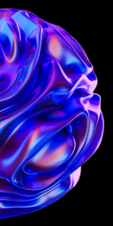
POMPOMPURiN HACKER

An OSINT & Threat Intelligence Analysis

HADESS

WWW.HADESS.IO



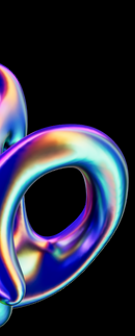
INTRODUCTION

Pompompurin, the notorious owner of BreachForums, has become a well-known figure in the cybercrime world. BreachForums, an underground marketplace for leaked data and illegal hacking services, quickly gained popularity as a hub for cybercriminals to trade stolen information. Pompompurin, who operated under the cover of anonymity, managed to cultivate a significant following within the dark web community. His involvement in facilitating and encouraging the sale of hacked data has made him a prime target for law enforcement and cybersecurity researchers worldwide.

Open Source Intelligence (OSINT) plays a crucial role in investigating individuals like Pompompurin. OSINT involves collecting and analyzing publicly available information from various online sources to piece together a detailed profile of threat actors. In the case of Pompompurin, investigators use techniques such as monitoring social media accounts, analyzing online forum activity, and identifying patterns in digital footprints to gain insight into his identity and operations. OSINT is especially powerful in cases like this because of the sheer amount of information freely available online, which, when analyzed carefully, can expose hidden connections between cybercriminals and their networks.

The use of OSINT in cybercrime investigations is often complemented by more advanced techniques, such as Threat Intelligence. Threat intelligence focuses on identifying emerging cyber threats, tracking malicious actors, and providing actionable insights to mitigate potential risks. In the case of Pompompurin, threat intelligence analysts closely track the activity on BreachForums, monitoring for new data breaches and identifying patterns in the types of data being traded. This approach helps build a comprehensive understanding of the cybercrime ecosystem and aids in tracking the individuals responsible for these illegal activities.

By combining OSINT with threat intelligence, cybersecurity professionals have been able to make significant progress in identifying Pompompurin’s real-world identity. These investigations highlight the importance of collaboration between researchers, law enforcement, and the cybersecurity community. The case of Pompompurin underscores the ongoing battle between cybercriminals and those working to disrupt their operations, showcasing the evolving nature of cyber threats and the methods used to combat them.



DOCUMENT INFO

HADESS

To be the vanguard of cybersecurity, Hadess envisions a world where digital assets are safeguarded from malicious actors. We strive to create a secure digital ecosystem, where businesses and individuals can thrive with confidence, knowing that their data is protected. Through relentless innovation and unwavering dedication, we aim to establish Hadess as a symbol of trust, resilience, and retribution in the fight against cyber threats.

At Hadess, our mission is twofold: to unleash the power of white hat hacking in punishing black hat hackers and to fortify the digital defenses of our clients. We are committed to employing our elite team of expert cybersecurity professionals to identify, neutralize, and bring to justice those who seek to exploit vulnerabilities. Simultaneously, we provide comprehensive solutions and services to protect our client's digital assets, ensuring their resilience against cyber attacks. With an unwavering focus on integrity, innovation, and client satisfaction, we strive to be the guardian of trust and security in the digital realm.

Security Researchers
Sashwin (linkedin.com/in/sashwin-0xp4tcher/)

TABLE OF CONTENT

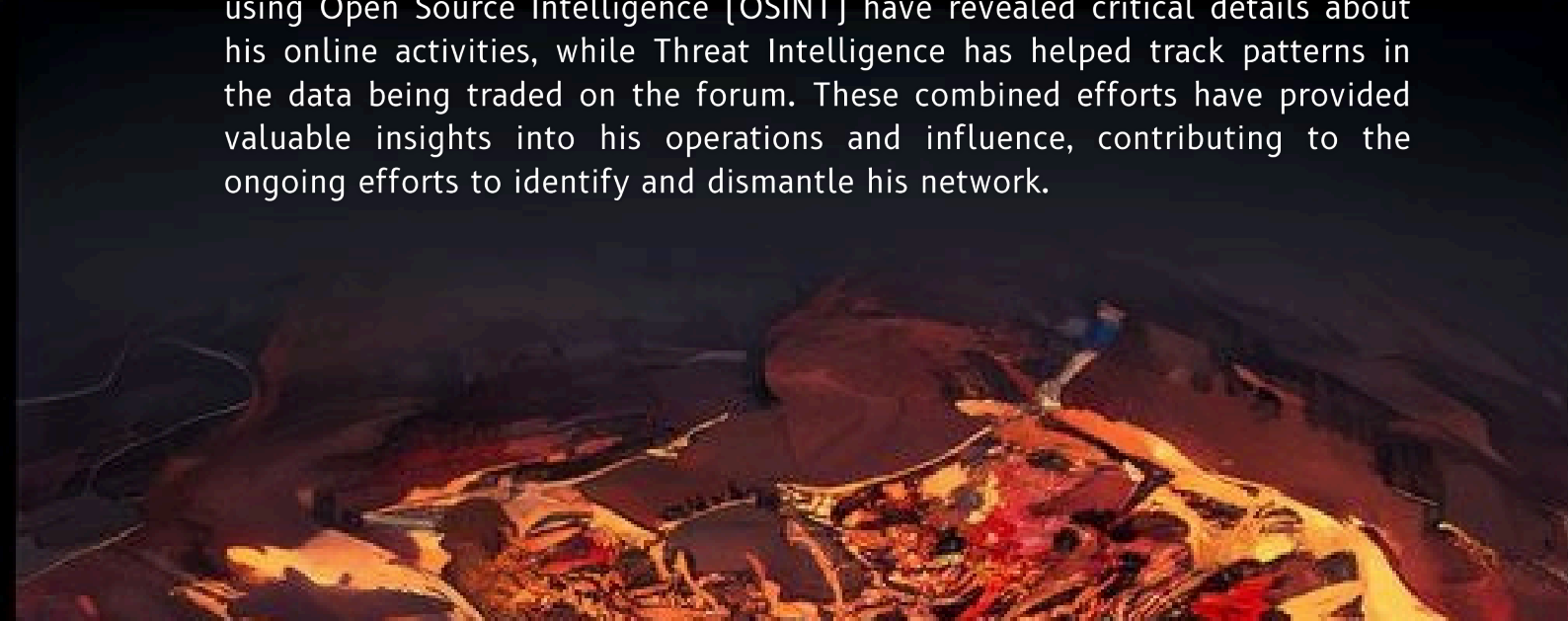
EXECUTIVE SUMMARY

Pompompurin, the enigmatic leader behind BreachForums, became a prominent figure in the dark web, managing a marketplace for the sale of stolen data and illegal hacking services. His involvement in facilitating cybercriminal activity has drawn significant attention from law enforcement agencies and cybersecurity professionals worldwide. Investigations into his identity and operations heavily rely on Open Source Intelligence (OSINT), which gathers publicly available information to uncover crucial details about his digital footprint.

In addition to OSINT, Threat Intelligence plays a key role in tracking the activities within BreachForums. By monitoring the types of data being traded and analyzing patterns of cybercrime activity, threat intelligence analysts have been able to map out Pompompurin's influence within the cybercrime ecosystem. Together, these approaches provide a holistic view of the investigation and contribute to efforts to expose and dismantle the operations of high-profile cybercriminals like Pompompurin.

Key Findings

Pompompurin, the owner of BreachForums, has established himself as a central figure in the dark web cybercrime ecosystem by managing an underground marketplace for stolen data and illicit services. Investigations using Open Source Intelligence (OSINT) have revealed critical details about his online activities, while Threat Intelligence has helped track patterns in the data being traded on the forum. These combined efforts have provided valuable insights into his operations and influence, contributing to the ongoing efforts to identify and dismantle his network.



01

OSINT IN THREAT INVESTIGATIONS

Pompompurin Hacker : An OSINT & Threat Intelligence Analysis

Introduction

from raidforum to intelxbroker

Threat intelligence and OSINT (Open Source Intelligence) are powerful tools in identifying individuals behind online aliases or nicknames, especially within hacker forums like BreachForums. OSINT relies on the analysis of publicly available data, such as social media profiles, posts, and online interactions, to uncover hidden identities. In the case of BreachForums, investigators could track the activities of key figures, such as "pompompurin" and "IntelBroker," using a combination of technical and social intelligence. Cross-referencing data leaks, social engineering, and monitoring online behaviors can provide valuable clues that lead to identifying the real-world individuals behind these pseudonyms.

When law enforcement targets forums like BreachForums, they often employ advanced threat intelligence techniques to trace users' footprints, both on the surface web and the dark web. For instance, identifying "pompompurin" involved a blend of digital forensics, tracking patterns of communication, and analyzing compromised systems. The use of VPNs, encrypted chats, and aliases presents challenges, but with the right intelligence frameworks and OSINT strategies, investigators are often able to piece together enough information to pursue legal action against cybercriminals, as seen with the arrest and sentencing of Fitzpatrick.

Osint - Scope of Osint

Open Source Intelligence (OSINT) refers to the collection and analysis of information that is publicly available. It encompasses data found in public records, social media platforms, websites, news articles, and other publicly accessible sources. OSINT has become an invaluable asset in various fields, including national security, law enforcement, corporate security, and journalism.

OSINT is distinct from other intelligence-gathering methods because it relies solely on open sources of information. These sources can be broadly categorized into:

* Media :
    * Newspapers, magazines
    * radio, and television broadcasts.
* Internet :
    * Websites, blogs, social media, and online forums.
* Public Records :
    * Government reports, financial disclosures
    * court records, and other official documents
* Professional and Academic Publications :
    * Journals, conference papers, and research studies.

Significance of OSINT in Investigations

In a bustling city, a detective named Ana was tasked with uncovering a network of cyber criminals. Without the resources for extensive undercover operations, she turned to Open Source Intelligence (OSINT). By analyzing public social media profiles, news articles, and online forums, she pieced together the digital footprints of the suspects. This cost-effective approach not only saved time and resources but also provided real-time insights, allowing her to track the criminals' activities and anticipate their next moves.

One day, Ana discovered a crucial lead through a seemingly innocuous blog post. Cross-referencing this with public records and other online data, she pinpointed the location of a hidden server used by the cyber criminals. This breakthrough was pivotal in dismantling the network and showcased how OSINT, with its ability to access and analyze vast amounts of public information, can be a powerful tool in modern investigations.

Role of Threat Intelligence in Investigations

Threat intelligence involves the collection, analysis, and interpretation of data about potential or current threats to an organization's security. This information is used to understand and mitigate threats, providing a proactive defense against cyber attacks.

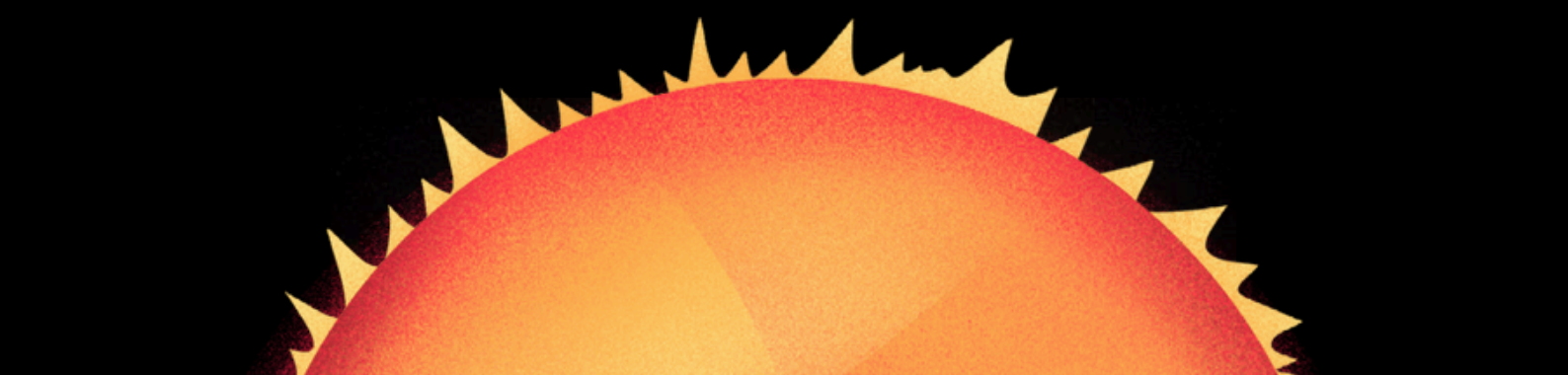
In investigations, threat intelligence plays a pivotal role in uncovering critical aspects of cyber threats. By analyzing threat intelligence, investigators can effectively identify and attribute cyber attacks to specific threat actors. This involves understanding their motives, methodologies, and the tools they employ. Furthermore, threat intelligence serves as a vital source of evidence, providing crucial data that supports legal and law enforcement proceedings. Beyond attribution, it offers a comprehensive view of the threat landscape, allowing investigators to connect disparate incidents and gain a deeper understanding of the broader context in which cyber threats operate. This contextual understanding enhances the effectiveness of investigations, ensuring thorough and informed responses to cyber incidents.

When investigating the notorious Pompompurin hacker, threat intelligence proved invaluable. By meticulously analyzing threat data, investigators could piece together Pompompurin's identity, motives, and methods. This analysis revealed unique patterns and tools used by the hacker, enabling the attribution of multiple cyber attacks directly to Pompompurin. The intelligence gathered provided critical evidence, forming a solid foundation for legal action and law enforcement involvement.

Moreover, threat intelligence offered a comprehensive understanding of the broader threat landscape. It allowed investigators to connect seemingly unrelated incidents, uncovering the intricate web of activities linked to Pompompurin. This contextual awareness was crucial in mapping out the hacker's network, ensuring that no stone was left unturned in the quest to bring Pompompurin to justice.

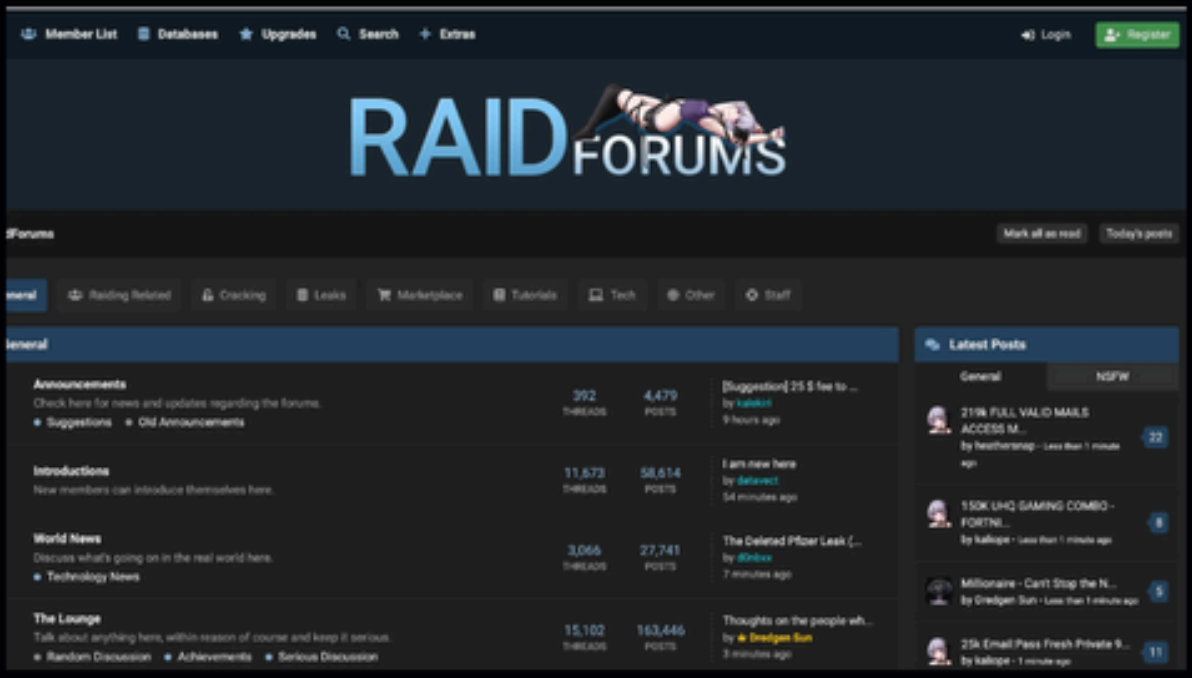
02

RAIDFORUM, BREACHFORUM, ...

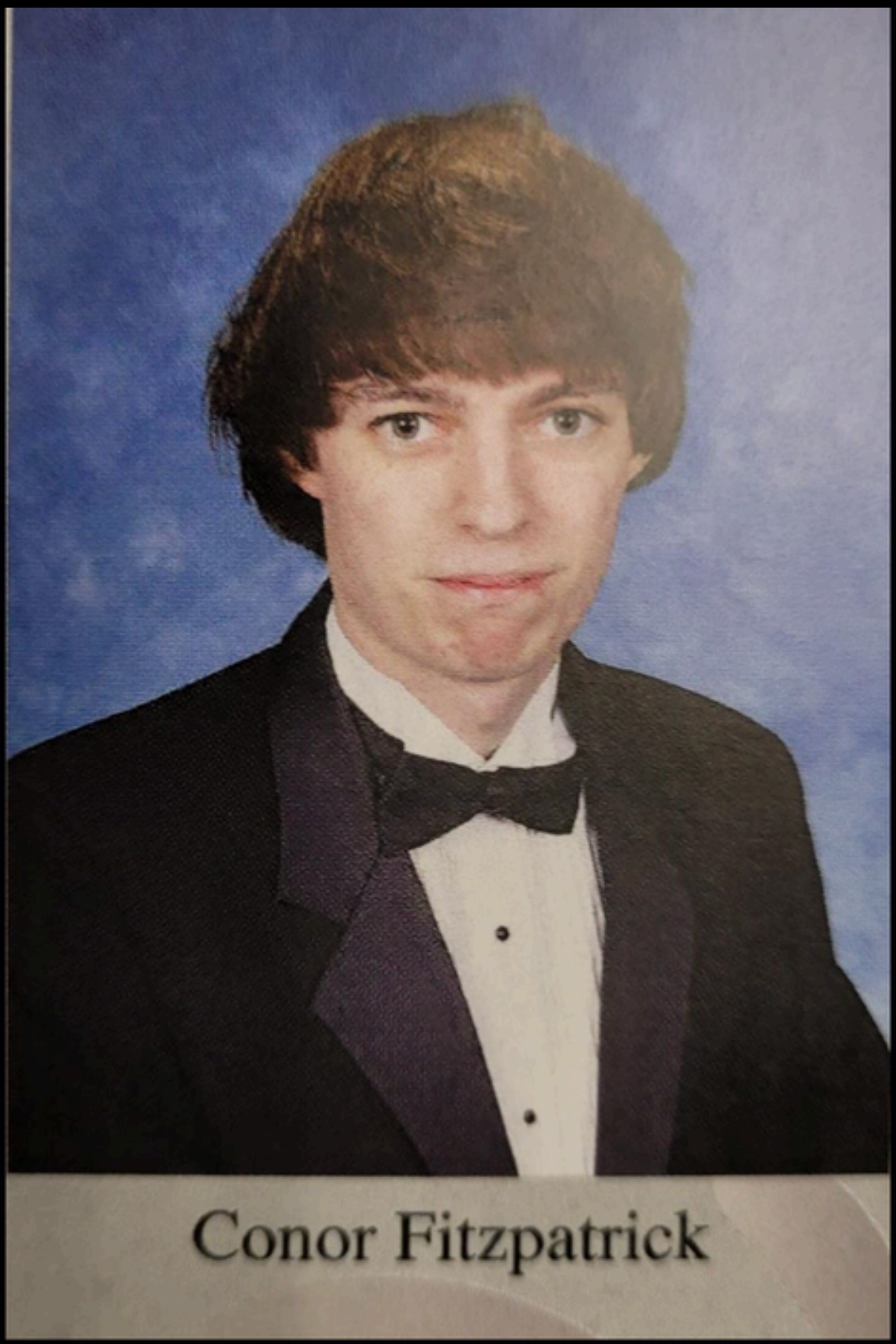


Background of Breachforum

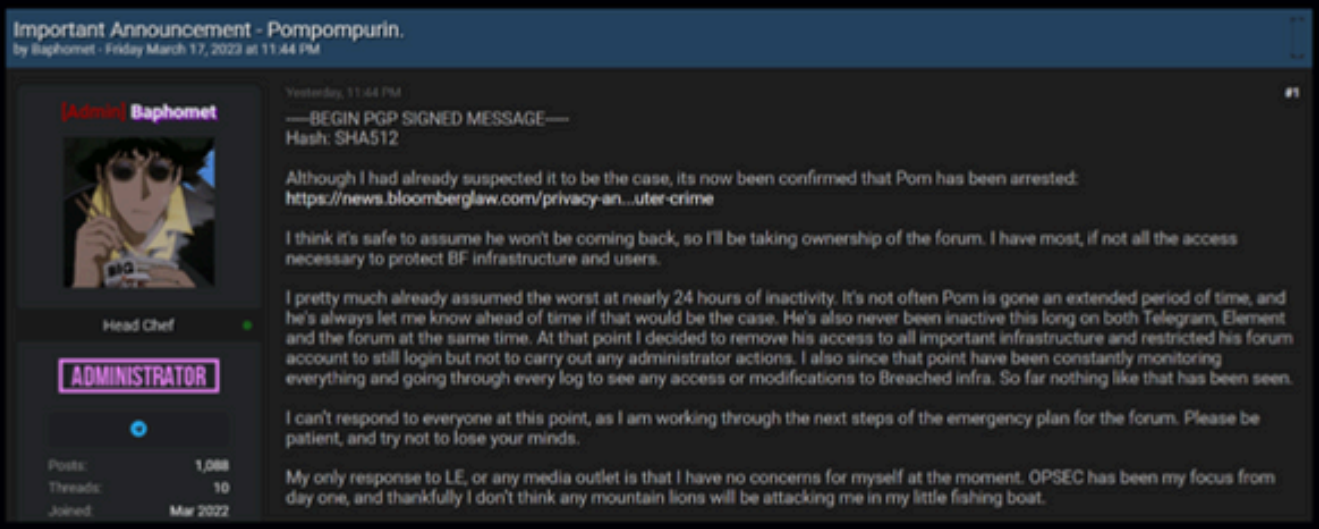
RaidForums, one of the most prominent underground forums for trading stolen data, was founded by a cybercriminal known as "Omnipotent." The platform gained popularity for hosting leaked databases, hacking tools, and illicit services. However, in early 2022, after years of investigation, law enforcement agencies, including the FBI, successfully seized RaidForums. Omnipotent was arrested and sentenced to jail, marking a significant victory for cybersecurity professionals and law enforcement. The operation that led to the forum's takedown was a major example of collaboration between global authorities using Open Source Intelligence (OSINT) and Threat Intelligence to track the activities and individuals involved in such platforms.



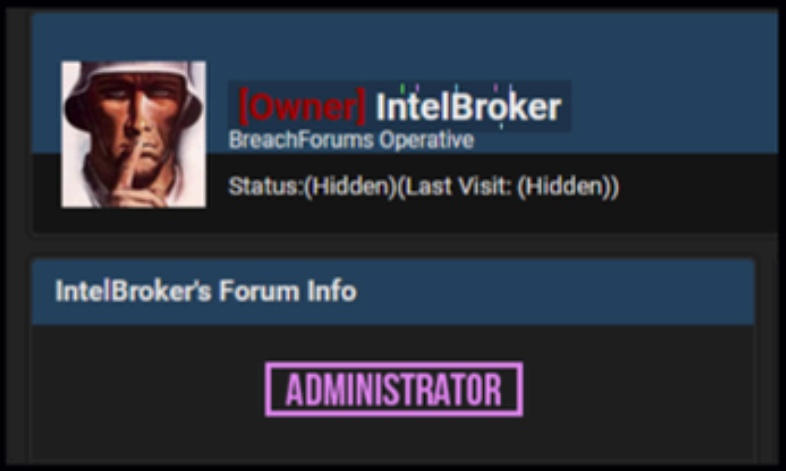
After the RaidForums takedown, another infamous cybercriminal, known as Pompompurin, quickly responded to the void in the dark web by creating BreachForums. In a tweet, Pompompurin invited hackers and former RaidForums users to join BreachForums, positioning it as the successor to the now-defunct platform. BreachForums quickly gained traction as the new go-to hub for cybercriminals to trade stolen data and engage in illicit activities. However, in early 2023, the FBI once again intervened, seizing BreachForums as part of an ongoing crackdown on dark web marketplaces. This action led to the arrest of Pompompurin, halting the forum's operations temporarily.



Following Pompompurin's arrest, another user known as "Baphomet" resumed the activity of BreachForums under a new domain. Baphomet's efforts helped maintain the forum's operations for a short period, but the forum was eventually terminated under its old top-level domain (TLD) after facing increasing pressure from law enforcement.



DESPITE THE FORUM'S TERMINATION, THE USER "INTELBROKER" BEGAN BOASTING ABOUT THE ACTIVITY AND CONTINUITY OF BREACHFORUMS, HINTING THAT THE CYBERCRIMINAL COMMUNITY WOULD CONTINUE OPERATING DESPITE THE DISRUPTIONS. THIS SERIES OF EVENTS HIGHLIGHTS THE CONSTANT EVOLUTION OF CYBERCRIMINAL FORUMS AND THE ONGOING STRUGGLE BETWEEN LAW ENFORCEMENT AND DARK WEB ACTORS.



```
PE[CC3A6F123D8BA8ACF36E83F46EBF2BE9] [2023-01-02T18_03_35.9379073].zip.zip
Url: https://signup.lan.leagueoflegends.com/es/signup/index
Username: Pompompurin
Password: marshalteamo666
Insertion Timestamp: 2023-10-09 12:00:00+02:00

PE[CC3A6F123D8BA8ACF36E83F46EBF2BE9] [2023-01-02T18_03_35.9379073].zip.zip
Url: https://signup.las.leagueoflegends.com/es/signup/index
Username: Pompompurin
Password: marshalteamo666
Insertion Timestamp: 2023-10-09 12:00:00+02:00

Url: https://signup.las.leagueoflegends.com/es/signup/index
Username: Pompompurin
Password: lucifer2005
Insertion Timestamp: 2023-08-11 17:01:20.227305+02:00

sources: ['gPotato.com']
username: pompompurin
password: badboyssky
lastbreach: 2006-11

sources: ['Stealer Logs']
username: pompompurin
password: marshalteamo666
lastbreach:
```

Leak intelligence plays a pivotal role in modern threat investigations, particularly when it comes to identifying and tracking cybercriminals. Tools like OSIVE (Open Source Intelligence Visualization Engine) and platforms such as OSINTLeak provide investigators with critical insights by analyzing data leaks and compromised databases. OSIVE, available through OSINTLeak, helps investigators aggregate and visualize leaked intelligence, such as email addresses, passwords, and other personal information found in dark web forums or underground marketplaces. Using these tools, threat intelligence analysts can map relationships, track digital identities, and correlate data across multiple leaks to gain a better understanding of threat actors' behaviors and networks.

Zynga	
domain	hellokitty.com
email	lowell@hellokitty.com
username	Pompompurin

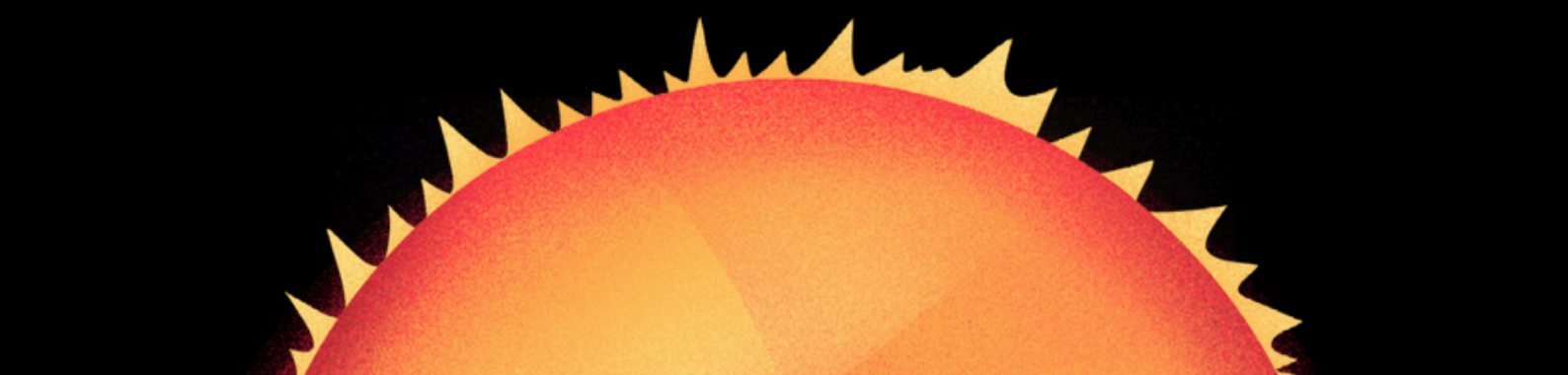
(click to view more)

stockx.com	
domain	gmail.com
email	pholsuwan1234@gmail.com
ip	54.175.108.129
name	Bawornwit Pholsuwan
phone	0066818701325

One of the key databases used to find information about Pompompurin is the BreachForums database, which is accessible through platforms like Breach.vip. When Pompompurin became a target of law enforcement, his involvement in BreachForums, where hackers traded massive amounts of stolen data, made him vulnerable to leak intelligence investigations. By cross-referencing user activity, leaked credentials, and other metadata from BreachForums' archives, OSINT investigators are able to trace patterns that lead back to Pompompurin. Even after the initial takedown of BreachForums, the availability of its database provides a wealth of information for continued investigations. The integration of OSINT tools like OSIVE and access to databases like BreachForums offers crucial capabilities for mapping out the networks of cybercriminals and revealing their identities, as investigators attempt to unmask high-profile figures like Pompompurin.

02

RAIDFORUM, BREACHFORUM, ...



Analysis Methods

1. Data correlation
    * Techniques for correlating collected data to identify patterns and connections
2. Sentiment Analysis
    * Using natural language processing (NLP) to gauge public sentiment and reactions
3. Network Analysis
    * Mapping relationships and interactions within the data to uncover networks

```
NAME: Conor Brian Fitzpatrick
SSN: 081-92-4399
DOB: 26th September 2002

ADDRESS: 531 UNION AVE, PEEKSKILL, NY 10566+4706
https://www.google.com/maps/@41.2799995,-73.9215499,3a,38.3y,100.19h,95.97t/data=!3m6!1e1!3m4!1so6jn8L3ol8MeD35R6kEZ4g!2e0!7i13312!8i665
6

DRIVERS LICENCE NUMBER: 507274801

PHONE:
 +1 9146423144 - [CELLCO PARTNERSHIP DBA VERIZON WIRELESS - NY (VERIZON WIRELESS)] - [MOBILE]
 +1 9144025399 - [CABLEVISION LIGHTPATH INC - NY] - [LANDLINE]
 +1 9146999668 - [VERIZON NEW YORK INC] - [LANDLINE]

SOCIALS:
 - Emails -
  pom@pompur.in
 - Twitter -
  https://twitter.com/xml
 - Telegram -
  https://t.me/paste

RELATIVES:
 - MOTHER -
  NAME: MARY MCCARRA FITZPATRICK
  DOB: 1967

 - FATHER -
  NAME: MARK E FITZPATRICK
  DOB: 1961

 - YOUNGER BROTHER -
  NAME: BRENDAN FITZPATRICK

 - SEVERELY AUTISTIC BROTHER -
  NAME: AIDEN FITZPATRICK
```

Step 1: Identity Verification and Background Check

Key Data Points:

* **Name**: Conor Brian Fitzpatrick
* **DOB**: 26th September 2002
* **SSN**: 081-92-4399
* **Driver's License**: 507274801
* **Address**: 531 Union Ave, Peekskill, NY 10566
* **Phone Numbers**: +1 9146423144, +1 9144025399, +1 9146999668

Tools & Methods:

1. **Public Records Search**:
    * Use public records search engines like **Whitepages**, **Spokeo**, or **Pipl** to verify the identity and cross-check details like the address, SSN, and DOB.
    * **Driver's License Lookup** (depending on local regulations, some websites offer vehicle registration or license checks).
2. **Address Verification**:
    * Use **Google Maps** with the provided link to confirm the physical location at 531 Union Ave, Peekskill, NY. Street view and address information will help identify the residence visually.
3. **Phone Number Lookup**:
    * Use reverse phone lookup services such as **TrueCaller**, **NumLookup**, or **SpyDialer** to determine if the provided phone numbers are valid and registered to the person. Cross-check the service providers like **Verizon Wireless** and **Cablevision Lightpath**.

Step 2: Social Media and Online Footprint Analysis

Key Data Points:

* Emails: pom@pompur.in
* Twitter: https://twitter.com/xml
* Telegram: https://t.me/paste

Tools & Methods:

1. Email Tracing:
    * Use email lookup tools such as Hunter.io, EmailRep, or HaveIBeenPwned to identify whether the email pom@pompur.in is linked to any public data breaches or other online services. You can also determine which services this email is registered on.
2. Twitter Analysis:
    * Perform a Twitter handle analysis using tools like Twitonomy or TweetBeaver. This helps map out tweet patterns, connections, followers, and any tweet history that could reveal personal or illegal activities.
3. Telegram Group Scraping:
    * Use Telegago or Telegram OSINT Tool to investigate the user's Telegram activity. Look for group memberships, shared files, or possible links to dark web forums or criminal communities.

Step 3: Relatives and Family Connections

Key Data Points:

* Mother: Mary McCarra Fitzpatrick (DOB: 1967)
* Father: Mark E. Fitzpatrick (DOB: 1961)
* Younger Brother: Brendan Fitzpatrick
* Severely Autistic Brother: Aiden Fitzpatrick

Tools & Methods:

1. Family Search Tools:
    * Use genealogy websites like FamilyTreeNow or Ancestry.com to trace family history and validate the relationships provided. This helps confirm personal connections and may reveal additional relatives.
2. Social Media Search:
    * Search for family members on Facebook, LinkedIn, or Instagram using their full names and dates of birth. This can help you map out the family's social connections, habits, and any visible ties to the target's activities.
3. Public Record Verification:
    * Use services like MyHeritage or PeopleFinders to search for addresses, phone numbers, or any previous criminal records linked to family members.

Step 4: Legal Documents and Court Records

Key Data Points:

* Name: Conor Brian Fitzpatrick
* FBI Arrest: Related to computer crimes, likely due to BreachForums operation.

Tools & Methods:

1. Court Document Search:
    * Search public court documents using CourtListener, PACER (Public Access to Court Electronic Records), or Justia Dockets. These platforms can provide access to legal filings, indictments, and related case materials.
    * Example: Searching for records related to the FBI arrest might reveal the exact charges, court proceedings, and sentencing.
2. Media Reports:
    * Use tools like Google News and Factiva to gather media reports related to Conor Brian Fitzpatrick's arrest. Articles from reputable sources like Krebs on Security or Bloomberg (as linked earlier) offer detailed insights into criminal activities and investigations.

Step 5: Dark Web and Underground Forums Search

Key Data Points:

* **Aliases/Username**: Pompompurin
* **Online Presence**: Admin of BreachForums, Skidbin, and other dark web communities.

Tools & Methods:

1. **Dark Web Monitoring**:
    * Use OSINT tools like **DarkOwl**, **IntelX**, or **Recorded Future** to monitor dark web forums and marketplaces for mentions of "Pompompurin" or other linked aliases. These platforms often index dark web activity and can provide a wealth of information.
2. **Forum Analysis**:
    * Investigate **BreachForums** and any remaining Skidbin archives to locate posts made by **Pompompurin**. Use forum scraping techniques or custom queries to extract data related to illegal activities.
    * Pay attention to underground connections and potential ties to other cybercriminals.

Step 6: Data Breach Search and Financial Information

Key Data Points:

* SSN: 081-92-4399
* Emails and Other Accounts

Tools & Methods:

1. HaveIBeenPwned:
    * Use this tool to see if the SSN, email, or any related accounts have been leaked in past data breaches. This helps determine if the person's data is compromised.
2. Financial Tracking:
    * You can use services like BeenVerified or LexisNexis to conduct background checks that include financial history, potential bankruptcy records, and asset ownership related to the target.

Findings & Threat Intelligence

In a recent turn of events, the cybersecurity landscape has been shaken by the FBI's decisive raids on Breach Forum, a notorious hub for illicit activities on the dark web. The aftermath revealed a complex web of exploits, compromised credentials, and unexpected vulnerabilities, shedding light on the inner workings of cyber criminal networks.

gov.uscourts.vaed.535542.2.0.pdf

4. Findings and Threat Intelligence - Carie

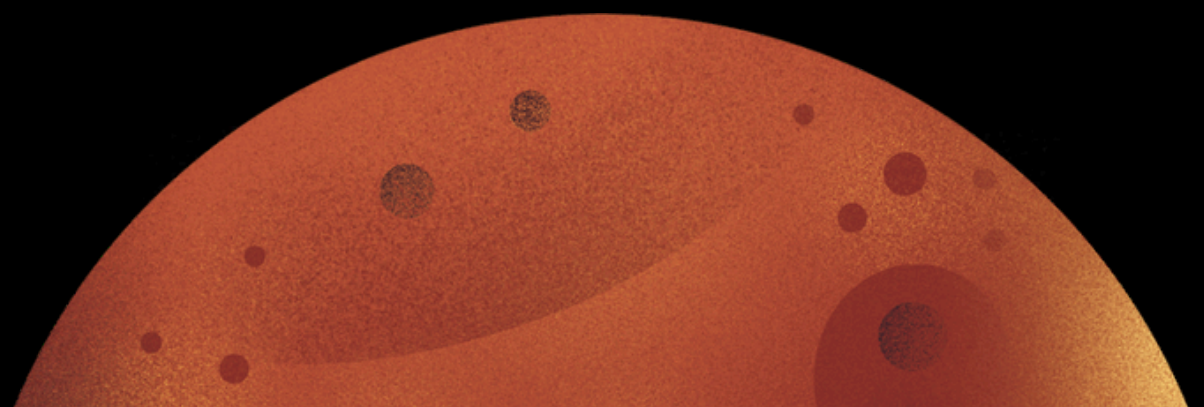
* Identified Threats
    * Summary of potential threats uncovered during the investigation
* Attribution and Source Verification
    * Methods for verifying the credibility and origin of collected data
* Risk Assessment
    * Evaluating the potential impact and likelihood of identified threats

5. Reporting and Recommendations - Carie

* Reporting Findings
    * Best practices for compiling and presenting the investigation results
* Mitigation Strategies
    * Recommended actions to address and mitigate identified threats
* Future Monitoring
    * Establishing ongoing monitoring processes to prevent future issues

03

PETER KLEISSNER



conflict between RaidForums and BreachForums with Peter Kleissner

The conflict between BreachForum, RaidForum, and the owner of IntelX, Peter Kleissner, is emblematic of the growing tension between dark web communities and open-source intelligence (OSINT) platforms. Kleissner, an Austrian cybersecurity expert and founder of IntelX, offers services that provide deep searches into leaked databases, exposing sensitive information from data breaches. This has put him at odds with members of underground forums like BreachForum and RaidForum, who viewed his work as a direct threat to their anonymity and operations.

BreachForum, led by Pompompurin, and RaidForum, previously run by Omnipotent, became notorious for facilitating the exchange of hacked data, personal information, and illicit services. As IntelX allowed users to search historical data breaches, it became a powerful tool for OSINT investigations, aiding law enforcement and private sector investigators in tracking cybercriminals. This led to significant hostility from dark web forum users, who saw Kleissner's platform as a gateway for authorities to trace their digital footprints.

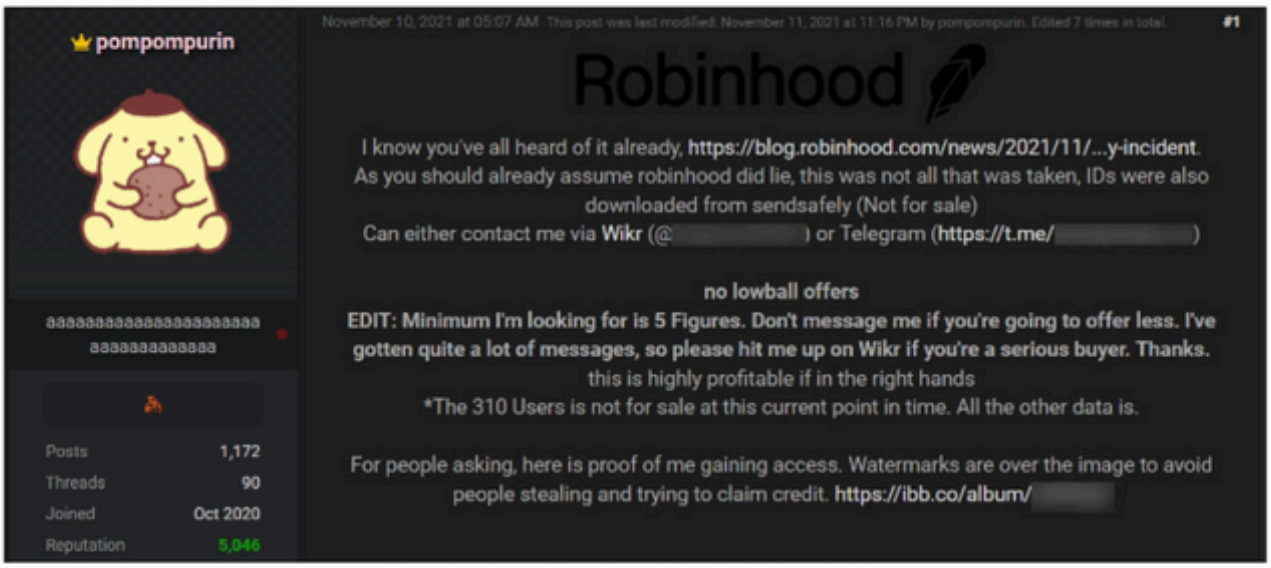
Members of these forums retaliated by doxxing Peter Kleissner, leaking his personal information, such as addresses, phone numbers, and family details, across their platforms. These actions were intended to intimidate and discredit him, positioning him as a target within the cybercriminal community. The doxxing was part of a broader effort to resist OSINT platforms like IntelX, which undermined the anonymity that dark web users relied on to evade detection.

The conflict highlights the fundamental divide between platforms like IntelX, which aim to shed light on illegal activities, and dark web forums that thrive on secrecy and data exploitation. As law enforcement continues to crack down on these underground marketplaces, the role of OSINT providers like IntelX becomes increasingly critical, further escalating tensions between cybercriminals and intelligence professionals.

```
          -= Kleissner Investments s.r.o. =-

ID Number     : 05425115

Registered    : 27 September 2016

Phone         : +420774346764

Email         : ripe@kleissner.investments

Address       : Na Strži 1702/65, 140 00 Praha 4-Nusle, Czechia

IP Ranges     : IPV4 -> 185.185.216.0/22  IPV6 -> 2a0b:6580::/29
                     -> 185.190.89.0/24        -> 2a10:64c0::/29
                     -> 185.194.12.0/24        -> 2a10:7140::/29


                  -= Peernet s.r.o. =-

ID Number     : 09951041

Registered    : 24th of February 2021

Phone         : +420774346764

Email         : ripe@peernet.org

Address       : Na Strži 1702/65, 140 00 Praha 4-Nusle, Czechia

IP Ranges     : IPV4 -> 185.254.123.0/24


          -= Domains =-

kleissner.at
Registrar      : easyname.eu

peterkleissner.com
Registered     : 2017-10-11
Expires        : 2022-10-11
Registrar      : dynadot

kleissner.pk
Registrar      : easyname.eu

kleissner.investments
Registered     : 2016-09-05
Expires        : 2022-09-05
Registrar      : Tucows Domains Inc.
```

HTTPS://DOXBIN.NET/UPLOAD/PETERKLEISSNERINTELX

In a forum post, pompompurin said he was selling 7 million Robinhood customers' stolen information for at least five figures, which is $10,000 or higher.



Threat actor selling the stolen Robinhood data

Source: BleepingComputer

The sold data includes 5 million email addresses, and for another batch of Robinhood customers, 2 million email addresses and their full names. However, pompompurin said they were not selling the data for 310 customers who had more sensitive information stolen, including identification cards for some users.

Robinhood did not initially disclose the theft of ID cards, and the threat actor states that they downloaded them from SendSafely, a secure file transfer service used by the trading platform when performing Know Your Customer (KYC) requirements.

"As we disclosed on November 8, we experienced a data security incident and a subset of approximately 10 customers had more extensive personal information and account details revealed," Robinhood told BleepingComputer after we contacted them regarding the sale of their data.

"These more extensive account details included identification images for some of those 10 people. Like other financial services companies, we collect and retain identification images for some customers as part of our regulatory-required Know Your Customer checks."

pompompurin told BleepingComputer that he gained access to the Robinhood customer support systems after tricking a help desk employee into installing a remote access software on their computer.

HTTPS://T.ME/INTELXIO/238
HTTPS://T.ME/INTELXIO/260

Security Researcher

https://www.linkedin.com/in/sashwin-0xp4tcher/

Conclusion

Pompompurin, the alias of Conor Brian Fitzpatrick, is a key figure in the cybercrime world as the administrator of BreachForums, a dark web platform notorious for facilitating data breaches and the exchange of stolen information. His arrest by the FBI in March 2023 brought an end to his role in one of the most significant data breach forums, where sensitive information, including personal and financial data, was traded. Pompompurin's involvement in the underground hacking community, coupled with his history of managing illicit platforms like Skidbin.net, positioned him as a prominent player in cybercrime, impacting both individuals and organizations globally.

The investigation into Pompompurin reveals the extent of his criminal activities, including managing illicit forums and handling stolen data. His personal information, which surfaced following his arrest, highlights the vulnerability of those operating in the dark web, where anonymity is often compromised. The takedown of BreachForums underscores law enforcement's growing focus on disrupting cybercriminal networks, and the arrest of figures like Pompompurin sends a clear message to the hacker community about the legal consequences of their actions.

HADESS

cat ~/.hadess

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:

WWW.HADESS.IO

Email

MARKETING@HADESS.IO

To be the vanguard of cybersecurity, hadess envisions a world where digital assets are safeguarded from malicious actors. We strive to create a secure digital ecosystem, where businesses and individuals can thrive with confidence, knowing that their data is protected. Through relentless innovation and unwavering dedication, we aim to establish hadess as a symbol of trust, resilience, and retribution in the fight against cyber threats.