



| Flash |

Advertised Malicious Tool Targets Gmail Accounts

F-2024-06-05a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Deep and Dark Web, Threat Actor, Network
Access

June 5, 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 09:00 AM (EDT) on June 5, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Advertised Malicious Tool Targets Gmail Accounts

› Key Findings

- 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 application programming interfaces (APIs) and policies, enabling threat actors to exploit session cookies and illicitly access Gmail user accounts.
- 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 the product is a “game changer” and recommending it to fellow threat actors.
- 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.
- Software tools targeting widespread and diverse software solutions that are becoming increasingly prominent in the workplace are almost certainly a coveted target for threat actors seeking to gain illicit access and conduct subsequent malicious activity.

Details

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 Software. Google services bypass**
By Plifal, May 20 in [Software] - malware, exploits, bundles, crypts

Plifal
byte
●



Paid registration
● 0

1 post

Joined
05/17/24 (ID: 168428)

Activity
coding / coder

Deposit
0.000009 \$

Posted May 20



Tired of your Google cookies not making it to your visit? Tired of crying when the post office died with a letter confirming the transfer?
Plifal is our unique solution to these painfully familiar problems.
Our service allows you to access your gmail accounts through exploit, bypassing the official Google API.
Even if your **cookie** dies after it is uploaded to our software, access all information, including information from related **Google** products.

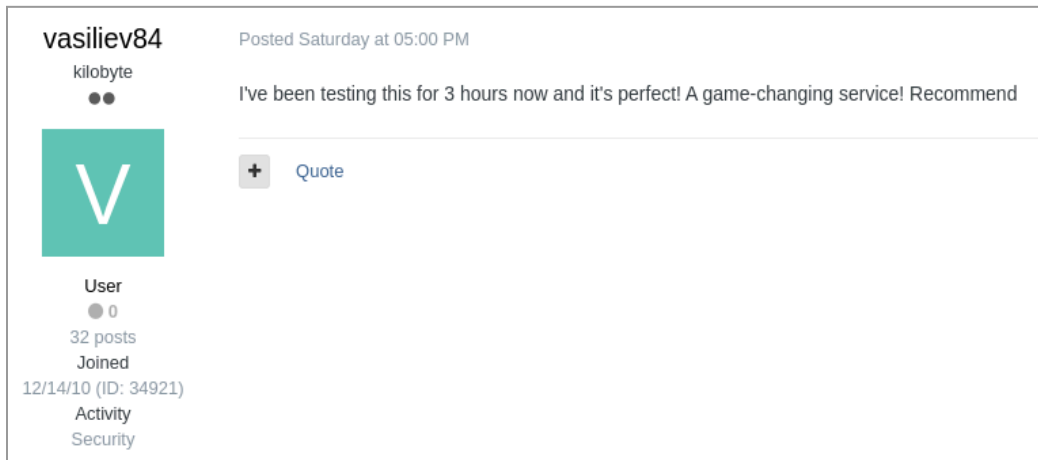
Plifal's post on the Exploit forum

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 “FrozzyD”, 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
- Google Workspace—Google's cloud-based productivity tool—is almost certainly the most widely-used collaborative workspace amongst organizations, with over 3 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 personally identifiable information (PII) or financial information, could be sold in deep and dark web (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.

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

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 a coveted target for 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.
- 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.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Develop a comprehensive incident response strategy.
- 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.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques and procedures (TTPs).

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	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.	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	Clear
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.	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%