SOCRadar®

Your Eyes Beyond

NETHERLANDS

Threat Landscape Report

2024

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary

The Netherlands, known for its progressive digital economy and strategic location in Europe, has become a focal point for cyber threats in recent years. As a leading hub for technology, finance, and logistics, the Dutch economy is intricately woven into the global digital fabric, making it a prime target for cybercriminals and state-sponsored threat actors.

Recent data indicates a sharp rise in cyber-attacks targeting Dutch critical infrastructure and key industries. These attacks are becoming increasingly sophisticated, as the evolving tactics, techniques, and procedures (TTPs) of these threat actors reflect a growing trend toward more complex and targeted cyber operations.

The Netherlands has seen an influx of cyber threats from various sources, including organized crime groups and nation-state actors. The country's prominence in international trade and its advanced technological infrastructure make it a lucrative target for cyber espionage, financial theft, and disruptive attacks.

The dark web plays a pivotal role in facilitating these cyber threats, providing a platform for exchanging malicious tools, stolen data, and illicit services. The anonymity offered by the dark web presents significant challenges for Dutch cybersecurity professionals in preempting and mitigating these threats.

This report delves into the detailed analysis of the threat landscape in the Netherlands, utilizing comprehensive data from both open-source and proprietary intelligence. By monitoring cyber activity and analyzing attack patterns, our team provides an in-depth overview of the threats faced by Dutch entities. The insights presented in this report aim to empower stakeholders across public and private sectors to bolster their cybersecurity measures, mitigate risks, and enhance the resilience of the Netherlands against future cyber threats.

Top Takeaways

Dark Web Dynamics

In 2023, a diverse group of 72 threat actors actively targeted Dutch enterprises, collectively posting 158 times on the dark web, predominantly trading in database sales, which underscores the criticality of data security measures.

Dark Eyes On Retail Trade

The retail trade industry, making up 14.81% of dark web activities, stood out as the primary industry targeted by threat actors worldwide, highlighting its strategic importance and vulnerability to digital threats.

Ransomware Resurgence

The Netherlands grappled with 186 unique ransomware incidents throughout the year, with 62 attacks pinpointing the country as the primary target, revealing a focused aggression by threat actors.

Notorious Ransomware Syndicates

Prominent ransomware groups, including Cl0p, LockBit 3.0, and ALPHV Blackcat, specifically targeted the Netherlands, signifying the high stakes and sophistication of the country's cyber threat landscape.

Top Takeaways

Stealer Logs

The widespread use of Stealer Logs in 2023 led to significant breaches, compromising critical data for thousands of individuals across the Netherlands.

Phishing in the Digital Economy

The year also saw 3,077 phishing attacks, with a marked emphasis on the emerging industry of Banking, casting a spotlight on the growing cyber risks in these innovative financial technologies.

Unprecedented DDoS Attacks

The Netherlands experienced a landmark DDoS attack involving 23 vectors and achieving a maximum bandwidth of 590 Gbps amidst a total of 48,178 DDoS incidents, illustrating the intense and escalating cyber assault landscape.

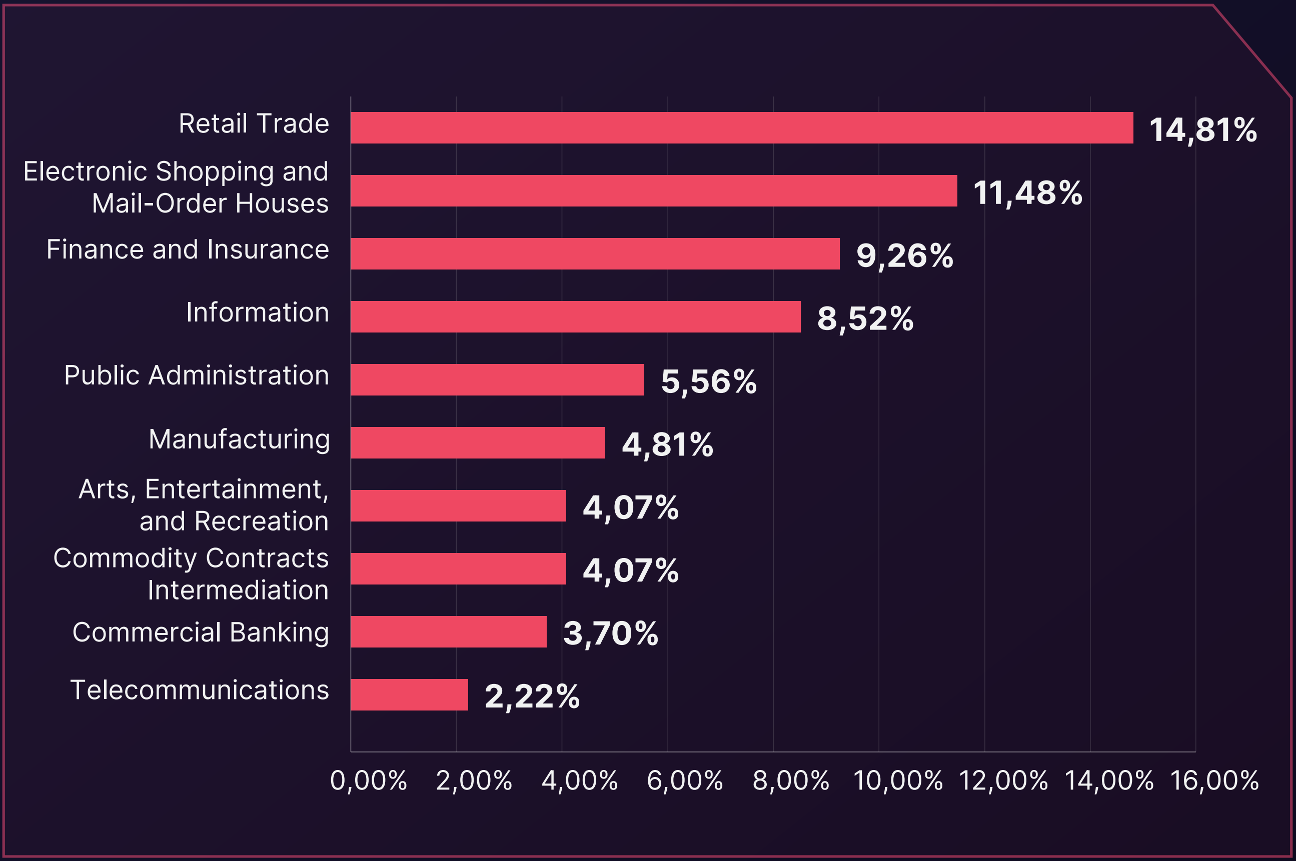
Technical Details

Dark Web Threats Targeting Dutch Entities

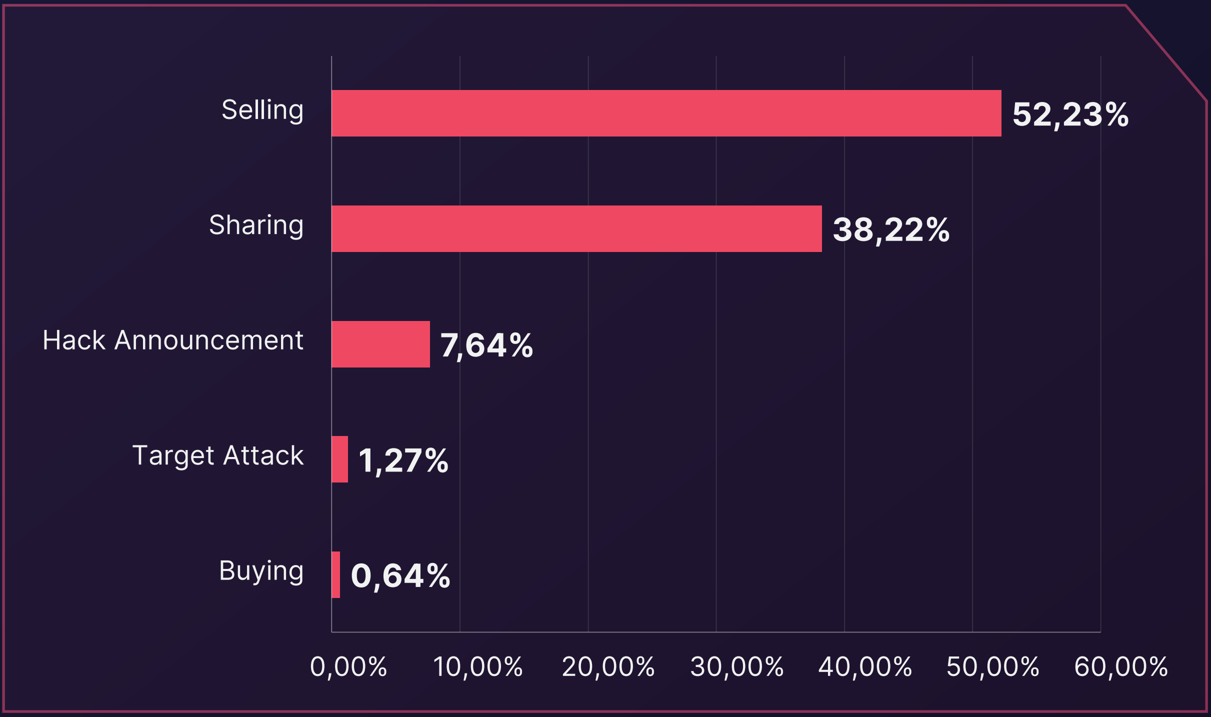
Over the preceding year, SOCRadar's Dark Web Analysts diligently monitored activities within the dark web, identifying notable trends and establishing connections between enterprises in the Netherlands and covert threat actors. Throughout 2023, Dutch entities encountered a continuous barrage of cyber threats, with various actors attempting to exploit successful intrusions by trading or leveraging their gains in dark web forums.

During this period, SOCRadar observed 158 dark web forum posts linked to 72 distinct threat actors. Retail trade emerged as the most prominently affected industry among the targeted industries, representing 14.81% of the identified cyber threats during this period. Following closely behind, Electronic Shopping and Mail-Order Houses and Finance and Insurance industries accounted for 11.48% and 9.26% respectively.

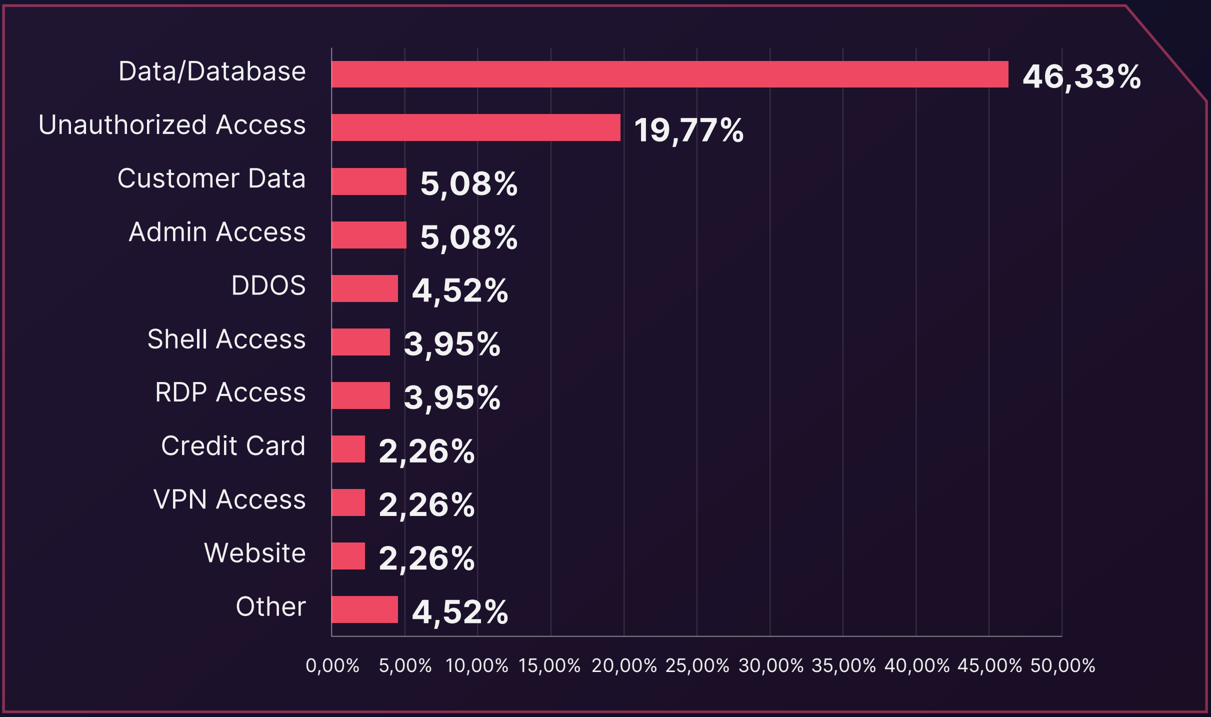
Industry Distribution of Dark Web Threats



Distribution of Dark Web Threats by Post Type



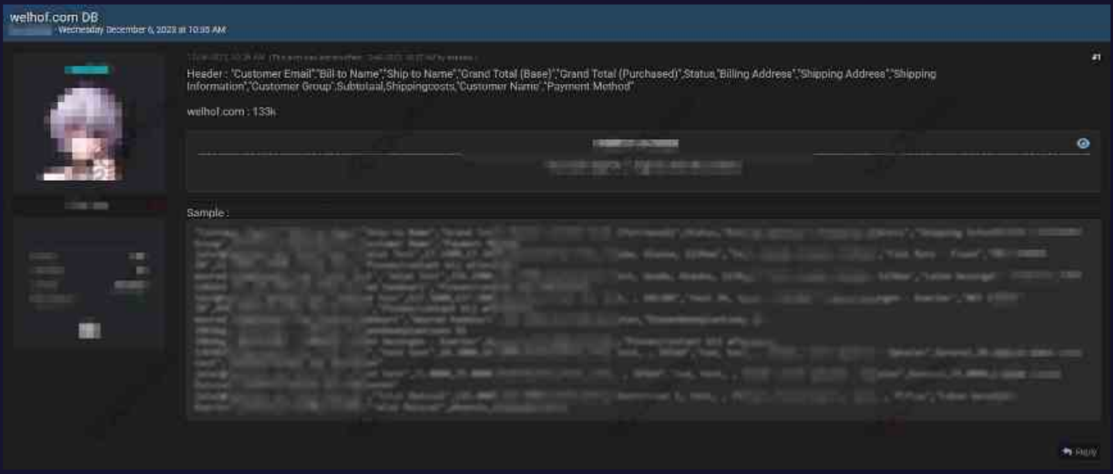
Distribution of Dark Web Threats by Threat Type



Recent Dark Web Activities Targeting Dutch Entities

06 Dec
2023

Database of Welhof is Leaked



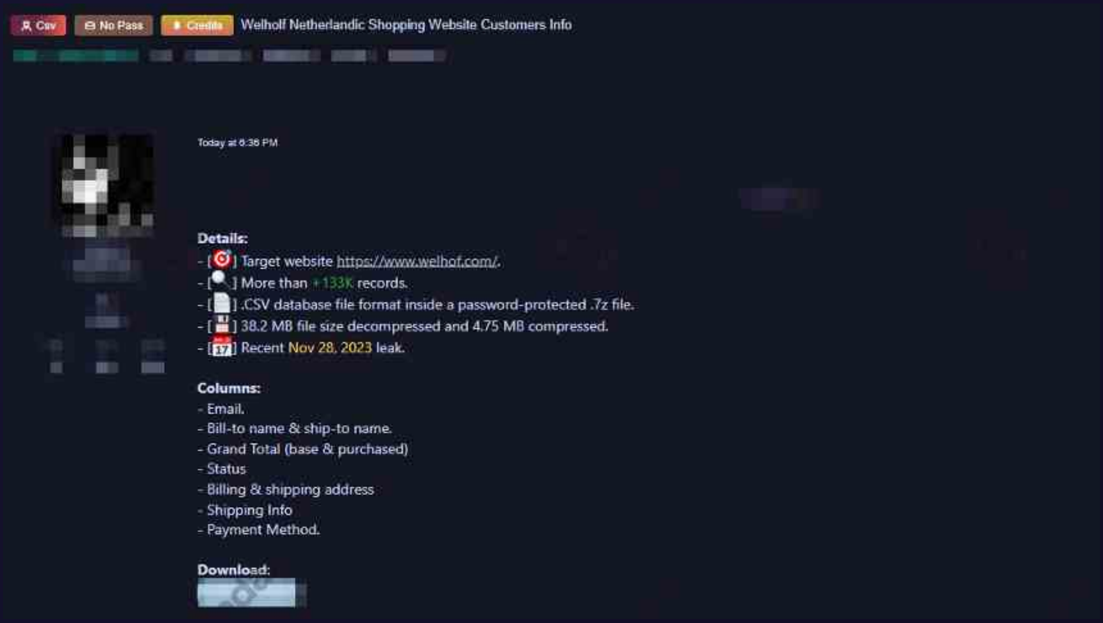
welhof.com DB
Wednesday December 6, 2023 at 10:35 AM

Header : "Customer Email","Bill to Name","Ship to Name","Grand Total (Base)","Grand Total (Purchased)",Status,"Billing Address","Shipping Address","Shipping Information","Customer Group",Subtotaal,Shippingcosts,"Customer Name","Payment Method"

welhof.com : 133k

Sample :

[redacted]



Csv No Pass Credits Welholf Netherlandic Shopping Website Customers Info

Today at 6:36 PM

Details:
- [🎯] Target website https://www.welhof.com/.
- [🔍] More than +133K records.
- [📄] .CSV database file format inside a password-protected .7z file.
- [💾] 38.2 MB file size decompressed and 4.75 MB compressed.
- [📅] Recent Nov 28, 2023 leak.

Columns:
- Email.
- Bill-to name & ship-to name.
- Grand Total (base & purchased)
- Status
- Billing & shipping address
- Shipping Info
- Payment Method.

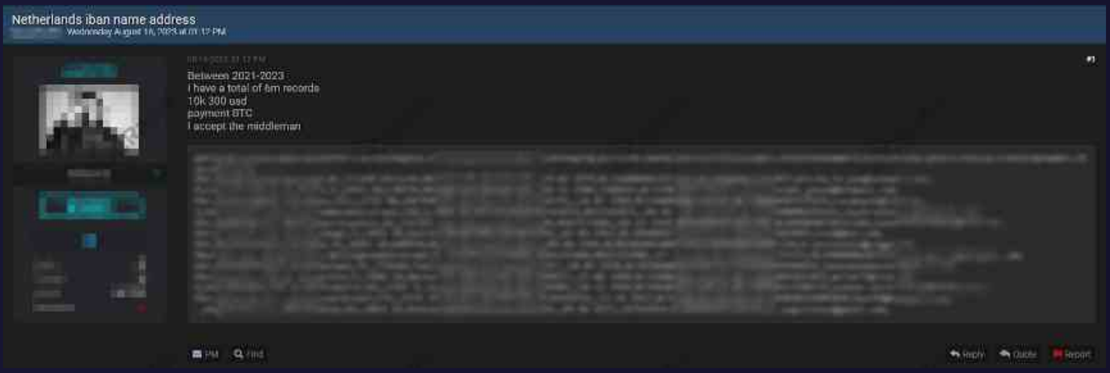
Download:

Screenshots of the forum post - Welhof DB is for sale

In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for Welhof, an online retail trade company. The leaked database contains sensitive customer information belonging to over 133,000 customers, including email addresses, billing and shipping addresses, order details, and payment methods.

16 Aug
2023

Data of Dutch Citizens are on Sale



Netherlands iban name address
[redacted] Wednesday August 16, 2023 at 01:12 PM

Between 2021-2023
I have a total of 6m records
10k 300 usd
payment BTC
I accept the middleman

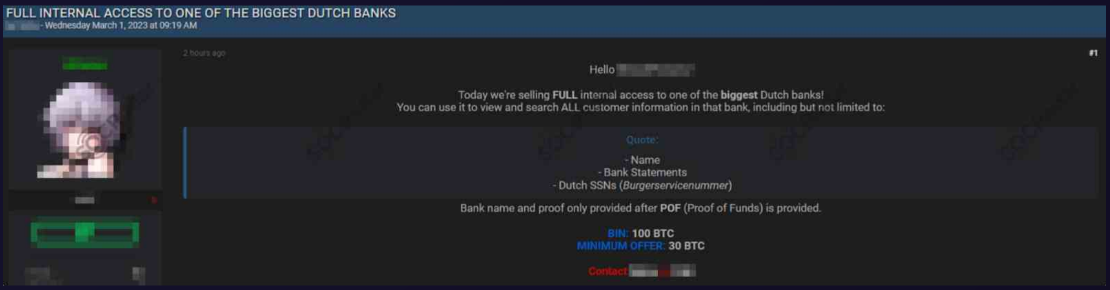
[redacted]

Screenshot of the forum post - Dutch Citizens' data

In a hacker forum monitored by SOCRadar, the personal information of 6 million Dutch citizens, including names, addresses, phone numbers, email addresses, and bank account details, is being sold on a hacker forum for $300 USD in Bitcoin, with the seller accepting middlemen for the transaction.

01 Mar
2023

Unauthorized Access Sale is Detected for a Dutch Bank



FULL INTERNAL ACCESS TO ONE OF THE BIGGEST DUTCH BANKS
[redacted] - Wednesday March 1, 2023 at 09:19 AM

2 hours ago

Hello [redacted]

Today we're selling **FULL** internal access to one of the **biggest** Dutch banks!
You can use it to view and search ALL customer information in that bank, including but not limited to:

> Quote:
>
> - Name
> - Bank Statements
> - Dutch SSNs (*Burgerservicenummer*)

Bank name and proof only provided after **POF** (Proof of Funds) is provided.

BIN: **100 BTC**
MINIMUM OFFER: **30 BTC**

Contact [redacted]

Screenshot of the forum post - Unauthorized access PoC being sold

In a hacker forum monitored by SOCRadar, an unauthorized access sale is detected, allegedly belonging to a bank that operates in the Netherlands. The access allegedly allows the buyer to view and search all customer information, including names, bank statements, and SSNs.

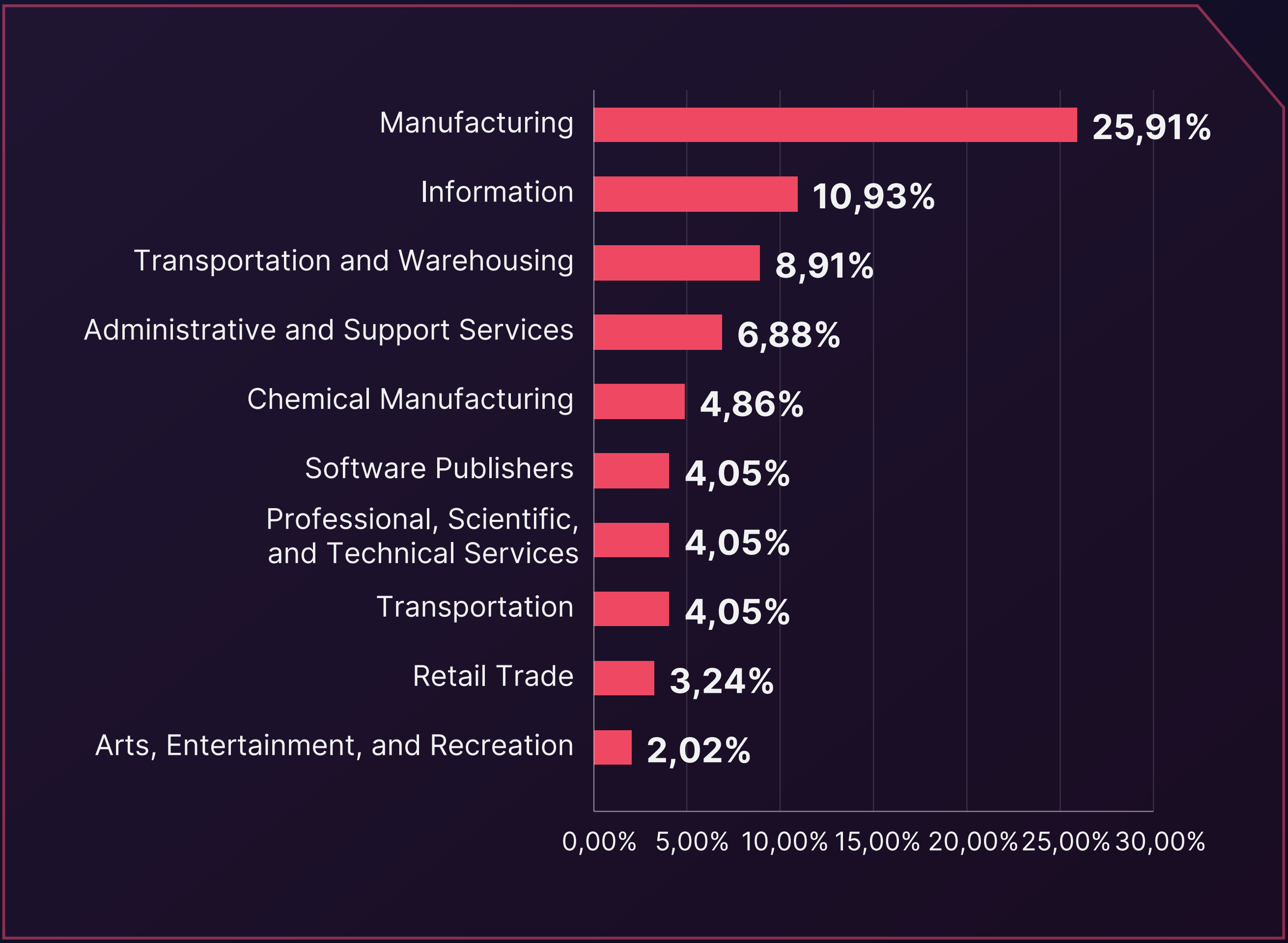
Ransomware Attacks Targeting Dutch Entities

Ransomware attacks represent significant threats to organizations, often resulting in dire consequences such as extensive data loss and the exposure of sensitive information. SOCRadar's surveillance has identified 186 instances of ransomware victim notifications attributable to various ransomware threat actors and/or groups.

Of the 186 ransomware attacks referenced, the Netherlands emerges as the primary target in 62 cases, with the nation also featuring among the most affected countries in the remaining 124 global incidents.

Manufacturing emerges as the most prominently affected sector among the targeted industries, representing 25.91% of the identified ransomware attacks during this period. Following this, the Information industry accounted for 10.93% of the attacks, while the Transportation and Warehousing industry experienced 8.91% of the ransomware incidents.

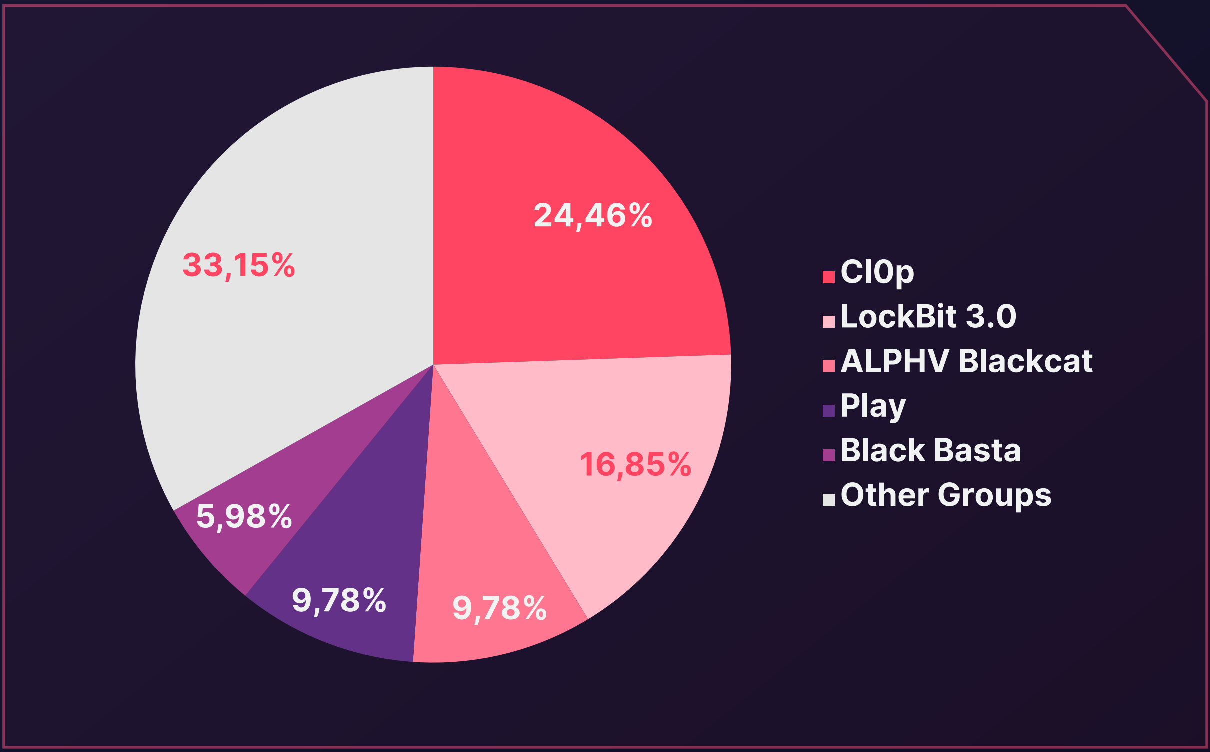
Distribution of Ransomware Attacks by Industry



Top Ransomware Groups Targeting the Netherlands

When examining the top ransomware groups targeting the Netherlands, Cl0p emerges as the most prolific threat, accounting for 24.46% of the attacks. Following closely, LockBit 3.0 represents 16.85% of the ransomware incidents, while both ALPHV Blackcat and Play contribute 9.78% to the total. Following closely behind, Black Basta accounted for 5.98% of the ransomware attacks. The remaining 33.15% is attributed to various other ransomware groups.

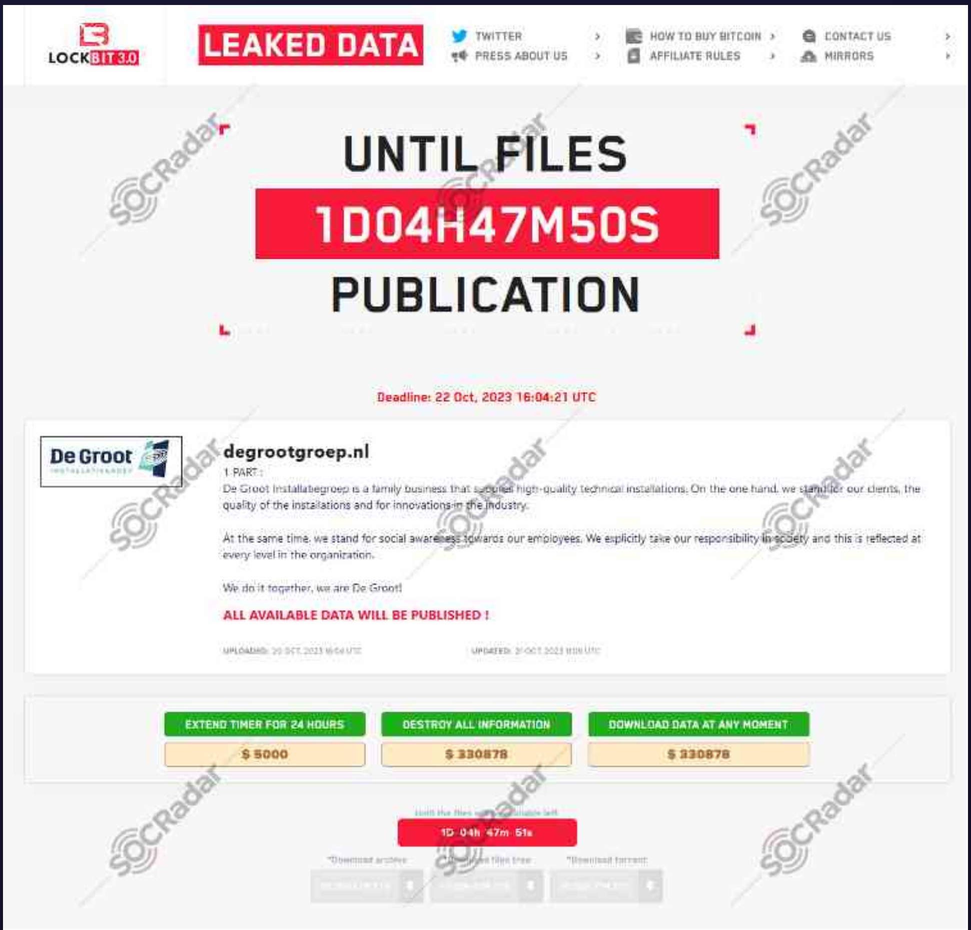
Top Ransomware Groups Targeting Targeting Netherlands



Recent Ransomware Attacks Targeting Dutch Entities

20 Oct
2023

The New Ransomware Victim of Lockbit 3.0: De Groot Installatiegroep



Deadline: 22 Oct, 2023 16:04:21 UTC

degrootgroep.nl

1 PART :

De Groot Installatiegroep is a family business that supplies high-quality technical installations. On the one hand, we stand for our clients, the quality of the installations and for innovations in the industry.

At the same time, we stand for social awareness towards our employees. We explicitly take our responsibility in society and this is reflected at every level in the organization.

We do it together, we are De Groot!

ALL AVAILABLE DATA WILL BE PUBLISHED !

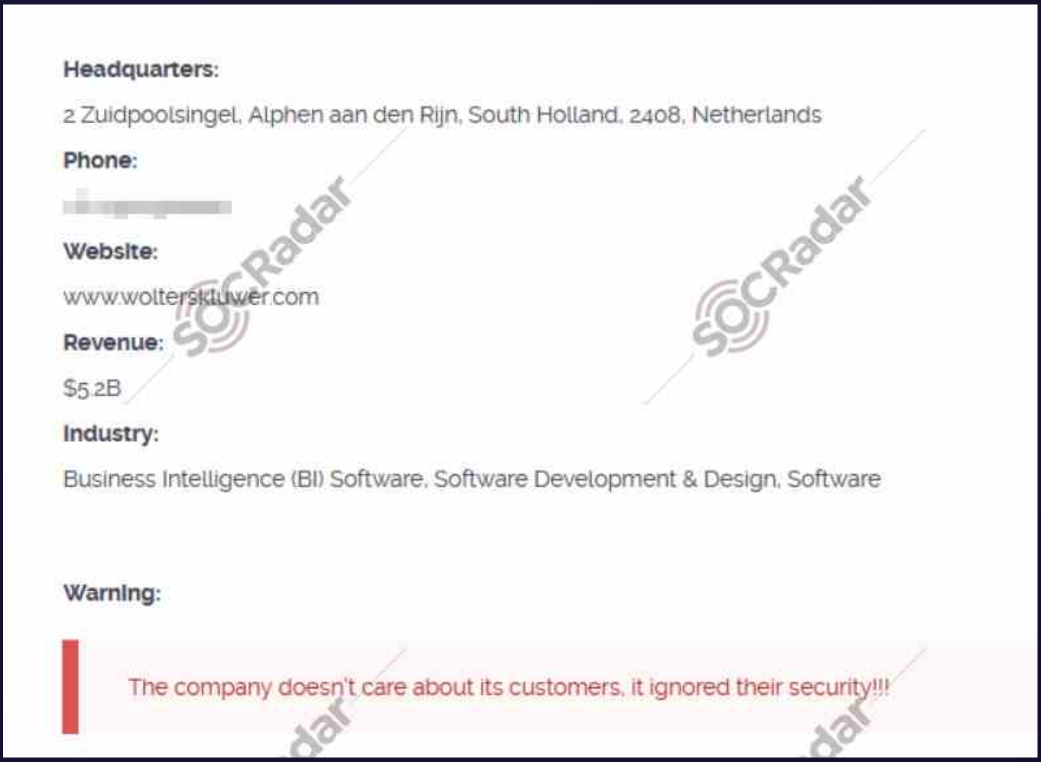
UPLOADED: 20 OCT, 2023 16:04 UTC UPDATED: 21 OCT, 2023 11:06 UTC

Screenshot from Lockbit 3.0 ransomware group's website

In the Lockbit 3.0 ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as De Groot Installatiegroep, a Dutch company specializing in technical installations. The ransomware group has published a ransom demand and threatens to release stolen data if the ransom is not paid.

06 July
2023

The New Ransomware Victim of Cl0p: Wolters Kluwer



Headquarters:

2 Zuidpoolsingel, Alphen aan den Rijn, South Holland, 2408, Netherlands

Phone:

[redacted]

Website:

www.wolterskluwer.com

Revenue:

$5.2B

Industry:

Business Intelligence (BI) Software, Software Development & Design, Software

Warning:

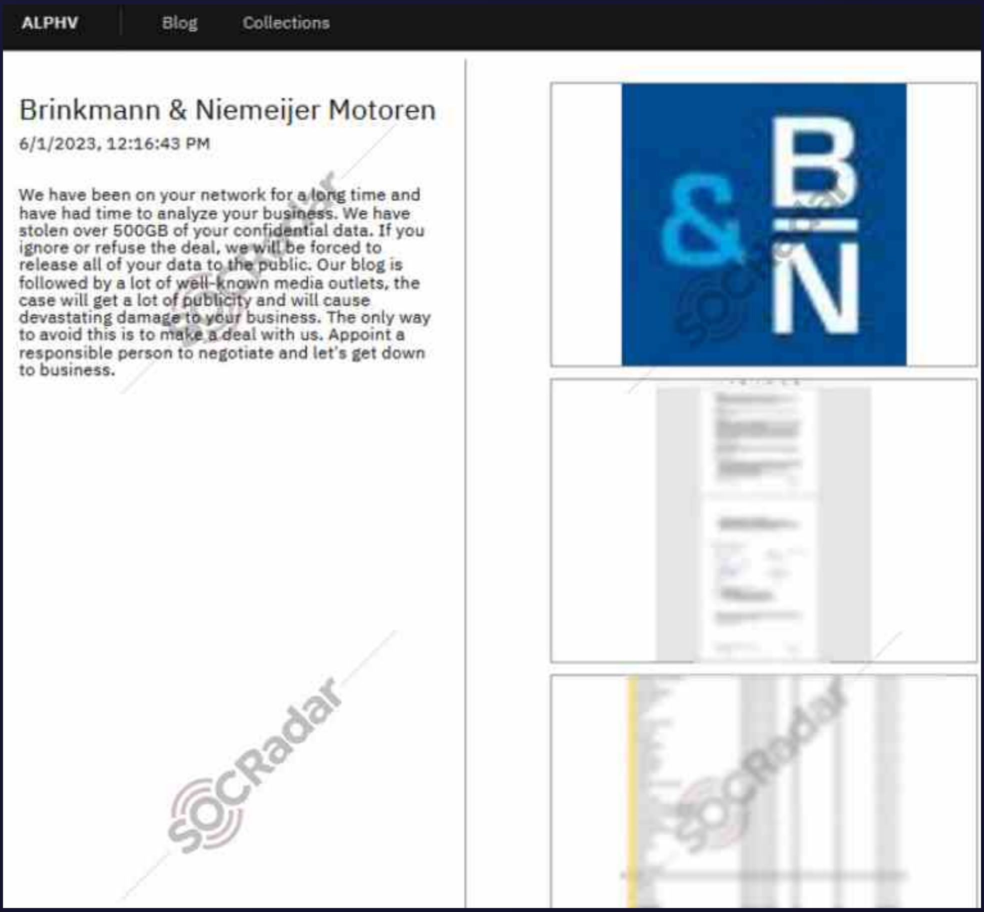
The company doesn't care about its customers, it ignored their security!!!

Screenshot from Cl0p ransomware group's website

In the Cl0p ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as Wolters Kluwer, a business intelligence software company. Following the interventions and investigations conducted by Wolters Kluwer officials, it was confirmed that customer data remained uncompromised. However, service interruptions occurred both during and after the intervention process.

02 Jun
2023

The New Ransomware Victim of ALPHV Blackcat: Brinkmann & Niemeijer Motoren



Brinkmann & Niemeijer Motoren

6/1/2023, 12:16:43 PM

We have been on your network for a long time and have had time to analyze your business. We have stolen over 500GB of your confidential data. If you ignore or refuse the deal, we will be forced to release all of your data to the public. Our blog is followed by a lot of well-known media outlets, the case will get a lot of publicity and will cause devastating damage to your business. The only way to avoid this is to make a deal with us. Appoint a responsible person to negotiate and let's get down to business.

Screenshot from ALPHV ransomware group's website

In the ALPHV / Blackcat ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Brinkmann & Niemeijer Motoren. The attackers claim to have stolen over 500GB of confidential data and threaten to release it publicly if a ransom is not paid.

Top Threat Actors Targeting Dutch Organizations

Cl0p Ransomware Group

Country of Origin: Russia

A Ransomware group that has been active since 2019 and currently brings up its name by exploiting zero-day vulnerabilities that existed in GoAnyWhere MFT and MOVEit MFT software.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	The US, Canada, The UK, Australia, Colombia, Sweden, Germany, India, Mexico, Turkey
Target Sectors:	IT, Healthcare, Finance, Professional Services, Retail, Media, Telecommunication
Attack Type:	Spearphishing, Zero-Day Exploitation, Compromised RDP, Ransomware, Data exfiltration, Double-extortion

-TTPs-

Exploit Public-Facing Application:	T1190
Exploitation for Privilege Escalation:	T1068
Exfiltration Over C2 Channel:	T1041

Cl0p is a cybercriminal entity recognized for its sophisticated extortion tactics and widespread dissemination of malware across the globe. The word “clop” comes from the Russian word “klop,” which means “bed bug,” a Cimex-like insect that feeds on human blood at night (mosquito). A distinguishing feature of Cl0p is the string “Don’t Worry C|0P” found in the ransom notes.

With a track record of extorting over $500 million in ransom payments, the group focuses on major organizations on a global scale. Gaining infamy in 2019, Cl0p ransomware group has executed notable attacks, employing extensive phishing initiatives and advanced malware to breach networks and coerce ransom payments, leveraging the threat of data exposure if demands remain unmet.

For more detailed information about the Cl0p Ransomware Group, you can visit our blog post.

Lockbit 3.0 Ransomware Group

Country of Origin: Russia

The most successful RaaS group operating since 2019. The group is continuously evolving and is highly active in deploying models such as double-extortion and initial access broker affiliates.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, Europe, Thailand, Taiwan
Target Sectors:	Manufacturing, Professional Services, IT, Healthcare, Finance, Education, Legal Services
Attack Type:	Phishing, RDP and VPN access Exploitation, Ransomware, Data Exfiltration, Double-extortion

-TTPs-

Exploit Public-Facing Application:	T1190
Remote Desktop Protocol:	T1021.001
Data Encrypted for Impact:	T1486

LockBit 3.0, a successor to LockBit and LockBit 2.0, operates as a Ransomware-as-a-Service (RaaS) group. Since January 2020, LockBit has shifted to an affiliate-based model, employing various tactics to target businesses and critical infrastructure organizations. They are known for employing strategies like double extortion and initial access broker affiliates, as well as recruiting insiders and hosting hacker recruitment contests. With over 1,500 victim announcements on the SOCRadar platform, LockBit emerged as the most active ransomware group in 2022 following Conti's shutdown. As of the first quarter of 2023, they remain the most prolific group, boasting over 300 announced victims.

For more detailed information about the Lockbit 3.0 Ransomware Group, you can visit our blog post.

ALPHV Blackcat Ransomware Group

BlackCat Ransomware

Country of Origin: Russia

BlackCat, or ALPHV, is a ransomware group known for being the pioneer to use Rust and the group first announced its RaaS affiliate program in a dark web forum in December 2021.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, Germany, Australia, France, Italy, Spain
Target Sectors:	Professional Services, Manufacturing, Healthcare, Finance, Information Technology
Attack Type:	Spearphishing, Stolen Credentials, RaaS, Ransomware, Triple-Extortion

-TTPs-

User Execution: Malicious File:	T1204.002
Defacement:	T1491
Data Encrypted for Impact:	T1486

BlackCat, or ALPHV, is a ransomware group known for being the first to use Rust -a cross-platform language programming language that allows for easy malware customization for different operating systems, such as Windows and Linux- successfully. The group has been able to evade detection and successfully encrypt their victims’ files by using Rust, which allows them to target multiple operating systems and bypass security controls that are not designed to analyze malware written in Rust.

For more detailed information about the ALPHV BlackCat Ransomware Group, you can visit our blog post.

Play Ransomware Group

Play Ransomware

Country of Origin: Unknown

Play Ransomware (PlayCrypt) is a ransomware group first observed in June 2022. The group commonly targets organizations based in Latin America but mainly focuses on Brazil.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	Latin America, India, Hungary, Spain, Netherlands, United States
Target Sectors:	Manufacturing, Education, Real Estate, Technology, Transportation, Healthcare
Attack Type:	Compromised Valid Accounts, LOLBins, Ransomware, Data Exfiltration

-TTPs-

Process Injection:	T1055
Input Capture:	T1068
Proxy:	T1090

Play Ransomware is a ransomware group notorious for their advanced tactics and the use of intermittent encryption, a method that allows them to partially encrypt files and evade detection. Initially observed in 2022, they target exposed RDP servers and exploit vulnerabilities in FortiOS to gain network access. Their operations include double extortion, where they threaten to leak stolen data if ransoms are not paid. The group has targeted various sectors, including IT companies, banks, and governmental organizations.

For more detailed information about the Play Ransomware Group, you can visit our blog post.

Black Basta Ransomware Group

Black Basta

Country of Origin: Russia

Black Basta is a ransomware group that has been active since April 2022 and they employ a double-extortion attack technique. The group was also observed to be linked to the FIN7(Carbanak).

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	North America and Europe
Target Sectors:	Manufacturing, Construction, Professional Services, Finance, Healthcare
Attack Type:	Valid Credentials, RaaS, Ransomware, Double-extortion

-TTPs-

Valid accounts:	T1078
Phishing: Spear-phishing attachment:	T1566.001
Exfiltration over C2 channel:	T1041

Black Basta is a notorious ransomware group that emerged in April 2022. Known for its double-extortion tactics, the group primarily targets western countries, with the United States being the most affected. Their attacks span various sectors, including manufacturing, healthcare, and more. Black Basta employs sophisticated methods such as social engineering and leveraging stolen credentials to gain initial access. They encrypt files using the ChaCha20 cipher and demand high ransoms, often reaching millions of dollars.

For more detailed information about the Black Basta Ransomware Group, you can visit our blog post.

Stealer Log Statistics
Top Domains in the Netherlands

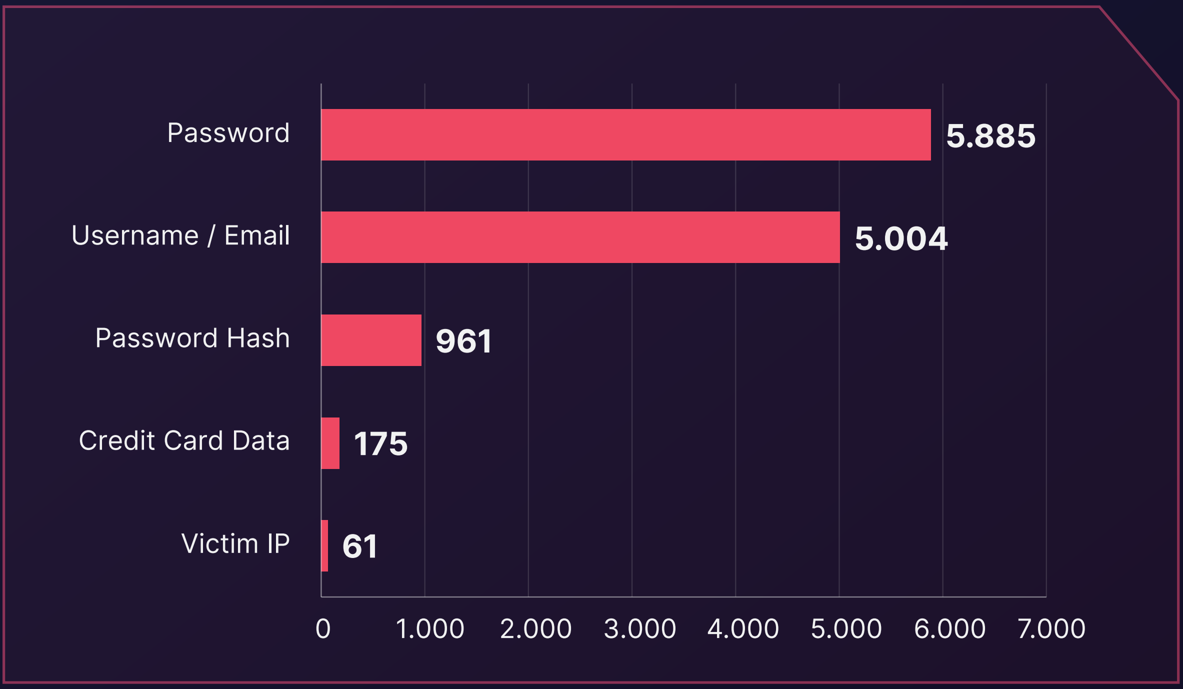
Throughout 2023, thousands of users' user IDs/email addresses, passwords, credit card data, password hashes, and victim IP address information were compromised via Stealer Logs from the computers of users who have accounts or access to some of the highest traffic domains in the Netherlands.

The table below lists the domains associated with the Netherlands with the highest traffic.

nu.nl
ad.nl
buienradar.nl
nos.nl
telegraaf.nl
markplaats.nl
funda.nl
npo.nl
digid.nl
ing.nl

The graph below showcases the distribution of the compromised user data obtained through Stealer Logs across the highest-traffic domains associated with the Netherlands.

Stealer Logs - Compromised Data



The data reveals significant dissemination of compromised information, including **5,885** passwords, **5,004** usernames/emails, **961** password hashes, **175** credit card data entries, and 61 compromised victim IPs, each representing significant instances of compromise.

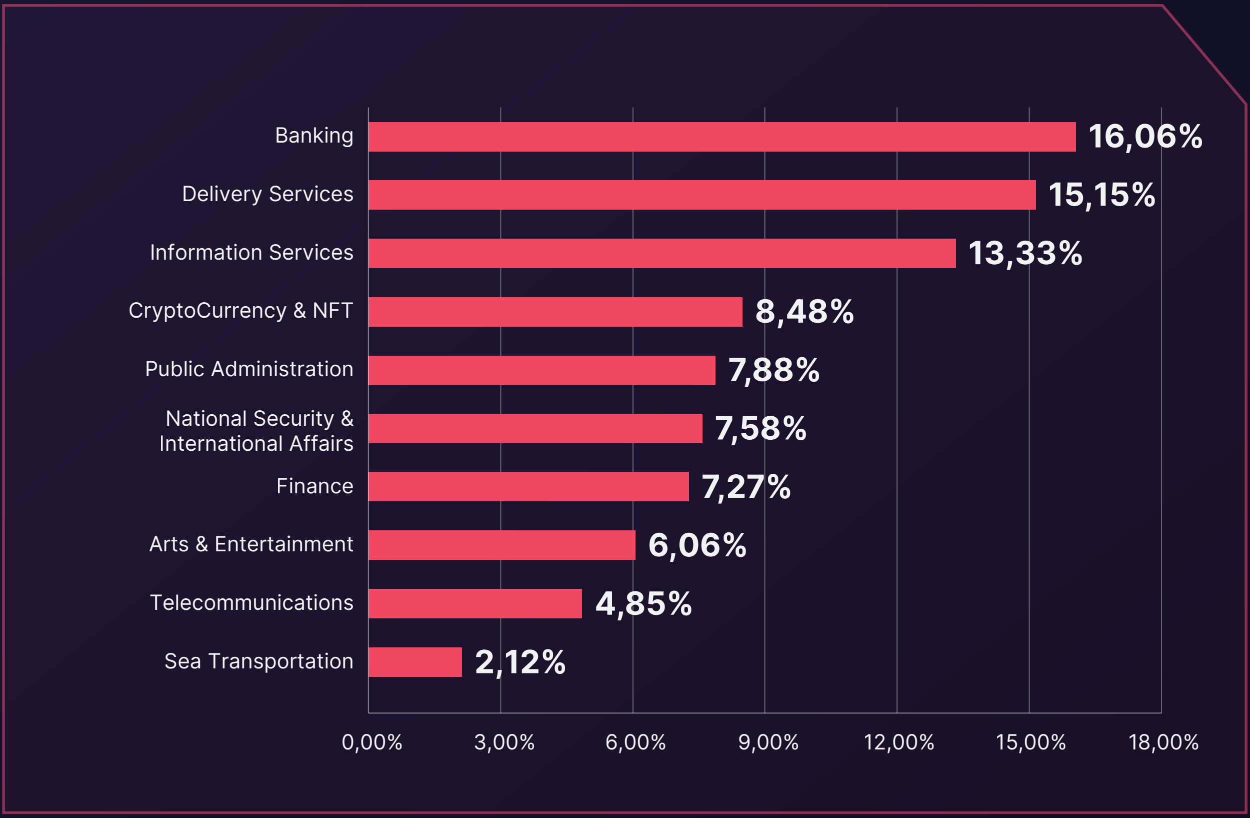
These discoveries emphasize the gravity of data compromise occurrences impacting users in the digital sphere of the Netherlands emphasizing the urgent necessity for robust cybersecurity protocols to efficiently alleviate such risks.

Phishing Threats Targeting the Netherlands

Phishing is an effective method to initially breach an organization's infrastructure by deceiving individuals into divulging sensitive credentials on fraudulent websites.

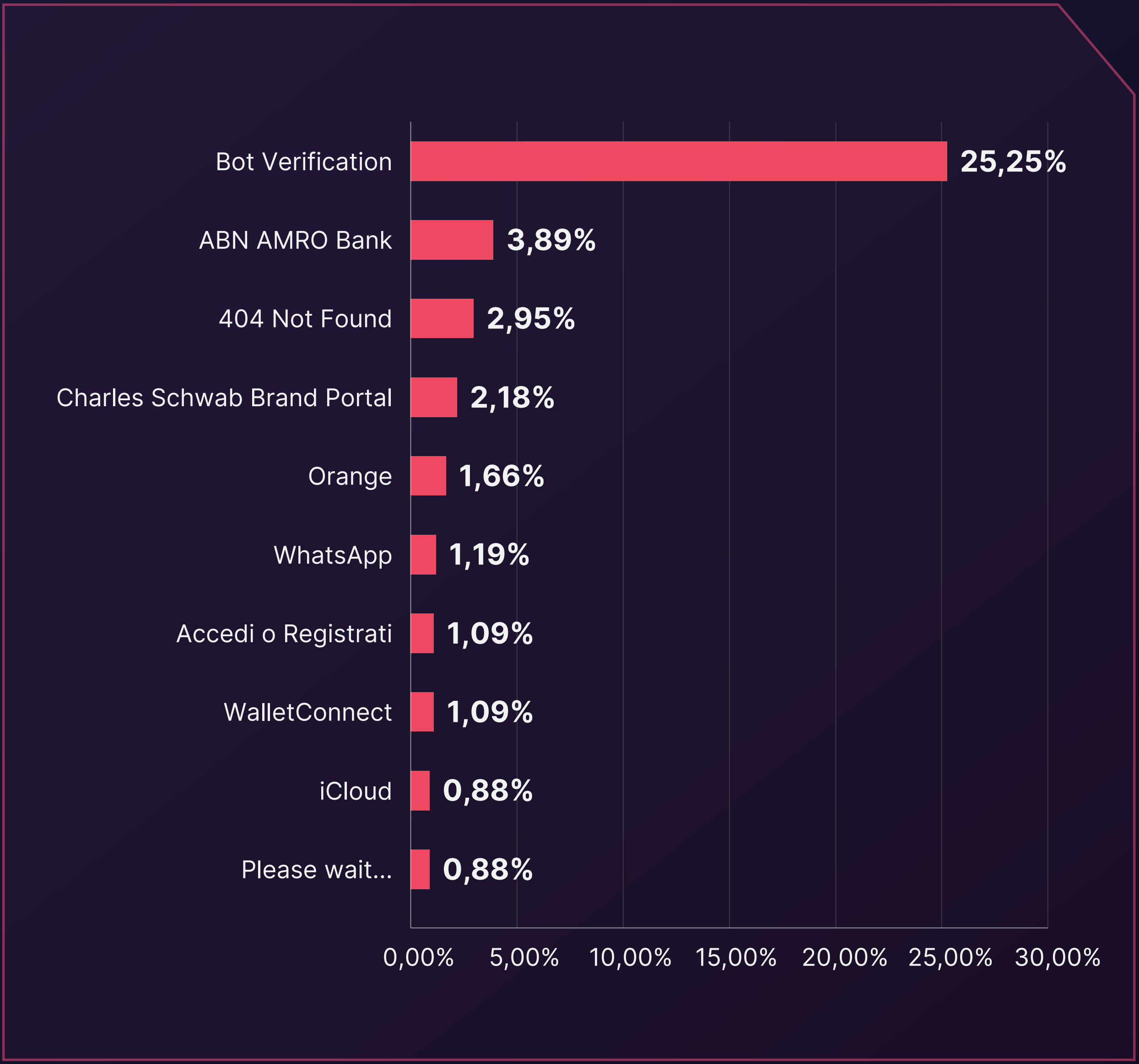
Typically, phishing attacks are coupled with social engineering tactics to acquire such credentials. Over the past year, Dutch enterprises have encountered **3,077 distinct instances of phishing attacks**, primarily targeting the **Banking** industry.

Phishing Attacks - Distribution by Industry



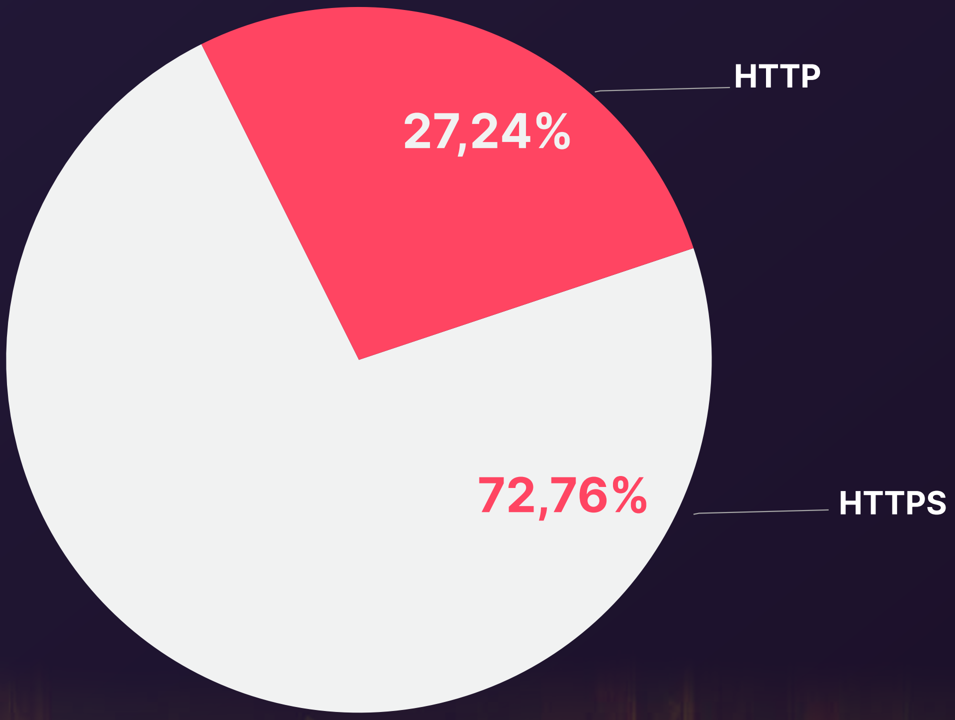
The graph below illustrates the distribution of Page Titles used by threat actors for phishing attacks. Notably, the data reveals a predominant usage of the **Bot Verification** page title.

Phishing Attacks - Distribution by Phishing Page Title



When closely examining the SSL/TLS protocols of domains prepared for phishing attacks by threat actors, we observe an increasing trend in the usage of HTTPS compared to the past.

Phishing Attacks- Distribution by SSL/TLS Protocol



DDoS Attack Statistics

The Netherlands experienced a dynamic DDoS threat landscape marked by considerable cyber activity in 2023.

- The most extensive multivector DDoS attack recorded encompassed **23 vectors**, featuring prevalent techniques such as **DNS Amplification** and **TCP Reset** attacks.
- The maximum bandwidth observed during a DDoS attack reached **590.00 Gbps** (peak aggregate bandwidth in one minute), indicating the severe capacity of these cyber threats.
- The highest recorded throughput during these incidents was **404.00 Mpps** (peak aggregate throughput in one minute), underscoring the intense rate at which data packets were sent.
- On average, each DDoS attack lasted for **22 minutes**, indicating a strategy focused on short but effective service disruptions.
- A total of **48,178** DDoS attacks were recorded throughout the year, illustrating a high frequency of cyber-attacks aimed at targets in the Netherlands.

Attack Vector	Number of Attacks in 2023
DNS Amp	12,996
TCP RST	8,716
TCP ACK	7,791
mDNS Amp	5,073
TCP SYN	4,883

The ongoing evolution of DDoS tactics underscores the critical importance of implementing stringent monitoring and resilient defense mechanisms to safeguard essential infrastructures and ensure uninterrupted service delivery. Enhance your DDoS defense with SOCRadar's DoS Resilience module, a sophisticated tool designed to assess and fortify your infrastructure's resilience to DoS attacks.

Lessons Learned: Key Insights and Strategic Recommendations

Upon examining the cybersecurity threats facing organizations in the Netherlands, several critical lessons and recommendations have emerged. These insights, enhanced by SOCRadar's capabilities, provide a strategic roadmap to bolster cyber resilience and safeguard operational integrity. Here are the key takeaways from our analysis:

Vigilance in an Evolving Cyber Threat Landscape

The dynamic nature of the cyber threat landscape, marked by an increase in dark web activities and ransomware incidents related to the Netherlands, demands constant vigilance. Organizations must keep pace with these changes by adapting their security strategies. By adopting a proactive approach like SOCRadar's Extended Threat Intelligence solution, organizations can enable themselves to gain real-time insights into emerging threats, positioning them to proactively counteract cyber adversaries.

Implementation of Multi-layered Security Measures

Given the broad spectrum of industries targeted by cyber threats, it is essential to implement multi-layered security defenses. SOCRadar supports these efforts with its proactive Threat Intelligence and monitoring services, ensuring comprehensive protection.

Consistent Guard Against Ransomware

The persistent threat posed by ransomware underscores the need for strong defensive and responsive strategies. SOCRadar's Attack Surface Management capabilities are crucial for businesses to identify potential ransomware threats and to formulate effective countermeasures.

Continuous Employee Education and Training

The ongoing risk of phishing attacks makes continuous education and training for employees imperative. Enhancing their ability to recognize phishing tactics and detection methods is vital. SOCRadar's Digital Risk Protection suite provides comprehensive VIP Protection and Brand Protection services, effectively addressing the challenges posed by identity-based attacks.

Robust Defenses Against Stealer Malware

With the Netherlands frequently targeted by Stealer malware, strengthening defenses against this malicious software is crucial. SOCRadar’s Identity & Access Intelligence module plays a vital role in detecting and mitigating data breach threats, enhancing an organization’s security framework.

Strategies Against DDoS Attacks

As DDoS attacks become more complex and voluminous, organizations must prioritize the implementation of robust DDoS mitigation strategies. This involves deploying advanced DDoS protection technologies that can absorb high-volume traffic and mitigate multi-vector attack strategies effectively.

Enhance your DDoS defense with SOCRadar's DoS Resilience module, a sophisticated tool designed to assess and fortify your infrastructure's resilience to DoS attacks. Leveraging state-of-the-art AI and cloud technologies, this module provides a crucial layer of protection for global organizations.

Conclusion

Adopting a proactive and comprehensive approach to cybersecurity is crucial for organizations in the Netherlands. By partnering with advanced solutions like SOCRadar, they can enhance their defenses and effectively navigate the evolving cyber threat landscape.

Building a culture of risk awareness and implementing proactive mitigation strategies fortifies defenses against dynamic threats. Utilizing Cyber Threat Intelligence empowers teams to respond to immediate threats and prepare for future challenges with confidence.

Collaboration among cybersecurity professionals, supported by robust CTI frameworks, is essential for safeguarding digital assets and maintaining organizational resilience against cyber threats.

Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by **21.000+ companies** in **150+ countries**

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

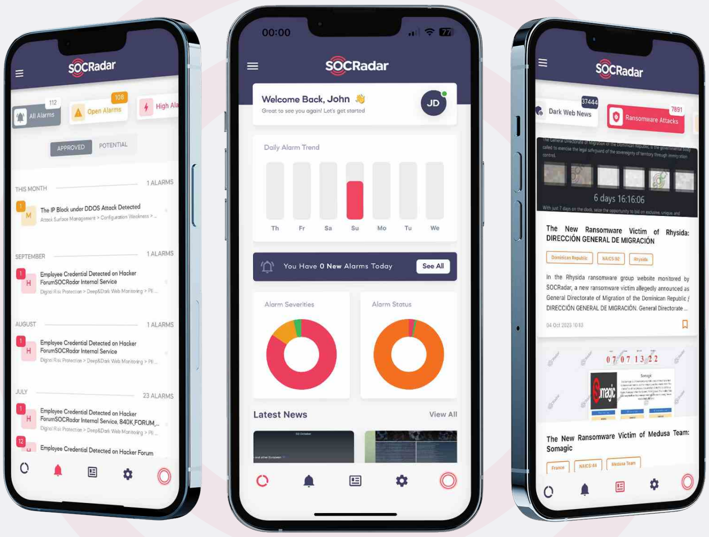
360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

MEET THE NEW MOBILE APP

Access threat intelligence, act on-the-go, and be instantly notified of new threats.View alerts, breaking Dark Web news, and new ransomware attacks

Download on the App Store



The IP Block under DDOS Attack Detected

Attack Surface Management > Configuration Weakness > ...

Employee Credential Detected on Hacker ForumSOCRadar Internal Service

Digital Risk Protection > Deep&Dark Web Monitoring > PII ...

Employee Credential Detected on Hacker ForumSOCRadar Internal Service, 840K FORUM_...

Employee Credential Detected on Hacker Forum

Welcome Back, John

Great to see you again! Let's get started

You Have 0 New Alarms Today

The New Ransomware Victim of Rhysida: DIRECCIÓN GENERAL DE MIGRACIÓN

In the Rhysida ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as General Directorate of Migration of the Dominican Republic / DIRECCIÓN GENERAL DE MIGRACIÓN. General Directorate ...

04 Oct 2023 10:13

The New Ransomware Victim of Medusa Team: Somagic

GET IT ON Google Play

Gartner Peer Insights Customer First

Gartner. Peer Insights™

4.8/5 ★★★★★