

Dark Web Profile: ShinyHunters

By Ameer Owda

Published: 2024-03-18 · Archived: 2026-08-10 02:00:25 UTC

[Update] July 31, 2025: “ShinyHunters Behind CRM Attacks on Qantas, Adidas, and Others”

Within the obscured world of the Deep/[Dark Web](#), where cybercrime flourishes amidst databases, initial access brokers, and a plethora of illegal activities, there exists a group known for leaking various databases and executing high-profile attacks. This group, at first glance, might seem like a benign assembly of Pokémon enthusiasts, given their name.

Yet, they stand accused of orchestrating [data breaches](#) that have consistently found their way onto [hacker forums](#). But their activities extend beyond mere data leaks; they are also the alleged proprietors of one of the most popular hacker forums, BreachForums. This group is none other than ShinyHunters.

ShinyHunters X(Twitter) profile

Who is ShinyHunters?

ShinyHunters (also known as **ShinyCorp**) is an international cyber threat group that first emerged in 2020. This group has quickly become infamous for orchestrating several high-profile data breaches. Despite the playful, Pokémon-inspired name that suggests a community of harmless enthusiasts, ShinyHunters is deeply entrenched in cybercrime, specializing in the theft and sale of vast databases.

Their activities span across the dark corners of the internet, a realm notorious for hosting a variety of illegal undertakings.

ShinyHunters' RaidForums Profile

Claiming responsibility for multiple significant cyberattacks, ShinyHunters has leaked the personal information of over a billion internet users. They've followed in the footsteps of other cybercriminal groups like **GnosticPlayer**, contributing to the alarming trend of mass data dumps.

Initially gaining notoriety for their involvement in substantial data breaches of notable companies such as Tokopedia—an esteemed Indonesian e-commerce platform—Mathway, and even Microsoft's [GitHub](#), they've consistently demonstrated their prowess and ruthlessness.

How Does ShinyHunters Hack?

ShinyHunters threat actor's card

ShinyHunters has gained notoriety for their sophisticated hacking techniques and large-scale data breaches. Their approach to hacking is both methodical and cunning, employing a variety of strategies to infiltrate and exploit

vulnerabilities in digital systems. Here's a simplified overview of how ShinyHunters typically conduct their hacking operations:

Scouring GitHub Repositories: One of their initial steps involves searching through companies' GitHub repositories. GitHub, a platform where developers store and manage their code, can sometimes inadvertently contain vulnerabilities. ShinyHunters meticulously examines this code to find any weak spots that can be exploited to gain unauthorized access to databases, allowing them to extract sensitive information.

Exploiting Unsecured Cloud Buckets: ShinyHunters have also exploited unsecured cloud buckets. Cloud buckets are online storage spaces where companies and individuals can store data and files. When these buckets are not properly secured, they're like open treasure chests waiting to be plundered.

Targeting Websites and Developer Tools: ShinyHunters also focuses on compromising websites and developer repositories. This often involves stealing login credentials or **API keys**, which are like digital keys that allow access to certain parts of a system. Once in possession of these keys, they can easily access databases and extract valuable data.

Deploying Phishing Attacks: A more deceptive tactic in their arsenal is [phishing](#). Phishing involves tricking individuals into revealing their personal login information. ShinyHunters craftily designs [emails](#) that appear to be from legitimate sources, like GitHub, containing links to fake login pages. When unsuspecting users enter their details on these pages, the hackers gain access to their accounts and any associated data.

Leveraging the Dark Web: ShinyHunters is not just about stealing data; they also know how to profit from it. They use the dark web, a hidden part of the internet known for illegal activities, to sell or trade the stolen information. Through platforms like Empire, Exploit, and [RaidForums](#), they reach buyers interested in acquiring hacked databases for various purposes.

SOCRadar can significantly bolster defenses against threats like ShinyHunters through its **Cloud Security Module (CSM)** and Source Code Leakage Monitoring feature. By identifying unsecured cloud buckets and classifying them based on their security status, SOCRadar helps prevent unauthorized access to sensitive data stored in the cloud.

Additionally, its proactive scanning of public and private repositories, including GitHub, for source code leaks or accidental disclosures of sensitive information, allows organizations to swiftly respond to vulnerabilities. Employing advanced algorithms and machine learning, SOCRadar [Threat Hunting](#) detects exposed private keys, authentication credentials, and API keys in real time, enabling immediate action to mitigate risks and protect against exploitation by groups like ShinyHunters.

SOCRadar's Source Code Leakage Monitoring

ShinyHunters' High-Profile Attacks

ShinyHunters is a name that became well-known for causing trouble in the digital world between April 2020 and July 2021. They cleverly used dark web platforms to sell and share data they stole from big companies. Their actions not only put millions of people's personal information at risk but also showed how skilled and dangerous cybercriminals can be.

These data breaches were highly prized by ShinyHunters, selling for substantial amounts at the time. While many [threat actors](#) sought ways to acquire these datasets for free, the rapid spread of ShinyHunters' name was inevitable.

Claimed Breach of Tokopedia by ShinyHunters

Sale of data allegedly belonging to Tokopedia. ([HackRead](#))

In May 2020, a database allegedly containing information on **91 million** users of Tokopedia, Indonesia's largest online store, was offered for sale on the dark web market. The data included over **71 million** unique email addresses, names, genders, birth dates, and passwords stored as SHA2-384 hashes.

ShinyHunters' Supposed Infiltration of Microsoft GitHub

A screenshot provided by ShinyHunters shows access to Microsoft's account ([HackRead](#))

Just days after making claims about Tokopedia, ShinyHunters claimed to have stolen over **500 GB** of data from Microsoft's private GitHub repositories. This breach was part of a broader data breach campaign they conducted across various organizations. They sought to prove their claims by providing screenshots showing access to various repositories. The breach reportedly compromised about 500GB of various code samples, projects, e-books, and more, with roughly 1GB of the data leaked by ShinyHunters on a hacker forum.

Alleged Sale and Leak of Wattpad User Data

Leak of Wattpad data breached by ShinyHunters on a hacker forum. ([BleepingComputer](#))

Another alleged breach by ShinyHunters involved Wattpad, a website allowing members to publish user-generated stories on various subjects. The data was initially sold for **\$100,000** before being publicly released on a hacking forum, where it was widely shared. This leak affected **271 million** users, including password hashes protected by bcrypt for 145 million users and 44 million by sha256. The types of breached data included full names, phone numbers, Facebook IDs, passwords, emails, usernames, dates of birth, etc.

Allegations of Hacking Pixlr

On January 16, 2021, ShinyHunters claimed to have leaked the records of **1.9 million** users of Pixlr, a free online photo editing application. These records contained information that could be used to carry out targeted phishing and [credential stuffing](#) attacks. The breached data types included ID, country, creation date, email, Google ID, last login, name, password, region, and update date. ShinyHunters stated they downloaded the database from the company's AWS bucket at the end of 2020.

ShinyHunters' Alleged Attack on Pizza Hut Australia

Pizza Hut Australia's statement (Source: X)

The group has made numerous claims up to the present day, and in September 2023, they made a significant assertion. The ShinyHunters hacking group claims to have stolen over **30 million** customer order records from

Pizza Hut Australia, alongside data from more than one million customers. They allegedly gained unauthorized access to Amazon Web Services buckets used by the pizza chain, extracting sensitive information, including customer names, email addresses, phone numbers, encrypted credit card data, and hashed passwords.

Although Pizza Hut did not directly respond to the incident claimed by ShinyHunters, they reported a breach in their systems shortly thereafter. While there has been no official statement linking the two events, researchers believe there is a connection and suspect ShinyHunters' involvement in the breach.

ShinyHunters Leak Over 70 Million Records Allegedly Stolen from AT&T

A hacker forum post shared by ShinyHunters claims that they breached AT&T systems. (SOCRadar)

In mid-August 2022, ShinyHunters made headlines again by claiming on a dark web forum that they had breached the systems of AT&T Inc., a major American multinational telecommunications holding company. They announced that they had obtained more than **70 million** records containing Personally Identifiable Information (PII) and placed these records up for auction with an opening bid of **\$200,000**. Despite the alarming claim, AT&T responded by stating that their systems had not been compromised.

The statement was posted by a different threat actor on 17 March 2024. (SOCRadar)

On March 17, 2024, a post surfaced on BreachForums, allegedly from a distinct threat actor, revealing a database purportedly linked to AT&T. According to the announcement, this data, containing **73,481,539 lines** of Social Security Numbers (SSN) and Dates of Birth (DOB), was claimed to have been leaked and offered for sale by ShinyHunters.

SOCRadar Breach Datasets

In the face of threats posed by actors like ShinyHunters, organizations need robust tools to detect and respond to breaches effectively. SOCRadar's [Breach Datasets](#) offer a valuable resource in this regard. By providing access to extensive collections of breached data, including information that may have been compromised by threat actors like ShinyHunters, the tool enables organizations to rapidly identify and understand the extent of breaches affecting them.

Why Do Threat Actors Share Leaked Data for Free?

The transient nature of information on the dark web is evident. Despite the initial sale at high prices by ShinyHunters, much of the data they've circulated has eventually found its way to public forums free of charge. This phenomenon isn't exclusive to the ShinyHunters group but rather a common occurrence across the dark web.

The tendency of threat actors to distribute leaked data for free after a period can stem from several factors, and understanding the motivations behind these actions can help [cybersecurity](#) analysts refine their defense strategies:

Reputation and Recognition: Some threat actors may distribute leaked data for free to gain reputation and distinguish themselves within cybercrime communities. This can be particularly true for newcomers or those seeking more attention. Presenting themselves as "generous" can build trust among potential future clients and attract the attention of other threat actors.

Diminishing Value of Data: Over time, data sets, especially those containing sensitive information (such as SSN, DOB, etc.), can lose their value due to supply and demand dynamics in the market. A data set that was highly valuable when initially offered for sale can decrease in value as the information is exploited or as newer data breaches emerge. At this point, distributing the data for free can extract the last bit of value from it.

Maximum Damage and Impact: Threat actors might aim to cause maximum social or economic damage by distributing the leaked data for free. For those driven by ideological motivations, inflicting harm on a company or society can be more important than financial gain. Making this information widely accessible increases risks for affected individuals and organizations.

Distraction and Misdirection: In some cases, threat actors might distribute data for free as part of a larger or more sensitive cyber operation. This can divert the attention of cybersecurity professionals and defense teams, misleading them about the actors' true intentions or next moves. This strategy can be used as part of more complex and coordinated attacks.

Complicating Legal Pursuit: The widespread distribution of data can complicate legal pursuits. Proving that a data set came from multiple sources becomes challenging, which can reduce the risk of threat actors being caught.

Each of these factors reveals the complex motivations and strategies behind the actions of threat actors. With the growing concern over personal and organizational security online, checking if your account has been compromised is more crucial than ever. SOCRadar offers a valuable tool in this regard – the Account Breach Check available at [SOCRadar Labs](#).

This feature allows individuals and organizations to quickly ascertain if their accounts have been exposed in any data breaches. By simply entering your email address, SOCRadar taps into its extensive breach database, which encompasses over 5 billion records, including 3.9 billion unique email addresses and over 4.2 billion breached accounts across 7,394 combolists.

SOCRadar Labs, Account Breach Check

ShinyHunters Hacker Sezyo Kaizen Sentenced to Prison

Sebastien Raoult, also known by his nickname “Sezyo Kaizen,” is a figure in the cybercrime world, particularly as a member of the ShinyHunters hacking group. At 22 years old, the French citizen has been sentenced to **three years** in prison by a court in Seattle, USA

Raoult's involvement was critical in crafting deceptive web pages that looked identical to legitimate business login pages. This tactic was part of a phishing scheme to harvest user credentials.

Once these credentials were obtained, the group proceeded to exploit them to gain unauthorized access to the victims' accounts. This led to further theft of corporate data and even penetration into company networks and third-party cloud storage services.

As part of his sentence, Raoult is also required to pay over **\$5 million** in restitution, a sum that underscores the significant impact of his actions on the affected companies and their users.

The Current Owners of One of the Most Popular Cybercriminal Forums: BreachForums

ShinyHunters has established itself as a dominant force in the dark web's cybercriminal landscape, notably taking ownership of one of the most frequented hacker forums. The group's engagement on RaidForums and the subsequent activities of [Pompompurin](#) on BreachForums have significantly bolstered their standing within the hacking community.

The closure of RaidForums and its first successor, BreachForum V1, by law enforcement led to the emergence of numerous forums vying to be recognized as the legitimate successor. Nevertheless, BreachForums V2, launched by ShinyHunters, has successfully filled the vacuum left by its predecessors. This success is attributed to the persistent acclaim of ShinyHunters from their RaidForums days and a strategic alliance with a threat actor known as Baphomet, who was one of the administrators alongside Pompompurin.

The return of BreachForums (SOCRadar)

ShinyHunters' reputation was instrumental in attracting former members renowned for their involvement in notable cyberattacks to join BreachForums. However, concerns about the forum potentially being a law enforcement honeypot led some previous members to stay away.

Stay ahead of cyber threats like ShinyHunter with SOCRadar's [Dark & Deep Web Monitoring](#) solution. Our 24/7 surveillance empowers organizations to proactively identify and neutralize threats across the surface, deep, and dark web. By combining advanced reconnaissance capabilities with expert threat analysis, we provide actionable intelligence to fortify your defenses. From uncovering the challenges of the anonymous dark web to monitoring forums for malicious activities, SOCRadar helps you navigate the digital landscape with confidence.

ShinyHunters Behind CRM Attacks on Qantas, Adidas, and Others

A wave of data breaches affecting Qantas, Adidas, Allianz Life, and LVMH first came to light earlier in 2025, involving advanced phishing and vishing attacks targeting Salesforce CRM users. Threat actors impersonated IT staff to trick employees into connecting malicious OAuth apps, often disguised as "My Ticket Portal," to internal systems. This allowed them to steal credentials and MFA tokens.

Insight into the UNC6040 Attack Tactics (Source: [Google](#))

At the time, the identity of the attackers was unknown. However, by July 2025, multiple victims reported receiving extortion emails in which the attackers identified themselves as ShinyHunters, suggesting the group's involvement. Google's Threat Intelligence team tracks the campaign as UNC6040, aligning it with ShinyHunters' known tactics in data-theft extortion.

This development raises new questions about the group's structure. In June, French authorities reportedly arrested a key ShinyHunters operator who had previously transferred control of BreachForums to IntelBroker. Despite the arrest, the campaign continues, suggesting that ShinyHunters is more than a single individual.

We believe the group now operates as a flexible extortion-as-a-service model. There are also signs of overlap with other threat groups such as [Scattered Spider](#) and possibly former members of Lapsus\$. While BreachForums is no longer active and attempts to revive it under the same name have failed to gain traction, the group's future leak distribution methods remain uncertain.

What is clear is that ShinyHunters continues to evolve. Monitoring Dark Web forums, leak sites, and extortion trends is essential to stay ahead of this persistent and adaptable threat.

ShinyHunters TTPs – MITRE ATT&CK Framework

Tactic	Technique ID	Technique	Description
Reconnaissance	T1589.001, T1589.002, T1598	Gather Victim Identity Information: Credentials/Email Addresses, Phishing for Information	Engaging in reconnaissance to gather information about targets' systems, networks, or credentials.
Initial Access	T1566, T1078.002, T1078.004	Phishing, Valid Accounts: Domain Accounts/Cloud Account	Using phishing and valid accounts to gain initial access or escalate privileges within networks or cloud environments.
Credential Access	T1528	Steal Application Access Tokens	Stealing application access tokens to access cloud services and bypass authentication mechanisms.
Discovery	T1580	Cloud Infrastructure Discovery	Performing discovery activities targeted at
Lateral Movement	T1210, T1072	Exploitation of Remote Services, Software Deployment Tools	Exploiting vulnerabilities in remote services or misusing software deployment tools for lateral movement.
Collection	T1530, T1213	Data from Cloud Storage Object, Data from Information Repositories	Collecting data from cloud storage and information repositories, including codebases and databases.
Exfiltration	T1567	Exfiltration Over Web Service	Exfiltrating stolen data using web services as a covert channel to bypass network monitoring.

Source: <https://socradar.io/dark-web-profile-shinyhunters/>