



| Brief |

The Underground Economist: Volume 4, Issue 12

B-2024-06-13b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actors,
Ransomware, Data Leak, Network Access

June 13, 2024

Scope Note

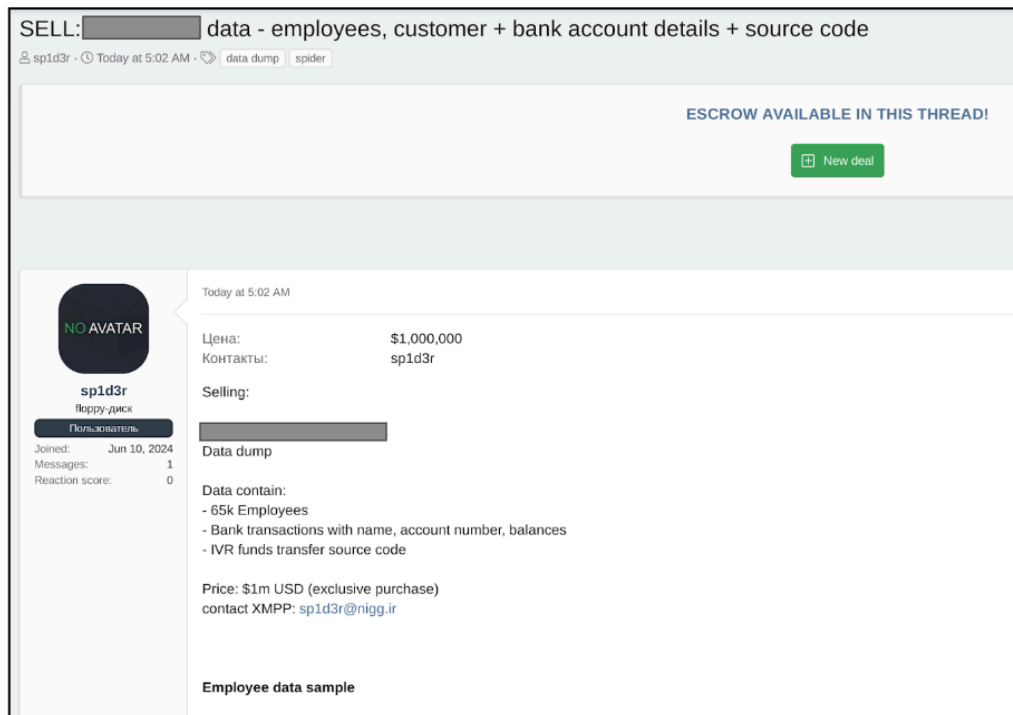
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 AM (EDT) on June 13, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 12

| Threat Actor Linked to ShinyHunters Advertises Extortionate Data Breach

On June 11, 2024, threat actor “sp1d3r” advertised the sale of a notably large leaked data set in the Russian-speaking dark web forum xss. The breach allegedly contains 65,000 records of data stolen from a U.S.-based financial organization that purportedly include both personal financial information (PFI) and personally identifiable information (PII). The asking price for the data is USD 1,000,000, exclusive to one buyer only. Although the advertisement does not specifically mandate the use of escrow, is it almost certainly a requirement for a transaction of this size to take place.

- The advertisement includes samples of the data, which are composed of account numbers, bank balances, interactive voice response (IVR) funds transfer source code, and details surrounding bank transactions.
- The PII included appears to contain large quantities of employee information, such as names, addresses, banking identification, and personal contact information.
- The offering of large and detailed information samples increases the authenticity of sp1d3r and the advertised data.



Sp1d3r's xss post, with victim anonymized by ZeroFox

Source: ZeroFox Intelligence

The owner of this stolen data has likely been implicated in the ongoing fallout of the alleged breach of cloud-based service provider Snowflake. Since the alleged breach on May 23, 2024, several of Snowflake's assumed customers' data has been advertised on deep and dark web (DDW) forums.

- Sp1d3r previously advertised the sale of data allegedly stolen from a U.S.-based automotive parts organization for USD 1.5 million on DDW forum Exploit on May 30, 2024.
- On May 29, 2024, "ShinyHunters" advertised data stolen from Ticketmaster in the English-speaking DDW forum BreachForums for USD 500,000.
- On May 24, 2024, untested threat actor "whitewarlock" advertised the sale of data allegedly stolen from a Europe-based financial organization for USD 2 million on Exploit.

While information of this nature has innate value in DDW forums and can be leveraged by threat actors wishing to conduct social engineering, blackmail, or fraudulent activity,

the exorbitant advertised price is very likely reflective of the victim being the sole intended buyer, rather than the advertisement being a realistic attempt to garner interest from the broader xss community. In parallel to other recently-announced victims, this is very likely a digital extortion attempt rather than a traditional data breach.

Like whitewarlock, sp1d3r is almost certainly synonymous with (or heavily associated with) threat actor ShinyHunters, who is very likely responsible for recent attacks against Snowflake customers. Sp1d3r registered on xss forum on June 10, 2024, and carries no reputation on the forum.

- ShinyHunters is an English-speaking black hat threat group that has been active on dark web forums for a considerable period, garnering a well-known—albeit controversial—reputation.
- Until its disruption by law enforcement (LE) entities on May 15, 2024, ShinyHunters was a moderator of the popular hacking forum BreachForums.

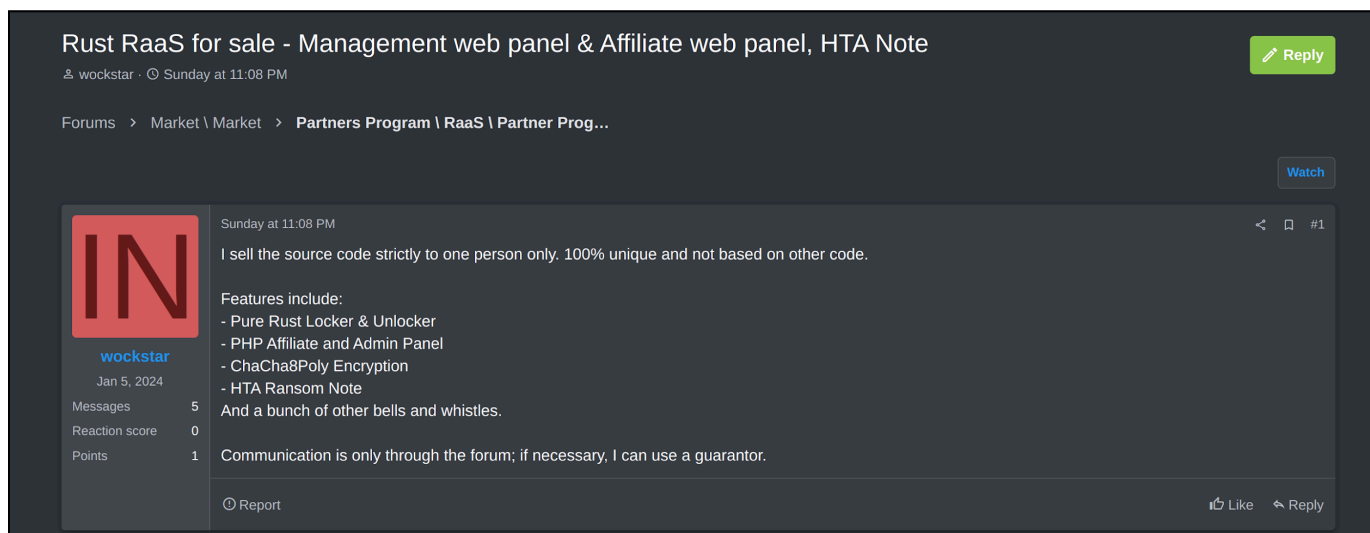
BreachForums—which ShinyHunters has used in the past primarily to disseminate data leaks—has been intermittently operational since LE operations. The consistent disruption of this forum is very likely a contributing factor toward ShinyHunters' employment of multiple aliases and use of numerous DDW forums to advertise stolen data.

In the coming weeks, it is very likely that additional alleged Snowflake customers will be implicated in data breaches, with the stolen information being advertised for sale in DDW forums. There is a roughly even chance that these will be posted by further, as-yet-unseen aliases associated with ShinyHunters across an array of forums, as the threat actor seeks to avoid LE scrutiny. In the medium to long term, there is a roughly even chance that ShinyHunters will seek to establish reputation and credibility within a single DDW forum, where operations and sales can take place more reliably.

| New Ransomware Project Advertised On The Deep and Dark Web

On June 9, 2024, the actor "wockstar" announced the sale of the source code for their custom-built ransomware-as-a-service (RaaS) project Rust, which includes both the management web panel and the affiliate panel, on the Russian-speaking, DDW forum RAMP. Should the source code be purchased, it is almost certain that another actor will continue to develop it for ransomware and digital extortion (R&DE).

- Wockstar claims that the source code will only be sold to one buyer and is a completely unique ransomware code.
- Allegedly, the code's features include a pure Rust locker and unlocker, a PHP affiliate and admin panel, ChaCha8Poly encryption, and an HTA ransom note.
- It is likely no price was stated in the post because negotiations could include various additions, such as a percentage of future profit made from using the source code.



Rust RaaS for sale - Management web panel & Affiliate web panel, HTA Note

wockstar · Sunday at 11:08 PM

Forums > Market \ Market > Partners Program \ RaaS \ Partner Prog...

IN
wockstar
Jan 5, 2024
Messages 5
Reaction score 0
Points 1

Sunday at 11:08 PM

I sell the source code strictly to one person only. 100% unique and not based on other code.

Features include:

- Pure Rust Locker & Unlocker
- PHP Affiliate and Admin Panel
- ChaCha8Poly Encryption
- HTA Ransom Note

And a bunch of other bells and whistles.

Communication is only through the forum; if necessary, I can use a guarantor.

Report

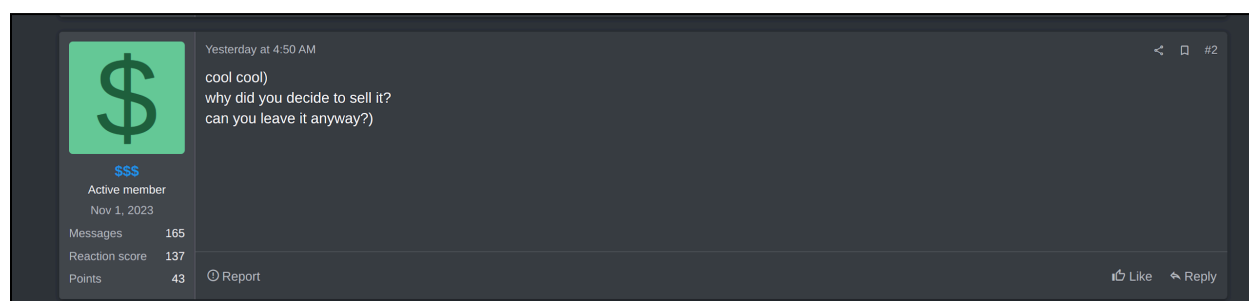
Like Reply

Wockstar's RAMP post *Source: ZeroFox Intelligence*

Wockstar responded to a question from "\$\$\$" in the thread about why they were selling the project, explaining that the software's developer is no longer working with them. Additionally, Wockstar stated they had originally planned to release the RaaS but has

now decided against doing this due to “heat” other partner programs are receiving from “glowing entities.” This is almost certainly a reference to recent LE activity conducted against ransomware collective LockBit.

- On February, 19, 2024, a joint international LE operation, seized LockBit’s victim leaksites, affiliate panel source code, and victim information and released free decryption tools. Furthermore, on May, 7, 2024, LE allegedly revealed the identity of “LockBitSupp”—a leadership figure in LockBit’s operation.



\$\$\$’s question to wockstar

Source: ZeroFox Intelligence

Wockstar’s activity likely suggests that threat actors are concerned about recent joint operations by international LE against RaaS operations. While this is a singular occurrence, there is a roughly even chance that more threat actors could seek to sell their source code in the future to other actors.

| Iranian Data Leak Advertised on the Dark Web

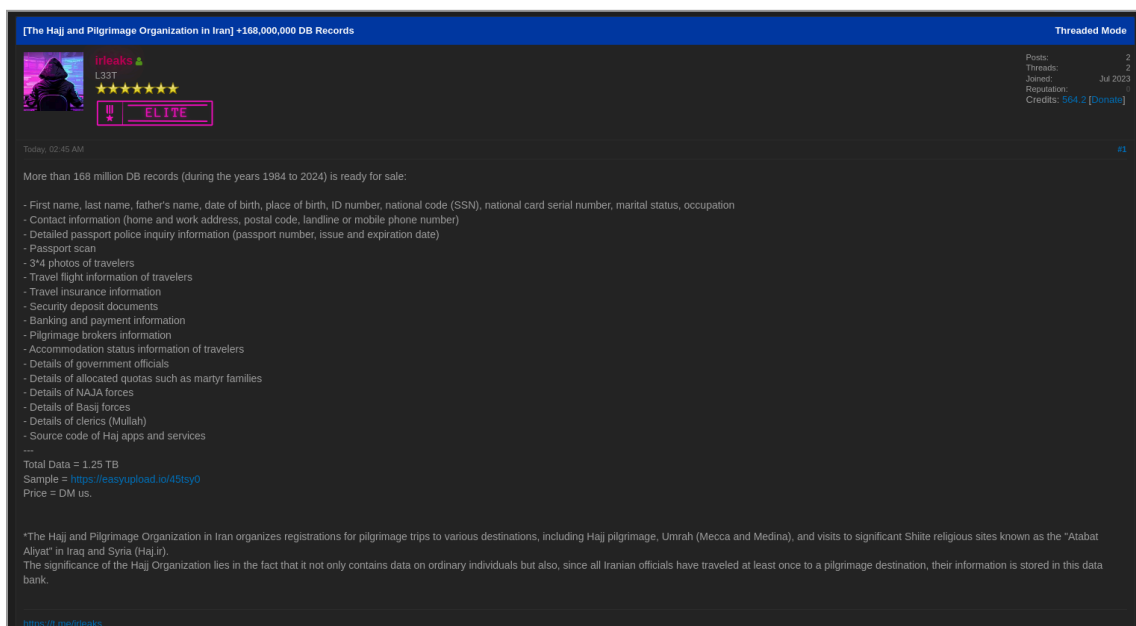
On June 4, 2024, untested English-speaking actor “irleaks” announced the sale of a large leaked data set pertaining to the Hajj and Pilgrimage Organization in Iran via the dark web Onniforums community. The data is stated to be substantive, totalling 1.25TB in size and containing over 168 million records spanning from 1984 to 2024. This data will very likely gain the attention of geopolitically and ideologically motivated actors.

- The Hajj and Pilgrimage Organization is an independent government agency in Iran that is responsible for managing and overseeing the Hajj pilgrimage and other religious pilgrimages for all Iranian citizens.

- The price is not specified and is likely a matter of negotiation. However, it is expected to be substantial due to the volume and sensitivity of the leaked data.

The leak allegedly contains a multitude of sensitive data. Additionally, it pertains to information on various organizations and individuals who work with or have used the Hajj and Pilgrimage Organization.

- Allegedly, government officials' information is implicated in the data. These individuals are stated to work with the organization in a government capacity, or the individuals have used the organization in a personal capacity.
- Data pertaining to security forces who cooperate with the agency (such as Iran's national police force, NAJA, and volunteer auxiliary force Basij, which is controlled by the Iranian Armed Forces) is included in the leak.
- PFI such as banking, payment, and pilgrimage broker information is allegedly included, as is PII consisting of contact information, citizen identification, ID data, photos, insurance, and travel information.



Irleaks' OnniForums post

Source: ZeroFox Intelligence

While the extent and content of the stolen information is unknown, its quantity and non-public nature means it will very likely be of interest to geopolitically or ideologically

motivated threat actors. Therefore, it is very likely that the advertisement is aimed toward hacktivists, state cyber capabilities, and state-affiliated groups that are known to be opposed to Iran. Additionally, financially-motivated threat actors, such as R&DE collectives, will likely be perceived as interested parties.

- Politically motivated actors, such as nation-states and state-sponsored actors, could use the data to target implicated government individuals in social engineering attacks with the intent of conducting espionage.
- Ideologically motivated actors, such as hacktivists, would likely leverage this data to disrupt Iranian organizations using denial-of-service (DoS) attacks or to influence them with information campaigns.
- Financially motivated actors would very likely utilize the data to conduct ransom R&DE attacks.

The resurgence of conflict between Israel and Hamas since October 2023 has seen Iran conducting cyberattacks against Israel, while also being the recipient of similar cyberattacks. While Iran has been critical of the approach Israel has taken in the war, Israel has condemned Iran's alleged support of Hamas .

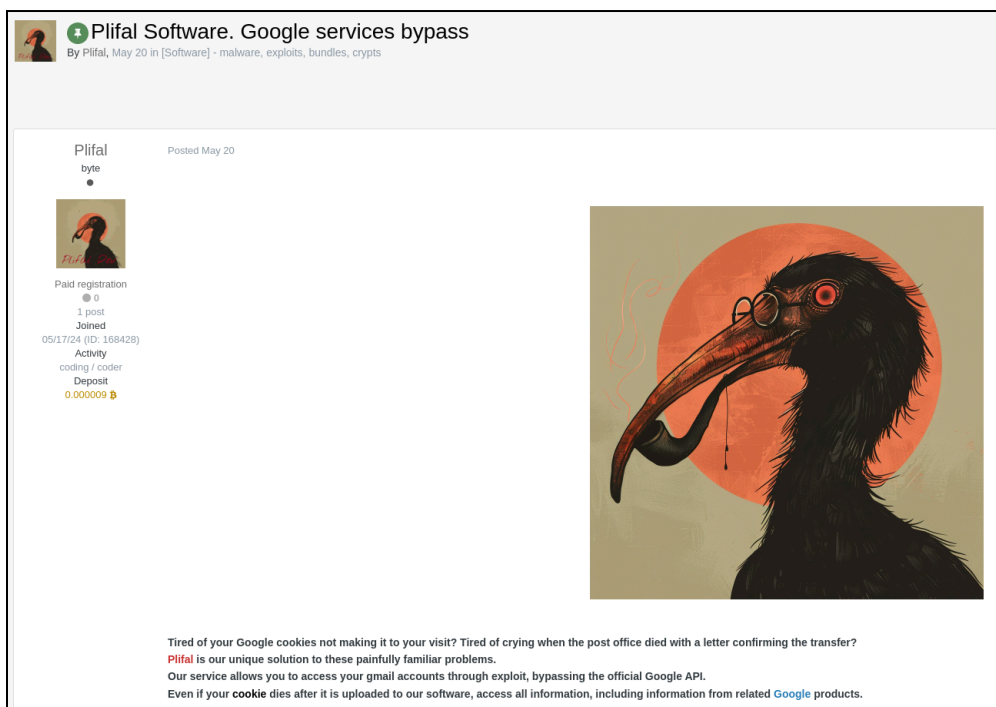
- On March 3, 2024, the pro-Palestinian and English-speaking threat collective "Handala Hack" allegedly gained remote access to Israeli radar systems. On April 13, 2024, the group then announced another breach of the radar systems, which was followed by an Iranian attack.
- The financially and ideologically motivated, pro-Israel hacking collective "R00KIT" claimed responsibility for targeting several Iranian-based organizations and agencies. These targets include a financial exchange system, an educational institution, a hospital, and an overseas logistics company.

The recent data leak is very likely related to the ongoing conflict, as threat actors likely seek to fulfill demand from geopolitically aligned actors for state-related data. Additionally, the leak likely indicates hacktivists and non-hacktivists that are primarily financially motivated are aligning over geopolitical events. Therefore, it is likely that data leaks implicating both Israel and Iran will continue to be advertised by threat actors on dark web forums while the Israel-Hamas war persists.

| Advertised Malicious Tool Targets Gmail Accounts

On May 20, 2024, untested actor “Plifal” announced a new malicious tool named Plifal Software on the Russian-speaking dark web forum Exploit. The tool allegedly bypasses Google APIs and policies, enabling threat actors to illicitly access Gmail user accounts. Plifal also claimed that the software can exploit other Google services, such as YouTube, Google Drive, and Google Photos.

- The software is available at a cost of USD 199 for a weekly subscription and USD 600 for a monthly subscription. A lifetime subscription is also advertised, though a price was not specified.
- Plifal did not explicitly agree to the use of escrow in the advertisement.
- The statement claims that the first five actors will receive a one-week subscription in order to review the software.



Plifal's post on the Exploit forum

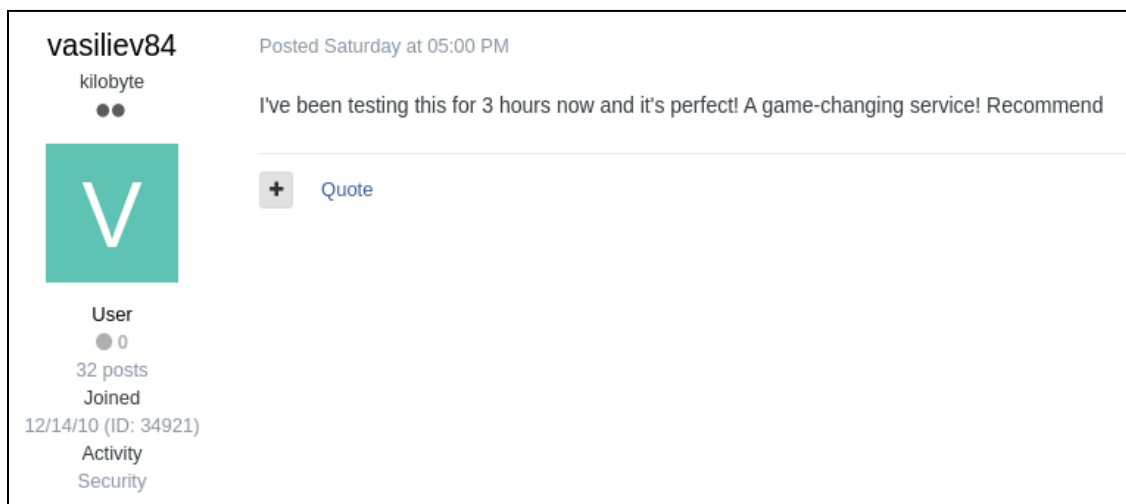
Source: ZeroFox Intelligence

There is a roughly even chance that Plifal Software requires the threat actor using it to already be in possession of appropriate session cookies, which (even when expired) can be leveraged to retain access to an active session. Though not specified by the

advertisement, it is likely that Plifal Software has the capability to circumvent correctly-configured, multi-factor authentication (MFA) protocols.

- Threat actors leverage a multitude of techniques to steal session cookies, such as the use of various types of malware, cross-site scripting, or man-in-the-middle techniques.

The advertisement garnered positive feedback from the Exploit community. On June 1, 2024, actor “vasiliev84” claimed that the software had operated as expected, stating that that the product is a “game changer” and recommending it to fellow threat actors. This was followed by a second post from “FrozyD” stating that the product had worked as anticipated at the time of purchase. This reception indicates there is a likely chance that Plifal Software functions as advertised, increasing the credibility of Plifal and his software tool, as well as the likelihood of its sale.



Exploit post exhibiting positive feedback for Plifal Software

Source: ZeroFox Intelligence

Malicious tools targeting Google software almost certainly seek to take advantage of its increasingly widespread use and diversification.

- Google’s email software platform, Gmail, is the most widely-used email service by a significant margin, with a reported 1.8 billion active users sending approximately 121 billion emails each day.¹

¹ [hXXps://www.demandsage\[.\]com/gmail-statistics/](https://www.demandsage.com/gmail-statistics/)

- Google Workspace—Google’s cloud-based productivity tool—is almost certainly the most widely-used collaborative workspace amongst organizations, with over three billion users. A disproportionate number of these are located in the United States.²

While the advertisement offers no further detail surrounding the capabilities of Plifal Software, illicit access to an individual or business Gmail account can enable a threat actor to conduct a myriad of malicious activities.

- Private data (such as emails, documents, contacts, and files saved in cloud storage) could be exfiltrated. This could enable and enhance further malicious activity, such as phishing attacks or Business Email Compromise (BEC).
- Stolen sensitive data, such as PII or PFI, could be sold in DDW marketplaces.
- There is a roughly even chance that the Google account itself could be compromised, enabling the intruder to access third-party websites to which the Google account has been connected. This could lead to the changing of credentials or fraudulent activity, such as impersonation.
- The compromised account could also be leveraged to conduct lateral movement, granting the threat actor access to adjacent networks within an organization. This would put any sensitive, proprietary, or business-critical information at risk of encryption or exfiltration.

2

[hXXps://developers.googleblog\[.\]com/en/year-in-review-12-awesome-ways-for-developers-to-learn-build-and-grow-with-google-workspace](https://developers.googleblog.com/en/year-in-review-12-awesome-ways-for-developers-to-learn-build-and-grow-with-google-workspace)

What Plifal can do:[Google Services \[Gmail, Drive, Photo, Keep, YouTube \]](#)

- the ability to download all messages from the mail
- multiple mail selection and mass processing
- search by mail: search by sender and header, with the ability to accurately select (starts/ends with, contains, equals). Ability to select a search query and view all emails containing it
- works on web sockets - optimization for teamwork from several machines
- loading all profiles from a cookie - dividing messages into folders as in the original mail
- convenient and intuitive interface for work
- ability to download attachments in emails
- the number of accounts is displayed
- added the ability to download all emails from mail
- the ability to unload account cookies
- logging account information
- the service works on requests - when purchasing a subscription, we provide APIs
- deleting a letter completely from the mail
- searching for letters in the mail
- folders as in the original mail

Prices:**1 week** - 199\$**1 month** - 599\$**Lifetime** - on request**The first 5 people are given a weekly subscription for a review****Exploit post outlining the capabilities of Plifal Software***Source: ZeroFox Intelligence*

Software tools targeting widespread and diverse software solutions that are becoming increasingly prominent in the workplace are almost certainly coveted by threat actors seeking to gain illicit access and conduct subsequent malicious activity. Tools such as Plifal Software are likely to become more common in DDW forums; similar tools are also likely to become more user friendly and diversified, increasing the potential threat vectors the software can target.

| Recommendations

- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Implement secure password policies with phishing-resistant MFA, complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques and procedures (TTPs).
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management process and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Proactively monitor for compromised accounts being brokered in DDW forums.
- Configure ongoing monitoring for Compromised Account Credentials.

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

Sources may use

TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

Amber

Sources may use

TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW MAY IT BE SHARED?

Recipients may NOT share

TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Recipients may ONLY share

TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that

TLP:AMBER+STRICT restricts sharing to the organization only.

Green

WHEN SHOULD IT BE USED?

Sources may use

TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

Clear

Sources may use

TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW MAY IT BE SHARED?

Recipients may share

TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

Recipients may share

TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%