

В СВЕТА НА ДИГИТАЛНИТЕ КРАДЦИ: АНАЛИЗ НА ВОДЕЩИТЕ КОМПЮТЪРНИ ВИРУСИ ЗА КРАЖБА НА ДАННИ

Димитър Йончев, Ива Костадинова

Университет по библиотекознание и информационни технологии

Резюме: Технологиите и мрежата трансформираха нашето битие. Днес младите хора живеят едновременно в реалността и в интернет. Пренасянето на дейностите онлайн обаче създаде нови рискове. Кражбата на информация вече е водеща форма на киберпрестъпност.

Тази статия проучва развитието на популярни фамилии софтуер за кражба на данни. Обект на интерес са вируси като *Lumma stealer*, *PDF malware*, *Fake scphas*, *AsyncRAT* и *Agent Tesla*. Направен е сравнителен анализ на техните актуални версии. Текстът описва основните им технически параметри и начини на действие. Изследването подчертава ключови тенденции, като автоматизация и модулна структура. Разглеждат се адаптивността на вируса и моделът „зловреден софтуер като услуга“ (MaaaS). Анализирани са щетите върху операционните системи и сигурността на файловете.

Материалът е полезен за създатели на защитен софтуер и експерти по сигурност. Той ще послужи и на системни администратори или обикновени потребители. Целта е всеки да защити по-ефективно своята лична информация.

Ключови думи: киберпрестъпност; вируси; анализ; сигурност; кражба

ВЪВЕДЕНИЕ

Дигиталната трансформация превърна компютърните системи в критична обществена инфраструктура. Данните са най-ценният, но и най-уязвимият ресурс на информационната епоха.

Зависимостта от дигитални услуги мотивира киберпрестъпниците да създават все по-сложни механизми за кражба на информация. Модерният зловреден софтуер е насочен към тиха и ефективна експлоатация на данни с цел монетизация. Финансовата стойност на информацията обхваща криптовалути, банкови детайли, корпоративни тайни и сесийни токени.

Зловредният софтуер от тип *Data Stealer* е сред най-динамичните заплахи (*Infosecurity Magazine*, 2025; *HP Development Company*, 2025). Той съчетава технически иновации, социално инженерство и автоматизация. Доклад на *Check Point Research* отчита 58% ръст в разпространението на тези заплахи, което доказва тяхната ефективност (*Check Point Software Technologies*, n.d.).

Концепцията за „Кражба на реалността“ описва атаки срещу характерната идентичност на лицата в мрежата (*Bradbury et al.*, 2020; *Park et al.*, 2024; *Ongun et al.*, 2012). Пред подкомисия в САЩ изследователката Лилиан Аблон класифицира участниците в киберзаплахите и обяснява монетизацията на данни (*Ablon*, 2018). Стойността на ресурса зависи от неговия вид и актуалност. Аблон идентифицира три целеви групи: лични данни (за кражба на самолич-

ност), финансови данни (за директно източване) и интелектуална собственост (за икономически шпионаж).

Научните изследвания анализират широк спектър от зловреден код и софтуерни предизвикателства пред защитата (Choi, 2023). Специализираната литература описва и механизми за компрометиране на криптоактиви чрез зловредни приложения. Тези схеми включват мигновено източване на дигитални портфейли, наемане на готови инструменти за кражба и криптоджекинг (Scharfman, 2024).

Настоящият доклад има за цел да представи задълбочен сравнителен анализ на пет от най-разпространените представители на този клас: Lumma Stealer, PDF Malware, Fake Captchas, AsyncRAT и Agent Tesla.

Тези заплахи са подбрани поради своята висока честота на срещане, разнообразие в техническата реализация и значителното им въздействие върху потребители и организации.

Докладът разглежда:

- техните механизми на заразяване;
- техническите им характеристики и поведенчески модели;
- методите им за прикриване и избягване на детекция;
- анализ на риска и въздействието;
- препоръки за защита и реакция при инциденти.

Целта е да се предостави цялостна картина на съвременните Data Stealer заплахи, която да бъде полезна както за специалисти по киберсигурност, така и за системни администратори, разработчици на защитни механизми и обикновени потребители.

МЕТОДОЛОГИЯ НА ИЗСЛЕДВАНЕТО

Методологията на настоящото изследване е изградена върху комбинация от качествени и количествени подходи, които позволяват систематично и обективно сравнение на разглежданите зловредни програми. Основната цел е да се анализира техният жизнен цикъл – от първоначалната инфекция до експлоатацията на данни и поддържането на устойчивост в системата.

Избор на обекти на изследване

Петте избрани заплахи – Lumma Stealer, PDF Malware, Fake Captchas, AsyncRAT и Agent Tesla – са подбрани въз основа на следните критерии (Centre for Internet Security, 2025):

- висока честота на разпространение през последните 3 години;
- разнообразие в техниките на атака (info-stealer, downloader, RAT, social engineering);
- значително въздействие върху потребители и организации;
- наличие на достатъчно публични проби за динамичен анализ;
- представителност за различни категории зловреден софтуер.

Този подбор позволява да се изгради широкоспектърен модел на съвременните Data Stealer заплахи.

Ограничения на изследването

Както всяко изследване, и това има своите ограничения:

- динамичният анализ може да бъде повлиян от анти-VM техники;
- някои проби може да са модифицирани версии;
- С2 инфраструктурата често се променя;
- социално-инженерните атаки зависят от човешкия фактор.

Въпреки това използваната методология предоставя достатъчно надеждна основа за извеждане на валидни изводи.

РЕЗУЛТАТИ

Настоящото изследване разглежда дигиталната трансформация и пренасянето на ежедневните ни дейности в интернет пространството и свързаното с това разкриване на нови хоризонти за развитието на високотехнологичните престъпления. В тази динамична среда кражбата на данни се утвърждава като основна цел за киберпрестъпниците, налагайки детайлно проучване на механизмите на съвременните заплахи

Сравнителен и анализ

Сравнителният анализ е структуриран по четири ключови показателя. Тези показатели позволяват да се изгради унифицирана рамка, чрез която да се сравнят заплахи с различна природа. Те са следните: динамика на атаката, степен на устойчивост, доминиращ риск и оценка на критичността. Данните от сравнителния анализ са поместени в таблица 1.

Таблица 1. Сравнителен анализ на Data Stealer заплахи по показатели

Вирус	Динамика на атаката	Степен на устойчивост	Доминиращ риск	Оценка на критичността
Lumma Stealer	Екстремно бърза експлоатация	Ограничена (липса на дългосрочно присъствие)	Незабавна кражба на криптоактиви	Висока
Agent Tesla	Средна скорост	Умерена устойчивост	Кражба на удостоверителни данни	Висока
AsyncRAT	Средна	Висока (перманентен достъп до системата)	Пълен контрол и наблюдение	Критична
Fake Captchas	Много висока	Ниска (разчита на потребителски действия)	Компрометиране на сесии (Cookies)	Висока
PDF Malware	Висока	Ниска (единичен входен механизъм)	Доставяне на вторичен зловреден код	Средна

MITRE ATT&CK съпоставка

За всяка разгледана заплаха е извършено прецизно картографиране към рамката MITRE ATT&CK. Анализът помага за точното идентифициране на об-

щите и уникалните тактики, техники и процедури (TTPs). Картографирането е в основата на изграждането на ефективни защитни стратегии, които са пряко базирани на реалните тактики на нападателите и гарантират по-високо ниво на сигурност за системите (MITRE. (n.d.). *MITRE ATT&CK*).

Картографирането на техниките към MITRE ATT&CK показва, че разглежданите заплахи използват:

- T1056.001 (Keylogging);
- T1539 (Steal Web Session Cookie);
- T1219 (Remote Access Software);
- T1547.001 (Registry Run Keys);
- T1081 (Credentials in Files).

Чрез картографирането се изгражда структуриран модел на защита, който не е насочен към конкретен вирус, а към цял клас техники. Чрез разделяне на всяка заплаха на специфични тактики, техники и процедури (TTP) се създава стандартизирана базова линия за откриване в корпоративната среда. Пълната матрица на поведението и анализът на пресечните точки на тези техники са обобщени и представени в Приложение 1 (Hristova, 2026). Резултатите и в двете таблици показват въздействието на идентифицираните заплахи. По този начин се преодолява разликата между абстрактните теоретични дефиниции на зловредния софтуер и реалните поведенчески данни. Циклите на изпълнение на петте изследвани заплахи са систематично картографирани към рамката MITRE ATT&CK.

Легенда на таблицата:

- [P] = Техниката е първична/критична за модула на атака.
- [S] = Техниката е вторична/наблюдавана в специфични кампании или варианти.
- [X] = Техниката не е характерна или липсва в изследвания отпечатък на зловредния софтуер.

Таблица 2. Сравнителна матрица на техниките на MITRE ATT&CK

MITRE ATT&CK Тактика	Техника/ ID	Lumma Stealer	Agent Tesla	Asyn-crAT	PDF Mal-ware	Fake Captchas
Initial Access	Phishing (\$T1566\$)	User Execution (\$T1204\$)	Command/Scripting Interpreter (\$T1059.001\$)	Credentials in Files (\$T1081\$)	Steal Web Session Cookie (\$T1539\$)	Remote Access Software (\$T1219\$)
Execution	[X]	[P]	[P]	[S]	[P]	[X]
	[P] (T1566.001)	[P]	[S]	[P]	[S]	[X]
Credential Access	[X]	[P]	[S]	[S]	[S]	[P]
	[P] (T1566.001)	[P]	[P]	[X]	[X]	[X]
Command & Control	[P] (T1566)	[P]	[S]	[X]	[X]	[S]

Въз основа на таблица 2 може да бъдат предоставени кодовете за очаквани щети и механизми на действие за различни видове вируси. Идеята е да се предприемат логически защитни мерки, както следва:

Фалшиви капчи (ClickFix): T1566.002 -> T1565.002 -> T1204.004 -> T1059.001 -> T1105 -> T1539.

Зловреден софтуер за PDF: T1566.001 -> T1204.002 -> T1059.007 -> T1105 -> (T1219 / полезен товар на infostealer) По избор: T1203, ако се използва експлойт за четене на PDF файлове (CVE).

Lumma Stealer: T1566 / малвертисинг -> T1204.002 или T1204.004 -> T1059.001 -> T1005, T1539.

Agent Tesla: T1566.001 -> T1204.002 -> T1056.001, T1081, T1115 -> изтичане.

AsyncRAT: T1566.001 -> T1204.002 -> T1219 -> T1547.001 -> T1105.

Ясно е, че атаките се извършват чрез различни кодове, но някои са често срещани. Това улеснява отбранителната работа.

Динамичен технически анализ на разглежданите заплахи чрез ANY.RUN

Динамичният технически анализ е проведен в контролирана среда (sandbox) върху 64-битова операционна система Windows 10. За изследването са използвани проби от MalwareBazaar и реални фишинг кампании. Той представлява основната част от изследването, тъй като разкрива реалното поведение на зловредния софтуер в контролирана среда. За целта е използвана платформата ANY.RUN, която позволява:

- проследяване на процеси;
- анализ на мрежови връзки;
- откриване на антианализ техники;
- наблюдение на файлови операции;
- визуализация на C2 комуникация.

Lumma Stealer

Dropper механизъм: Пробата Bafopa.exe функционира като класически зловреден софтуер (malware), чиято основна и единствена цел е да проникне в компютъра на жертвата, да „достави“ и да инсталира друг, често много по-опасен вирус. Първоначално файлът стои пасивно в папка Downloads. Преди стартиране той не извършва никакви подозрителни действия. Веднъж активиран, този зловреден софтуер зарежда основния полезен товар (program.exe) директно в паметта. Това поведение е типично за съвременните инфостийлъри. Целта е да се минимизират следите върху диска и да се избегне засичане.

Основни функции: Lumma Stealer притежава широк набор от злонамерени функции. Софтуерът краде бисквитки (T1539) и извлича локални файлове от системата (T1005). Той може да краде криптовалuti чрез четене на паметта на браузър. Всички събрани данни се структурират автоматично в JSON формат. След това информацията се изпраща към множество командни C2 домейни.

Антианализ техники: Вирусът използва сложни методи за избягване на защита. Неговата C2 инфраструктура се променя динамично в реално време. Хакерите често използват компрометирани легитимни домейни за прикритие. Целият изходящ трафик е криптиран, за да се затрудни проверката му. Lumma Stealer прилага и специални техники за разпознаване и избягване на среди, в които могат да се стартират програми или да се изпълнява код, без да навреди на операционната система (sandbox среди).

PDF Malware – задълбочен технически анализ

Поведение при отваряне: При отваряне на зловредния файл първоначално се стартира легитимният процес Acrobat.exe. Веднага след това системата създава множество подпроцеси с името AcroCEF.exe. Един от тези процеси се използва за установяване на външна връзка към команден C2 сървър. Тази активност често остава незабелязана от потребителя.

Техники за прикриване: Зловредният софтуер използва интелигентни методи за маскиране. Той разчита на легитимни процеси на Adobe, за да избегне засичане от антивирусните системи. Мрежовият трафик е маскиран като стандартна HTTPS връзка към доверени домейни. За изпълнение на зловредния код в документа често се вграждат скрити JavaScript обекти.

Роля като downloader: Този вид PDF файлове често служат като първоначален вектор за заразяване. Те функционират като инструмент за изтегляне на по-сложни вируси. Чрез тях в системата проникват заплахи като Agent Tesla и AsyncRAT. Също така те често осигуряват достъп за инфостийлъри като Lumma Stealer. По този начин обикновеният PDF документ се превръща във входна точка за цяла серия от атаки.

Fake Captchas – задълбочен технически анализ

Социално инженерство: Атаката разчита на измамна визуална манипулация. Потребителят вижда интерфейс, който имитира легитимен Windows Update. Браузърът се превключва автоматично в режим на цял екран (fullscreen), за да скрие подозрителните елементи. Жертвата бива подведена да копира злонамерен PowerShell код под предлог, че потвърждава своята идентичност.

Технически етапи: Процесът на заразяване преминава през няколко прецизни стъпки. Първо, от потребителя се изисква да отвори диалоговия прозорец Run чрез клавишната комбинация Windows + R. След поставяне и изпълнение на скрипта PowerShell изтегля зловреден файл в системната папка Temp. Преди активиране се извършва щателна проверка за наличие на виртуална машина. Ако средата е реална, кодът се инжектира в легитимния процес OOBEMaintenance.exe. Накрая в браузъра се инсталира зловредно разширение за кражба на данни.

Антианализ техники: Вирусът прилага строги механизми за самозащита. Той проверява версията и настройките на BIOS, за да установи дали се намира в тестова среда. Системата сканира за активни процеси, характерни за вирту-

ални машини (VM). Проверяват се и специфични системни параметри, за да се гарантира, че атаката няма да бъде анализирана от изследователи по сигурността.

AsyncRAT – задълбочен технически анализ

Стартиране чрез PowerShell: Процесът на заразяване започва с изпълнението на специализиран скрипт. Dropper-ът използва PowerShell, за да зареди зловредния софтуер директно в оперативната памет. Този метод е известен като „безфайлова“ атака. По този начин на твърдия диск не остават следи, които традиционните защити да засекат.

Техники за маскиране: AsyncRAT прилага сложни тактики за прикриване на своята дейност. Той често използва легитимния инструмент `aspnet_compiler.exe`, за да скрие злонамерения код. Вирусът имитира системни процеси на Windows, за да не буди подозрение в диспечера на задачите. За допълнителна сигурност нападателите често използват легитимни цифрови подписи за своите компоненти.

Осигуряване на устойчивост: Зловредният софтуер е проектиран да оцелява дълго в компрометираната система. Той създава планирана задача в Windows (Scheduled Task) с подвеждащото име `ChromeReporter`. Тази настройка гарантира автоматичното стартиране на вируса след всеки рестарт на компютъра. Така хакерите запазват своя пълен контрол върху машината за неопределено време.

Agent Tesla – задълбочен технически анализ

Антианализ техники: Agent Tesla използва агресивни методи, за да остане скрит от системните администратори. Той автоматично деактивира услугата Windows Event Log, за да спре записването на системни събития. Основният му .NET код е подложен на тежка обфускация. Това прави анализа и декомпилирането на софтуера изключително трудни за изследователите.

Кражба на данни: Този зловреден софтуер е специализиран в мащабно извличане на конфиденциална информация. Той краде запазени пароли, бисквитки и данни за автоматично попълване (autofill) от браузърите. Вирусът извлича и настройките за Wi-Fi мрежи, както и идентификационни данни за VPN клиенти. Обект на интерес са и FTP акаунтите, използвани за пренос на фирмени файлове.

C2 комуникация: Методите за изпращане на откраднатата информация са модерни и ефикасни. Agent Tesla често използва Telegram API за комуникация с нападателите. Целият мрежов трафик е криптиран, за да се заобиколят системите за мониторинг. Данните се изпращат в реално време, което позволява на хакерите да реагират светкавично.

ДИСКУСИЯ

На базата на така направения анализ са подготвени следните препоръки за защита, групирани по целева насоченост:

Превантивни мерки и безопасност

Необходимо е винаги да се проверяват съмнителните файлове в платформи като ANY.RUN или VirusTotal. Необходимо е да се използва само лицензиран софтуер и да се избягват пиратски версии. Също така трябва да се активират функциите Enhanced Protection и HTTPS-only в браузъра. Потребителите трябва да бъдат изключително внимателни към подозрителни URL адреси и фишинг опити. При съмнение за пробив незабавно трябва да се прекъсне връзката с интернет. Следва преинсталиране на операционната система на чисто от външен носител.

Еволюция към специализация и модулност

Един от най-значимите изводи от изследването е тенденцията към специализация на зловредния софтуер. Днес се наблюдава ясна специализация на заплахите. Тя обхваща инфостийлър за кражба на данни (Lumma Stealer, Agent Tesla), механизми за изтегляне на зловреден код (PDF Malware), социално-инженерни атаки (Fake Captchas) и инструменти за дългосрочен контрол (AsyncRAT).

Този специализация позволява на атакуващите да изграждат многослойни атаки, при които всеки компонент изпълнява строго определена роля. Този модел наподобява индустриална верига, в която различни инструменти работят в синхрон, за да постигнат максимален ефект.

Комбинирани атаки, усложняване на техниките за прикриване и синергия между заплахите

Всички разгледани заплахи демонстрират напреднали методи за избягване на детекция. Един от най-важните изводи е, че съвременните атаки рядко използват само един инструмент. Може да се комбинират в различна комбинация, както следва:

- Lumma Stealer + AsyncRAT;
- PDF Malware + Agent Tesla;
- Fake Captchas + Lumma Stealer.

В зависимост от тази комбинация навлизането на тези Malware позволява на атакуващите да постигнат някоя от следните заплахи:

- първоначална компрометация;
- кражба на данни;
- дългосрочен контрол;
- повторна инфекция;
- скрито наблюдение.

Това превръща атаките в многостепенни операции, които могат да останат незабелязани седмици или месеци. Това показва, че съвременният зловреден софтуер е ориентиран към дълбоко прикриване, а не към груба сила. Това усложнява работата на антивирусните системи и изисква нови подходи за откри-

ване, базирани на поведенчески анализ, машинно обучение и мониторинг на аномалии.

Необходимост от многослойна защита

На базата на анализа става ясно, че ефективната защита изисква многослоен подход, включващ:

- технически мерки (антивирус, EDR, DNS защита);
- организационни мерки (политики, процедури);
- образователни мерки (обучение на потребители);
- реакционни мерки (инцидентен отговор);
- мониторинг в реално време.

Нито един слой сам по себе си не е достатъчен. Само комбинацията от тях може да осигури адекватна защита (Wang, Wang, 2025).

Значение за бъдещето на киберсигурността

Анализът на съвременните заплахи очертава комплексна и динамична еволюция в киберсигурността. Наблюдава се трансформация на киберпрестъпността във високоефективна индустрия. Водеща тенденция е пълната автоматизация на векторите на атака. В близко бъдеще се очаква провеждането на масирани кампании срещу критична инфраструктура без постоянна човешка намеса. Алгоритмите ще откриват и експлоатират уязвимости в рамките на милисекунди, което радикално ще съкрати времето за реакция на защитните системи.

Ключов катализатор в този процес е целенасочената интеграция на изкуствен интелект от страна на атакуващите субекти. Технологията позволява създаването на адаптивен зловреден софтуер, който модифицира собствения си код за избягване на сигнатурна детекция. Успоредно с това методите на социалното инженерство стават психологически по-прецизни. Използването на deepfake аудио и видео генерира измами, които са трудно различими от легитимните комуникации. Това задълбочава уязвимостта на човешкия фактор и затруднява експертния анализ.

Тревожен аспект е интеграцията на зловреден код в легитимни облачни услуги. По този начин компрометираният трафик се маскира в потока от легални бизнес процеси. Рискът се мултиплицира от модела „зловреден софтуер като услуга“ (Malware-as-a-Service – MaaS), който снижава техническата бариера за нападателите и увеличава броя на инцидентите. Тези фактори налагат радикална промяна в парадигмата на цифровата отбрана. Традиционните пасивни защити са неефективни. Необходима е проактивна, динамична архитектура за сигурност, базирана на машинно обучение, която открива аномалии в поведението и изолира заплахите в реално време.

ЗАКЛЮЧЕНИЕ

Съвременната киберсреда се характеризира с изключително висока динамика, непрекъсната еволюция на заплахите и нарастваща сложност на атакуващите механизми. Анализът на петте разгледани Data Stealer заплахи – Lumma

Stealer, PDF Malware, Fake Captchas, AsyncRAT и Agent Tesla – ясно показва, че киберпрестъпността вече не се основава на единични, изолирани атаки, а на цялостни екосистеми, които комбинират технически, психологически и организационни подходи за максимално въздействие.

В заключение може да се обобщи, че:

- Data Stealer заплахите са сред най-опасните и най-разпространените форми на киберпрестъпност;

- те демонстрират висока степен на специализация и адаптивност;
- комбинират технически и психологически техники;
- често работят в синергия;
- изискват многослойна защита;
- разбирането на техните TTPs е ключово за ефективна превенция.

Настоящият анализ предоставя цялостна картина на съвременните Data Stealer заплахи и може да служи като основа за разработване на защитни стратегии, обучение на потребители и подобряване на организационните политики за сигурност.

REFERENCES

- Ablon, L. (2018, March 15). *Data thieves: The motivations of cyber threat actors and their use and monetisation of stolen data* [Testimony]. House Financial Services Committee. https://democrats-financialservices.house.gov/uploaded-files/03.15.2018_lilian_ablon_testimony.pdf
- Centre for Internet Security. (2025, November 14). *Top 10 malware Q3 2025*. <https://www.cisecurity.org/insights/blog/top-10-malware-q3-2025>
- Check Point Software Technologies. (n.d.). What is Agent Tesla malware? *Cyber Hub*. <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/agent-tesla-malware/>
- Check Point Software Technologies. (n.d.). What is Lumma malware? *Cyber Hub*. <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/lumma-malware/>
- Chen, T. M. (2003). Trends in viruses and worms. *The Internet Protocol Journal*, 6(3), 23–33. https://jianhua.cis.k.hosei.ac.jp/course/net/Reference/20IPJ_sep2003.pdf
- Choi, K.-S., Lee, C. S., Merizalde, J. (2023). Spreading viruses and malicious codes. In *Handbook on crime and technology* (pp. 232–250). Edward Elgar Publishing.
- HP Development Company. (2025, February 6). “I am not a robot”: CAPTCHAs being used to spread malware, HP warns [Press release]. <https://www.hp.com/us-en/newsroom/press-releases/2025/i-am-not-a-robot-captchas-being-used-to-spread-malware-hp-warns.html>
- Infosecurity Magazine. (2025, February 4). *Surge in infostealer attacks threatens EMEA organisations*. <https://www.infosecurity-magazine.com/news/surge-in-infostealer-attacks-emea/>

- MITRE. (n.d.). *MITRE ATT&CK®*. Retrieved February 1, 2026, from <https://attack.mitre.org/>
- Bradbury, M., Maple, C., Yuan, H., Atmaca, U. I., Cannizzaro, S., “Identifying Attack Surfaces in the Evolving Space Industry Using Reference Architectures.” In *2020 IEEE Aerospace Conference, Big Sky, MT, USA: IEEE*, Mar. 2020, pp. 1–20. doi: 10.1109/AERO47225.2020.9172785.
- Scharfman, J. (2024). Wallet drainers, crypto stealers and cryptojacking. In *The cryptocurrency and digital asset fraud casebook*, Volume II (pp. 123–145). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-60836-0_10
- Park, S., Lee, M., Na, S., Lim, J. “Destructive Malwares on MITRE ATT&CK Tactics for Cyber Warfare: A Brief Survey and Analysis.” In *Mobile Internet Security*, vol. 2095, I. You, M. Choraś, S. Shin, H. Kim, and P. V. Astillo, Eds. In *Communications in Computer and Information Science*, vol. 2095. Singapore: Springer Nature Singapore, 2024, pp. 260–270. doi: 10.1007/978-981-97-4465-7_19.
- Ongun, T. et al., “PORTFILER: Port-Level Network Profiling for Self-Propagating Malware Detection.” In *2021 IEEE Conference on Communications and Network Security (CNS)*, Tempe, AZ, USA: IEEE, Oct. 2021, pp. 182–190. doi: 10.1109/CNS53000.2021.9705045.
- Wang, S., Wang, Y. (2025). Malware classification technology combining multi-modal fusion with deep learning algorithms. *Journal of Cyber Security and Mobility*, 14(3), 597–622. <https://doi.org/10.13052/jcsm2245-1439.1434>
- Hristova, T. (2026, June 1). *A MITRE ATT&CK-Based Comparative Framework for Five Prevalent Data-Stealer Threats: Application to Lumma Stealer Sandbox Analysis*. <https://doi.org/10.17605/OSF.IO/M7ECS>

THE REALM OF DIGITAL THEFT: A COMPARATIVE ANALYSIS OF PROMINENT DATA STEALERS

Abstract: *Technology and the web have transformed our existence. Today, young people live simultaneously in reality and on the internet. However, moving activities online has created new risks. Data theft is now a leading form of cybercrime.*

This article explores the development of popular Data stealer software families. The focus is on malware such as Lumma Stealer, PDF malware, Fake Captchas, AsyncRAT, and Agent Tesla. A comparative analysis of their latest versions is provided. The text describes their core technical parameters and methods of operation.

The study highlights key trends such as automation and modular architecture. It examines malware adaptability and the “Malware-as-a-Service” (MaaS) model. The impact on operating systems and file security is also analysed.

This material is valuable for security software developers and cybersecurity experts. It is also intended for system administrators and everyday users. The goal is to enable everyone to protect their personal information more effectively.

Keywords: *cybercrime; malware; analysis; cybersecurity; data theft*

Dimitar Yonchev, Student

ORCID:0009-0009-9861-3115, WoS, SCOPUS ID

Scientific Advisor: Iva Kostadinova

University of Library Studies and Information Technologies

Sofia, Bulgaria

E-mail: 2452@unibit.bg

Assist. Iva Kostadinova, PhD

ORCID: 0000-0002-1600-5477, WoS: AHB-6267-2022, SCOPUS

ID:57205603432

University of Library Studies and Information Technologies

Sofia, Bulgaria

E-mail: i.kostadinova@unibit.bg