НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

THE SURGE IN SMOKELOADER ATTACKS ON UKRAINIAN INSTITUTIONS

EXECUTIVE SUMMARY

This report presents a troubling escalation in cyber threats by russian cybercriminals who have dramatically increased their use of Smokeloader malware against Ukrainian financial and government organizations since May of this year. Smokeloader, a sophisticated and evasive malware strain, has become the weapon of choice for these threat actors, enabling them to infiltrate and compromise critical institutions. This report provides an in-depth analysis of the evolving tactics and strategies employed by these cybercriminals, shedding light on their motives, methodologies, and potential impact.

The rise in Smokeloader-based attacks in the context of geopolitical tensions raises pressing concerns about broader threats for Ukrainian organizations, which emerge not only from russian state-sponsored APT threat actors, but also from russian cybercrime groups.

SMOKELOADER MIST

Emerging from the depths of the darknet market in 2011, the Smokeloader malware has evolved into a potent tool that has recently set its sights on Ukrainian organizations. This malware boasts a sophisticated array of functionalities, making it a prized asset for threat actors. Its capabilities include discreet system infiltration, data exfiltration, and enabling remote access with remarkable finesse. The price of admission to this malicious toolkit varies, with options ranging from **$400 for the basic bot to $1,650 for the complete package**, featuring all available plugins and functions.

Since May 2023, russian cybercrime threat actor have orchestrated a range of attacks against Ukrainian targets using Smokeloader as their weapon of choice. Each month launching big waves of phishing attacks and leaning towards financial themes in malicious emails.

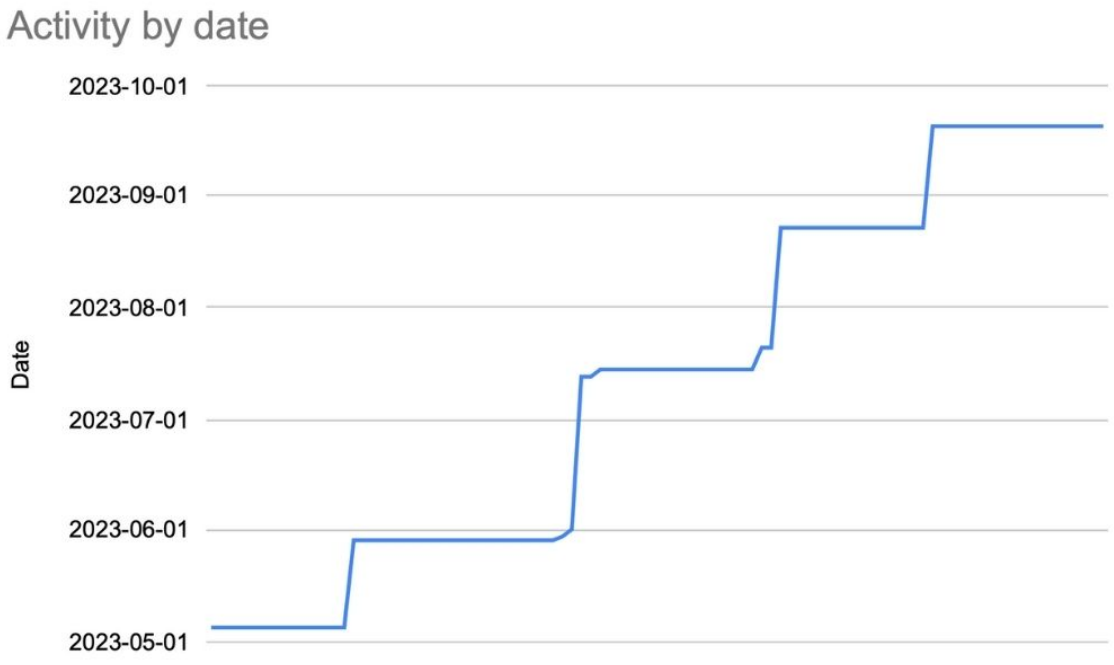


Figure.1 Chronology of threat actor activity

Our extensive analysis of their network infrastructure reveals a striking prevalence of russian domain registrars like REGRU, REGTIME and RU-CENTER, hinting at possible connections to russian cybercriminal operations.

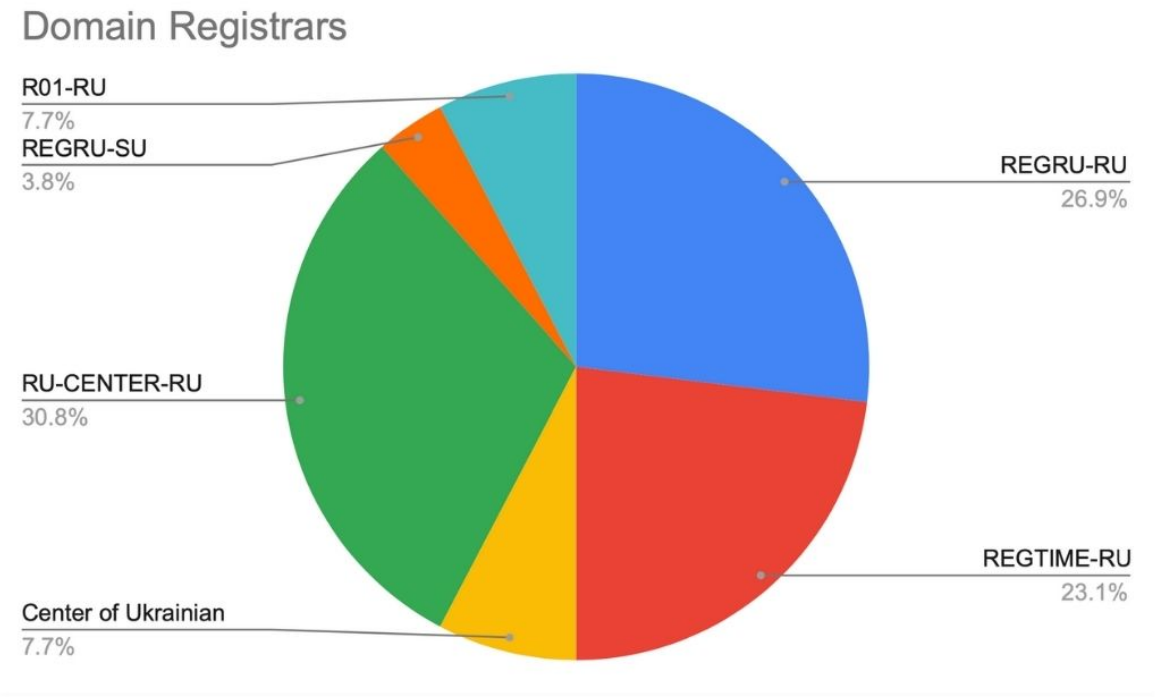


Figure.2 Breakdown of domain registrars used by cybercriminals

DECEPTIVE TACTICS

Recent Smokeloader campaigns have exhibited a high degree of sophistication in their tactics and methods, with a pronounced focus on financial themes. These malicious operations commence with meticulously crafted phishing emails designed to lure victims. Financial themes dominate the content, creating a sense of urgency and relevance for recipients.

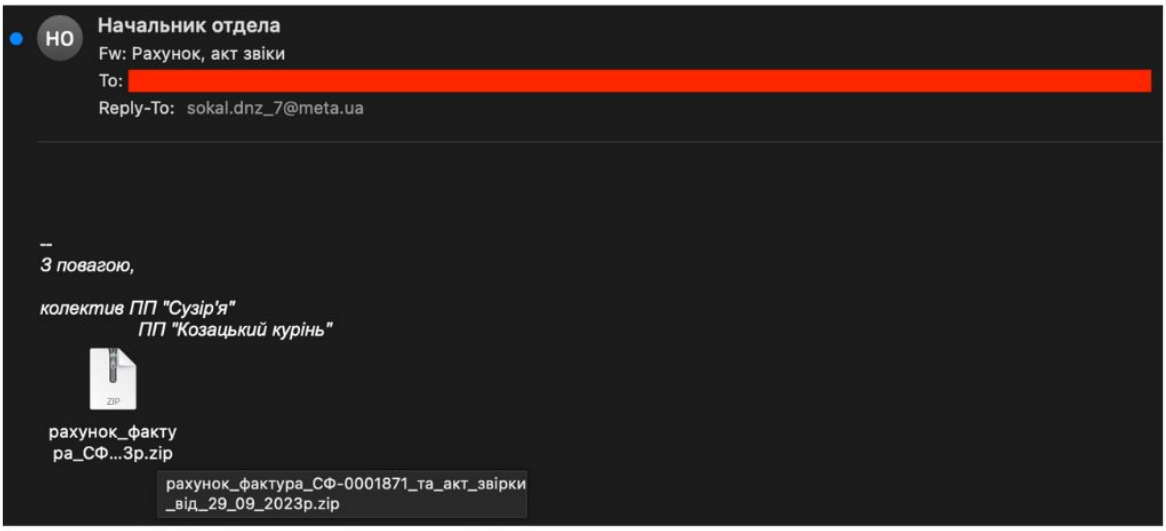


Figure.3 Financially themed phishing email with Smokeloader

However, the true deception lies in the attachment – typically an archive file encapsulated multiple times. Inside this digital labyrinth, buried amidst seemingly benign documents, are the financially themed files that serve as the ultimate bait. Victims are led through these encapsulated layers until they reach the heart of the payload – Smokeloader.

Notably, these campaigns have displayed telltale signs that hint at the involvement of russian cybercriminals. Misspellings and discrepancies in the names of Ukrainian documents within the malicious attachments suggest a lack of linguistic finesse.

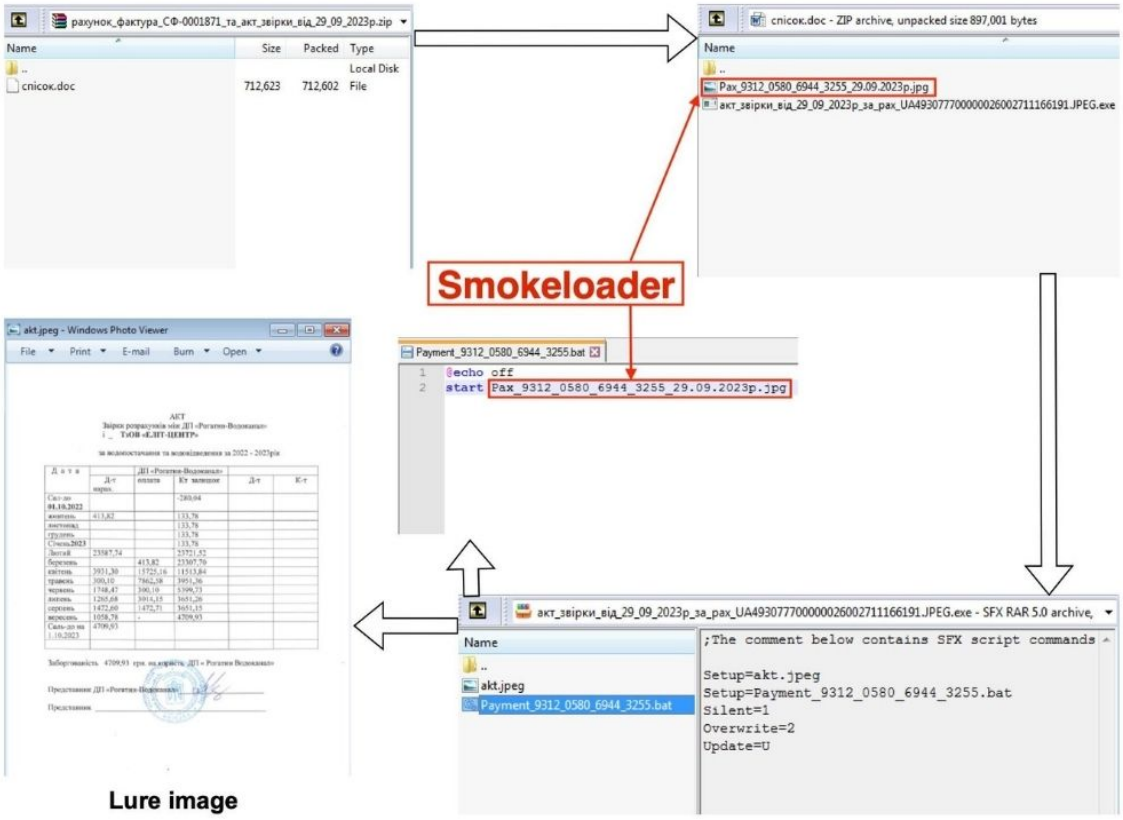


Figure.4 Example of Smokeloader infection chain

In the process of main payload malware extraction, legitimate financially themed documents are displayed to the victims to reduce suspicion and make it look more credible. Serving as a decoy, these legitimate documents are stolen from previously compromised organisations.

Per its execution Smokeloader malware unfolds as a complex and clandestine operation and once unveiled, it embarks on a mission to establish connections with a pre-defined list of domains. Notably, this list of command and control (C2) domains is meticulously hardcoded within the malware's configuration:

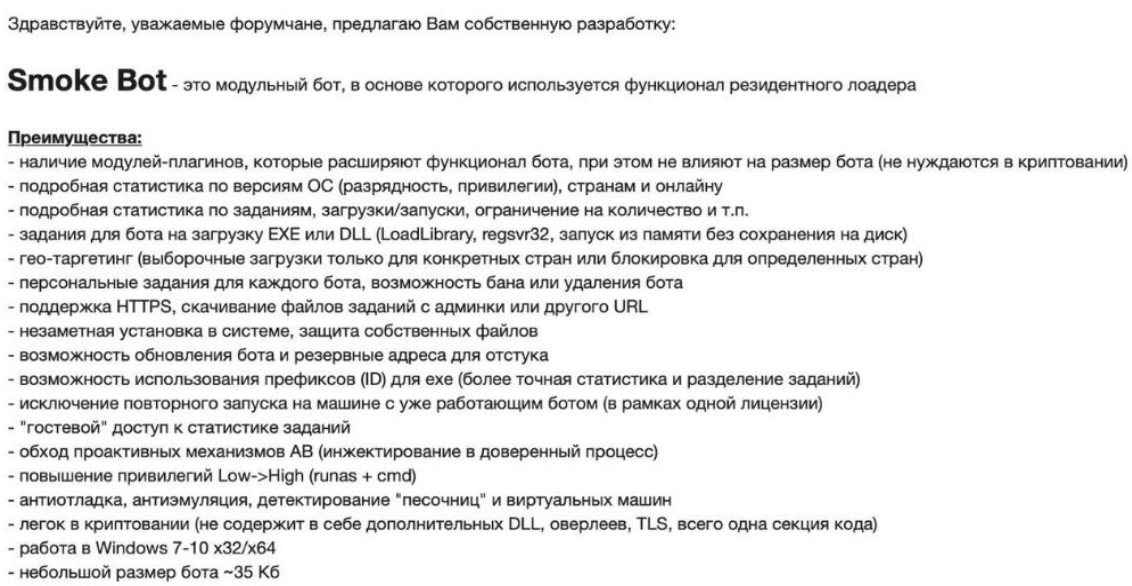
{"Version": 2022, "C2 list": ["http://super777bomba.ru/", "http://dublebomber.ru/", "http://yavasponimayu.ru/", "http://nomnetozhedenyuzhkanuzhna.ru/", "http://restmantra.by/", "http://prostosmeritesya.ru/", "http://iloveua.ir/", "http://kozachok777.ru/", "http://ipoluchayteudovolstvie.ru/", "http://propertyminsk.by/", "http://tvoyaradostetoya.ru/", "http://propertyiran.ir/", "http://moyabelorussiya.by/"]}

However, the craftiness of Smokeloader lies in its selective communication. Many of these domains remain intentionally inaccessible, acting as digital decoys to divert attention and complicate detection efforts.

MULTIFACETED FUNCTIONALITY

Smokeloader, a long-standing presence on darknet markets since 2011, emerges as a multifunctional and highly evasive malware strain. It boasts a formidable repertoire of functionalities designed to safeguard itself from analysis and detection. This malware's self-preservation tactics include an array of anti-debug, anti-hooking, and anti-VM features, creating a digital fortress that challenges cybersecurity experts.

Beyond mere self-defense, Smokeloader exhibits a cunning ability to extract crucial system information, such as operating system details and geographical data, offering threat actors valuable insights into the infected system's environment. Employing techniques like process hollowing and a variety of evasion strategies, Smokeloader adeptly conceals its presence, slipping through security measures undetected.



Здравствуйте, уважаемые форумчане, предлагаю Вам собственную разработку:

Smoke Bot - это модульный бот, в основе которого используется функционал резидентного лоадера

Преимущества:
- наличие модулей-плагинов, которые расширяют функционал бота, при этом не влияют на размер бота (не нуждаются в криптовании)
- подробная статистика по версиям ОС (разрядность, привилегии), странам и онлайну
- подробная статистика по заданиям, загрузки/запуски, ограничение на количество и т.п.
- задания для бота на загрузку EXE или DLL (LoadLibrary, regsvr32, запуск из памяти без сохранения на диск)
- гео-таргетинг (выборочные загрузки только для конкретных стран или блокировка для определенных стран)
- персональные задания для каждого бота, возможность бана или удаления бота
- поддержка HTTPS, скачивание файлов заданий с админки или другого URL
- незаметная установка в системе, защита собственных файлов
- возможность обновления бота и резервные адреса для отстука
- возможность использования префиксов (ID) для exe (более точная статистика и разделение заданий)
- исключение повторного запуска на машине с уже работающим ботом (в рамках одной лицензии)
- "гостевой" доступ к статистике заданий
- обход проактивных механизмов AB (инжектирование в доверенный процесс)
- повышение привилегий Low->High (runas + cmd)
- антиотладка, антиэмуляция, детектирование "песочниц" и виртуальных машин
- легок в криптовании (не содержит в себе дополнительных DLL, оверлеев, TLS, всего одна секция кода)
- работа в Windows 7-10 x32/x64
- небольшой размер бота ~35 Кб

Figure.5 Thread of selling Smokeloader malware on the darknet forum

Further enhancing its capabilities, Smokeloader encompasses a modular design, facilitating the expansion of its functionality. These modules empower the malware to adapt and evolve, tailoring its malicious operations to the specific objectives of the threat actors.

Module	Features
STEALER	Collects credentials and cookies from different applications (browsers, email clients, FTP).
FORM GRABBER	Intercepts web browser POST requests before they go through encryption.
PASS SNIFFER	Intercepts credentials of most common applications and protocols (FTP, POP3, IMAP, SMTP).
FAKE DNS	DNS Spoofing. Returns incorrect IP address for domain name according to the specific rule.
FILE SEARCH	Performs search of files and sends them to adversaries.
PROCMON	Monitors and interacts with processes.
DDOS	Executes DDoS attacks.
KEYLOGGER	Intercepts keystrokes.
REMOTE PC	Surveys and controls remote PC with file manager features.
EMAIL GRABBER	Collects email addresses.

In some recent cases, the attackers managed to compromise the process of money transfers, effectively seizing control of the transaction flow. Instead of funds reaching their intended destination, the attackers cunningly substituted the legitimate account details with their own. This resulted in divertion of organization's funds into the coffers of the attackers. Such instances underscore the evolving tactics of cybercriminals, who now not only seek to infiltrate but also manipulate critical financial processes to siphon off resources.

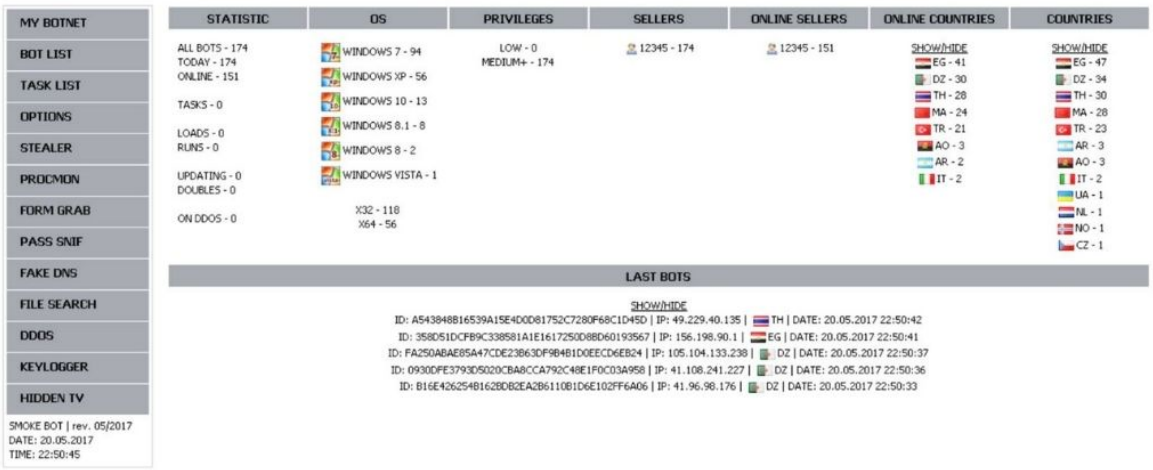


Figure.6 Smokeloader admin panel

CONCLUSION

The recent surge in Smokeloader attacks orchestrated by russian cybercriminals against Ukrainian institutions underscores the ever-evolving and diversified nature of cyber threats facing the nation. These assailants have not only intensified their operations but have also demonstrated a remarkable adaptability in their tactics, targeting the heart of financial operations. The threat landscape in Ukraine has thus evolved into a multifaceted arena, with financially motivated cybercriminals joining the fray alongside state-sponsored actors.

In light of these developments, organizations in Ukraine are urged to remain vigilant and proactive in their cybersecurity posture. It is imperative to invest in personnel training to enhance awareness about financially themed phishing emails, the primary entry point for Smokeloader attacks. Securing endpoints, configuring intrusion detection systems (IDS) for real-time threat detection, and implementing strict restrictions on the execution of scripts and executables from archives are essential measures to fortify defenses.

Furthermore, continuous threat intelligence gathering and sharing through platforms like MISP (Malware Information Sharing Platform) for indicators of compromise are critical. Staying updated about emerging threats and the tactics employed by adversaries is paramount for building a resilient defense against the evolving Smokeloader threat and its multifaceted challenges. In this dynamic landscape, proactive and collaborative cybersecurity efforts are the keys to safeguarding Ukraine's digital frontiers.

INDICATORS OF COMPROMISE OF THE LATEST CAMPAIGN

Type	Value
domain	dublebomber.ru
domain	yavasponimayu.ru
domain	nomnetozhedenyuzhkanuzhna.ru
domain	prostosmeritesya.ru
domain	ipoluchayteudovolstvie.ru
domain	super777bomba.ru
domain	specnaznachenie.ru
domain	zakrylki809.ru
domain	propertyminsk.by
domain	iloveua.ir
domain	moyabelorussiya.by
domain	tvoyaradostetoya.ru
domain	zasadacafe.by
domain	restmantra.by
domain	kozachok777.ru
domain	propertyiran.ir
domain	sakentoshi.ru
domain	popuasyfromua.ru
domain	diplombar.by
domain	ukr-net-download-files-php-name.ru
ip-address	85.143.172.45
sha256	fdf8a89e8c90ed065378oacc77c180185b8971e62d2a02dcaabcfc456d05bd96
sha256	493f708129bf25ff4bb734c179d336f223d9d21ea53b7e5e52f9535a72415bfd
sha256	6999f5f3c6824f27b5a1fb436c59d369f6f1ec08365d48cd1c8d21d1058eaafc
sha256	9a528b2b31d9d59018878fdf3b9d8db235df606500c67a4b8be3075701b014fc
sha256	d895f40a994cb9041688ib88fadd2de5af165eec1cd41b0ddd08fa1d6b3262bb
sha256	2c44c9b445d2efc2f46e463d933da2ffc1d3ba6718bd67d3957c3f916b7c79fe
sha256	41b74077e7707dfce2752668a3201e3bc596ade5594535c266e3249c2e697cb2
sha256	40c9bc7186f21b6e2a7da28632e70d9b9bce01cc63c692d4383ac03e13e45533
sha256	ac1aedd7d08d3e92ded28d07944d8a8039650a36dec8b4a5d7b675ce2c5512c4
sha256	ebbf474d69519b7ded60c1dab807dab492c33d9caf76e6495c2ee92be573011e
sha256	739e735aa73cfdbfc08c696e0426434aa78139110b416313d2a39d93915ee318
sha256	0f9334434746 9ebef7b0d6768f6f50928b8e6df7bc84a4293b7c4a7bb5b98072
sha256	7d7262ab5298abd0e91b6831e37ef0156ded4fdceeaf8f8841c9a80d31f33f8e
sha256	b24c99ca816f7ac8ca87a352ed4f44be9d8a21519dd1f408739da958b580be0c
sha256	cfc44f1399e3d28e55c32bcc73539358e5ac88c0d6a19188a52b161b506bea91
sha256	a8a3130c779904e23b50d69b4e73a714b345e296feebb9f64a732d5c73e7973b
sha256	0a83fcb0b40f35bf6020ad35cedf56b72a6f650a46dc781b2ea1c9647e0f76cc
filename	1.Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.js
filename	2.Акт_звірки_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.js
filename	3.Витяг_з_реєстру_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.js
filename	mstsc.exe
filename	Список_документів_для_ознакомлення.pdf
filename	Список_документів_для_ознайомлення.zip

INDICATORS OF COMPROMISE OF THE LATEST CAMPAIGN

Type	Value
filename	Список_документів_для_ознайомлення.zip
filename	лист.pdf
filename	2.Акт_звірки_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.js
filename	mstsc.exe
filename	лист.zip
filename	ЗАЯВА.xlsx
filename	Рахунок_до_оплати_389.zip
filename	Рахунок_до_оплати_389.pdf
filename	Рахунок_до_оплати_389.exe
filename	pax_389.exe
filename	Рахунок_до_оплати_389.zip