

# ShinyHunters' 22-Year-Old Member Pleads Guilty to Cyber Extortion, Causing \$6 Million in Damage

[cyberwarzone.com/shinyhunters-22-year-old-member-pleads-guilty-to-cyber-extortion-causing-6-million-in-damage/](https://cyberwarzone.com/shinyhunters-22-year-old-member-pleads-guilty-to-cyber-extortion-causing-6-million-in-damage/)

October 1, 2023



## ShinyHunters' 22-Year-Old Member Pleads Guilty to Cyber Extortion, Causing \$6 Million in Damage



### Introduction

How safe is your company from phishing attacks? A 22-year-old French citizen recently pleaded guilty<sup>1</sup> in the United States for his role in a criminal group known as ShinyHunters. The group targeted dozens of companies and extorted them using stolen customer data, leading to damages of approximately \$6 million.

### How ShinyHunters Operated

The French hacker was skilled in creating phishing websites<sup>2</sup>, replicating the login pages of targeted companies. Isn't it alarming how easy it is for criminals to clone legitimate websites? Employees were then tricked into logging into these fake pages via phishing emails.

Once victims entered their credentials, the data was sent back to **ShinyHunters**. With these login details in hand, the group members accessed various accounts to dig for additional data and credentials.

### Accessing Cloud Storage and More

Don't you think it's time to reconsider the security of third-party services? The criminals were able to gain entry into cloud storage services, third-party service providers, and company networks. Here, they stole even more sensitive data, proving that the breach of a single account can have a domino effect<sup>3</sup>.

### Extortion and Public Threats

If companies did not pay the ransom, ShinyHunters threatened to release the stolen data publicly. We believe this highlights the urgency for companies to strengthen their cyber defenses. According to the indictment, the attacks led to the theft of hundreds of millions of customer records.

### Legal Consequences

The French hacker was arrested last year in Morocco and was extradited to the U.S. earlier this year. He faces a maximum prison sentence of nearly 30 years. However, he has struck a plea deal, which will likely result in a reduced sentence.

## Questions Answered

---

- **How did ShinyHunters operate?** Through phishing websites and emails to steal credentials.
- **What did they do with the stolen data?** Used it for extortion and threatened public exposure.
- **What are the legal consequences for the French hacker?** A maximum prison sentence of nearly 30 years, possibly reduced due to a plea deal.

## References

1. <https://www.justice.gov/usao-wdwa/pr/french-cybercriminal-pleads-guilty-fraud-and-aggravated-identity-theft-hacking-private> ↵
2. <https://www.security.nl/posting/812428/Fransman+bekent+afpersen+bedrijven+met+miljoenen+gestolen+klantgegevens> ↵
3. <https://www.bleepingcomputer.com/news/security/shinyhunters-member-pleads-guilty-to-6-million-in-data-theft-damages/> ↵