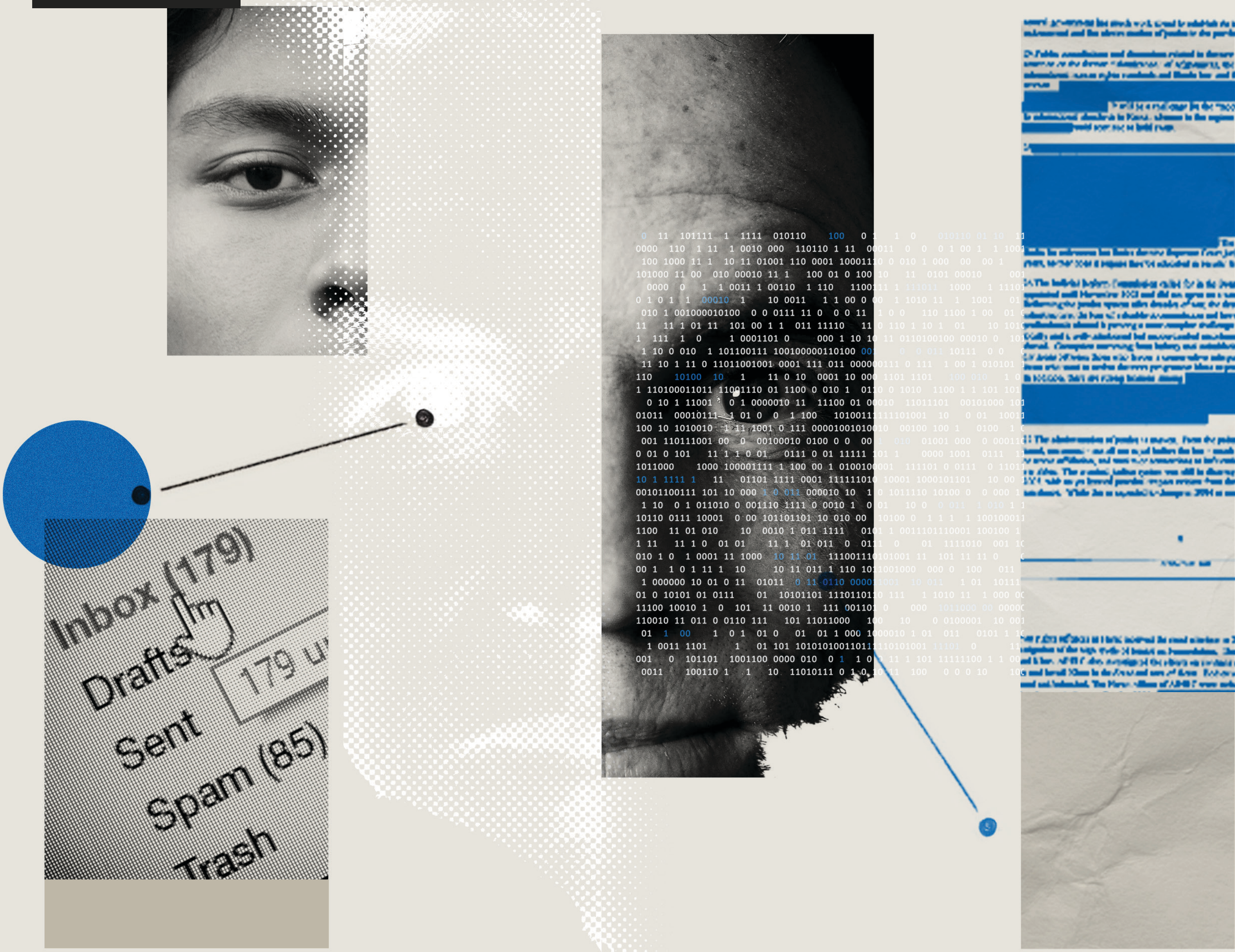
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

August 20, 2025



Behind the Curtain: How Lumma Affiliates Operate

Insikt Group conducted a first-of-its-kind analysis of multiple Lumma affiliates within a vast, interconnected information-stealing ecosystem.

The Lumma affiliate ecosystem relies on numerous services and previously unseen tools, including a cracked email checker and a phishing kit tied to another active cyber actor.

Lumma affiliates often run multiple schemes at once and use underground forums as hubs for recruitment, tools, and monetizing stolen data through markets and fraud services.

Executive Summary

Insikt Group delivers a first-of-its-kind analysis of multiple Lumma affiliates operating within a vast, interconnected information-stealing ecosystem. The Lumma infostealer has been around since 2022, and its ecosystem is supported by a broad array of operational enablers, including proxy networks, virtual private networks (VPNs), anti-detect browsers tailored for multi-account management, exploit and crypting services, and detection evasion tools designed to ensure stealth and continuity. The investigation revealed previously undocumented tools and demonstrated that Lumma affiliates frequently operate multiple schemes simultaneously. For instance, one affiliate was identified operating rental scams, while others simultaneously leveraged multiple malware-as-a-service (MaaS) platforms, including Vidar, Stealc, and Meduza Stealer, likely to bolster operational agility, improve success rates, and mitigate the risks linked to detection and law enforcement takedowns. In addition, several Lumma affiliates are tied to distinct threat actor personas across underground forums, reinforcing their deep integration within the broader cybercriminal ecosystem.

In the short term, defenders should adhere to security best practices by monitoring for exfiltration events, deploying detections such as YARA, Sigma, and Snort rules to uncover both current and historical infections, restricting downloads from websites, and potentially using allow-lists. Organizations should train employees to recognize signs of illegitimate downloads, redirects associated with malvertising, and increasingly common techniques like ClickFix attacks. Additionally, defenders should monitor dark web and underground forums for leaked credentials and malware logs. In the long term, defenders must continuously observe the cybercriminal ecosystem to anticipate emerging threats and adapt security policies and practices accordingly.

Looking ahead, Insikt Group anticipates that the MaaS Lumma and its affiliate network will remain active, having long been a frontrunner in the cybercriminal ecosystem due to its technical sophistication, rapid adoption of new techniques, and demonstrated resilience, as evidenced by its ability to reestablish infrastructure within days of a major law enforcement takedown. While the long-term impact of such operations on Lumma's MaaS affiliate network remains uncertain, there has been no indication of affiliates abandoning the platform or of viable alternatives emerging. Ultimately, Lumma and its affiliates exemplify how modern cybercriminal operations operate as decentralized networks, where even effective disruptions often yield only short-term setbacks. Achieving sustained mitigation will require persistent law enforcement pressure and focused intelligence efforts to monitor and counter the evolving tactics of individual affiliates.

Key Findings

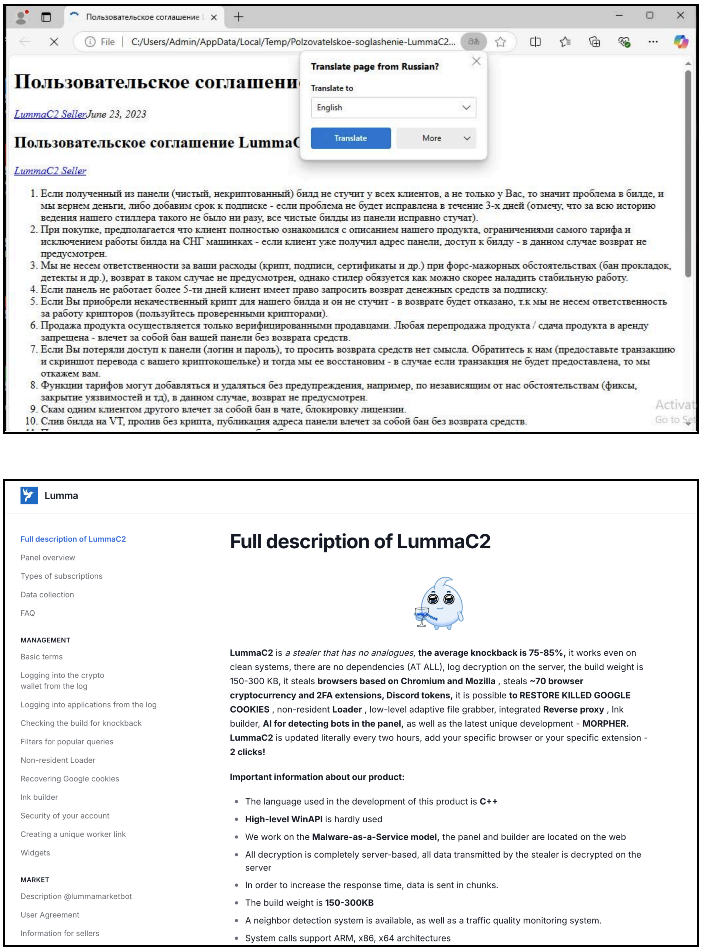
- Insikt Group uncovered previously unreported tools used by Lumma affiliates, including a cracked email credential validation tool circulated on underground forums and a phishing page generator tied to another actor active across multiple forums.
- Lumma affiliates were observed running multiple scams in parallel, some enabled by their use of Lumma, such as using stolen logs for rental fraud. In addition, several affiliates appeared to use multiple infostealers simultaneously, including Vidar, Stealc, and Meduza Stealer, to maximize success rates and mitigate disruptions from detection or law enforcement action.
- Lumma affiliates heavily rely on underground and specialized carding forums as essential operational hubs. They leverage these platforms to recruit collaborators, obtain critical resources such as crypting services and privacy-enhancing services, and efficiently monetize stolen credentials, financial data, and infostealer logs through built-in black markets, fraud tools, and community-backed support networks.

Table of Contents

Background

Lumma, sometimes referred to as LummaC2, was the most widespread infostealer in 2024 based on Recorded Future's malicious infrastructure analysis, and despite facing law enforcement actions in May 2025, it continues to pose a significant threat, actively exfiltrating data from individuals, organizations, and governments. While infostealers like Lumma are now a well-known menace in the cybersecurity landscape, many questions remain: What does a typical day look like for an infostealer affiliate? How do they operate, who are they, what other activities are they involved in, where are they based, and how are the stolen logs ultimately used?

Over the past twelve months (the second half of 2024 through the first half of 2025), Insikt Group has conducted a comprehensive investigation into a broad network of Lumma affiliates operating across multiple countries. Drawing on a wide range of intelligence sources, including two affiliate guidance manuals (see **Figure 1**), Recorded Future Malware Intelligence, Recorded Future Identity Intelligence malware logs, and other proprietary investigative methods, Insikt Group has uncovered detailed, unique insights into these affiliates' operations and tradecraft.


Пользовательское соглашение
File
C:/Users/Admin/AppData/Local/Temp/Polzovatelskoe-soglashenie-LummaC2...
Translate page from Russian?
Translate to
English
Translate
More
Activat
Go to Se

Пользовательское соглашени

LummaC2 SellerJune 23, 2023

Пользовательское соглашение LummaC

LummaC2 Seller

1. Если полученный из панели (чистый, некриптованный) билд не стучит у всех клиентов, а не только у Вас, то значит проблема в билде, и мы вернем деньги, либо добавим срок к подписке - если проблема не будет исправлена в течение 3-х дней (отмечу, что за всю историю ведения нашего стиллера такого не было ни разу, все чистые билды из панели исправно стучат).
2. При покупке, предполагается что клиент полностью ознакомился с описанием нашего продукта, ограничениями самого тарифа и исключением работы билда на СНГ машинках - если клиент уже получил адрес панели, доступ к билду - в данном случае возврат не предусмотрен.
3. Мы не несем ответственности за ваши расходы (крипт, подписи, сертификаты и др.) при форс-мажорных обстоятельствах (бан прокладок, детекты и др.), возврат в таком случае не предусмотрен, однако стилер обязуется как можно скорее наладить стабильную работу.
4. Если панель не работает более 5-ти дней клиент имеет право запросить возврат денежных средств за подписку.
5. Если Вы приобрели некачественный крипт для нашего билда и он не стучит - в возврате будет отказано, т.к мы не несем ответственность за работу крипторов (пользуйтесь проверенными крипторами).
6. Продажа продукта осуществляется только верифицированными продавцами. Любая перепродажа продукта / сдача продукта в аренду запрещена - влечет за собой бан вашей панели без возврата средств.
7. Если Вы потеряли доступ к панели (логин и пароль), то просить возврата средств нет смысла. Обратитесь к нам (предоставьте транзакцию и скриншот перевода с вашего криптокошельке) и тогда мы ее восстановим - в случае если транзакция не будет предоставлена, то мы откажем вам.
8. Функции тарифов могут добавляться и удаляться без предупреждения, например, по независящим от нас обстоятельствам (фиксы, закрытие уязвимостей и тд), в данном случае, возврат не предусмотрен.
9. Скам одним клиентом другого влечет за собой бан в чате, блокировку лицензии.
10. Слив билда на VT, пролив без крипта, публикация адреса панели влечет за собой бан без возврата средств.

Lumma
Full description of LummaC2
Panel overview
Types of subscriptions
Data collection
FAQ
MANAGEMENT
Basic terms
Logging into the crypto wallet from the log
Logging into applications from the log
Checking the build for knockback
Filters for popular queries
Non-resident Loader
Recovering Google cookies
Ink builder
Security of your account
Creating a unique worker link
Widgets
MARKET
Description @lummamarketbot
User Agreement
Information for sellers

Full description of LummaC2

LummaC2 is *a stealer that has no analogues,* **the average knockback is 75-85%,** it works even on clean systems, there are no dependencies (AT ALL), log decryption on the server, the build weight is 150-300 KB, it steals **browsers based on Chromium and Mozilla** , steals **~70 browser cryptocurrency and 2FA extensions, Discord tokens,** it is possible **to RESTORE KILLED GOOGLE COOKIES** , non-resident **Loader** , low-level adaptive file grabber, integrated **Reverse proxy** , Ink builder, **AI for detecting bots in the panel,** as well as the latest unique development - **MORPHER. LummaC2** is updated literally every two hours, add your specific browser or your specific extension - **2 clicks!**

Important information about our product:

- The language used in the development of this product is **C++**
- **High-level WinAPI** is hardly used
- We work on the **Malware-as-a-Service model,** the panel and builder are located on the web
- All decryption is completely server-based, all data transmitted by the stealer is decrypted on the server
- In order to increase the response time, data is sent in chunks.
- The build weight is **150-300KB**
- A neighbor detection system is available, as well as a traffic quality monitoring system.
- System calls support ARM, x86, x64 architectures

***Figure 1**: Lumma manuals from 2023 (top) and 2024 (bottom) (Source: Recorded Future)*

The findings are presented in two sections: The first examines the affiliates' technical ecosystems, detailing their use of info-stealing techniques, favored tools and services, and recurring operational behaviors. The second explores how Lumma affiliates are embedded in the broader underground economy. It analyzes their participation in cybercrime forums, use of additional infostealer malware families, and involvement in other types of online fraud and scams.

Threat Analysis

Operational Infrastructure and Tradecraft

Privacy Enhancing Services

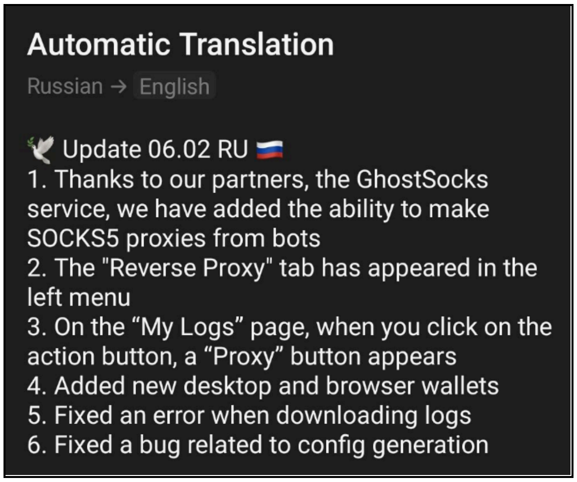
Proxy Services

Insikt Group observed multiple Lumma affiliates leveraging various proxy services, detailed in **Table 1**; Pia Proxy was the most frequently used service. Proxies can be used for legitimate purposes such as privacy and research, but they are frequently exploited by cybercriminals to mask identities, avoid detection, and bypass restrictions. Some services, such as ASocks and the malware-based FACELESS, among others, have been openly marketed on cybercrime forums; ASocks has been linked to fake VPNs that convert Android devices into proxies, while FACELESS leverages malware to hijack IoT devices for the same purpose. Insikt Group evaluated the proxy services by type based on several criteria, including whether they were promoted on cybercriminal forums.

Domains	Name	Type	Prevalence Across Affiliates
piaproxy[.]com	PIA Proxy	Cybercriminal	High
ghostsocks[.]net	GhostSocks	Cybercriminal	High
asocks[.]com	ASocks	Cybercriminal	Medium
faceless[.]cc	FACELESS	Cybercriminal	Medium
hotsocks[.]biz	HotSocks	Cybercriminal	Medium
hotsocks[.]ws	HotSocks	Cybercriminal	Medium
nsocks[.]net	NSOCKS	Cybercriminal	Medium
proxyline[.]net	Proxy Line	Cybercriminal	Medium
vn5socks[.]net	VN5Socks	Cybercriminal	Medium
gridpanel[.]net	GridPanel	Likely cybercriminal	Low
3389rdp[.]com	RDP Shop	Unclear	N/A
922proxy[.]com	922 Proxy	Likely cybercriminal and possibly a rebrand of 911 Proxy	N/A
smartproxy[.]pxf[.]io	Smartproxy	Unclear	N/A
swiftproxy[.]io	Swift Proxy	Unclear	N/A

***Table 1**: Proxy services used by Lumma affiliates (Source: Recorded Future)*

Of note, in early 2024, Lumma began collaborating with the GhostSocks team, a residential proxy plugin, enabling affiliates to create SOCKS5 proxies from infected bots, as announced via Lumma's official channel (see **Figure 2**) (1, 2). By 2025, Lumma expanded this offering, providing affiliates with backconnect proxy access to compromised machines. This allowed threat actors to conduct attacks that appeared to originate from the victim's device, significantly improving their ability to bypass access controls such as Google's cookie-based protections, a mechanism Lumma routinely exploits to refresh expired tokens.


Automatic Translation

🕊 Update 06.02 RU 🇷🇺
1. Thanks to our partners, the GhostSocks service, we have added the ability to make SOCKS5 proxies from bots
2. The "Reverse Proxy" tab has appeared in the left menu
3. On the "My Logs" page, when you click on the action button, a "Proxy" button appears
4. Added new desktop and browser wallets
5. Fixed an error when downloading logs
6. Fixed a bug related to config generation

***Figure 2**: Announcement of GhostSocks-Lumma partnership (Source: X)*

In at least one instance, Insikt Group identified a Lumma affiliate linked to build ID vcs1q5 — and known as "blackowl23" on cybercriminal forums such as Cracked, Nulled, Sinisterly, Eternia, and Cracking during 2022 and 2023 — using IP addresses associated with the Ngioweb botnet. This botnet has been previously linked to the cybercriminal proxy service NSOCKS, as well as others such as VN5Socks and Shopsocks5. The associated IP addresses, likely no longer part of the botnet due to public reporting and other mitigating actions, are listed in **Appendix A**. Many of the IP addresses had been previously validated by Insikt Group and reported on publicly.

VPN Services

According to research conducted by Insikt Group, all analyzed Lumma affiliates were using VPN services in some capacity, with many using multiple providers. A selection of the VPN services observed in use by these affiliates is presented in **Table 2**.

Domain	Service Name	Prevalence Across Affiliates
expressvpn[.]com	ExpressVPN	Medium
nordvpn[.]com	NordVPN	Medium
protonvpn[.]com	Proton VPN	Medium
surfshark[.]com	Surfshark VPN	Medium
tunnelbear[.]com	TunnelBear	Medium

***Table 2**: VPN services used by Lumma affiliates over the past year (Source: Recorded Future)*

Anti-Detection and Multi-Account Browsers

Lumma affiliates frequently rely on specialized privacy-focused and anti-detect browsers (see **Table 3**) to evade identification, bypass security measures, and manage multiple fraudulent accounts simultaneously. These tools allow the threat actors to maintain operational security (OPSEC) by obscuring their true identity, location, and digital fingerprints. Among the most prevalent browsers used by Lumma affiliates is Dolphin, recognized widely as one of the best anti-detect browsers tailored explicitly for managing multiple threat actor-controlled accounts without detection. Dolphin's capabilities are mirrored by Adspower, Hidemyacc, and Kameleo, which similarly facilitate seamless multi-account operations, thereby enhancing operational efficiency and anonymity. Octo Browser, another prominent tool among cybercriminals, provides advanced fingerprint masking, further complicating efforts by law enforcement and threat intelligence professionals to track threat activities to their source.

The Brave browser, while designed primarily for enhanced user privacy rather than outright anti-detection, appeals to threat actors due to its robust built-in security and privacy features, such as aggressive ad and tracker blocking. Although less explicitly tailored for multi-account management, its privacy-focused approach provides valuable baseline protection for threat actors seeking to maintain anonymity online.

Browser	Domain	Prevalence Across Affiliates
Dolphin	dolphin-anty[.]com	High
Octo Browser	octobrowser[.]net	High
Brave	brave[.]com	Medium
Adspower	adspower[.]com	Low
Hidemyacc	hidemyacc[.]com	Low
Kameleo	kameleo[.]io	Low

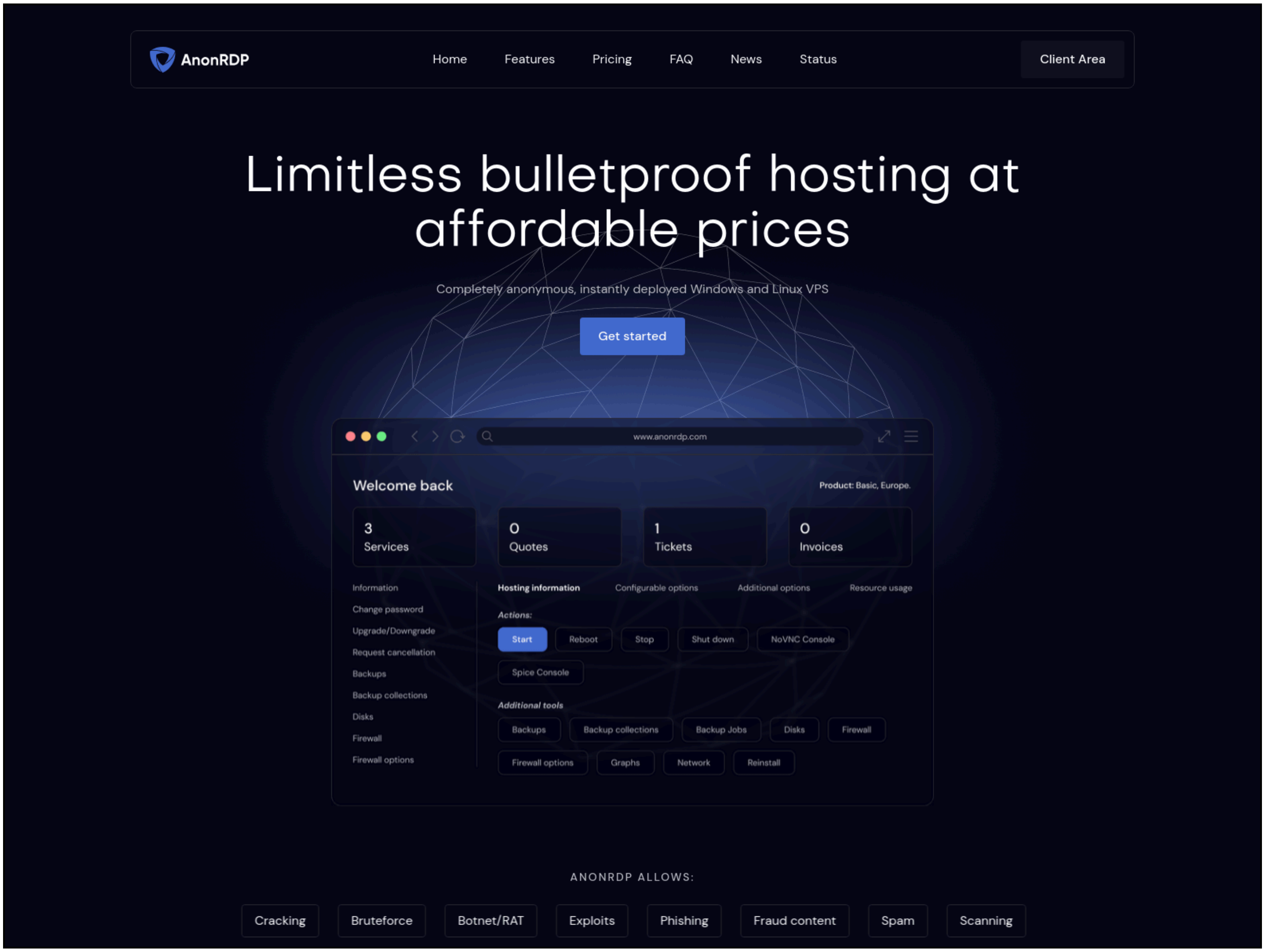
***Table 3**: Anti-detect browsers for multi-account management used by Lumma affiliates (Source: Recorded Future)*

Hosting Providers

While Lumma supplies core C2 infrastructure through its MaaS offering, its affiliates rely on separate hosting providers likely aimed at supporting phishing efforts, payload deployment, and other malicious activity. Many of the hosting providers linked to the analyzed Lumma affiliates appear legitimate, but some stood out for seemingly catering directly to cybercriminals and enabling malicious activity, including AnonRDP, Bulletproof Hosting, and Hostcay, which have been used by the Lumma affiliate linked to the build ID re0gvc.

AnonRDP

AnonRDP (*anonrdp[.]com*) is a self-proclaimed bulletproof hosting provider specializing in anonymous VPS and RDP services, with a strong focus on privacy and resistance to takedown (see **Figure 3**). It requires no identity verification and accepts only cryptocurrency payments, such as Bitcoin and Monero, processed through the payment service provider NOWPayments and, allegedly, the cryptocurrency exchange ChangeNOW. Its tolerance of malicious activity is further confirmed by advertisements on deep web forums such as BreachForums, Hack Forums, Nulled, and Patched. As illustrated in **Figure 3**, the website explicitly acknowledges supporting activities such as hosting, distributing, or controlling botnets, remote access trojans (RATs), phishing, fraudulent content, spam, and more. According to public reports, AnonRDP is operated by Yashvir Keshave, an individual with a known history of involvement in the underground ecosystem, including config (configuration) creation, cracking tools, and digital account trading.



Limitless bulletproof hosting at affordable prices

Completely anonymous, instantly deployed Windows and Linux VPS

***Figure 3**: AnonRDP website (Source: urlscan.io)*

Following the arrest of Yuri Meruzhanovich Bozoyan, co-founder and CEO of Aeza Group LLC, on April 1, 2025, Insikt Group observed that AnonRDP had attempted to poach Aeza customers with 50% discounts. The extent of the poaching's success remains uncertain.

Bulletproof Hosting

Similarly, Bulletproof Hosting (*bulletproofhosting[.]org*) markets itself as an offshore, privacy-centric hosting provider that offers anonymous, takedown-resistant infrastructure, accepts cryptocurrency payments, and has no ID requirements (see **Figure 4**). The website promotes lenient content policies, explicitly permitting adult material, piracy, gambling, and other content typically banned by conventional hosts. It claims to defend against DMCA notices, abuse complaints, and Spamhaus listings, using techniques like FastFlux and hosting in offshore or hardened facilities with minimal regulatory oversight. With 24/7 support managed by self-described "cyber-tech experts," the platform is positioned as a resilient service catering to users seeking both anonymity and consistent uptime, which are often appealing to threat actors and controversial content operators.

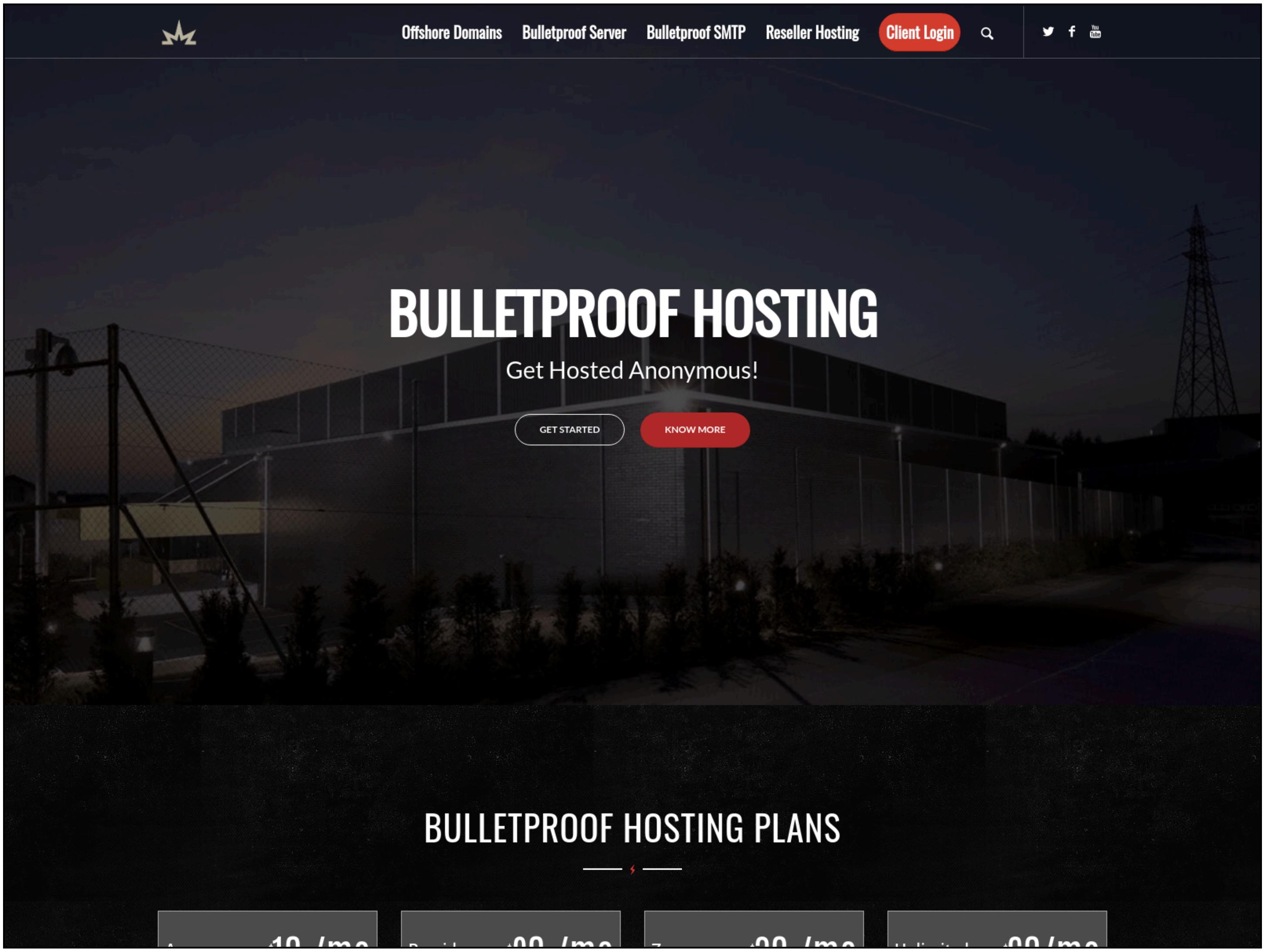
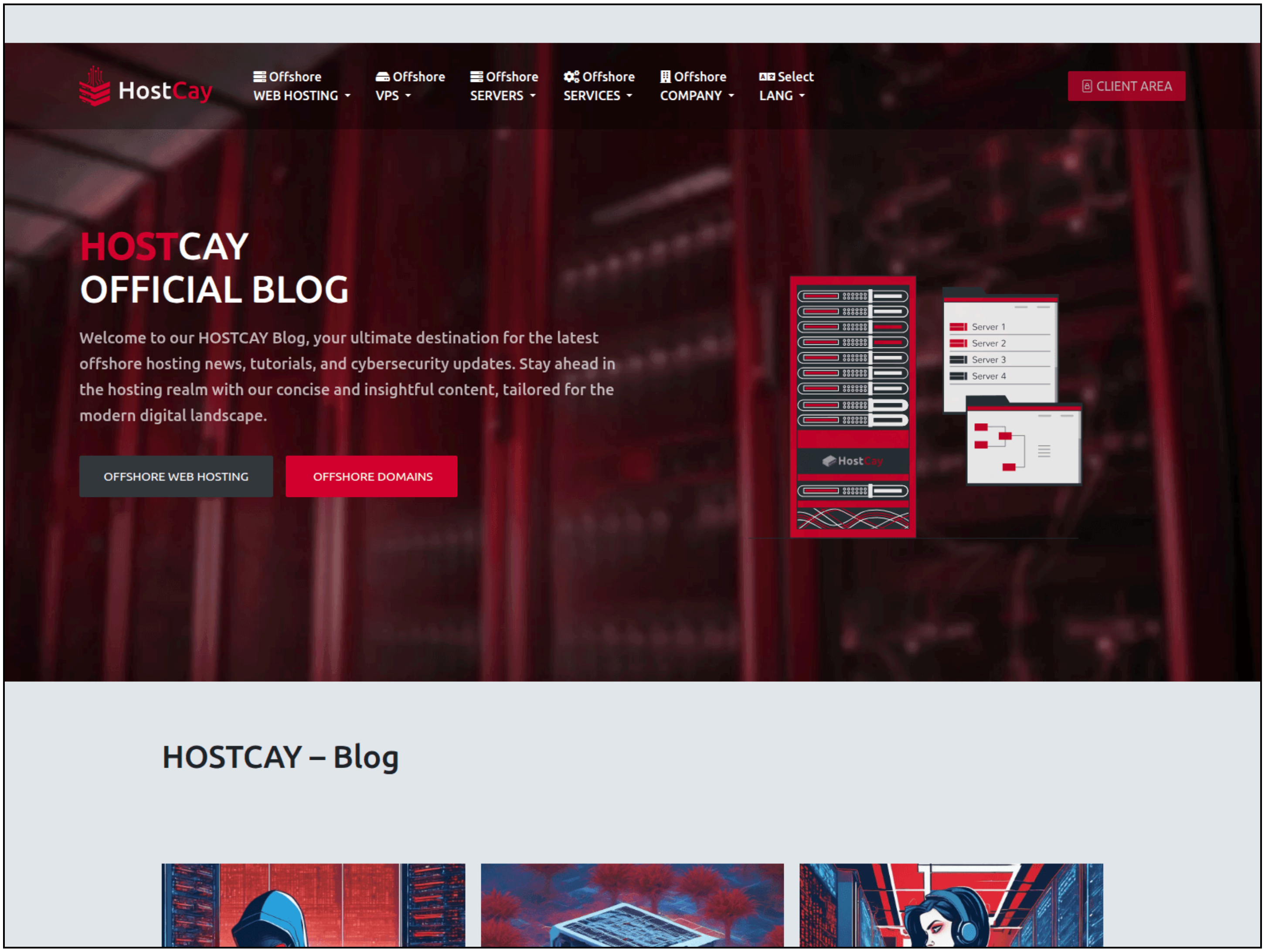


Figure 4: *Bulletproof Hosting website (Source: urlscan.io)*

HostCay

HostCay (*hostcay[.]com*) is a privacy-focused, offshore hosting provider founded in 2023 and operated by Netacel Inc., an international business company (IBC) registered in Seychelles. HostCay specializes in hosting services that prioritize freedom of speech, whistleblower support, and resistance to content takedown requests (see **Figure 5**). It is known for its support for anonymous crypto payments, no ID requirements, and strong free speech protections.



HOSTCAY
OFFICIAL BLOG

Welcome to our HOSTCAY Blog, your ultimate destination for the latest offshore hosting news, tutorials, and cybersecurity updates. Stay ahead in the hosting realm with our concise and insightful content, tailored for the modern digital landscape.

HOSTCAY – Blog

***Figure 5**: HostCay website (Source: urlscan.io)*

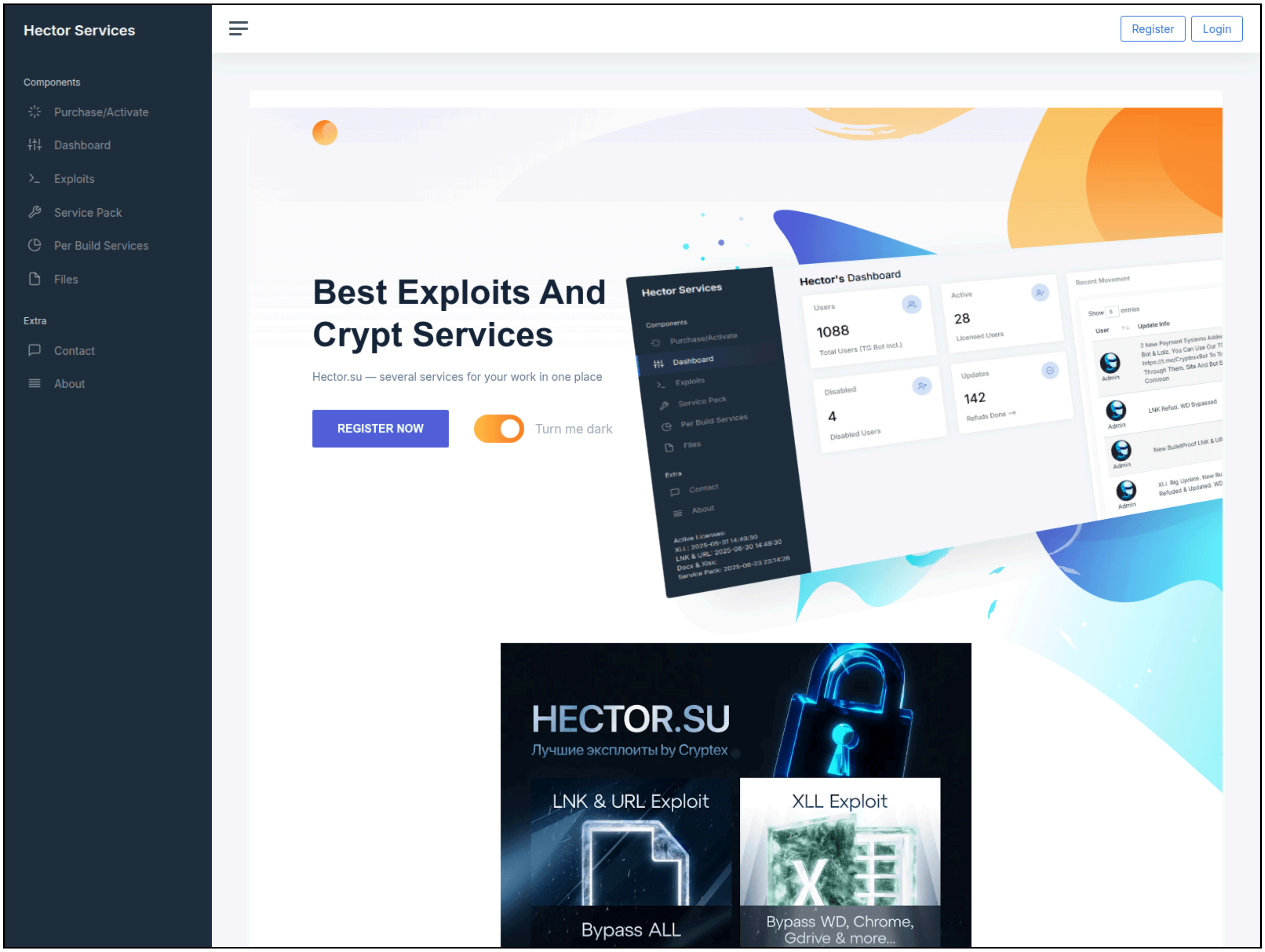
Lumma affiliates have also been observed leveraging numerous legitimate hosting providers and services, including the file hosting platform MEGA (*mega[.]nz*), the file and text sharing service Temp[.]sh (*temp[.]sh*), and the image hosting service ImgBB (*imgbb[.]com*). They have also made use of various URL shortening services such as *shorturl[.]at* and *free-url-shortener[.]rb[.]gy*.

Exploit and Crypting Services

One notable service supporting Lumma operations is run by an actor known as "@cryptexxx." Rather than being a Lumma affiliate directly, @cryptexxx is the operator of a crypting and exploit service known as Hector (advertised via the domain *hector[.]su*) that caters to malware distributors, among others (see **Figure 6**). The HTML content of *hector[.]su* includes meta keywords — such as `crypt`, `exe`, `exploits`, `chrome`, `bypass`, `lnk`, `url`, `xls`, `xll`, `doc`, `docx`, `pdf`, `builder`, `macro`, or `popup` — indicating a broad toolkit for creating malicious payloads across various file formats (from Office macros to Chrome exploits). Forum discussions corroborate that this service provides fully undetectable (FUD) droppers and document exploits for delivering malware. For example, one hacker forum user explicitly directs others to "see URL exploit on *hector[.]su*" as a resource for a Gmail-attachable, FUD exploit. Such exploits often take the form of weaponized Office files, like malicious Excel add-in files (`.XLL`) or macro-laced documents, which can embed the Lumma payload and are designed to slip past email scanners and antivirus protections.

Recent evidence illustrates how these tools are used in practice. In mid-2025, an underground vendor advertised an updated Office exploit that is "up to date, works in 2025 and attachable on Gmail, plus FUD," explicitly boasting that it can bypass Gmail's filters. The same offering also highlights a Windows Defender runtime bypass, with an AV scan report showing 0/26 detections. This means a Lumma affiliate could generate a trojanized file (such as an Excel `.xll` file or a malicious shortcut/URL file) that delivers the stealer while evading both email gateway scanning and endpoint antivirus protections.

By leveraging @cryptexxx's crypting service and exploit builder, the affiliate essentially outsources the difficult aspects of stealth and delivery. It is a clear example of the cooperative nature of LummaC2 operations: the malware developer provides the infostealer malware, the service operator (@cryptexxx) supplies an obfuscation and exploit toolkit, and the affiliate uses these tools to distribute the payload to victims.



Best Exploits And Crypt Services

Hector.su — several services for your work in one place

2 New Payment Systems Added Bot & Lolz. You Can Use Our T https://t.me/CryptexxBot To T Through Them. Site And Bot B Common

LNK Refud. WD Bypassed

New BulletProof LNK & UR

XLL Big Update. New Bu Refuded & Updated. WD

Active Licenses:
XLL: 2025-05-31 14:49:30
LNK & URL: 2025-06-30 14:49:30
Docx & Xlsx:
Service Pack: 2025-06-23 23:14:26

Figure 6: Hector website (Source: urlscan.io)

Email-Linked Services and Tools

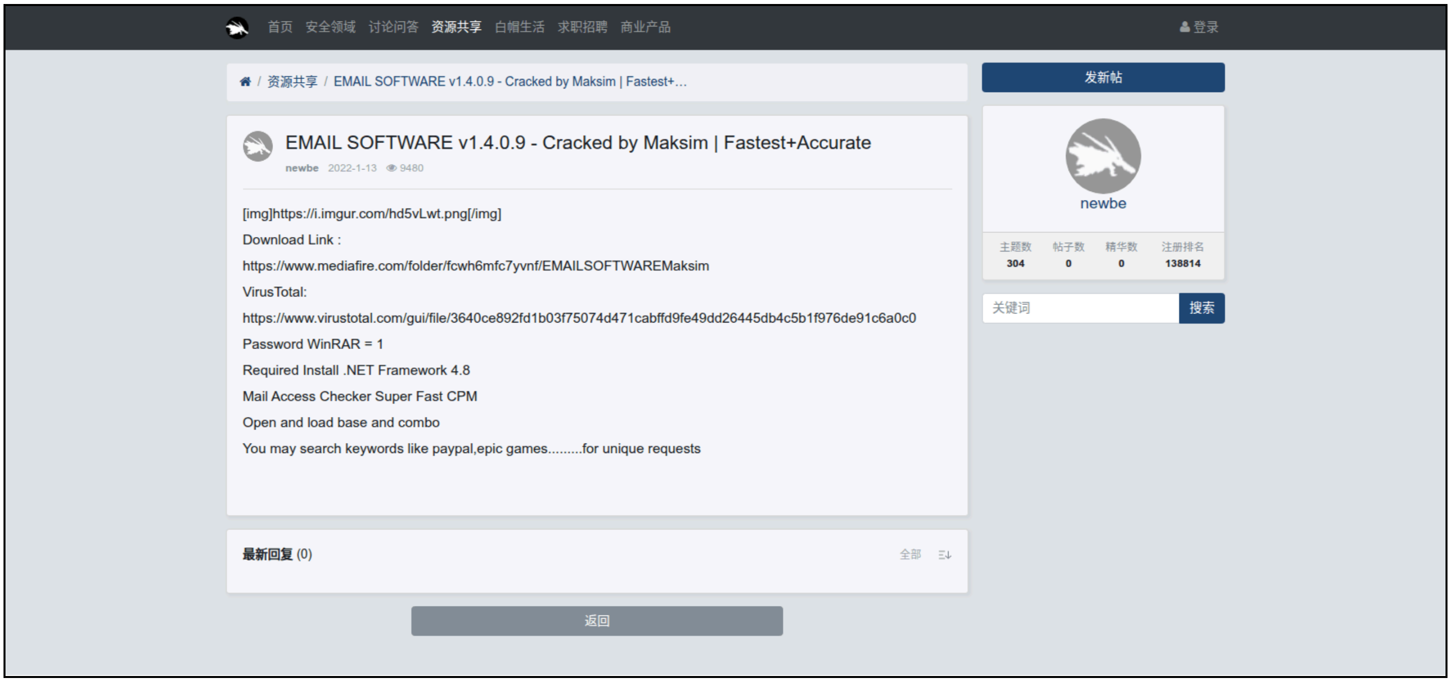
Insikt Group observed multiple Lumma affiliates using a range of email and spam-related services, including a credential validation tool known as "EMAIL SOFTWARE 1.4.0.9 cracked by Maksim" and a phishing page creation tool known as "DONUSSEF", both of which have likely been deployed in at least one confirmed case.

EMAIL SOFTWARE 1.4.0.9 cracked by Maksim

EMAIL SOFTWARE 1.4.0.9 cracked by Maksim[1] is a cracked version of a Windows .NET-based email credential verification tool (see **Figure 7**). It is designed to validate email and password combinations against mail servers using protocols like IMAP and POP3. Users can input large lists of email credentials (often referred to as "combo lists") to check which combinations are valid.[2] The tool also allows users to

[1] SHA256: 3640ce892fd1b03f75074d471cabffd9fe49dd26445db4c5b1f976de91c6a0c0
[2] *hxxps://spyhackerz[.]org/forum/threads/cracked-by-maksim-e-mail-access-checker-1-4-0-9.140317/*

search for specific keywords within email content. The tool is distributed as a password-protected `.rar` archive on various hacking and cracking forums (such as DemonForums or XReactor), with users reporting prices of up to $250 on underground marketplaces.



EMAIL SOFTWARE v1.4.0.9 - Cracked by Maksim | Fastest+Accurate

newbe 2022-1-13 9480

[img]https://i.imgur.com/hd5vLwt.png[/img]

Download Link :

https://www.mediafire.com/folder/fcwh6mfc7yvnf/EMAILSOFTWAREMaksim

VirusTotal:

https://www.virustotal.com/gui/file/3640ce892fd1b03f75074d471cabffd9fe49dd26445db4c5b1f976de91c6a0c0

Password WinRAR = 1

Required Install .NET Framework 4.8

Mail Access Checker Super Fast CPM

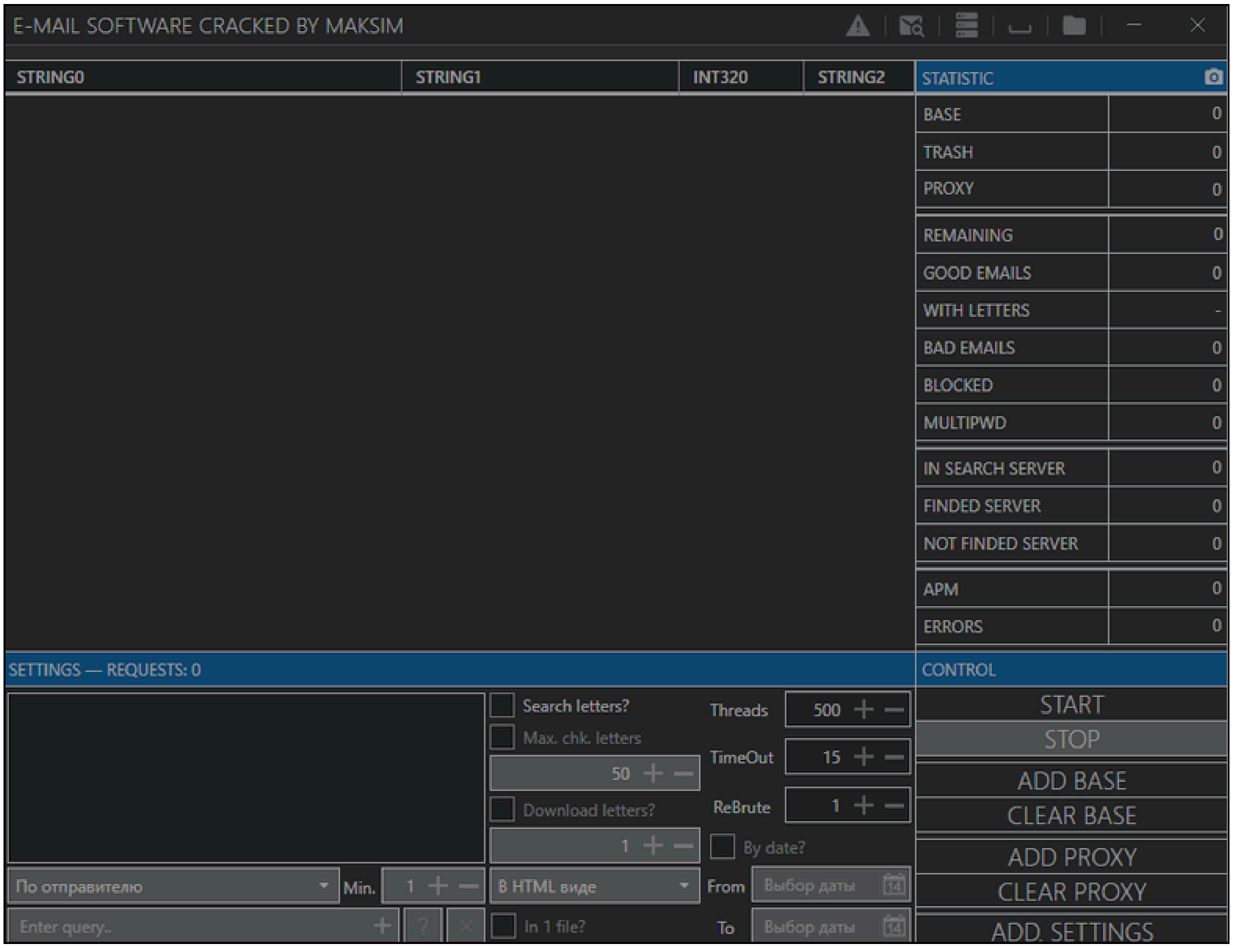
Open and load base and combo

You may search keywords like paypal,epic games.........for unique requests

主题数	帖子数	精华数	注册排名
304	0	0	138814

Figure 7*: EMAIL SOFTWARE 1.4.0.9 cracked by Maksim advertised on forum[.]cnsec[.]org (Source: urlscan.io)*

The tool features a user interface with several configuration options, including a status overview of processed email addresses, a control panel to start or stop validation, and proxy management capabilities, among other functionalities (see **Figure 8**).



E-MAIL SOFTWARE CRACKED BY MAKSIM

STRING0	STRING1	INT320	STRING2

STATISTIC	
BASE	0
TRASH	0
PROXY	0
REMAINING	0
GOOD EMAILS	0
WITH LETTERS	-
BAD EMAILS	0
BLOCKED	0
MULTIPWD	0
IN SEARCH SERVER	0
FINDED SERVER	0
NOT FINDED SERVER	0
APM	0
ERRORS	0

SETTINGS — REQUESTS: 0

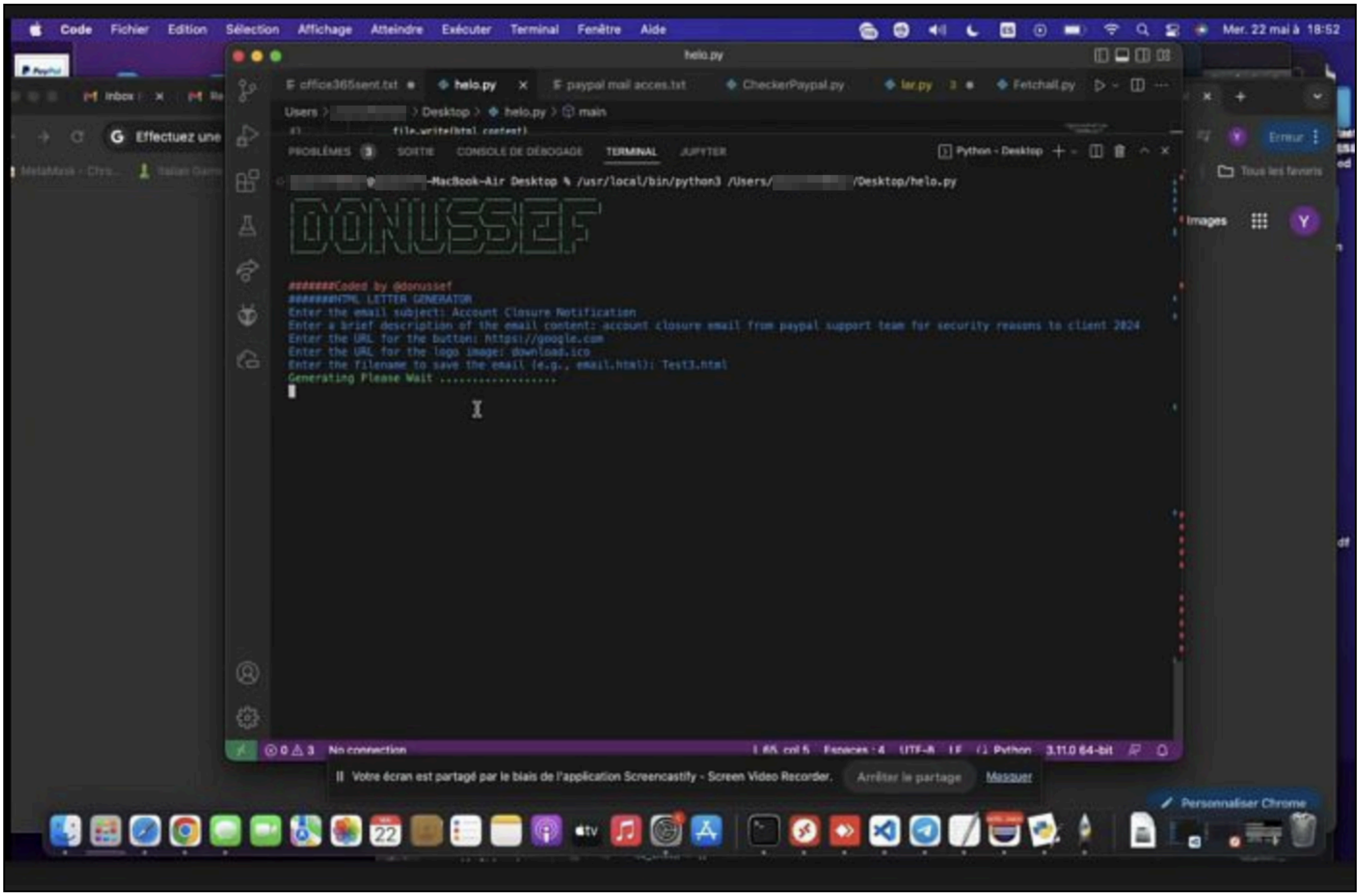
□ Search letters?
□ Max. chk. letters: 50
□ Download letters?: 1
По отправителю — Min. 1
В HTML виде
□ In 1 file?
Threads: 500
TimeOut: 15
ReBrute: 1
□ By date?
From: Выбор даты
To: Выбор даты
Enter query..

***Figure 8**: Graphical user interface (GUI) of EMAIL SOFTWARE 1.4.0.9 cracked by Maksim (Source: Recorded Future)*

Insikt Group assesses that the Lumma affiliate blackowl23 has used or continues to use the tool to validate stolen credentials, which are then leveraged in the follow-on real estate scam detailed in the section blackowl23's Involvement in Real Estate Scam, among other scams. Based on identified configurations, it is possible that the affiliate has customized the tool.

DONUSSEF

Insikt Group identified another tool, known as "DONUSSEF", which was demonstrated in a publicly accessible video hosted on Google Drive at the time of analysis (see **Figure 9**). Believed to be used by blackowl23, the tool is designed to generate phishing pages via the command line using AI. It prompts the user to input URLs, a subject line, and a brief description of the intended phishing content, and then produces an HTML file as output.

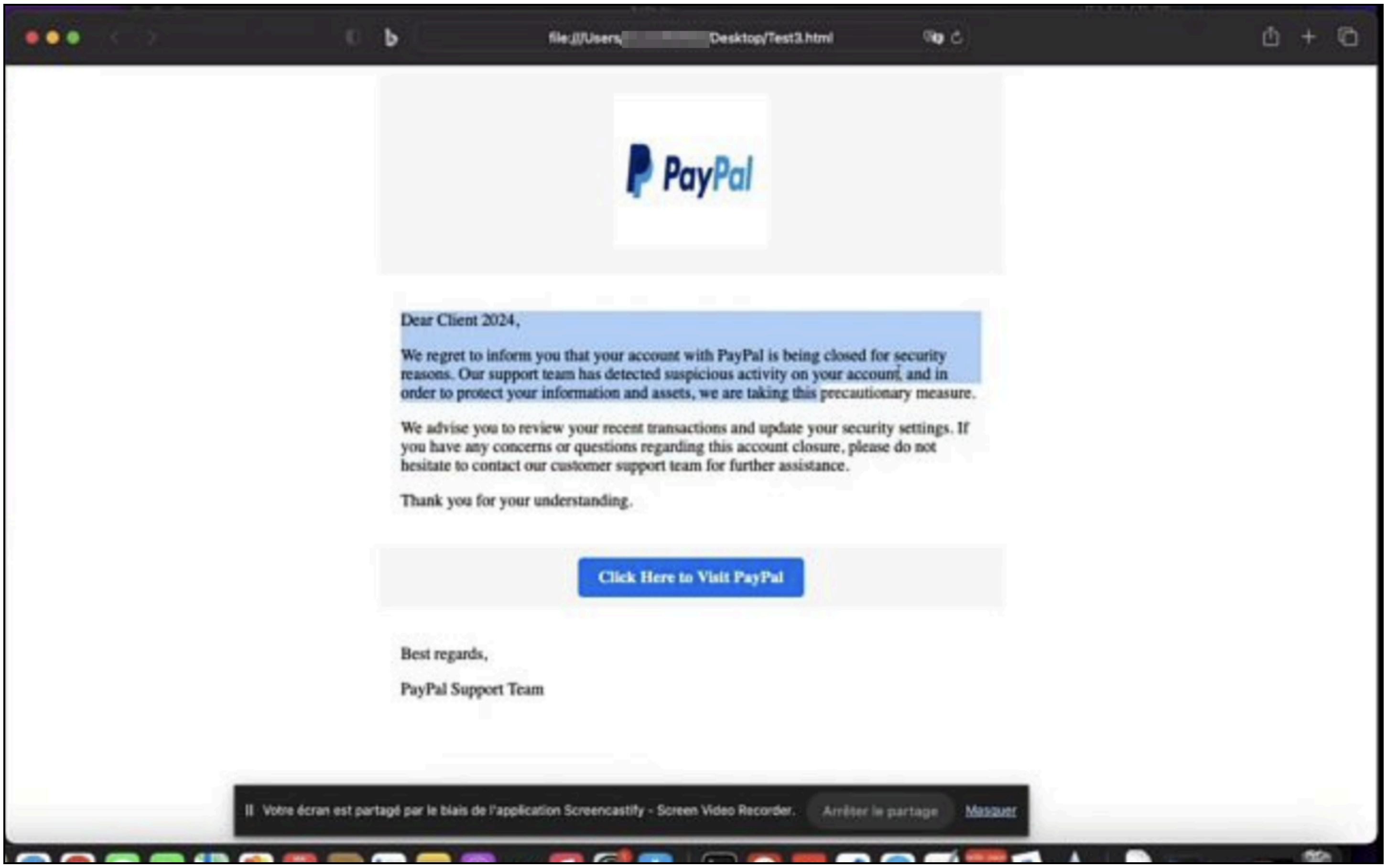


```
[redacted]@[redacted]-MacBook-Air Desktop % /usr/local/bin/python3 /Users/[redacted]/Desktop/helo.py
DONUSSEF

#######Coded by @donussef
#######HTML LETTER GENERATOR
Enter the email subject: Account Closure Notification
Enter a brief description of the email content: account closure email from paypal support team for security reasons to client 2024
Enter the URL for the button: https://google.com
Enter the URL for the logo image: download.ico
Enter the filename to save the email (e.g., email.html): Test3.html
Generating Please Wait ....................
```

***Figure 9**: Demo video of DONUSSEF (Source: Recorded Future)*

The full range of phishing pages the tool can generate remains unclear, as Insikt Group was unable to independently test it. In the demo, it was shown creating only PayPal phishing pages (see **Figure 10**). Due to the unavailability of the actual HTML pages, Insikt Group was unable to assess their effectiveness or determine whether they have appeared in any known campaigns.



file:///Users/[redacted]/Desktop/Test3.html

Dear Client 2024,

We regret to inform you that your account with PayPal is being closed for security reasons. Our support team has detected suspicious activity on your account, and in order to protect your information and assets, we are taking this precautionary measure.

We advise you to review your recent transactions and update your security settings. If you have any concerns or questions regarding this account closure, please do not hesitate to contact our customer support team for further assistance.

Thank you for your understanding.

Best regards,

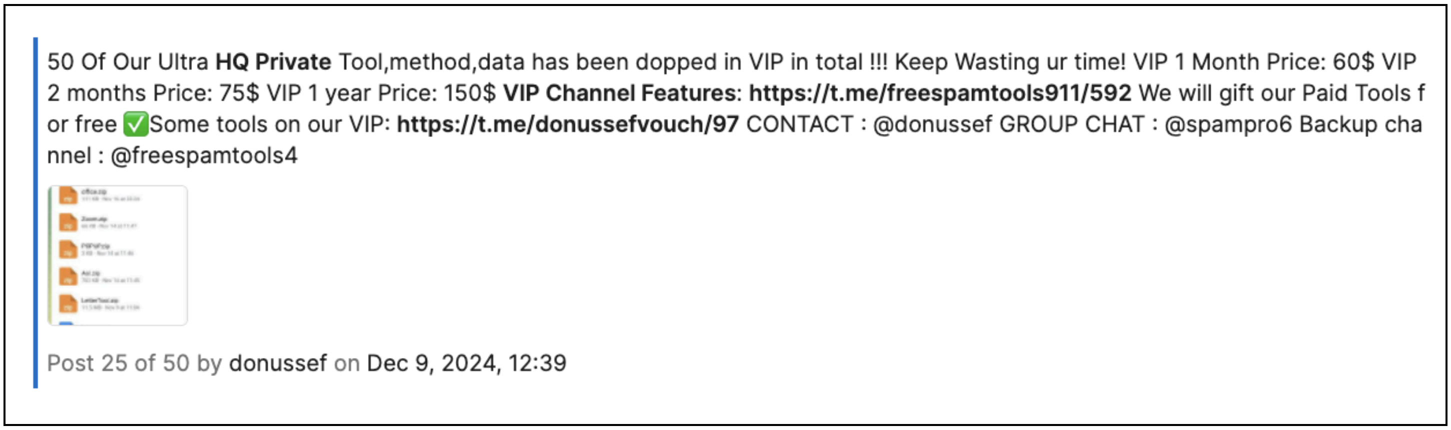
PayPal Support Team

Votre écran est partagé par le biais de l'application Screencastify - Screen Video Recorder.

***Figure 10**: PayPal phishing page generated by DONUSSEF (Source: Recorded Future)*

Through further investigation, Insikt Group identified a YouTube channel likely associated with the suspected creator of DONUSSEF. The actor used the channel to demonstrate at least two additional tools: one marketed as an email sender with a 100% inbox delivery rate, and another for SMS spamming (referred to as "`ULTRA-checker.py`" in the video). Both videos were uploaded on December 18, 2022, from a device using French-language settings. In one of the demo videos, the actor used and accessed two email accounts, *ussefescobar@seznam[.]cz* and *ussefakkar@outlook[.]com*, which are believed to be linked to the actor.

The `ULTRA-checker.py` tool includes references to two Telegram channels: @donussef and @rdpvendor. At least one of these accounts appears to be active in Telegram communities associated with spam-related tools (see **Figure 11**). Insikt Group found no additional links between the suspected creator of DONUSSEF and blackowl23.



50 Of Our Ultra **HQ Private** Tool,method,data has been dopped in VIP in total !!! Keep Wasting ur time! VIP 1 Month Price: 60$ VIP 2 months Price: 75$ VIP 1 year Price: 150$ **VIP Channel Features: https://t.me/freespamtools911/592** We will gift our Paid Tools for free ✅Some tools on our VIP: **https://t.me/donussefvouch/97** CONTACT : @donussef GROUP CHAT : @spampro6 Backup channel : @freespamtools4

Post 25 of 50 by donussef on Dec 9, 2024, 12:39

Figure 11*: @donussef advertising tooling on Telegram (Source: Recorded Future)*

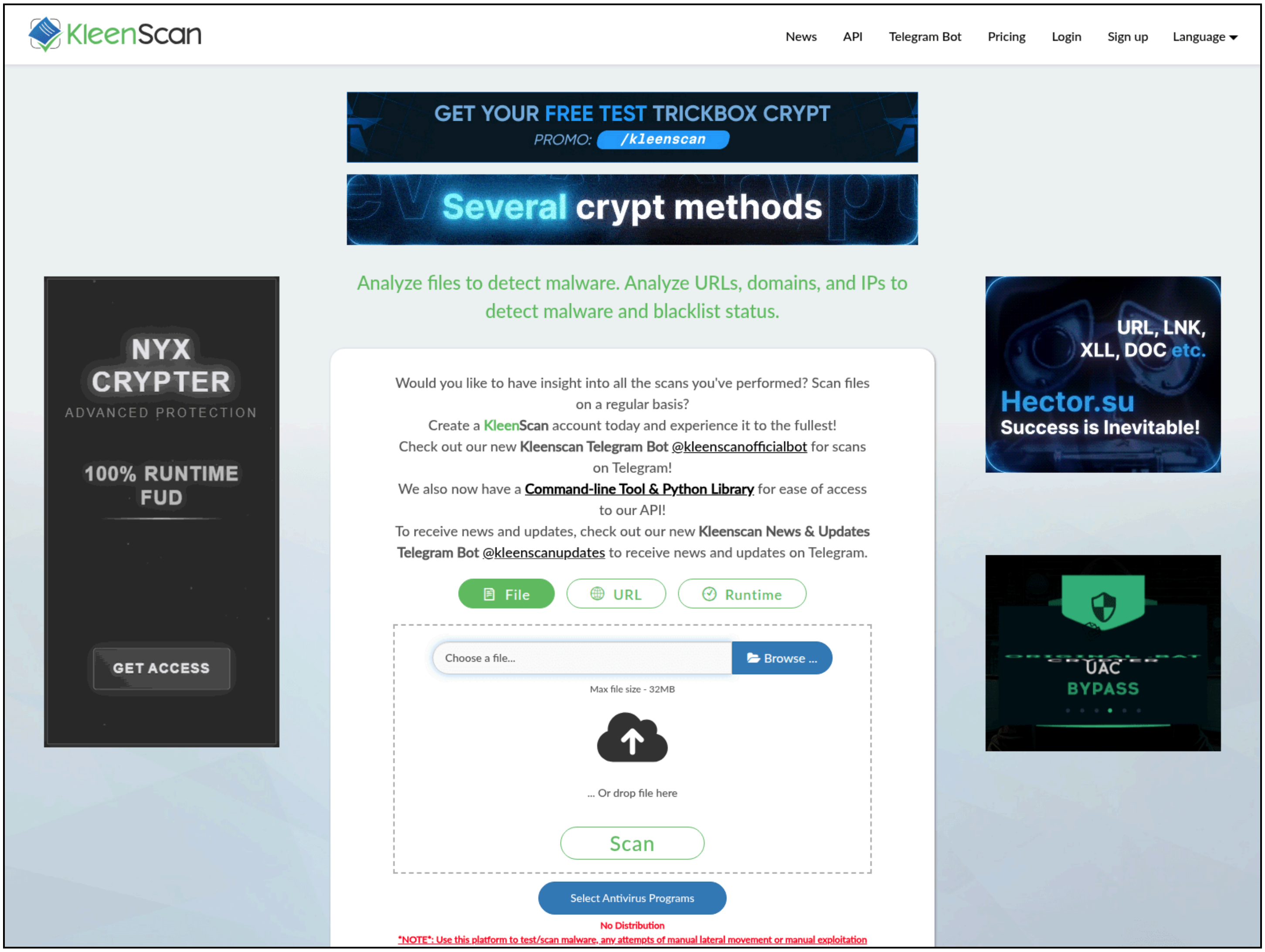
Other Email Sender and Lead Generation Services

Insikt Group identified several other, often legitimate email-related services used by Lumma affiliates for multiple purposes, including Joz Data (*jozdata[.]com*), Mailchimp (*mailchimp[.]com*), Spamir (*spamir[.]fr*), and Mandrill (*mandrillapp[.]com*), among others. Joz Data provides validated, segmented email lists for marketing and lead generation. Mailchimp is a legitimate platform for designing and managing email campaigns. Spamir offers tools for bulk email and SMS delivery, often linked to spam or phishing activity despite being presented as a testing toolkit. Mandrill, a paid add-on to Mailchimp, is a transactional email API used to send one-to-one, event-triggered messages such as password resets and order confirmations via SMTP or API.

AVCheck and Alternatives

Like many threat actors deploying malware or related infrastructure, Lumma affiliates actively seek tools to test detection beyond standard sandbox environments. Over the past twelve months, Insikt Group observed multiple affiliates using at least two such services: AVCheck (*avcheck[.]net*), which was seized by law enforcement in May 2025; and, more recently, KleenScan (*kleenscan[.]com*). There were also signs that at least one affiliate used *avscan[.]net*, although its presence and nature could not be confirmed at the time of analysis, as the domain appeared to be listed for sale.

KleenScan is an alternative malware-scanning service frequently used by and marketed to cybercriminals to test malicious files, URLs, and domains against multiple antivirus engines (see **Figure 12**). It offers a user interface, API, and command-line client, and even a Telegram bot (@kleenscanofficialbot) for uploads and real-time or runtime scans, all while explicitly promising a "No Distribution" policy so that submitted samples will not be shared with antivirus vendors. Although Insikt Group observed Lumma affiliates using KleenScan prior to AVCheck's seizure in May 2025, public reporting indicates that cybercriminals have increasingly turned to platforms like KleenScan as an alternative due to the seizure. Notably, KleenScan advertises *hector[.]su* (see **Figure 12**), an exploit broker further detailed in the section Exploit and Crypting Services.



Analyze files to detect malware. Analyze URLs, domains, and IPs to detect malware and blacklist status.

Would you like to have insight into all the scans you've performed? Scan files on a regular basis?
Create a KleenScan account today and experience it to the fullest!
Check out our new Kleenscan Telegram Bot @kleenscanofficialbot for scans on Telegram!
We also now have a Command-line Tool & Python Library for ease of access to our API!
To receive news and updates, check out our new Kleenscan News & Updates Telegram Bot @kleenscanupdates to receive news and updates on Telegram.

Max file size - 32MB

... Or drop file here

No Distribution

NOTE: Use this platform to test/scan malware, any attempts of manual lateral movement or manual exploitation

***Figure 12**: KleenScan website (Source: urlscan.io)*

Phone and SMS Services

Lumma affiliates heavily abuse virtual phone and SMS services (see **Table 4**) such as OnlineSim, SMS-Activate, and Zadarma. These platforms provide throwaway phone numbers for SMS or voice verification, which the threat actors use to bypass OTP-based security and create fake accounts without using personal identifiers. Lumma affiliates can automatically receive 2FA codes or activation PINs on virtual numbers, allowing them to register malware distribution sites, cloud drives, or messaging accounts without exposing their real phone lines. This identity obfuscation is crucial in the Lumma ecosystem, as it frustrates attribution and takedown efforts by making infrastructure ownership seem transient.

In practice, using these services for OTP bypass and fake account generation helps Lumma crews widen their attack surface. Disposable SMS numbers let attackers circumvent SMS-based two-factor authentication by redirecting one-time passcodes to attacker-controlled inboxes. This means that even if a stolen account is protected by SMS 2FA, Lumma affiliates can try to reroute the OTP to a virtual number they control, effectively nullifying the protection. Services like Zadarma (a VoIP provider) further enable criminals to receive calls or texts on virtual lines, or even perform spoofed voice calls as part of OTP interception bots and vishing schemes. Within the Lumma affiliate program, guides and community chatter encourage the use of these tools for operational security, from registering throwaway email and Telegram accounts to setting up C2 panels or scam payment accounts.

Service Name	Domain	Notes
OnlineSim	onlinesim[.]io	Burner eSim Provider
SMS-Activate	sms-activate[.]org	Burner eSim Provider
SMS-Activate	sms-activate[.]io	Burner eSim Provider
Zadarma	zadarma[.]com	VoIP Service

***Table 4**: Phone and SMS-linked services used by Lumma affiliates (Source: Recorded Future)*

Messaging Platforms

Lumma affiliates integrate multiple secure messaging and information-sharing tools into their daily workflows to enhance operational security, maintain anonymity, and minimize digital footprints. Affiliates commonly use uTox, a decentralized peer-to-peer messaging client employing end-to-end encryption via the Tox protocol. This tool facilitates persistent, secure communications, supporting text, voice, and video messaging, and is frequently combined with Tor proxies to conceal affiliate identities and avoid central server dependencies.

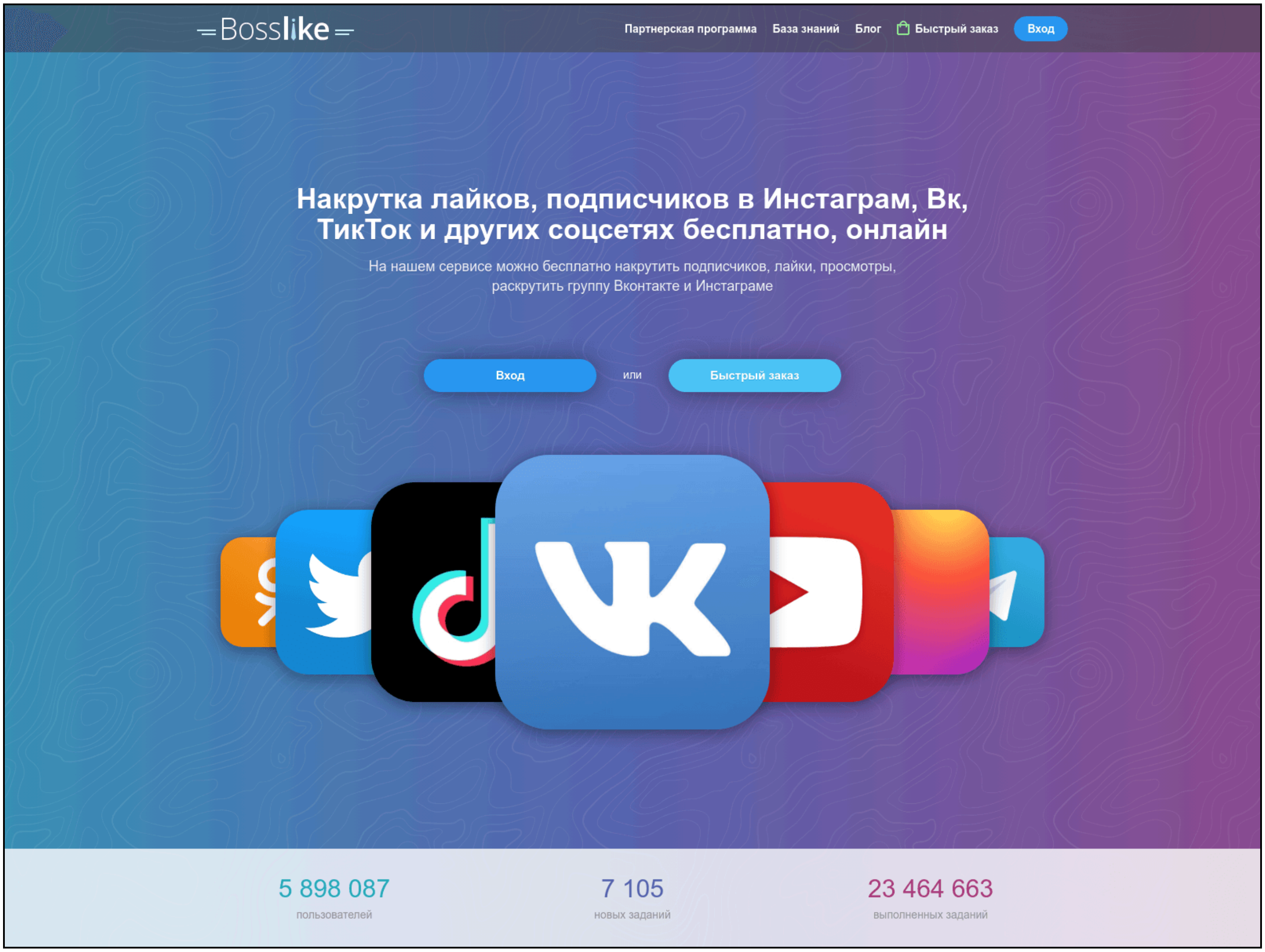
Mobile affiliates within the Lumma ecosystem prefer secure XMPP-based Android applications like Xabber and *c0nnect[.]pro*. Both apps offer encrypted communications via off-the-record encryption, multi-account management, and compatibility with private, controlled XMPP servers, making them ideal for discrete coordination while on the move. Affiliates often configure these applications to run in tandem with Tor proxies, further obfuscating metadata and reducing digital exposure.

For scenarios requiring transmission of ephemeral, sensitive information, such as credentials, passwords, or instructions, Lumma affiliates frequently rely on Privnote, a web-based service that generates encrypted notes that self-destruct after being read once. This capability significantly reduces the affiliate's potential forensic footprint by leaving no persistent records and enables secure, rapid exchanges of operational details.

Collectively, these tools form a layered communication architecture employed by Lumma affiliates, effectively balancing persistent communications, mobile flexibility, and ephemeral secure exchanges to minimize risks and enhance stealth.

Social Media Optimization

In at least one case, Insikt Group observed a Lumma affiliate leveraging the service Bosslike (*bosslike[.]ru*), which claims to offer free and rapid boosts for likes on platforms such as Instagram, VK, and TikTok (see **Figure 13**), likely in support of scam-related activities.



Накрутка лайков, подписчиков в Инстаграм, Вк, ТикТок и других соцсетях бесплатно, онлайн

На нашем сервисе можно бесплатно накрутить подписчиков, лайки, просмотры, раскрутить группу Вконтакте и Инстаграме

5 898 087 пользователей

7 105 новых заданий

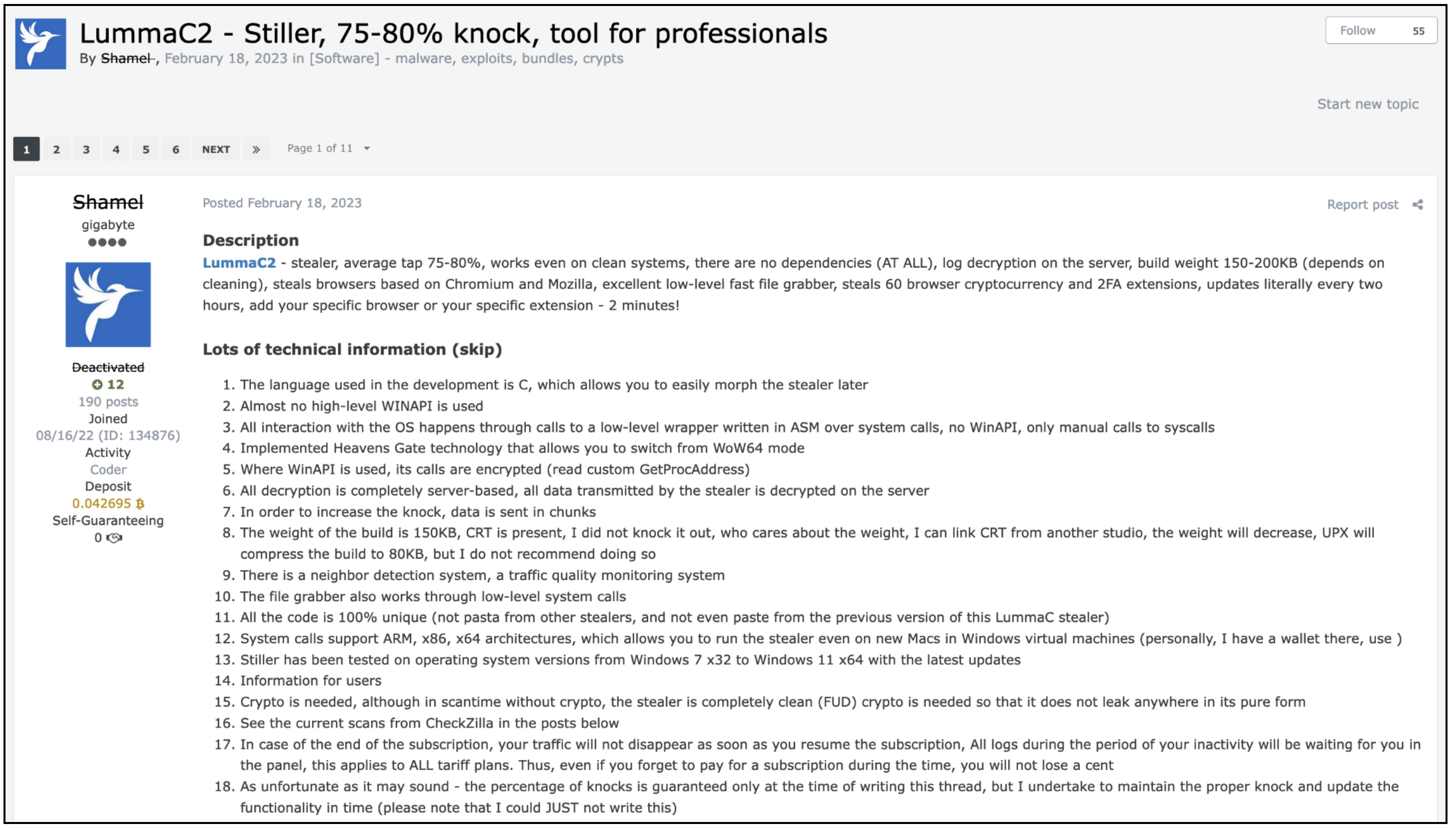
23 464 663 выполненных заданий

***Figure 13**: Bosslike website (Source: urlscan.io)*

Affiliates’ Embedding in the Cybercriminal Ecosystem

Forum Involvement

Lumma’s affiliate ecosystem thrives on underground forums that act as hubs for collaboration, resources, and marketplaces. Russian-language cybercrime forums like XSS and Exploit serve as launchpads for Lumma’s MaaS, and they are where the stealer was initially advertised and vetted by the community. These forums attract technically adept threat actors and lend credibility to new malware offerings through reputation systems and moderator oversight. Affiliates frequent them not only to obtain Lumma builds but also to engage with trusted escrow and arbitration services, ensuring safer transactions when purchasing tools or settling disputes with partners. The established trust on forums like Exploit and XSS provides a reliable environment for affiliates to do business, from renting servers to resolving conflicts, under the watch of experienced moderators.



LummaC2 - Stiller, 75-80% knock, tool for professionals

By ~~Shamel~~, February 18, 2023 in [Software] - malware, exploits, bundles, crypts

~~Shamel~~
gigabyte
●●●●
~~Deactivated~~
12
190 posts
Joined
08/16/22 (ID: 134876)
Activity
Coder
Deposit
0.042695 ฿
Self-Guaranteeing
0

Posted February 18, 2023

Description

LummaC2 - stealer, average tap 75-80%, works even on clean systems, there are no dependencies (AT ALL), log decryption on the server, build weight 150-200KB (depends on cleaning), steals browsers based on Chromium and Mozilla, excellent low-level fast file grabber, steals 60 browser cryptocurrency and 2FA extensions, updates literally every two hours, add your specific browser or your specific extension - 2 minutes!

Lots of technical information (skip)

1. The language used in the development is C, which allows you to easily morph the stealer later
2. Almost no high-level WINAPI is used
3. All interaction with the OS happens through calls to a low-level wrapper written in ASM over system calls, no WinAPI, only manual calls to syscalls
4. Implemented Heavens Gate technology that allows you to switch from WoW64 mode
5. Where WinAPI is used, its calls are encrypted (read custom GetProcAddress)
6. All decryption is completely server-based, all data transmitted by the stealer is decrypted on the server
7. In order to increase the knock, data is sent in chunks
8. The weight of the build is 150KB, CRT is present, I did not knock it out, who cares about the weight, I can link CRT from another studio, the weight will decrease, UPX will compress the build to 80KB, but I do not recommend doing so
9. There is a neighbor detection system, a traffic quality monitoring system
10. The file grabber also works through low-level system calls
11. All the code is 100% unique (not pasta from other stealers, and not even paste from the previous version of this LummaC stealer)
12. System calls support ARM, x86, x64 architectures, which allows you to run the stealer even on new Macs in Windows virtual machines (personally, I have a wallet there, use)
13. Stiller has been tested on operating system versions from Windows 7 x32 to Windows 11 x64 with the latest updates
14. Information for users
15. Crypto is needed, although in scantime without crypto, the stealer is completely clean (FUD) crypto is needed so that it does not leak anywhere in its pure form
16. See the current scans from CheckZilla in the posts below
17. In case of the end of the subscription, your traffic will not disappear as soon as you resume the subscription, All logs during the period of your inactivity will be waiting for you in the panel, this applies to ALL tariff plans. Thus, even if you forget to pay for a subscription during the time, you will not lose a cent
18. As unfortunate as it may sound - the percentage of knocks is guaranteed only at the time of writing this thread, but I undertake to maintain the proper knock and update the functionality in time (please note that I could JUST not write this)

Figure 14: *LummaC2 administrator (image text machine-translated from Russian) (Source: Exploit Forum)*

At the same time, mass-market cybercrime communities such as LolzTeam (*zelenka[.]guru*) have become a hotbed for recruiting and training the foot soldiers of Lumma’s operations. These more accessible forums host dedicated sections for “traffers,” threat actors who specialize in spreading infostealer malware, and are actively used to assemble affiliate teams and educate newcomers. On LolzTeam, for example, seasoned criminals advertise infostealer affiliate programs that provide novices with everything needed to start distributing malware. In one case, a team on LolzTeam offered free crypted Lumma builds and even SEO support to new recruits, taking a percentage of profits from stolen cryptocurrency assets. This low barrier to entry, combined with forum-posted tutorials on fraud techniques and operational security, turns platforms like LolzTeam into a workforce pool for infostealer distribution. The forums' community-driven vetting, including rules against targeting certain regions and public feedback on schemes, further helps affiliates learn effective and "acceptable" tactics. Common fraud methodologies are frequently discussed and popularized on these boards, giving Lumma affiliates insight into monetization tricks and victim manipulation strategies.

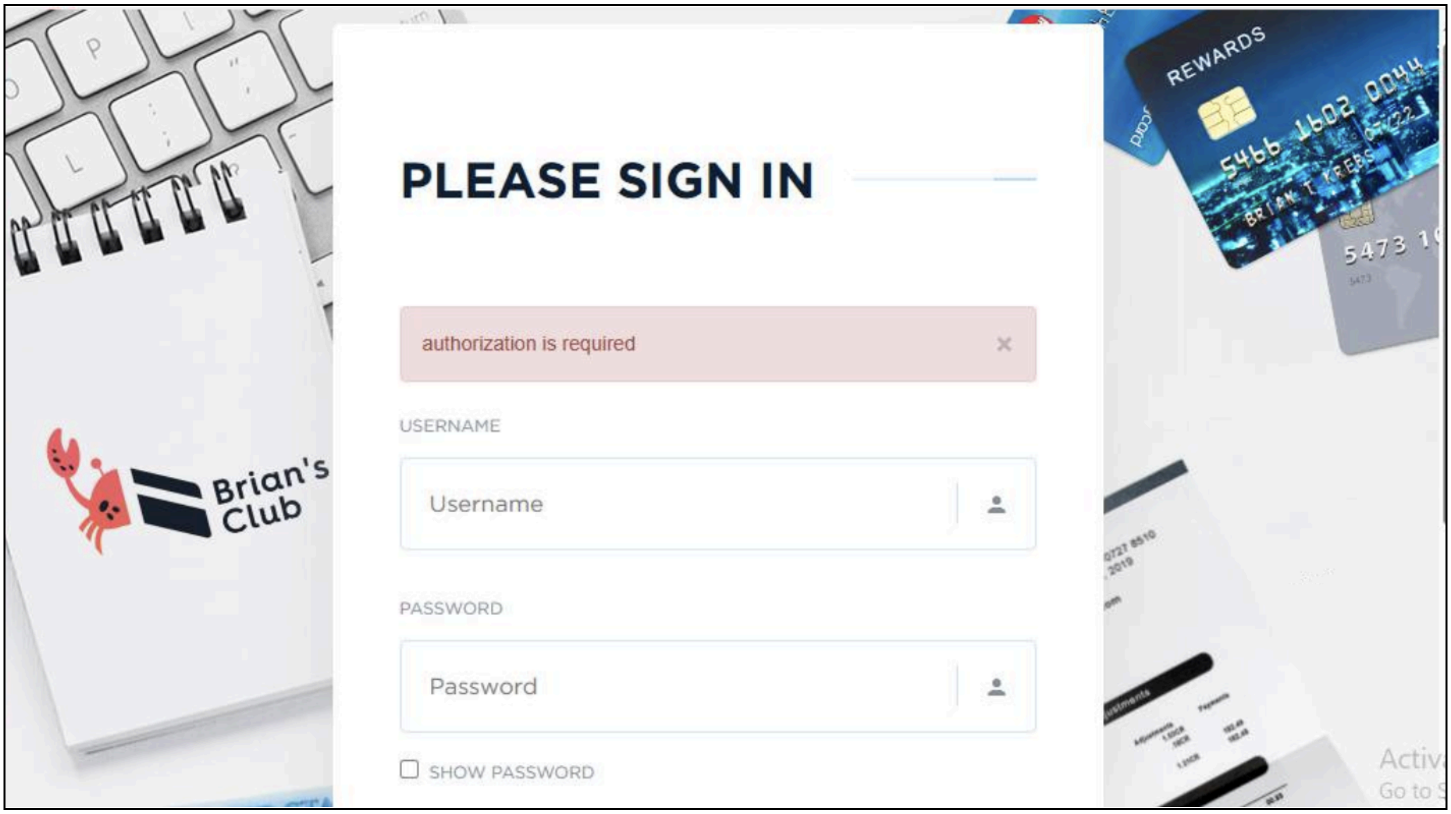
Perhaps most critically, these underground forums provide ready-made marketplaces and services that Lumma affiliates leverage to monetize stolen data and optimize their campaigns. Infostealer logs are in high demand, and forums link affiliates to bustling marketplaces where this data is bought and sold. Russian Market (*rm1[.]to*), for example, is an automated shop accessible via forum circles that has been described as "the Amazon of stolen credentials" for its massive inventory and one-click purchase convenience. By late 2024, Lumma had become the dominant source of credentials on Russian Market, accounting for roughly 92% of stolen log listings, underscoring how extensively Lumma affiliates dump their haul on such platforms for profit. Other venues like LolzTeam's own marketplace and *xleet[.]pw* similarly include sections for infostealer logs, compromised accounts, and digital goods, allowing affiliates to quickly sell data from Lumma infections to the highest bidder. Beyond data sales, forum marketplaces connect Lumma affiliates to initial access brokers and financial fraud services that help convert stolen information into cash. Affiliates can find buyers for enterprise login credentials or enlist money laundering and cash-out services advertised across these forums.

Underground forums double as one-stop shops for the technical and operational support that Lumma affiliates need. Dedicated threads run by the Lumma developers or peer community members offer technical assistance, update announcements, and troubleshooting advice in real time. This means an affiliate can turn to forum communities for help with builder configuration, antivirus evasion tips, or to share intelligence on law enforcement takedowns. The forums also host a range of malware-adjacent services crucial to running stealthy campaigns. Providers of bulletproof hosting, VPNs, and traffic distribution congregate on all major forums. The same service providers frequently advertise on multiple sites, which makes it easy for affiliates to obtain resilient servers and web domains to host Lumma malware. Crypting services are equally accessible; for instance, the popular Cassandra crypter and others are promoted in forum marketplaces, enabling affiliates to continuously encrypt and repackage Lumma payloads to evade antivirus detection.

There is a rich ecosystem of offerings, such as exploit kits, fake document templates, spambot rentals, and credential checkers, which affiliates can source from these communities to enhance their operations. Together, these forums provide Lumma affiliates with a comprehensive suite of tools that have been vetted by the community. This practical and operational value is why Lumma's affiliate network remains deeply embedded in underground forums: they provide not only the means to deploy and hide the malware, but also the mechanisms to cash in on its outputs, all within a semi-structured community that enforces trust among thieves.

Carding Shops

Lumma Stealer affiliates turn to specialized carding shops like *b1ackstash[.]cc*, *stashpatrick[.]io*, BriansClub (see **Figure 15**) (*bclub[.]cm* and *briansclub[.]cm*), and *binsoficial666[.]activo[.]mx* to efficiently monetize the financial data they've stolen. Insikt Group notes that these sources vary widely in credibility; shops like BriansClub are considered authoritative within the payment fraud ecosystem, while *binsoficial666[.]activo[.]mx* has a very poor reputation. Unlike general cybercrime boards, carding websites are dedicated to trading payment data and attract a built-in customer base of fraudsters looking for credit card numbers, bank logins, and personal info. Lumma affiliates capitalize on this demand by selling freshly obtained card records and "fullz"[3] in bulk, often earning a percentage for each sale through the forum's escrow or shop system. In essence, carding platforms let Lumma affiliates quickly turn stolen card data into profit, with high-volume outlets like BriansClub historically trafficking millions of compromised cards supplied by malware affiliates.



authorization is required ×

Figure 15: *Landing page for BriansClub (Source: BriansClub)*

Beyond sales, carding forums offer operational support for fraud that broader hacking forums do not. Lumma affiliates frequent these communities to learn and collaborate on card-not-present (CNP) fraud using stolen card credentials to buy goods or launder money online. The forums host vetted tutorials for abusing e-commerce sites and payment processors, helping thieves bypass anti-fraud measures.

[3] A slang term for a package of information containing a person's full information (such as their real name, address, and a form of identification).

Members also advertise criminal services such as providing “drop” addresses (safe delivery points for goods bought with stolen cards) or converting illicit purchases into cash. Additionally, these forums supply validation tools and services critical to fraud operations. Lumma affiliates can purchase or access credit card checkers that automatically test which cards from their stealer logs remain valid and have credit available, ensuring they only spend time on live cards. They might also acquire Bank Identification Number (BIN) lists and other utilities, using the community’s pooled resources to maximize successful transactions. Carding sites enable Lumma affiliates to offload infostealer loot in bulk, complementing sales on broader crime forums. A single Lumma infection yields an expansive log of credentials, cookies, system data, and often multiple financial accounts; parsing and individually selling each asset can be labor-intensive. Carding marketplaces or associated breach data shops let affiliates resell entire stealer logs or specific datasets to other criminals who specialize in exploiting them. For example, high-value logs from Lumma, containing not just cards but bank account passwords or cryptocurrency wallet keys, are often posted on underground markets or offered via automated bot vendors shortly after exfiltration. This practice allows Lumma affiliates to monetize stolen information at scale: they can quickly sell bundles of fresh logs to brokers or fraud rings while focusing their own efforts on new infections. In tandem with general hacking forums, these carding forums provide the ecosystem for cashing out Lumma’s results. They offer a one-stop underground economy where affiliates convert stolen data into money through direct sales of CVVs and “fullz,” the provision of guidance and tools for fraudulent transactions, and the bulk resale of stolen logs. This significantly enhances both the profitability and practicality of Lumma operations.

Use of Additional Infostealers

Insikt Group observed several Lumma affiliates leveraging other infostealers alongside Lumma.

Meduza Stealer, Vidar, and CraxsRAT Used by Likely Mexico-Based Lumma Affiliate

The affiliate linked to Lumma build ID re0gvc, a likely Mexico-based threat actor operating under multiple aliases across various forums, was observed using Meduza Stealer infrastructure tied to IP address *195[.]133[.]18[.]15*. Like Lumma, Meduza Stealer is a Windows-based MaaS infostealer, designed to extract credentials, browser data, and crypto wallets while evading detection through anti-analysis and geo-filtering techniques.

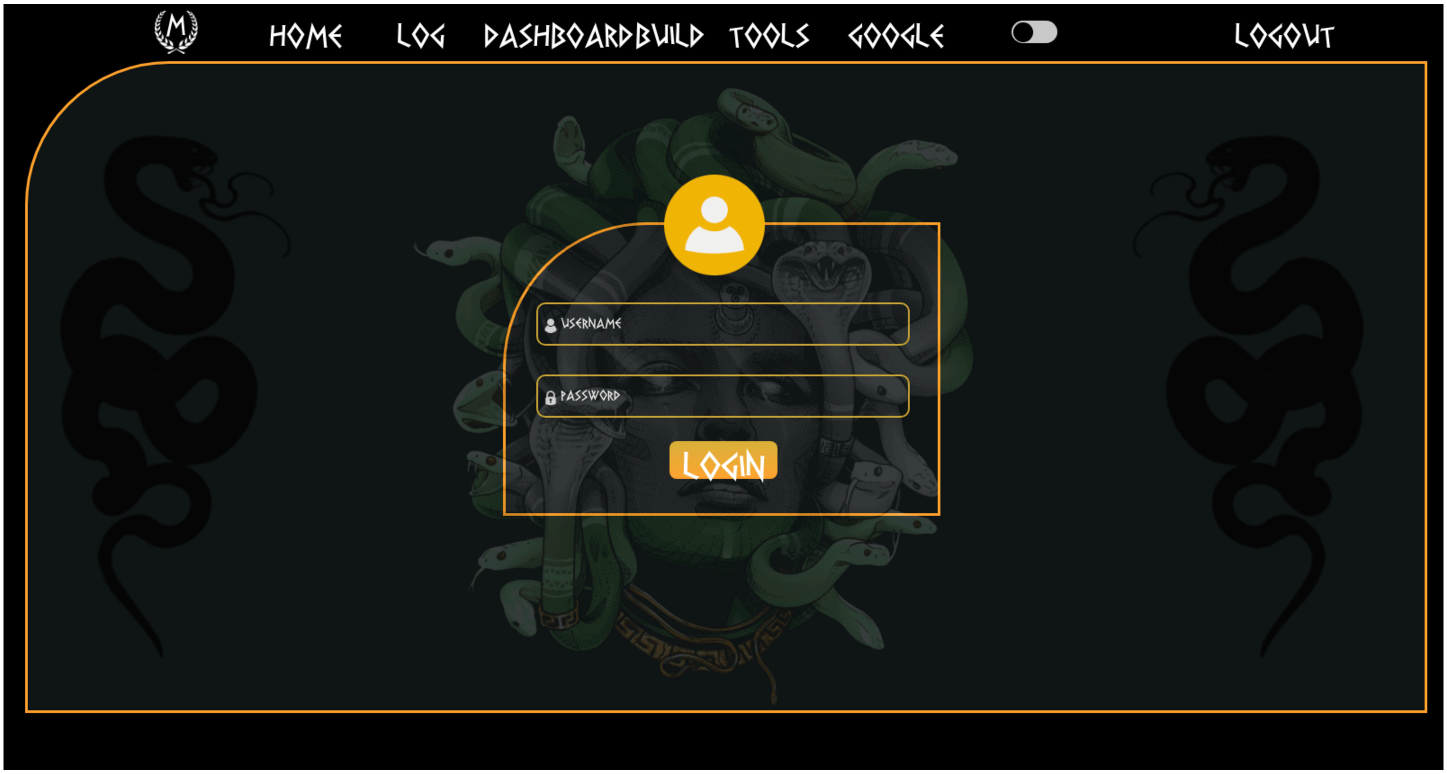
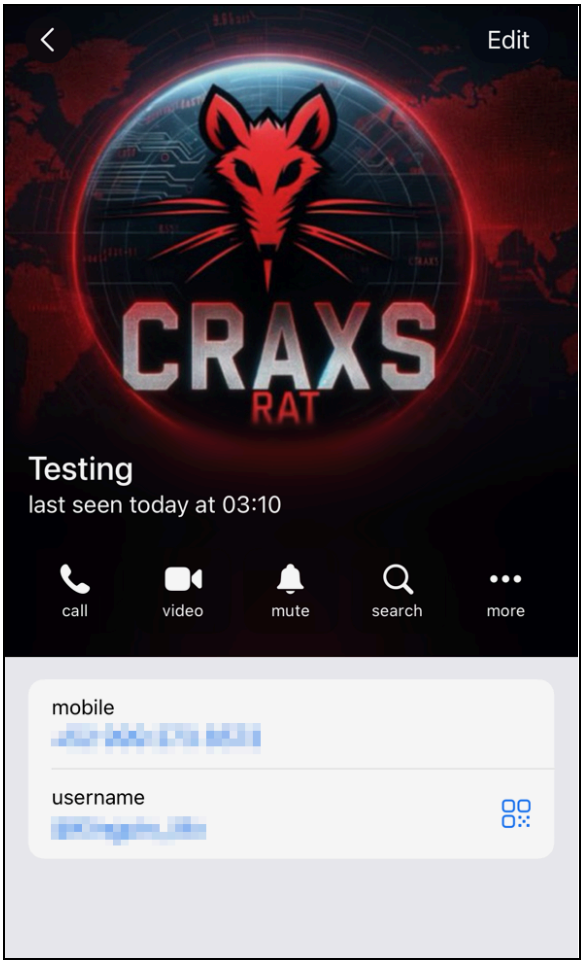


***Figure 16**: Meduza Stealer panel on hxxp://195[.]133[.]18[.]15/auth/login (Source: urlscan.io)*

Insikt Group also identified high-confidence indicators that the same threat actor used Vidar, a Windows-based infostealer, along with medium-confidence evidence suggesting the use of CraxsRAT, an Android-based RAT, based on Telegram profile images likely tied to the affiliate (see **Figure 17**). While this indicates this affiliate may have also targeted mobile devices, Insikt Group found no associated samples, infrastructure, or campaigns to confirm this activity.



Testing
last seen today at 03:10

mobile
[redacted]

username
[redacted]

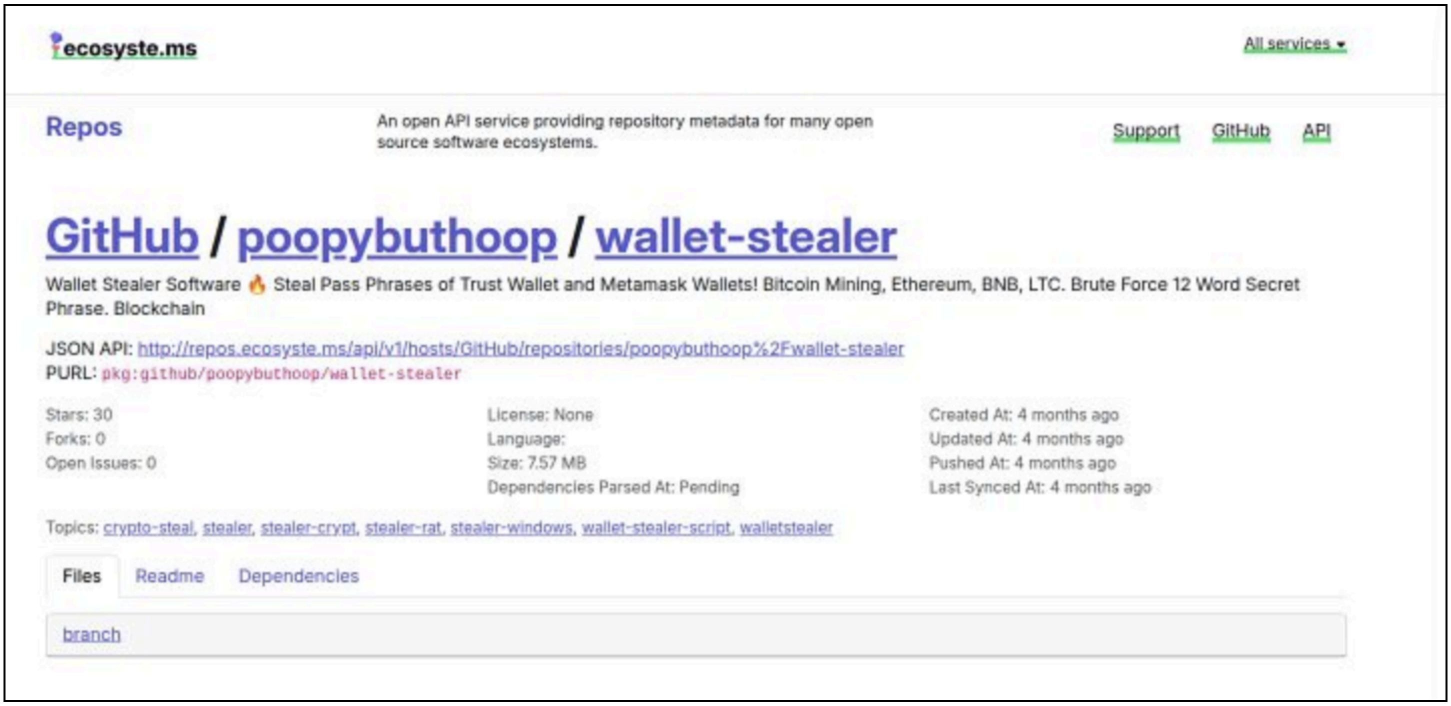
Figure 17: *Telegram account linked to Kingping_Mx (Source: Recorded Future)*

Stealc Used by Lumma Affiliate suffergrime

Another affiliate linked to Lumma build IDs test222 and eLMNFu, known as “suffergrime” on various forums and operating under multiple other aliases, including duckfuck, cryptplease, ultracool2201, borodach, and dedo4ek, appears to have used StealC alongside Lumma. Stealc is a modular, evasive information stealer written in C and distributed as an MaaS. More specifically, suffergrime has been observed interacting with the Stealc management panel on the URL *hxxp://94[.]232[.]249[.]208/6a6fe9d70500fe64/main.php*. Insikt Group assesses that the affiliate is likely a Spanish speaker, with indications suggesting a possible origin in South America.

worldmix10k’s Interest in Wallet and Vilsa Stealer

In addition to the cases above, Insikt Group observed a Lumma affiliate associated with build ID 1dacrp and likely known as “worldmix10k” expressing interest in two additional stealers: a “Wallet Stealer” previously hosted on a GitHub repository named “poopybuthoop”, and Vilsa Stealer, an infostealer that had been publicly reported on earlier. Although the GitHub repository was no longer accessible at the time of analysis, a historical snapshot was preserved by Ecosyste.



An open API service providing repository metadata for many open source software ecosystems.

GitHub / poopybuthoop / wallet-stealer

Wallet Stealer Software 🔥 Steal Pass Phrases of Trust Wallet and Metamask Wallets! Bitcoin Mining, Ethereum, BNB, LTC. Brute Force 12 Word Secret Phrase. Blockchain

JSON API: http://repos.ecosyste.ms/api/v1/hosts/GitHub/repositories/poopybuthoop%2Fwallet-stealer
PURL: `pkg:github/poopybuthoop/wallet-stealer`

Stars: 30
Forks: 0
Open Issues: 0

License: None
Language:
Size: 7.57 MB
Dependencies Parsed At: Pending

Created At: 4 months ago
Updated At: 4 months ago
Pushed At: 4 months ago
Last Synced At: 4 months ago

Topics: crypto-steal, stealer, stealer-crypt, stealer-rat, stealer-windows, wallet-stealer-script, walletstealer

***Figure 18**: Repository linked to poopybuthoop (Source: Ecosyste)*

Notably, a search for the string "worldmix10k" led Insikt Group to a Lumma sample[4] with the build ID "1dacRP--worldmix10k", linked to the same affiliate. This sample used *techmindzs[.]live* and *earthsymphzony[.]today* as its C2 domains, as well as a SteamCommunity URL, *hxxps://steamcommunity[.]com/profiles/76561199822375128*, for dead drop resolving. Insikt Group could not identify the exact infection chains linked to the sample.

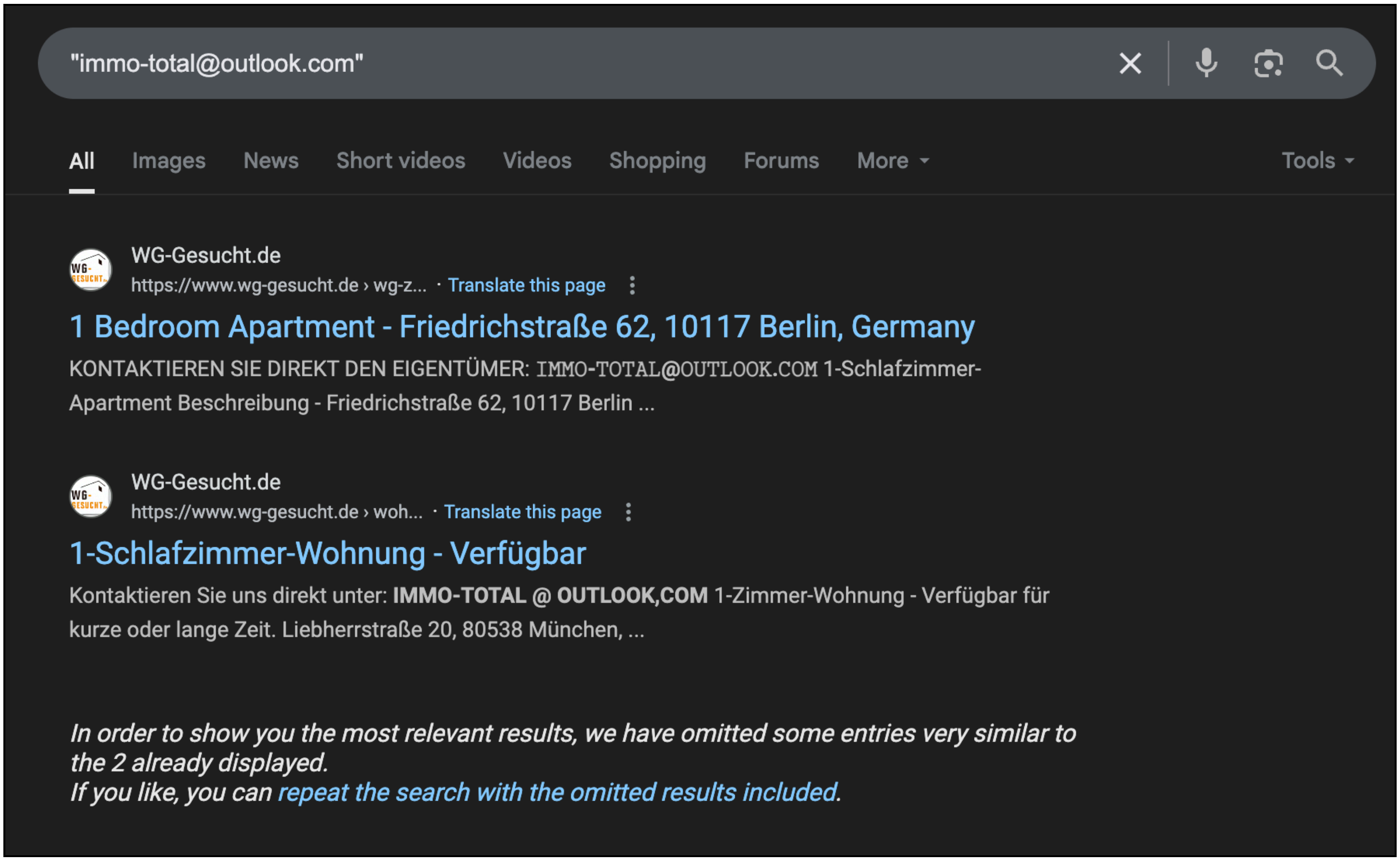
Involvement in Other Scams

Analysis of multiple Lumma affiliates over the last twelve months revealed that many are not only using multiple infostealers concurrently, as outlined in the section Use of Additional Infostealers, but are also likely involved in a variety of distinct scam operations. One of these scams, linked to the Lumma affiliate known as blackowl23, drew particular attention from Insikt Group and is explored in greater detail below.

blackowl23's Involvement in Real Estate Scam

Insikt Group uncovered evidence indicating that blackowl23 has been involved in a real estate scam in which rental listings, likely both actor-created and compromised, on platforms like the German website WG-Gesucht were used to deceive victims into making payments before apartment viewings. As part of this scheme, blackowl23 has used the email addresses *immo-total[@]outlook[.]com* and *mwimport[@]outlook[.]de* (see **Figure 19**).

[4] SHA256: b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630



"immo-total@outlook.com"

WG-Gesucht.de
https://www.wg-gesucht.de › wg-z... · Translate this page

1 Bedroom Apartment - Friedrichstraße 62, 10117 Berlin, Germany

KONTAKTIEREN SIE DIREKT DEN EIGENTÜMER: IMMO-TOTAL@OUTLOOK.COM 1-Schlafzimmer-Apartment Beschreibung - Friedrichstraße 62, 10117 Berlin ...

WG-Gesucht.de
https://www.wg-gesucht.de › woh... · Translate this page

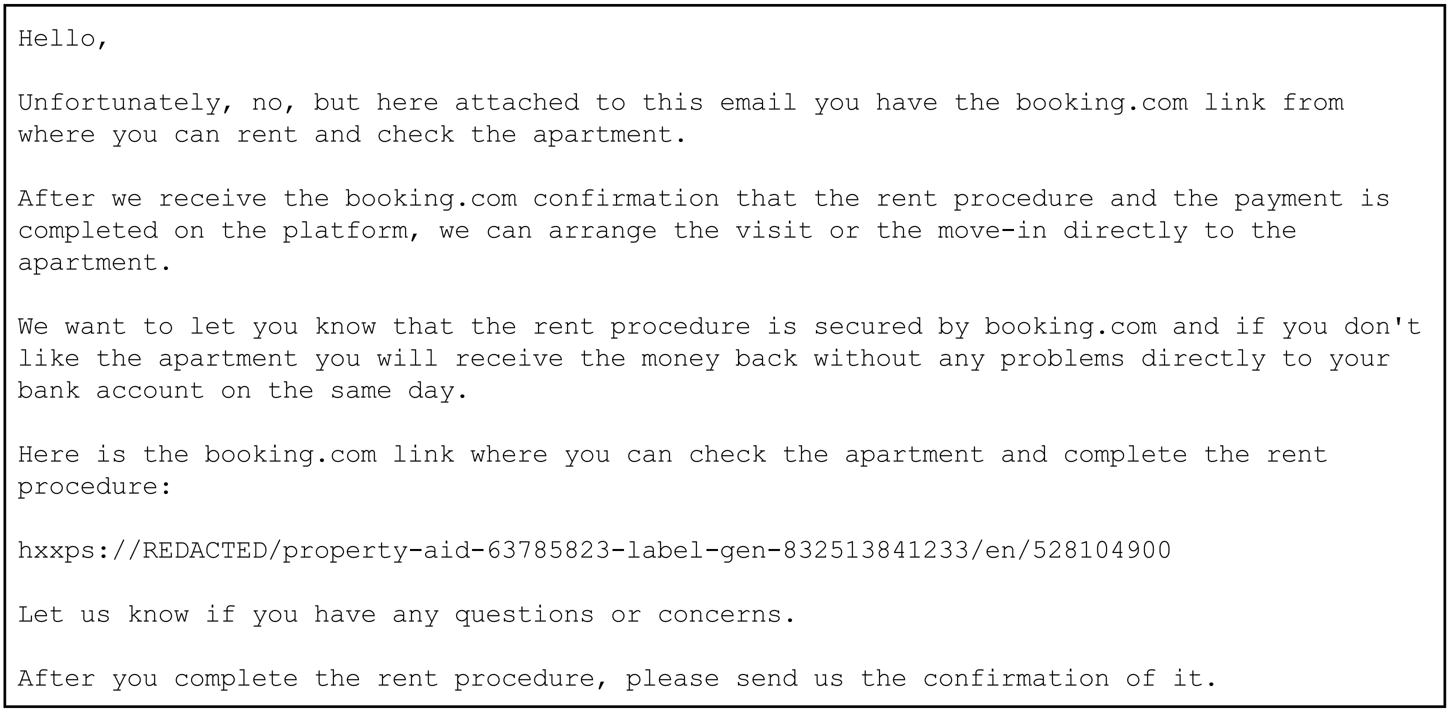
1-Schlafzimmer-Wohnung - Verfügbar

Kontaktieren Sie uns direkt unter: **IMMO-TOTAL @ OUTLOOK,COM** 1-Zimmer-Wohnung - Verfügbar für kurze oder lange Zeit. Liebherrstraße 20, 80538 München, ...

In order to show you the most relevant results, we have omitted some entries very similar to the 2 already displayed.
If you like, you can repeat the search with the omitted results included.

***Figure 19**: WG-Gesucht advertisements showing up in a Google search (Source: Recorded Future)*

More specifically, the affiliate claimed to have had "bad experiences in the past with people wanting to rent the property," stating that when they "got to the property, there was no one there," which resulted in "cancelled business appointments, wasting time and money." Using this as justification, they asked victims to make payments via Booking.com, asserting that the process was secure and that victims would be refunded if they were dissatisfied with the apartment (see **Figure 20**). Notably, the same URL path (`property-aid-63785823-label-gen-832513841233`) observed in this activity was also seen in the final-stage URL of a rental scam campaign reported by Fortian in 2024. In that instance, victims were deceived into reserving accommodations, and the domain used appears to be a typosquatting variant, *booking[.]eu-apt-booking[.]homes*, hosted via Cloudflare.



Hello,

Unfortunately, no, but here attached to this email you have the booking.com link from where you can rent and check the apartment.

After we receive the booking.com confirmation that the rent procedure and the payment is completed on the platform, we can arrange the visit or the move-in directly to the apartment.

We want to let you know that the rent procedure is secured by booking.com and if you don't like the apartment you will receive the money back without any problems directly to your bank account on the same day.

Here is the booking.com link where you can check the apartment and complete the rent procedure:

hxxps://REDACTED/property-aid-63785823-label-gen-832513841233/en/528104900

Let us know if you have any questions or concerns.

After you complete the rent procedure, please send us the confirmation of it.

***Figure 20**: Text sent to the target of a Lumma affiliate (Source: Recorded Future)*

Insikt Group also uncovered supporting evidence that the affiliate employed a similar scheme: claiming to have escrow agents worldwide, sending victims a payment link to secure a reservation, and promising that the funds would be held safely and transferred to “one of [their] available bank accounts.” In this case, Insikt Group was unable to recover the actual payment link.

While the affiliate may have created their own accounts on platforms like WG-Gesucht, evidence shows they possess a large number of compromised WG-Gesucht credentials. Insikt Group hypothesizes that at least some of these credentials were stolen through the affiliate’s Lumma infections. In this context, it's important to note that while selling logs is generally lucrative, the value of certain credentials, such as those for platforms like WG-Gesucht, likely comes from their use in follow-on scams rather than direct resale, which may explain why some buyers may show limited interest in them.

Outlook

Insikt Group's unique investigation into Lumma affiliates uncovered a large infostealing ecosystem enabled by a diverse set of tools and services, including proxies, VPNs, anti-detect browsers, exploit kits, crypting services, and malware detection tools. During the investigation, Insikt Group identified previously unreported tools and demonstrated how affiliates frequently run multiple scams in parallel, such as rental fraud, while leveraging additional infostealers like Vidar, Stealc, and Meduza Stealer, likely to enhance success rates and reduce the impact of detection or law enforcement disruption. Looking ahead, Lumma affiliates will likely further diversify their presence across specialized and niche forums, integrating more deeply with cryptocurrency-focused platforms and encrypted messaging ecosystems, complicating detection and disruption efforts.

While many tactics and tools appear standardized across affiliates, who are likely influenced by shared guides provided by the Lumma MaaS operators, meaningful operational differences exist. These nuances are crucial for defenders, as understanding individual affiliate behaviors offers a clearer picture of how specific threats emerge and evolve within a broader ecosystem. In addition, the findings underscore that many Lumma affiliates are not casual participants, but embedded actors with deep ties to the cybercriminal underground. Their adoption of layered tool sets and diversification across malware families suggests both maturity and adaptability.

Looking ahead, although recent law enforcement efforts temporarily disrupted Lumma's infrastructure, the group's swift recovery with minimal changes underscores its resilience and operational discipline. The longer-term impact of the law enforcement efforts on the individual affiliates hinges on Lumma's ability to rebuild trust and retain them, a goal it pursues through swift restoration of its infrastructure, proactive communication, and likely feature enhancements. More broadly, the recent law enforcement operations underscore how modern cybercriminal operations function as decentralized networks, where even successful disruptions tend to have only short-term effects. Sustained mitigation will require ongoing law enforcement pressure and targeted intelligence to track the evolving tactics of individual affiliates, in addition to seeking to disrupt Lumma's infrastructure.

Appendix A — Ngioweb Botnet-Linked IP Addresses Used by Lumma Affiliate blackowl23

IP Address	Port	ASN
162[.]210[.]192[.]136	60136	AS30633
174[.]138[.]176[.]77	26714	AS19318
174[.]138[.]176[.]78	59315	AS19318
195[.]154[.]43[.]189	41623	AS12876
209[.]159[.]153[.]19	37726	AS19318
212[.]83[.]137[.]94	59351	AS12876
212[.]83[.]138[.]186	60126	AS12876
212[.]83[.]138[.]245	50029	AS12876
212[.]83[.]143[.]103	55734	AS12876
212[.]83[.]143[.]118	10696	AS12876
212[.]83[.]143[.]159	50297	AS12876
212[.]83[.]143[.]191	14618	AS12876
38[.]91[.]107[.]229	64336	AS63023
38[.]91[.]107[.]2	56581	AS63023
51[.]83[.]116[.]4	50610	AS16276
66[.]29[.]129[.]52	24732	AS22612
67[.]213[.]210[.]115	55168	AS13213
67[.]213[.]212[.]50	10718	AS13213

Appendix B — Indicators of Compromise (IoCs)

```
Ngioweb IP Addresses:
38[.]91[.]107[.]2
38[.]91[.]107[.]229
51[.]83[.]116[.]4
66[.]29[.]129[.]52
67[.]213[.]210[.]115
67[.]213[.]212[.]50
162[.]210[.]192[.]136
174[.]138[.]176[.]77
174[.]138[.]176[.]78
195[.]154[.]43[.]189
209[.]159[.]153[.]19
212[.]83[.]137[.]94
212[.]83[.]138[.]186
212[.]83[.]138[.]245
212[.]83[.]143[.]103
212[.]83[.]143[.]118
212[.]83[.]143[.]159
212[.]83[.]143[.]191

Lumma Sample:
b8e02f2bc0ffb42e8cf28e37a26d8d825f639079bf6d948f8debab6440ee5630

Meduza Panel:
hxxp://195[.]133[.]18[.]15/auth/login

Stealc Panel:
hxxp://94[.]232[.]249[.]208/6a6fe9d70500fe64/main.php
```

Appendix C — MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure: Domains	T1583.001
Resource Development: Acquire Infrastructure: Virtual Private Server	T1583.003
Resource Development: Acquire Infrastructure: Server	T1583.004
Resource Development: Acquire Access	T1650
Resource Development: Obtain Capabilities: Tool	T1588.002
Resource Development: Compromise Accounts: Email Accounts	T1586.002
Command and Control: Proxy: External Proxy	T1090.002

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com