BLACKFOG™

Exploring The Motivations Behind the Rising Trend of Data Exfiltration



Contents

Overview 3

What’s The Appeal of Data Exfiltration? 4

Data Exfiltration Target Types 7

The Costs of Data Exfiltration 8

How to Prevent Data Exfiltration 10

Looking For Assistance? 11

Take a look at the reasons for the rise of data exfiltration during attacks, including their impact on organizations, the types of data targeted, and the high costs involved. Discover effective prevention strategies, as well as third-generation cybersecurity solutions such as BlackFog's automated ADX.

Data exfiltration is currently a component of 91% of ransomware attacks, according to our 2023 Ransomware Attack Report. This is consistent with the growing pattern of cyber attacks that use data exfiltration for extortion and other purposes. Hackers usually demand a ransom to be paid in order to either provide decryption tools or to keep stolen data hidden. They can take money covertly because of the anonymity that digital currencies offer. Businesses rely heavily on data, and the threat of losing important data gives hackers the leverage to demand a ransom.

1

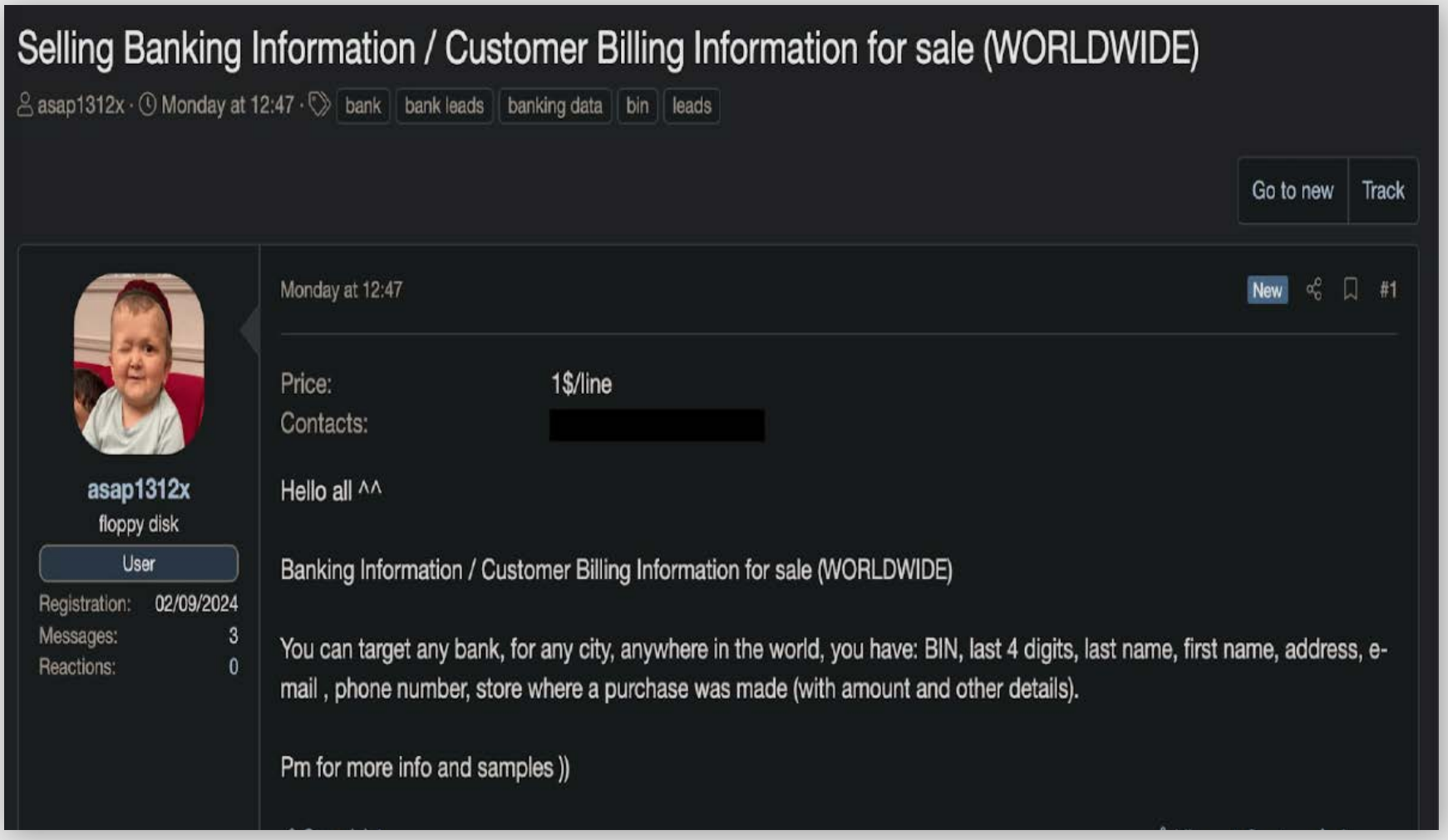
What's The Appeal?

What Makes Data Exfiltration So Appealing to Attackers? A Few Things:

Encrypting an entity's data no longer ensures the leverage attackers once had because many organizations have adopted reliable backup systems.

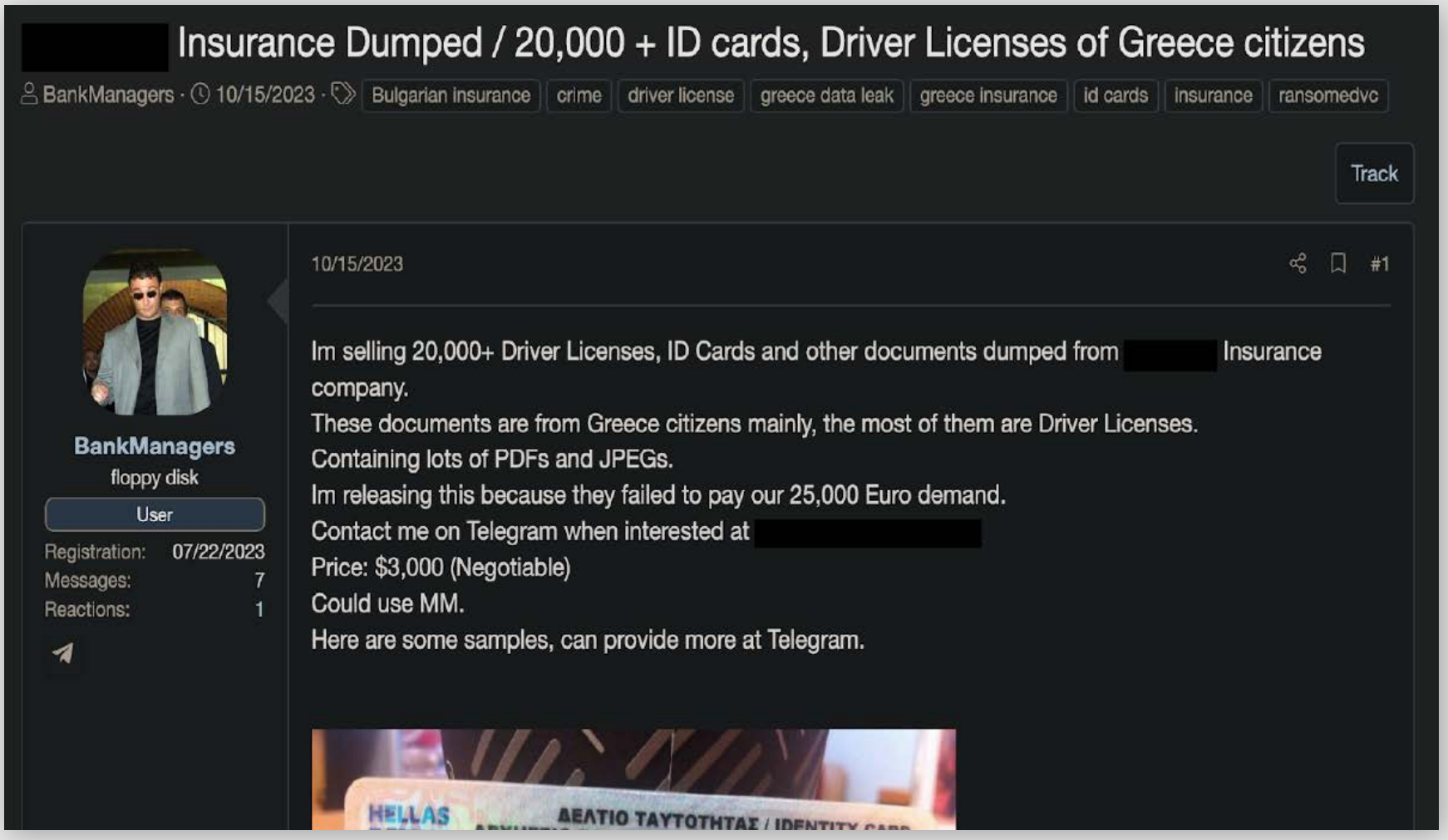
As a result, ransomware attacks that rely solely on data encryption are much less effective. Organizations can resume their operations rather quickly without having to pay a ransom.

Data monetization is another concern. Attackers can sell the stolen information on cybercrime forums and networks, making money off the information, even if the targeted organization chooses not to pay a ransom. On black markets, sensitive data like financial records, intellectual property, and personally identifiable information (PII) can command high prices.



An example of personally identifiable information being sold

Individuals can also become victims on a personal level. The data harvested during exfiltration can be used to victimize individuals directly, through identity theft, financial fraud, or even blackmail. This not only increases the potential revenue for attackers but also amplifies the pressure on the victim organization to meet the attackers' demands.



An example of individual identification documents being shared

Last but not least, regulatory fines play a big role.

A financial penalty for noncompliance with the adoption of stronger regulatory frameworks, like the new SEC rules addressing cybersecurity and data protection, is almost a given when it comes to the unauthorized distribution of data.

Attackers frequently understand that this may be used to apply extra pressure, and as a technique, we have even seen them report victims directly to the SEC in certain instances.

2

Target Types

Hackers Typically Target Different Types of Data Depending on The Victim:

Category	Examples	Rationale/Impact	Industry Examples
Personally Identifiable Information (PII)	Names, addresses, social security numbers	Attractive for identity theft, can be used to commit further crimes	Healthcare, financial services, retail
Operational Data	Transaction records, supply chain details	Less sensitive but critical for business operations; loss poses operational risks	Manufacturing, retail, logistics
Intellectual Property (IP)	Proprietary code, confidential research	Considered the crown jewels of a company; leaks can devastate competitive advantage	Technology, pharmaceuticals, automotive
Internal Corporate Data	Plans, reports, strategy documents	Provides valuable intelligence for competitors, can undermine strategic initiatives	All industries, particularly high-tech and consultancy
Financial Information	Financial statements, banking details, investment strategies	Directly impacts financial integrity and investor confidence; can lead to financial fraud	Financial services, investment firms, corporates

3

The Costs of Data Exfiltration

The Costs of Data Exfiltration Are Steep, Both Immediate and Long-Term:

Cyber attacks involving data exfiltration result in extensive and multifaceted costs, causing immediate and long-term damages to an organization's operations, finances, legal standing, reputation, and even business viability.

Operational impacts include the suspension of business operations, leading to disruptions and downtime in critical systems. This directly affects productivity, transactions, and revenue generation while expenses continue to accumulate. IT resources must also be redirected to conduct forensic analyses, restore backups, patch vulnerabilities, and enhance security measures during this disruptive period.

Victims of data exfiltration often face legal action and class action lawsuits from affected customers and partners seeking damages. Organizations may also incur substantial regulatory fines for violating privacy statutes, such as HIPAA, HITECH, GDPR, and state breach notification laws. These fines can range from tens to hundreds of thousands of dollars per violation.

High-profile cyber attacks not only impact direct victims but also erode trust among consumers in an organization's customer base. This leads to reputational damage and higher customer churn long after the incident. Rebuilding trust and reputation can take years

due to increased public scrutiny and negative perceptions of the brand's security measures.

The reputational fallout also affects an organization's ability to attract new customers and business opportunities. Existing partners and prospects may avoid contracts and transactions due to perceived negligence in cybersecurity and data practices. This directly impacts future revenue streams from both private and public sector clients.

For small and mid-sized businesses (SMBs), the cumulative financial damages, legal liabilities, and loss of customer trust often become overwhelming, leading to operational collapse.

Many are forced to lay off a significant portion of their workforce and ultimately shut down. Even larger enterprises can experience significant drops in valuation and impacts across various business lines.

4

How Can Organizations Prevent Data Exfiltration?

Here are some techniques that organizations should consider to prevent data exfiltration from taking place in the first place:

1. Implement a layered cybersecurity approach with multiple defenses at different points. This includes firewalls, intrusion detection/prevention systems, endpoint protection, access controls, encryption, etc. Traditional cybersecurity solutions struggle to defend against these sophisticated attacks, making a layered approach to more effective.

2. Conduct regular cybersecurity awareness training for all employees. Train them to identify phishing emails and other social engineering techniques that might be used for exfiltration. Educate them on secure practices like strong passwords and not opening unknown attachments.

3. Perform regular data cleanses and analyses to remove sensitive data that is no longer needed. The less sensitive data stored, the lower the risk and potential impact of exfiltration. Properly archive or destroy legacy data.

4. Remove unauthorized or legacy software and applications that are no longer in use. Older unpatched software and applications pose security risks and expand the overall potential attack surface. Conduct audits to identify unused or out of date programs and uninstall/disable them.

5. Use preventative technologies such as anti-data exfiltration (ADX) that monitor and detect attempted unauthorized data transfers. These can detect and block exfiltration attempts in real-time via email, web upload, removable media or other exfiltration vectors.

5

Looking For Assistance?

Take Your Next Steps with BlackFog

When it comes to cyber attacks, data exfiltration is the end goal. The attackers cannot succeed in the absence of it. Absence of data exfiltration means absence of extortion, ransomware, and data breaches.

These days, a solid cybersecurity strategy must include third-generation cybersecurity solutions that prioritize stopping data exfiltration.

BlackFog's fully automated, round-the-clock ADX technology guards against cyber attacks in real time and makes sure that even if hackers are able to get past conventional defenses, they won't be able to erase any data. Click here to schedule a demo.

BLACKFOG™

ABOUT BLACKFOG

BlackFog is the leader in on-device data privacy, data security and ransomware prevention. Our behavioral analysis and anti data exfiltration (ADX) technology stops hackers before they even get started. Our cyberthreat prevention software prevents ransomware, spyware, malware, phishing, unauthorized data collection and profiling and mitigates the risks associated with data breaches and insider threats. BlackFog blocks threats across mobile and desktop endpoints, protecting organizations data and privacy, and strengthening regulatory compliance.

All contents copyright © 2024 BlackFog, Inc. All rights reserved. The BlackFog logo and name are trademarks of BlackFog, Inc. All other trademarks are the property of their respective owners.

Except as specifically stated herein, none of the material may be copied, reproduced, distributed, republished, downloaded, displayed, posted, or transmitted in any form without authorized, prior written permission from BlackFog, Inc. Permission is granted for you to make a single copy of this document solely for informational uses within your organization, provided that you keep intact all copyright and other proprietary notices. No other use of the information provided is authorized.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners. The information contained in this document represents the current view of BlackFog, Inc. on the issues discussed as of the date of publication.
