A cybercriminal is sentenced, will it make a difference? - Help Net Security

By Help Net Security

Published: 2024-03-07 · Archived: 2026-04-02 12:24:50 UTC

The darknet is home to many underground hacking forums in which cybercriminals convene, freely sharing stories, tactics, success stories and failures. Their unguarded discussions allow our team to peek into the politics and ethics behind recent adversary activities. The threat intelligence we gather is harnessed to continuously enhance protections for Cynet partners and customers.

In this piece, we'll probe a notorious ransomware gang, ShinyHunters, to shed light on cybercriminal incentives and the objectives they pursue, as well as the effects for victims — and steps your team can take to reduce risk.

You can also use the "Ransomware Readiness Assessment Guide" to quickly evaluate your current exposure.

The sentencing of a cybercriminal

On January 10, a French citizen was sentenced to 3 years in prison plus a fine of $5 million. He had pleaded guilty to conspiracy to commit wire fraud and aggravated identity theft. The 22-year-old had originally faced 29 years behind bars.

The charges stemmed his involvement with a shadowy hacker group called ShinyHunters, believed to have formed in 2020. ShinyHunters is responsible for stealing data from over 60 organizations. The stolen data, which often PII (Personal Identifiable Information) and financial credentials, is then held for ransom. If ShinyHunters's demands for payment are not met, the victim's data is sold or leaked across various dark web marketplaces. This behavior indicates financial motivation; their activities appear unaffiliated with a political or activist agenda.

His role in ShinyHunters was to create specialized phishing pages masquerading as a target company's login portal to lure employees to enter their credentials. With these stolen credentials, the group infiltrated company networks and stole data from any assets that could later be leveraged for extortion.

Ransomware rampage

ShinyHunters hit the scene with a massive exfiltration of account data from Tokopedia, Indonesia's largest e-commerce company. ShinyHunters posted for sale the information of 15 million Tokopedia accounts for a meager €2.13 on May 2, 2020. Later, the full database of 91 million Tokopedia accounts was offered for $5,000.

The account data included email addresses, full names and birth dates, as well as hashed user passwords that other threat actors dehashed, or cracked, before sharing publicly.

Another notable breach attributed to ShinyHunters targeted the apparel company Bonobos, a subsidiary of Express, Inc. On January 17th, 2021, a Bonobos database in the form of a 70GB SQL file was offered for free download on the hacker forum RaidForums. The database included millions of email addresses, phone numbers, the last four digits of credit card numbers, hashed passwords, and user password history. As with the Tokopedia leak, threat actors dehashed or cracked the passwords for use in credential stuffing attacks.

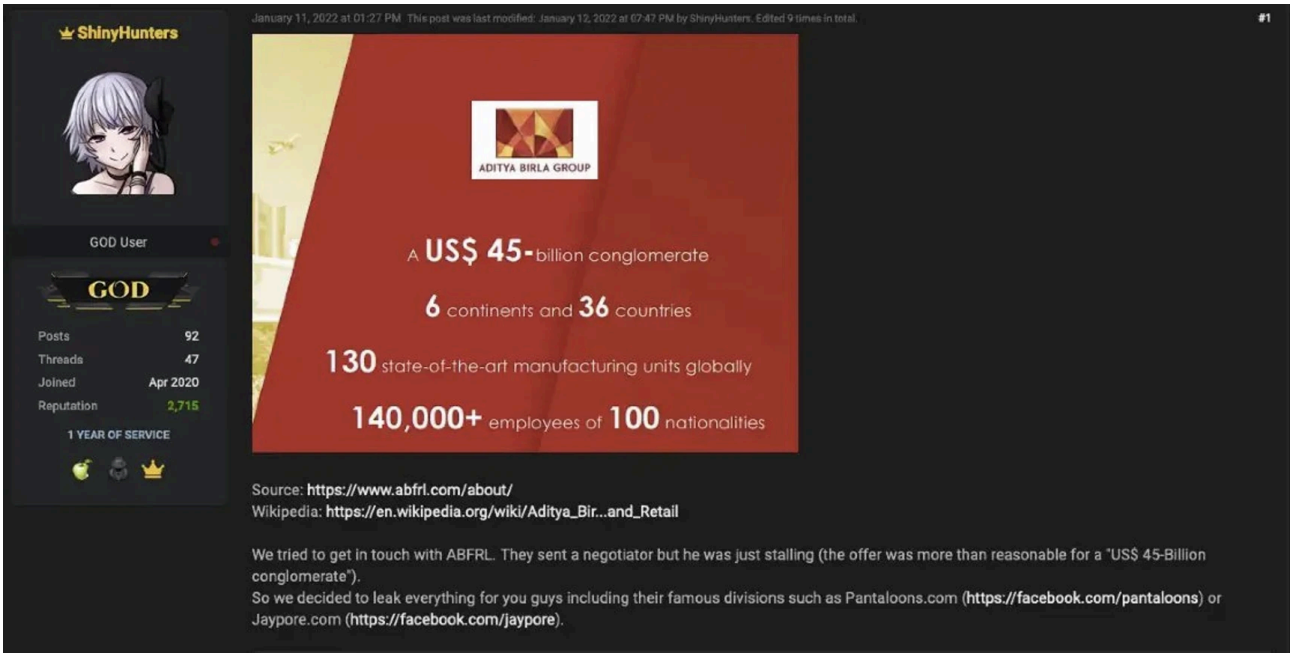
Bonobos believes that the group exfiltrated the data by exploiting access to a backup file that was hosted outside the company's internal network, on an external cloud environment, back in August 2020.

The most recently confirmed ShinyHunters victim is Aditya Birla Fashion and Retail (ABFRL), based in India, one of the world's largest fashion retail companies.

On January 11, 2022, after ransom negotiations for an undisclosed sum broke down, ShinyHunters dropped a major leak for free on RaidForums. Its 700GB of stolen data included:

- Sensitive ABFRL employee and customer data (full name, email, birth date, physical address, gender, age, marital status, salary, religion, and more).
    - This includes around 5.4 million unique email addresses and passwords hashed in the long deprecated MD5 hashing algorithm.
- 21 GB of ABFRL invoices containing sensitive customer payment details.
- ABFRL's website source code and server reports.

Although ABFRL detected ShinyHunters while the attack was in progress, the hacking group says they still had uninterrupted access to the company's sensitive data.



ShinyHunters techniques

A ShinyHunters staple is spear-phishing, where phishing emails and fake login pages are crafted to target specific companies and collect credentials for later use to exfiltrate data — usually sensitive customer or employee information — from the victim's network and environments. After exfiltration, any further credentials that are found are used to expand access the victim's network or third-party services. The group then holds exfiltrated data for ransom, urging the victim to pay or spectate as their data is sold in various darknet forums and marketplaces, or even released publicly for free.

It was also reported that, in some instances, the group breached companies' cloud computing providers and hijack them to mine for cryptocurrency, causing the victim companies to get stuck with the bill.

Fallout

The effects of ShinyHunters's attacks transcend the technical damage to the internal operations of its victims, such as through source code exfiltration. By compromising the customer databases of companies lacking sufficient security measures, ShinyHunters caused reputational damage on victims and, in severe cases, left them exposed to legal actions. Indeed, several ShinyHunters victims currently face class action lawsuits stemming from the theft of sensitive customer that was distributed amongst threat actors.

Conclusion

It remains to be seen if the aforementioned sentencing will deter his coconspirators in ShinyHunters from further illicit activity. Regardless of their life decisions, what we know for certain is that ransomware risk as a global liability is rising rapidly.

After attack volume increased by 50% in 2023, security teams must take action to reduce their risk of ransomware. This is especially true for small-to-medium enterprises (SMEs) with lean security teams. 82% of ransomware attacks target SMEs.

Cynet's all-in-one cybersecurity solution is purpose-built to help small teams fight back. It's affordable, easy to use and backed by CyOps, Cynet's built-in MDR service. We're available 24/7 to monitor your environment, accelerate incident response or simply answer your questions.
