context of CyberNiggers' breach activities, providing insights into their evolution and methods.

IntelBroker: A Pivotal Figure

As mentioned above, at the forefront of CyberNiggers stands a phonk-enjoyer hacker, IntelBroker, a notorious member with a track record of orchestrating high-profile cyberattacks. Operating within the realm of initial access brokering, IntelBroker specializes in identifying and selling access to compromised systems, paving the way for various malicious activities. Details about IntelBroker also shed light on the group.

IntelBroker's profile picture

Background:

- **Track Record:** IntelBroker probably has been an active participant in the cyber threat landscape since at least late 2022. Notable breaches attributed to IntelBroker include successful attacks on Weee Grocery Service, Autotrader, Volvo, Hilton Hotels, and AT&T.
- **Methodology:** The modus operandi of IntelBroker mostly revolves around locating and selling access to compromised systems. Their focus on the initial access stage of cyberattacks makes them a critical component in the broader cybercrime ecosystem. Although he first tries to sell the access he has obtained, when he cannot make a successful sale in this area, he probably engages in infiltration efforts of his own and manages to steal some data; Sample also offers the data it shares for sale on the forum.

IntelBroker of CyberNiggers, selling access for Dunkin Brands, their targets are various

High-Profile Exploits:

- **US Military:** IntelBroker's claim of breaching General Electric, leading to the alleged compromise of military files related to DARPA, underscored the group's and the IntelBroker's audacious targets and

potential national security implications. It was also the time when both the group and IntelBroker made their voices heard the most.

Unique Threat Landscape:

- **Low Asking Price:** The peculiar aspect of IntelBroker's and CyberNiggers' recent activities is the surprisingly low asking price for access to sensitive information. For instance, the offer to sell access to DARPA files for $500 raises questions about the authenticity and motivations behind such a seemingly undervalued proposition. In a tweet, they also stated that they sold sensitive US-based data for **$4000**. In other words, it can be said that the price range generally hovers around relatively low numbers.
- **Focus on Initial Access:** As stated above in the Methodology, IntelBroker's specialization in the initial access stage positions them as a crucial player in the broader cyber threat landscape. Their ability to exploit misconfigured systems and unprotected databases contributes to the evolving tactics within the cybercrime ecosystem.

VPN Access for US based companies

- **A Potential Ransomware Operation:** IntelBroker also stated in a post that it was working on its own ransomware strain. Of course, getting ransomware into the hands of a threat actor specialized in access can greatly increase the attack vector and destructiveness. However, it can be said that it previously sold the access gained to ransomware groups. So it is an actor who has long been associated with the ransomware landscape

IntelBroker's post about its ransomware progress

- **Solo Operation:** Despite the collective identity of CyberNiggers, IntelBroker stands out as an individual threat actor. This distinction raises questions about the extent of their capabilities and the motivations driving their solo endeavors.

Understanding IntelBroker's role within CyberNiggers provides valuable insights into the tactics employed. Furthermore, since the tactics of the group are parallel to IntelBroker and considering that the members of the group can also work individually, understanding IntelBroker's actions and capacity also provides a general view of the entire group.

The Group's Extent and the Implications on Security

The cyber onslaught orchestrated by CyberNiggers extends far beyond individual data breaches. This section explores the profound implications of the group's activities on national security and the specific organizations that have fallen victim to their sophisticated cyberattacks.

Let's look at the implications through the General Electrics incident, which is the news that is most covered in the media.

General Electric (GE) and DARPA Compromise:

- The alleged breach of General Electric, a multinational industrial giant, and the compromise of military files associated with the Defense Advanced Research Projects Agency (DARPA) raised concerns.
- Especially, GE's involvement in cutting-edge aerospace technology, including hypersonic jets and military drones, amplified the severity of the breach. The compromised information could have potentially provided adversaries with insights into critical defense projects, posing a direct threat to **national security**.

Potential Consequences:

- **Military Advantage:** The stolen military files could grant adversaries a strategic advantage by exposing classified information related to military strategies, troop deployments, weapons systems, and intelligence operations.
- **Technological Innovation at Risk:** With GE's collaboration with DARPA on diverse projects, the breach jeopardizes not only current military initiatives but also the technological innovations that influence broader consumer technology.

Operational Impact on Organizations:

- **Reputational Damage:** The mere speculation of a breach may have inflicted substantial reputational damage on impacted organizations. If confirmed, the companies may face severe financial losses, legal consequences, and a decline in public trust.
- **Legal and Compliance Ramifications:** A confirmed breach would trigger legal and compliance consequences for impacted organizations. The exposure of sensitive data, like SQL database files, aviation system guidelines, and military documents, could result in legal actions and regulatory penalties.

Understanding the extent of the group is a more complicated issue. However, the key point that stands out and will uncover the rest is financial gain.

Pattern of Attacks:

- **Diverse Target Portfolio:** CyberNiggers exhibits a pattern of targeting a diverse portfolio of organizations, including Autotrader, Volvo, Hilton Hotels, and AT&T. This suggests a strategic approach to gather varied sets of information and potentially fulfill different objectives.
- **Targeting of US:** While NATO-Aligned countries seem to be their main targets, their cyber attacks are for financial gain, not hacktivist visions, even if their cyber attacks may contain political statements. By far, the country they target the most is the US. However, they have a diverse list of target countries such as the UK, South Africa, India, and Turkey.

Political Agenda:

- **Racism:** As can be easily understood from the name of the group, they have a racist attitude. Of course, such an agenda may also be interpreted as a language they use to attract attention and create chaos on the way to their goals, rather than choosing a target based on "being a racist".

- **Excluding Russia:** Although we said above that they are motivated by financial gain rather than a political agenda, as stated in an interview, the group member IntelBroker seems to be a native Serbian or Russian speaker, and it is obvious that Russia is excluded among the group's targets. According to IntelBroker's own statement, it resides in Russia.

Understanding the implications of these cyber intrusions extends beyond the immediate impact on targeted organizations. The potential compromise of national security-related data emphasizes the critical need for robust cybersecurity measures and international collaboration to counter such threats effectively.

Conclusion: Navigating the Cybersecurity Landscape

The evolving activities of CyberNiggers, marked by the alleged breach of General Electric and IntelBroker's significant role, emphasize the dynamic and persistent nature of cyber threats. As organizations and security professionals grapple with emerging challenges, understanding the intricacies of threat groups like CyberNiggers becomes paramount. The collective response to breaches, the validation of claims, and the development of robust cybersecurity measures are crucial components in mitigating the impact of cyber adversaries. The cybersecurity landscape demands vigilance, adaptability, and collaborative efforts to safeguard critical infrastructure, national security, and individual privacy.

SOCRadar Dark Web Monitoring offers an extensive monitoring solution for every surface of the web, allowing organizations to detect and address threats spanning the surface, deep, and dark web layers. Leveraging our capabilities in reconnaissance and threat analysis, we provide practical intelligence to enhance your organization's proactive security measures. By combining automated external cyber intelligence with a specialized team of analysts, we empower Security Operations Center (SOC) teams to effectively manage threats beyond their traditional boundaries.

SOCRadar Dark Web Monitoring

Revival and Recruitment of CyberNiggers Group

A recent post on BreachForums announced the revival and active recruitment for the group CyberNiggers. This post, made by the moderator, IntelBroker, lays out specific criteria and expectations for potential members, which includes racist motivations and a history of cybercrimes, such as providing free leaks or engaging in data breaches. The group openly promotes disdain for law enforcement and requires members to maintain operational security.

The recent post about new version of CyberNiggers

This resurgence is noteworthy as it follows significant law enforcement activities that led to arrests and the seizure of related forum data in the past. The group's comeback highlights ongoing challenges in combating cybercrime communities that thrive on racial hatred and criminal activities. This development underscores the need for vigilant monitoring and enhanced cybersecurity measures to mitigate the threats posed by such groups.

Possible MITRE ATT&CK TTPs

Below are **possible** TTPs with their explanations.

Tactic	Technique	Details / Examples
Initial Access	T1190 – Exploit Public-Facing Application	Breaching General Electric and Weee Grocery Service by exploiting vulnerabilities in public-facing applications.
Execution	T1203 – Exploitation for Client Execution	Utilizing compromised systems to execute unauthorized commands or software.
Persistence	T1098 – Account Manipulation	Possibly maintaining access to compromised systems through account manipulation, as indicated by activities in various organizations.
Privilege Escalation	T1068 – Exploitation for Privilege Escalation	Gaining higher-level privileges through exploitation of system weaknesses.
Defense Evasion	T1027 – Obfuscated Files or Information	Likely obfuscating malicious files or data to evade detection, as seen in sophisticated cyber attacks.
Credential Access	T1003 – Credential Dumping	Accessing credentials, possibly through methods like database access or system compromise.
Discovery	T1083 – File and Directory Discovery	Discovering files and directories in the compromised systems, as in the case of DARPA files in GE breach.
Lateral Movement	T1078 – Valid Accounts	Using valid accounts to move laterally across networks, inferred from the pattern of diverse organization targets.
Collection	T1005 – Data from Local System	Collecting data from compromised systems, as seen in breaches of organizations like Colonial Pipeline.
Exfiltration	T1041 – Exfiltration Over C2 Channel	Likely exfiltrating data over a command and control channel, given the nature of their operations.
Impact	T1486 – Data Encrypted for Impact	Potential for ransomware use, as mentioned by IntelBroker or may have led into a ransomware attack..
Command and Control	T1132 – Data Encoding	Communicating with compromised systems using encoded data.
