SmokeLoader Malware Targets Ukraine’s Auto & Banking Sectors via Open Directories

Published: 2025-02-06 · Archived: 2026-04-05 18:00:22 UTC

TABLE OF CONTENTS

SmokeLoader: A Brief OverviewOpen Directory Findings: What We DiscoveredFinal NoteConclusionNetwork Observables and Indicators of Compromise (IOCs)Host Observables and Indicators of Compromise

Hunt researchers identified an **open directory hosting SmokeLoader samples alongside lure documents targeting Ukraine's automotive and banking sectors**. A second related directory contained the same malware but with different lures, suggesting a broader campaign. The misconfigured servers exposed the staging and distribution methods used in this campaign, offering direct insight into the threat actor's operational tactics.

SmokeLoader remains a tool for cybercriminals and suspected Russian threat actors, often used for initial access before delivering secondary payloads such as credential stealers and remote access trojans (RATs). Recent reports highlight its continued **deployment in operations against Ukrainian organizations**, reinforcing its role in both cybercrime and espionage-driven attacks.

The following sections examine the findings, analyze the malware and lure files, and break down the malicious infrastructure supporting this activity.

SmokeLoader: A Brief Overview

First identified in 2011, **SmokeLoader** has evolved into a versatile and persistent threat in the cyber landscape. Originally designed as a malware loader, it remains a preferred tool for adversaries due to its **lightweight nature and ability to execute additional payloads on compromised systems**. Its modular framework allows operators to tailor functionality, making it effective for both large-scale operations and more targeted intrusions.

While SmokeLoader has long been **associated with financially motivated campaigns**, its **presence in operations against Ukrainian organizations** highlights its continued adaptability. Its obfuscation techniques and ability to deliver a variety of secondary malware ensure it remains a reliable choice for threat actors looking to maintain access, evade detection, and distribute additional payloads as needed.

Open Directory Findings: What We Discovered

Browsing Hunt's **AttackCapture™** listing for recently scanned open directories, researchers identified an exposed server at **2.59.163[.]172**, hosted on the Global Connectivity Solutions LLP network in Poland. The directory contained multiple **Windows executables and PDF files** labeled "invoce," a likely misspelling of "invoice." The file names suggest the actor leveraged financial-themed lures, a common tactic in phishing campaigns.

As shown in the figure below, **Hunt automatically detected and tagged several of these files as SmokeLoader samples**. A subfolder named "ukraine" stands out, suggesting a deliberate focus on Ukrainian targets. The directory's structure and contents indicate it was set up to deliver malware rather than being an incidental collection of files.

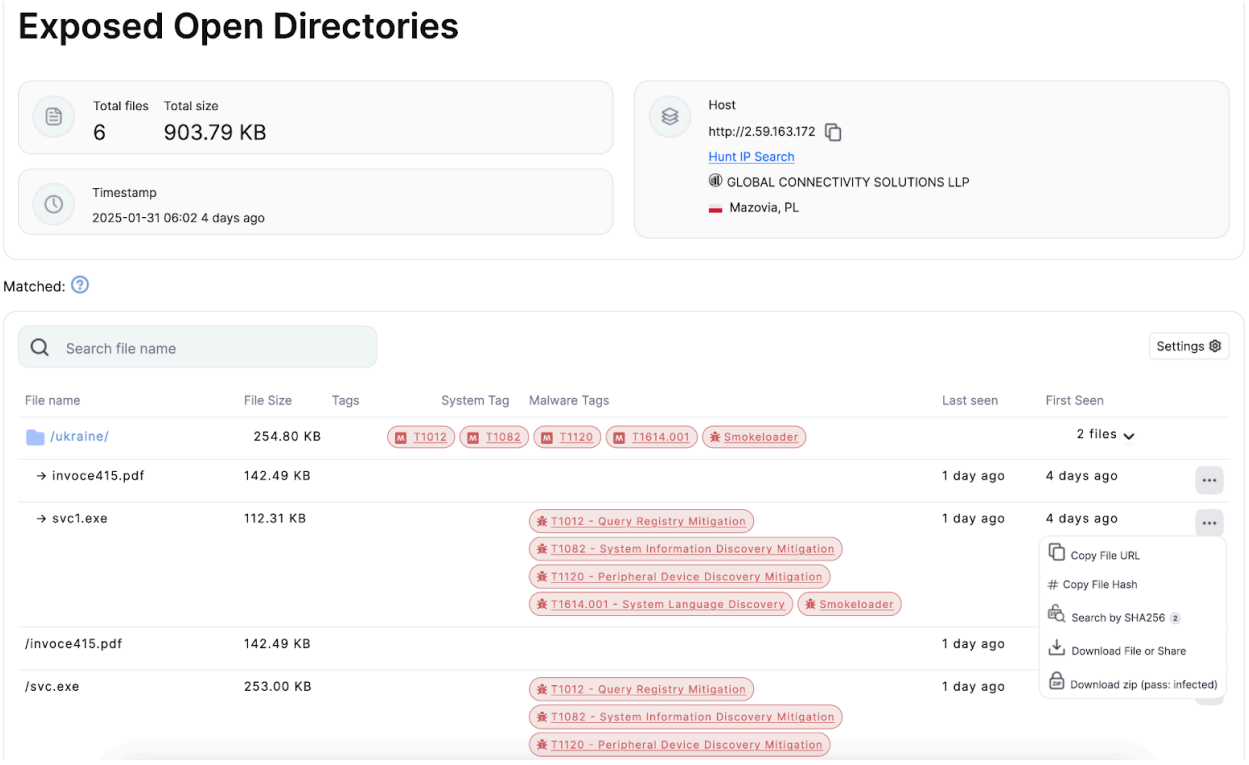


Figure 1: Contents of the open directory at 2.59.163[.]72 in Hunt.

In AttackCapture™, pivoting on files is as simple as clicking on the three dots next to the file and selecting "Search by SHA256." In this case, the number next to the option was 2, indicating the same executable file was hosted in another directory.

That second server, located at 88.151.192[.]50 and hosted on the **Global Connectivity Solutions LLP** network in Ukraine, contained the same three Windows files--svc.exe, svc1.exe, and svc2.exe--indicating that both servers were likely part of the same staging infrastructure.

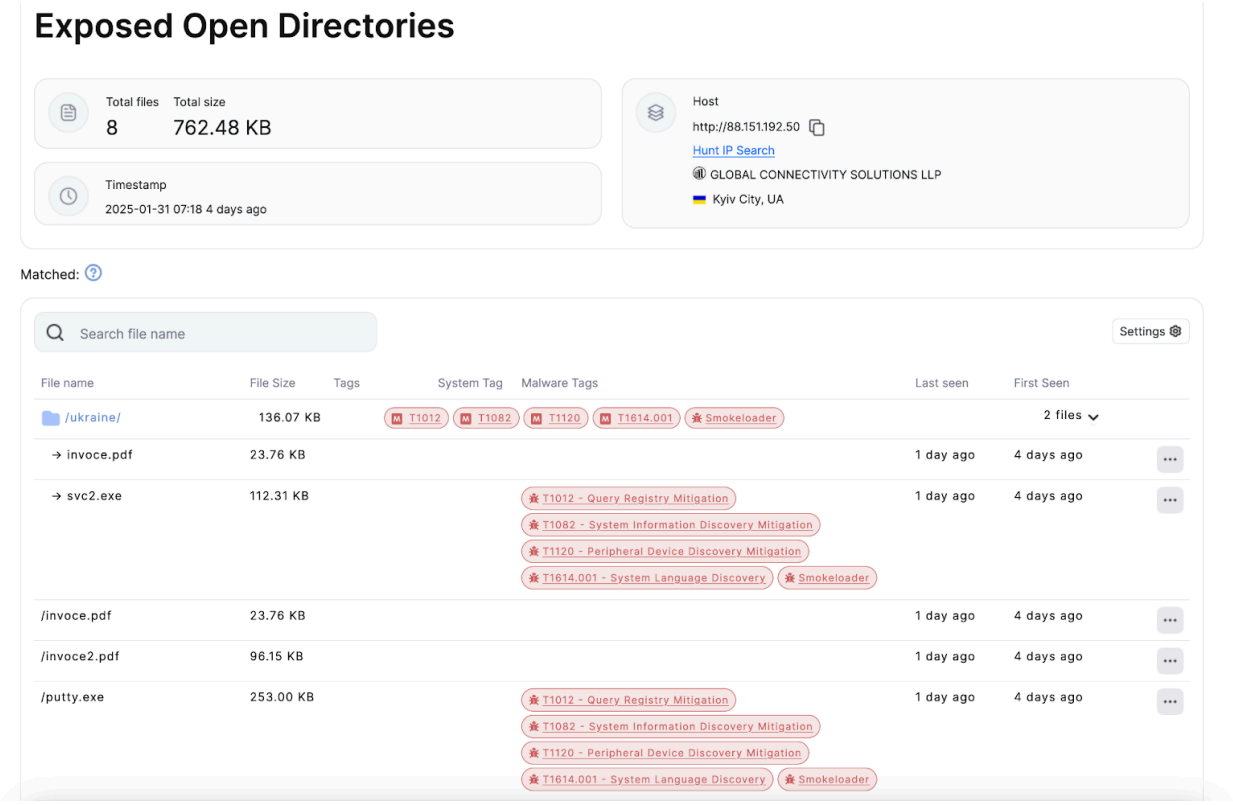


Figure 2: Screenshot of similarly named executables in Hunt.

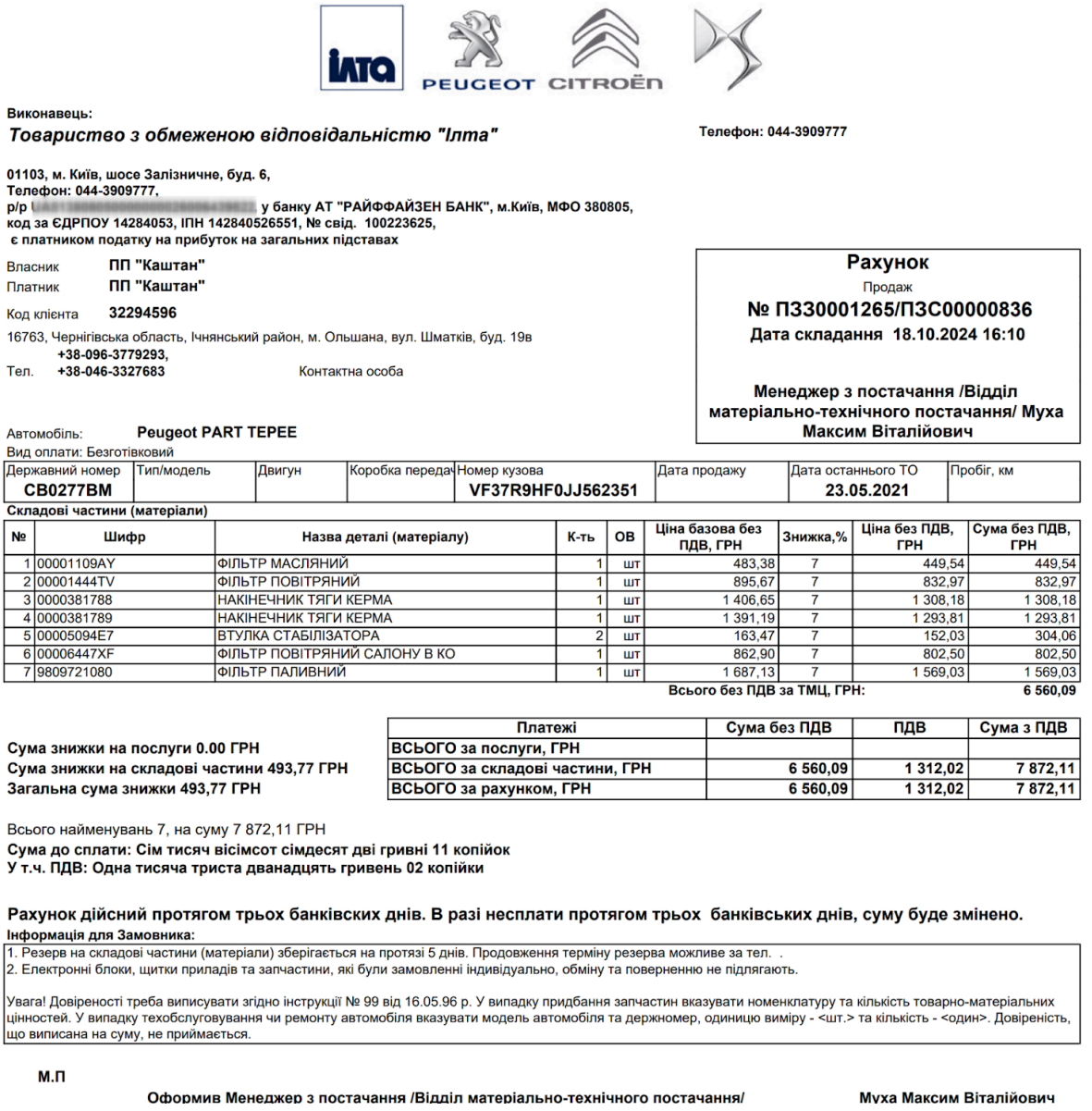
The above screenshot shows the directory structure closely mirrors our first server, including the **"ukraine"** subfolder. However, there are two key differences:

- The PDF files are named invoce.pdf and invoce2.pdf.
- A newly detected file, **putty.exe**, appeared alongside the SmokeLoader samples. While unrelated to the financial lures, its presence suggests an attempt to **deceive users seeking to download or execute the legitimate SSH client**, a common tactic for malware delivery.

A single domain resolves to this IP, **www[.]connecticutproperty[.]ru**, which will appear again later in this post.

PDF Lures

Among the files found on the initial server, a single PDF, "invoce415.pdf," was used in conjunction with the malicious files. The document posing as an invoice from Ілта (Ilta), an official importer of **Peugeot vehicles in Ukraine** since 1992. The company provides **sales, service, and leasing options** for Peugeot, Citroën, and DS vehicles, making it a plausible lure for targeting individuals or businesses in the automotive sector.



Виконавець:
Товариство з обмеженою відповідальністю "Ілта" **Телефон: 044-3909777**

01103, м. Київ, шосе Залізничне, буд. 6,
Телефон: 044-3909777,
р/р [redacted] у банку АТ "РАЙФФАЙЗЕН БАНК", м.Київ, МФО 380805,
код за ЄДРПОУ 14284053, ІПН 142840526551, № свід. 100223625,
є платником податку на прибуток на загальних підставах

Власник **ПП "Каштан"**
Платник **ПП "Каштан"**

Код клієнта **32294596**

16763, Чернігівська область, Ічнянський район, м. Ольшана, вул. Шматків, буд. 19в
+38-096-3779293,
Тел. **+38-046-3327683** Контактна особа

Рахунок
Продаж
№ ПЗ30001265/ПЗС00000836
Дата складання 18.10.2024 16:10

Менеджер з постачання /Відділ матеріально-технічного постачання/ Муха Максим Віталійович

Автомобіль: **Peugeot PART TEPEE**
Вид оплати: Безготівковий

Державний номер	Тип/модель	Двигун	Коробка передач	Номер кузова	Дата продажу	Дата останнього ТО	Пробіг, км
CB0277BM				**VF37R9HF0JJ562351**		**23.05.2021**	

Складові частини (матеріали)

№	Шифр	Назва деталі (матеріалу)	К-ть	ОВ	Ціна базова без ПДВ, ГРН	Знижка,%	Ціна без ПДВ, ГРН	Сума без ПДВ, ГРН
1	00001109AY	ФІЛЬТР МАСЛЯНИЙ	1	шт	483,38	7	449,54	449,54
2	00001444TV	ФІЛЬТР ПОВІТРЯНИЙ	1	шт	895,67	7	832,97	832,97
3	0000381788	НАКІНЕЧНИК ТЯГИ КЕРМА	1	шт	1 406,65	7	1 308,18	1 308,18
4	0000381789	НАКІНЕЧНИК ТЯГИ КЕРМА	1	шт	1 391,19	7	1 293,81	1 293,81
5	00005094E7	ВТУЛКА СТАБІЛІЗАТОРА	2	шт	163,47	7	152,03	304,06
6	00006447XF	ФІЛЬТР ПОВІТРЯНИЙ САЛОНУ В КО	1	шт	862,90	7	802,50	802,50
7	9809721080	ФІЛЬТР ПАЛИВНИЙ	1	шт	1 687,13	7	1 569,03	1 569,03
						Всього без ПДВ за ТМЦ, ГРН:		**6 560,09**

Сума знижки на послуги 0.00 ГРН
Сума знижки на складові частини 493,77 ГРН
Загальна сума знижки 493,77 ГРН

Платежі	Сума без ПДВ	ПДВ	Сума з ПДВ
ВСЬОГО за послуги, ГРН			
ВСЬОГО за складові частини, ГРН	**6 560,09**	**1 312,02**	**7 872,11**
ВСЬОГО за рахунком, ГРН	**6 560,09**	**1 312,02**	**7 872,11**

Всього найменувань 7, на суму 7 872,11 ГРН
Сума до сплати: Сім тисяч вісімсот сімдесят дві гривні 11 копійок
У т.ч. ПДВ: Одна тисяча триста дванадцять гривень 02 копійки

Рахунок дійсний протягом трьох банківських днів. В разі несплати протягом трьох банківських днів, суму буде змінено.
Інформація для Замовника:

1. Резерв на складові частини (матеріали) зберігається на протязі 5 днів. Продовження терміну резерва можливе за тел. .
2. Електронні блоки, щитки приладів та запчастини, які були замовленні індивідуально, обміну та поверненню не підлягають.

Увага! Довіреності треба виписувати згідно інструкції № 99 від 16.05.96 р. У випадку придбання запчастин вказувати номенклатуру та кількість товарно-матеріальних цінностей. У випадку техобслуговування чи ремонту автомобіля вказувати модель автомобіля та держномер, одиницю виміру - <шт.> та кількість - <один>. Довіреність, що виписана на суму, не приймається.

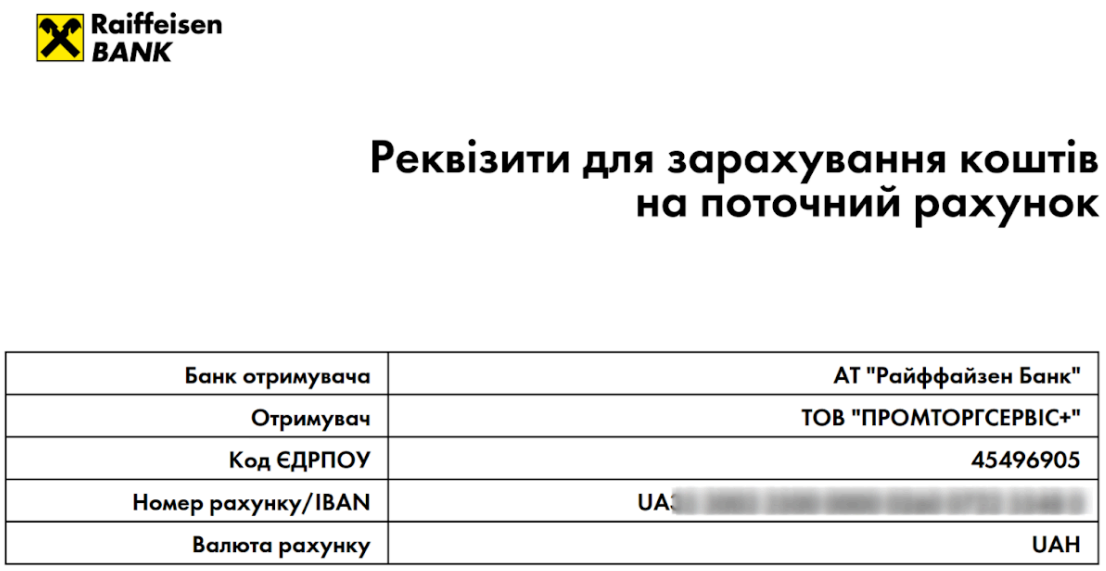
М.П

Оформив Менеджер з постачання /Відділ матеріально-технічного постачання/ **Муха Максим Віталійович**

Figure 3: Lure document posing as an invoice for vehicle services.

While fake invoices are a common phishing tactic, **referencing a well-known Ukrainian business adds credibility to the lure**, increasing the chances that a recipient will engage with it. This document was likely distributed as part of a phishing operation, where the attacker urged the recipient to download and open the file, leading to the execution of SmokeLoader.

Within the second directory, the first of the two PDFs, invoce.pdf **appears to be an account statement from Raiffeisen Bank**, a major commercial bank in Ukraine. Raiffeisen was designated a systemically important bank by the National Bank of Ukraine in 2024.



Raiffeisen BANK

Реквізити для зарахування коштів на поточний рахунок

Банк отримувача	АТ "Райффайзен Банк"
Отримувач	ТОВ "ПРОМТОРГСЕРВІС+"
Код ЄДРПОУ	45496905
Номер рахунку/IBAN	UA[redacted]
Валюта рахунку	UAH

Figure 4: Screenshot of invoce.pdf mimicking Raiffeisen Bank.

The second file, invoce2.pdf, is another financial statement dated at the end of July 2024. The document purports to be from __Sense Bank, one of Ukraine's largest financial institutions. Previously known as Alfa-Bank before 2022, Sense Bank remains a recognizable name in the country's financial sector, making it an effective lure for phishing attempts.

Виписка за рахунками

за 31.07.2024

sense bank

Сформована 01.08.2024 07:32
користувачем **168567F1**

Банк АТ "СЕНС БАНК" Код банку 300346
IBAN UA 05 300346 0000026008016856701 СТОВ " ЗЛАГОДА "
Вал. **980/UAH** Дата **31.07.2024**
Дата попередньої операції **30.07.2024**

					Дебет	Кредит
				Вхідний залишок	0.00	1332612.79
№ з.п.	№ док	Дата	Код банку	№ рахунка	Дебет	Кредит
1	2104	31.07.2024	300335	UA 32 300335 0000000260022236417	139000.00	0.00
2	2103	31.07.2024	300335	UA 32 300335 0000000260022236417	1220000.00	0.00
3	917	31.07.2024	334851	UA 81 334851 0000026003962481899	0.00	26750.35
				Усього оборотів	1359000.00	26750.35
				Вихідний залишок	0.00	363.14

Усього документів	3	на суму:	1385750.35
У том числі:			
За дебетом рахунку	2	на суму:	1359000.00
За кредитом рахунку	1	на суму:	26750.35

Усього документів	**3**	**на суму:**	**1385750.35**
У том числі:			
За дебетом рахунку	**2**	**на суму:**	**1359000.00**
За кредитом рахунку	**1**	**на суму:**	**26750.35**

Figure 5: Lure document imitating Sense Bank.

Malware Analysis

Recent reporting from **AhnLab and Trend Micro** detailed SmokeLoader campaigns leveraging **7-Zip archives** for delivery. While that specific technique was not present in the open directories we analyzed, there were noticeable overlaps-**lure documents targeting Ukrainian organizations**, domains following **similar naming patterns**, and a **known SmokeLoader command-and-control server**.

Once executed, SmokeLoader **injects into explorer.exe** and creates a duplicate of itself in the **AppData directory** under the name **"hbasjiu"** to evade detection. It then establishes communication with the following command-and-control servers via **HTTP POST requests**:

- **94.156.177[.]72:80**
- **2.59.163[.]71:80**

Notably, network traffic analysis revealed that each request contained a **dynamically changing Referer header**, with values generated from **domain generation algorithm (DGA) domains**.

The malware's configuration also contained hardcoded domains, though no additional payloads were observed during analysis:

- **http://constractionscity1991[.]lat**
- **http://restructurisationservice[.]ru**
- **http://connecticutproperty[.]ru**

```
POST / HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://fpqunrgqdttjullf.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 135
Host: restructurisationservice.ru

Data Raw: a1 5f 78 55 80 45 51 bc c0 42 d3 b9 fd b3 5e 4a 5d 43 b3 5f 6a ce 40 2b dc 22 cd 6c 73 f4 73 55 cb 56 dd 8a 46 aa 06 3b 2f
cb cd 11 b3 45 16 4d a6 60 28 1e cf 32 6d 2d d9 82 ec 5e cd da f3 84 e5 8c 8d e0 18 1d ce ca bf 4a 72 43 29 be 8a 42 67 bb
Data Ascii: _xUEQB^J]C_j@+"lssUVF;/EM`(2m-^JrC)BgZJpI0Z5>@SwA@DZ
```

```
HTTP/1.1 404 Not Found
Server: nginx
Date: Tue, 04 Feb 2025 21:39:31 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Data Raw: 31 39 66 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20
48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74
20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64
3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6
f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e
6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20
74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73
74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e  [TRUNCATED]
Data Ascii: 19f<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Foun
d</h1><p>The requested URL / was not found on this server.</p><p>Additionally, a 404 Not Found error was encountered while trying to
use an ErrorDocument to handle the request.</p><hr><address>Apache/2.4.62 (Debian) Server at restructurisationservice.ru Port 8
0</address></body></html>0
```

Figure 6: Example C2 communications (Source: Joe Sandbox).

Final Note

Hunt users can explore additional open directories hosting SmokeLoader and multiple other malware families in AttackCapture™ by searching for the tag.

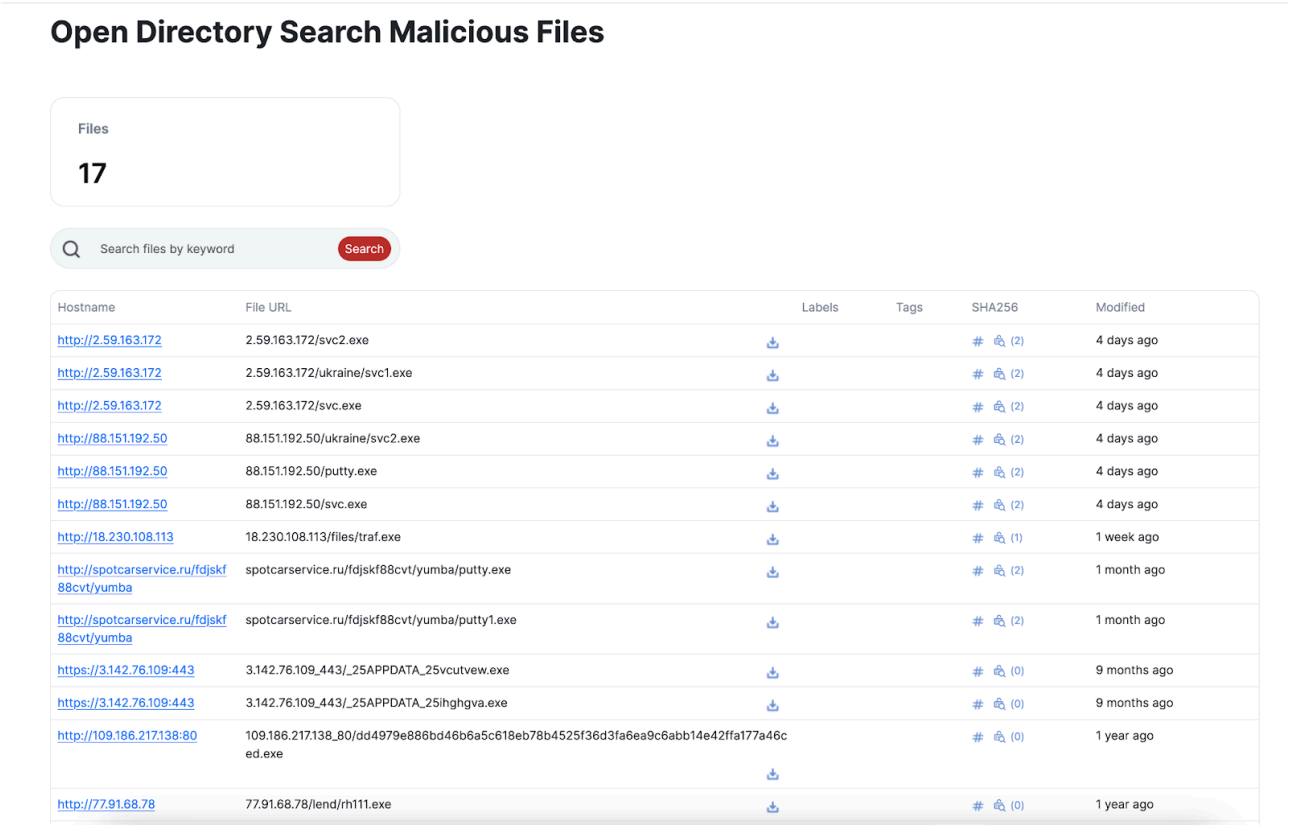


Figure 7: Results of searching AttackCapture™ for the SmokeLoader tag in Hunt.

Conclusion

Our findings highlight how **open directories continue to expose malware distribution operations**, providing direct visibility into **threat actor infrastructure, targeting, and execution methods**. The uncovered servers contained **SmokeLoader samples staged alongside financial-themed lure documents** impersonating Ukrainian banks and businesses---tactics consistent with previously observed campaigns.

By tracking open directories, defenders can gain **early insight into adversary behaviors**, helping to identify **active malware campaigns before deployment at scale**. Researchers can use **AttackCapture™** to search for SmokeLoader and other malware families, uncovering additional staging servers and refining detection strategies.

Network Observables and Indicators of Compromise (IOCs)

IP Address	ASN	Domains	Notes
2.59.163[.]172	GLOBAL CONNECTIVITY SOLUTIONS LLP	N/A	Open directory containing lure PDF documents and SmokeLoader samples.
88.151.192[.]71	GLOBAL CONNECTIVITY SOLUTIONS LLP	www.connecticutproperty[.]ru	Shares Windows executables with 2.59.163[.]172.

IP Address	ASN	Domains	Notes
94.156.177[.]72	Railnet LLC	downloadmanager[.]ru oncomnigos[.]ru consultationoffice[.]ru www[.]spotcarservice[.]ru www[.]fileexportinc[.]ru restructurisationservice[.]ru fileexportinc[.]ru constractionscity1991[.]lat	Known SmokeLoader C2. The following domains also resolved to 66.63.187[.]25 in late December 2024: constractionscity1991[.]lat ns2.constractionscity1991[.]lat

Host Observables and Indicators of Compromise

Filename	SHA-256
invoce415.pdf	9833cbd22fd50181f8939114920e883bacf8d727337f5dcdf4450d0312eca188
svc.exe	f8bd5f0408409ea63a270d5aad8da5f0cb557f9a82e0da3e8077cbe589288054
svc1.exe	1118a93cc63a70ba8348182f7012ddbeecf890345941c82376ac967faf55a295
svc2.exe	4b00565a29eeb0446393d0538e8f24de232339cf3ffb6a76a2bce3ba160c2066
invoce.pdf	5e7602b9073b8cf5c1a6afc6d0c8366545da65d2b48eb109f1bd9f40a58e73c0
invoce2.pdf	7991bfff4eb5f50aa9f5d3d95064411987a29de9621fc5afca9e4978ca568941
putty.exe	f8bd5f0408409ea63a270d5aad8da5f0cb557f9a82e0da3e8077cbe589288054
