



| Brief |

The Underground Economist: Volume 4, Issue 9

B-2024-05-03a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Phishing

May 3, 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 9:00 AM (EDT) on May 3, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 9

| New Ransomware-as-a-Service Operation Attempts to Build Credibility

On April 24, 2024, well-regarded threat actor “rtgtgth” posted in the Russian-speaking deep and dark web (DDW) forum RAMP advertising their new Ransomware-as-a-Service (RaaS) operation, “psoglav” (translates from Russian to “dog-headed”), and their search for affiliates.

Rtgtgth claims that the service will be constantly developed based on user feedback, with a primary focus on reliable encryption. Many of the software functionalities specified are those typical of advanced ransomware tools, such as being written in pure C with no external dependencies, lateral movement, and backup deletion. Other notable features include:

- Compatibility with all versions of the Windows operating system;
- Fast file encryption with reliable decryption methods;
- Disabling of processes that may interfere with the encryption process; and
- No internet connection required to process the software.



rtgtgth

Apr 7, 2023

Messages 18

Reaction score 6

Points 3

Wednesday at 6:26 AM

We offer work with our Psoglav Ransomware.

At the moment, all the most necessary functions are present and work stably.

We will constantly develop the project based on user feedback.

When developing the project, we focused on the reliability of encryption.

Some features of our :

- written in C#
- Works successfully on all Windows.
- Encryption occurs using AES-256+RSA-2048 algorithms;
- Fast file encryption
- Files ALWAYS have the ability to be decrypted correctly;
- no Internet required to process files;
- The network is processed after all disks have been processed;
- Before encryption begins, the ransomware disables common processes that may interfere with high-quality file encryption and stops services;
- Delete shadow copy;
- Delete itself
- Each partner has his own private master key;

Post by rtgtgth advertising psoglav Raas

Source: ZeroFox Intelligence

The post further outlines the collective's plans to never deceive their victims, stating that stolen information will always be decrypted and returned after a ransom payment is made. Extortion methods that require the victim to make additional follow-up payments are forbidden, and affiliates not adhering to these procedures will be banned from the service.

Important :

- we are focused only on long-term cooperation. If you write to us with a request to decrypt one of the partners, there will be no dialogues, you will simply be redirected to this partner. Particularly persistent ones will be subject to a permanent ban;
- For the first 3 partners, the first decryptions are free (temporary promotion);
- We never deceive our victims and always issue a decryption after payment. We do not accept extortion methods that require additional payment after payment. If you have a different opinion on this matter, you and I are not on the same path. If you break one of these rules, you will be banned forever;
- In the process of work, we provide partners with free test (not giant) files of up to 2 pieces per ID;
- The cost to decrypt one ID card is \$150

To work with us you need:

- Brief information about you: your experience, distribution method and processing countries,
- Mail that will be indicated in information messages
- Your contacts, the more, the better.

Our contacts / Our contacts:

Tox ID: 6AA88CA3992A1AD63EE3F98A245DC580F4AC1B05C04A4C9C417D22176569694AB27ECB55365E



Post by rtgtgth stating affiliate terms and conditions

Source: ZeroFox Intelligence

This announcement is very likely indicative of newer RaaS operations' intent to capitalize upon a perception of discontent and distrust amongst affiliates—particularly those that have been affected by recent disruptive law enforcement (LE) activity and are seeking new malicious services with which to associate.

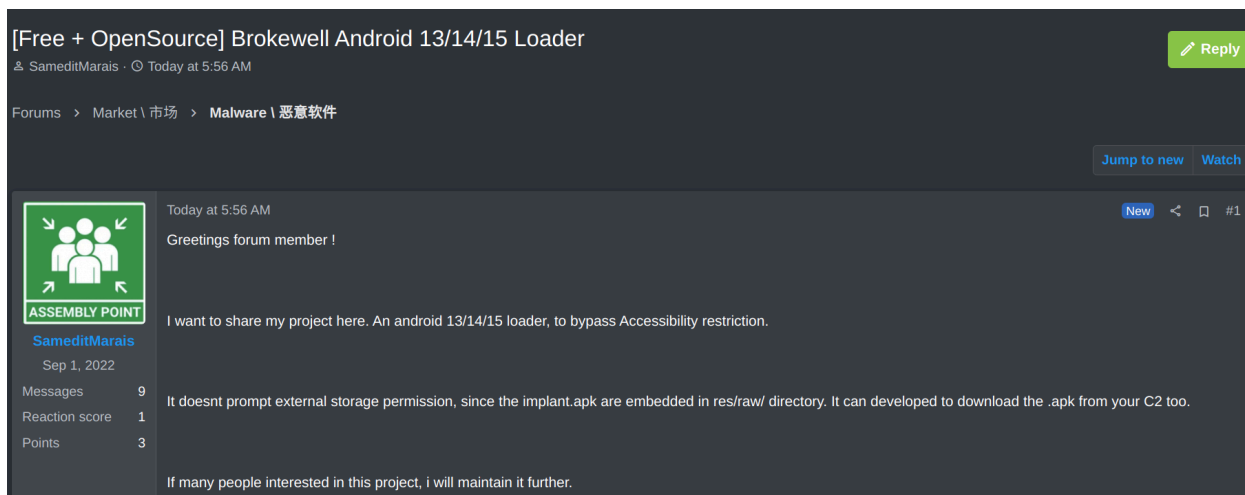
- In recent months, affiliates have very likely been subjected to exit scams whereby payment was not received following successful extortion attacks.
- At least one recent extortion attack took place during Q1 2024 that resulted in a victim organization not being returned its stolen data upon payment of the ransom. This resulted in widespread media coverage and is likely contributing to low victim payout rates.

There is a roughly even chance that both new and existing RaaS operations will increasingly focus on creating services considered “credible” by forum moderators, ransomware and digital extortion (R&DE) affiliates, and victim organizations in an attempt to attract and retain affiliates and encourage victims to meet ransom demands.

| Free Android Malware Shared in Deep and Dark Web Forum

On April 22, 2024, positive-reputation threat actor “SameditMarais” posted in the DDW forum RAMP advertising a new malware project dubbed “Brokewell.” Brokewell is alleged to be a loader capable of targeting Android versions 13, 14, and 15 by downloading malicious .apks onto victim devices.

- An Android Package (.apk for short) is a file format used by the Android operating system for the distribution and installation of mobile applications, games, and other software and have previously been used by threat actors to conceal malicious software and bypass security features.
- While Android 14 was released in Q3 2023 and is almost certainly globally widespread, Android 15 is not due to be released for general use until Q4 2024. It will almost certainly be released for limited use before this, however.



[Free + OpenSource] Brokewell Android 13/14/15 Loader

& SameditMarais · Today at 5:56 AM

Forums > Market \ 市场 > **Malware \ 恶意软件**

Jump to new Watch

Today at 5:56 AM

Greetings forum member !

ASSEMBLY POINT

SameditMarais

Sep 1, 2022

Messages 9

Reaction score 1

Points 3

I want to share my project here. An android 13/14/15 loader, to bypass Accessibility restriction.

It doesnt prompt external storage permission, since the implant.apk are embedded in res/raw/ directory. It can developed to download the .apk from your C2 too.

If many people interested in this project, i will maintain it further.

RAMP post advertising Brokewell

Source: ZeroFox Intelligence

SameditMarais claimed that Brokewell does not prompt the user to grant access permissions when installing .apk files from external storage, while also bypassing other accessibility restrictions that were not specified. SameditMarais also specified that Brokewell can be acquired for free, along with user instructions, from a Gitea repository. Further direct assistance is available from the threat actor's Telegram channel.

The advertisement claimed that further development of the loader will continue should it garner sufficient community interest. This would very likely see the tool become chargeable and continually improved.

this project is intended to bypass android 13/14/15 Accessibility permission restriction.

How to use

1. clone this repository
2. set APK name by changing app_name on app/src/main/res/values/strings.xml
3. set APK icon by adding new image asset on app/src/main/res/. then adjust android:icon="@mipmap/ic_launcher" on AndroidManifest.xml
4. put your RAT (the one that need accessibility) on app/src/main/res/raw/implant.apk
5. on MainActivity.java file, change String IMPLANT_PKGNAME = ""; according to your implant.
6. generate your new/random signing CERTIFICATE with this command: keytool -genkey -v -keystore brkwlkey -alias brkwlkey -keyalg RSA -keysize 2048 -validity 1337 -storepass VerSecPass -keypass VerSecPass -dname 'CN=RUSSIA,O=MOSCOW,C=RU'
7. by default, this project are using "com.brkwl.apkstore" as PKGNAME. you can set yours by changing "applicationId" on app/build.gradle file. You can also enable the random package name generator so every release build will have a different & unique PKGNAME.

Brokewell user instructions

Source: ZeroFox Intelligence

Android malware is very likely in high demand among malicious actors in DDW forums, due primarily to the widespread use of potentially vulnerable targets and the versatility of potential attack vectors that could be exploited. Compromised devices could be subject to data or identity theft, digital extortion, or performance degradation. It is very likely that Brokewell is currently underdeveloped, though likely still poses a threat to Android devices.

| New Ransomware-as-a-Service Operation Claims Innovative Features

On April 19, 2024, positive-reputation threat actor “Bezzle” announced a new RaaS operation named Apos in the Russian-speaking DDW community RAMP. Bezzle proclaims Apos is the “fastest” and “most technically advanced” product on the market.

Similar to other RaaS offerings, Apos offers a bespoke victim negotiation platform, a dedicated victim leak site, and support from Bezzle. The post claims that affiliates are able to retain 90 percent of any ransom payouts, with Bezzle taking 10 percent. While 90 percent is almost certainly higher than average RaaS offerings, this has become more common during 2024, particularly amongst newer RaaS collectives.

- Bezzle further specifies that any affiliate able to generate USD 1 million will be able to negotiate more favorable terms, though details are not specified. Such affiliates will also be authorized to leverage Apos infrastructure to conduct denial-of-service (DoS) attacks.

Thursday at 8:42 PM

New < > #1

Introducing **Apos** - a new generation affiliate program

We offer the fastest and most technically advanced product on the market, which at the same time is easy to use. The product is developed in pure C without any dependencies. A strong encryption algorithm is used along with the Diffie-Hellman key exchange protocol. All cryptography is implemented in code without the use of external libraries.

SOFTWARE FEATURES

- Automatic creation of builds with your settings (unlimited number)
- Multithreaded encryption
- File name encryption
- Custom add-on extension
- Replacing the Windows desktop background
- Stopping Windows processes and services
- Removing shadow copies and system backups
- Clearing system logs after encryption is complete
- White\Black lists of file names, folders, file extensions
- Hybrid encryption in Fast, Intermittent or Full modes depending on file extension
- Ability to configure how many bytes will be encrypted in Fast mode, and what percentage of the file will be encrypted in Intermittent mode
- Ability to add or exclude hidden files and/or hidden folders from encryption
- Network distribution via SMB
- Automatic stopping of ESXi virtual machines

RAMP post by Bezzle advertising Apos software features*Source: ZeroFox Intelligence*

The announcement specifies a list of software features and capabilities supposedly included in the service, many of which, while not necessarily innovative, are almost certainly offered primarily by more advanced RaaS platforms that are designed to compromise Windows-based systems. These features include:

- The software being written entirely in the programming language C;
- No dependencies or external library requirements;
- An unlimited, automatic creation of builds with customizable user settings;
- The removal of shadow copies and system backups; and
- The ability to stop Windows process and services.

Some of the claimed features are less common, however, and are very likely indicative of an attempt to separate the Apos service from its competition and appeal to potential affiliates. The first of these is Network distribution via SMB. This very likely refers to the attacker's ability to conduct lateral movement within the target network by exploiting vulnerabilities within Microsoft Windows Server Message Block, enhancing persistence.

- Ability to add a note to specific folders, even if they do not contain encrypted files
- Customizable process name displayed in Task Manager
- Work in the background (without any visual elements)
- Protection against re-encryption of already encrypted files
- Encrypting Windows builds to bypass Antivirus solutions*

Encryption modes :

Fast mode encrypts the first N bytes of the file.

Intermittent mode encrypts a specified percentage of all bytes in a file, distributing encrypted stripes evenly throughout the file with a specified segmentation.

Full mode encrypts the entire file.

Command line arguments allow you, if necessary, to overwrite some of the settings specified when creating the build. You will find a more detailed description of all product features in the User Guide.

Supported platforms :

Windows XP - 11 (x86 and x64)

Windows Server 2003 - 2022 (x86 and x64)

All x64 Linux distributions, and all major x86 Linux distributions

All x64 ESXi, BSD and NAS

Continuation of RAMP post by Bezzle advertising Apos software features

Source: ZeroFox Intelligence

The “protection against re-encryption of already encrypted files” is also a feature rarely seen in new RaaS offerings. This is almost certainly intended to serve as a safeguard against competing R&DE operatives, as well as any other threat actors who have gained simultaneous illicit access to the victim’s network. There are numerous ways in which this could occur, with the following being the most likely:

- The threat actor buys illicit network access from an initial access broker (IAB) in a DDW forum. In some cases, a threat actor can ensure that they are the sole buyer of the access, paying an often-premium price to ensure that the access is subsequently removed from the market. In the majority of cases, however, these sales are not limited to a single buyer, with the attack becoming a “first come, first served” opportunity.
- A software vulnerability that enables illicit network access becomes common knowledge within DDW forums, enabling numerous R&DE affiliates to conduct attacks. However, it is very likely that the majority of these instances do not result in the same networks being targeted but, rather, different organizations operating the same vulnerabilities.

CONDITIONS

- All payments are made to your wallet
- Leak site
- A platform for communicating with companies. You can negotiate on your own or with our help
- 24/7 support
- Until reaching \$1M we take 10%

After reaching the total amount of \$1M, the following services will become available to you:

- DDoS attacks
- Ringing

All conditions are individual and subject to change.

Spoiler: ONE

Apos Security

RAMP post by Bezzle advertising Apos

Source: ZeroFox Intelligence

There is a very likely chance that these circumstances will arise more frequently within DDW forums over the coming months, due primarily to the instability that ensued following the disruption of both ALPHV and LockBit in Q4 2023 and Q1 2024, respectively. The cessation of their operations is almost certain to have led to the increasing number of active R&DE collectives observed by ZeroFox and to growing competition between both RaaS offerings and affiliates caused by an increasingly fragmented R&DE ecosystem.

It is very likely that RaaS operators anticipate a void in the R&DE marketplace where ALPHV—and to a lesser extent LockBit, which continues to conduct limited activity—used to dominate. RaaS offerings are very likely to become increasingly competitive during 2024 as a result, with collectives offering affiliates more software features, better technical support and digital infrastructure, and higher payouts and loyalty incentives. At the time of writing this report, ZeroFox has observed no Indicators of Compromise (IoCs) associated with Apos ransomware.

| 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 multi-factor authentication (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%