ON2IT AND AMS-IX PRESENT: THREAT TALKS

Threat Talks
Data Exfiltration

threat-talks.com

How attackers extract sensitive data from your environment

Data exfiltration is the unauthorized transfer of data from a network, typically after an attacker has already gained access. It's a common goal in many cyber incidents, whether the motive is financial, strategic, or political.

Attackers often use legitimate channels to move data, including HTTPS, FTP, and cloud apps, which helps them avoid detection. In more advanced operations, they may obfuscate stolen data within other network traffic or split it into chunks to avoid triggering security tools.

In 2020, cybercriminals exfiltrated hundreds of millions of customer records from Microsoft and Facebook alone. For individuals, data that is stolen through exfiltration can result in costly consequences such as identity theft, credit card or bank fraud and blackmail or extortion. For organizations, the consequences are at the very least more costly, ranging from disrupted operations to compromised trade secrets, and loss of customer trust to regulatory fines.

If attackers were inside your network right now, would you know? How long could they stay hidden? Could your systems catch the signs of data slipping out in real time?

In this Threat Talks infographic we will discuss the following threat:

- Data bouncing

65%

of organizations experienced data exfiltrations in 2023

Source: Proofpoint 2024 Voice of the CISO Report

63%

of data breaches involve credential data being exfiltrated

Source: Verizon DBIR 2025

204

the average time to detect a data exfiltration incident is 204 days

Source: IBM Cost of a Data Breach Report 2024

94%

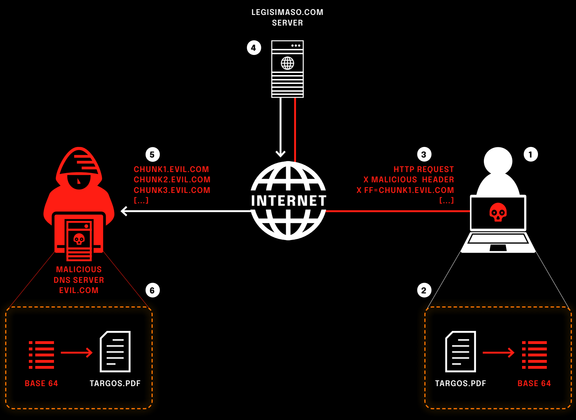
of ransomware attacks in 2024 featured data exfiltrations

Source: BlackFog's 2024 State of Ransomware Annual Report

Data bouncing

How to disguise stolen data's trail

Data bouncing involves routing stolen data through multiple intermediate servers (like compromised hosts, VPNs, or anonymizers) before reaching its final destination. This tactic hides the original source and complicates forensic tracking and attribution.



1. Initial Compromise

The attacker gains unauthorised access to the victim system, either directly or by deploying a malware.

2. Preparing the Data for Exfiltration

The attacker encodes the target binary contents in Base64, and splits the result into small chunks.

3. Exfiltration via Data Bouncing

Each Base64 chunk is embedded in subdomains of attacker-controlled domains (e.g., chunk1.evil.com, chunk2.evil.com, etc.). These subdomains are inserted into HTTP headers, such as X-Forwarded-For, Referrer, or Client-IP, and sent in requests to legitimate but "vulnerable" servers.

4. The "Helper" Servers

The legitimate servers, due to reasons like logging, threat intelligence enrichment, proxy resolution, or DNS-based geolocation, resolve the crafted subdomains, unwittingly helping the attacker by forwarding DNS queries.

5. Interception by Malicious DNS

The attacker's DNS server (e.g., evil.com) receives and logs the DNS queries, each containing a chunk of the Base64-encoded data.

6. Rebuilding the Stolen Data

The attacker collects all logged chunks, reorders them if needed, concatenates them, and decodes the Base64 string to reconstruct the original binary file.

threat-talks.com

ON2IT ZERO TRUST INNOVATORS

amsix

CONTACT US