



Brief

The Underground Economist: Volume 3, Issue 24

B-2023-12-07a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Threat Groups, Ransomware, Deep and Dark Web

December 7, 2023

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 (EST) on December 6, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 3, Issue 24

Mass Access Brokering Event Impacting Corporate Citrix VPN Users

On November 26, 2023, highly-regarded threat actor “Punktir” announced the auction of access to at least 711 compromised Citrix Virtual Private Network (VPN) instances with verified credentials on the Russian-speaking forum exploit[.]in. Since 2020, Citrix VPN has been one of the most widely-exploited products used by access brokers to gain a foothold into corporate networks.

The post very likely represents a legitimate mass access brokering event; Punktir has a strong reputation and states that they will accept escrow at the buyer’s expense. The post alleges that:

- There are no two-factor authentication (2FA) protected instances.
- There are no duplicates of previously-sold login portal links.
- The auction has a starting bid of USD 700, and it is USD 35,000 for a “blitz” or “buy now” price to acquire the total package without waiting for the auction to expire.

P

711 citrix with revenue >5kk and PC login, starting at \$10 per line

By Punktir, 21 hours ago in Auctions

Start new topic

Punktir

gigabyte

●●●●

P

Seller

34

143 posts

Joined

02/18/21 (ID: 114266)

Activity

virology / malware

Posted 21 hours ago

There are 711 lines in the list with verified logins and passwords on request /VPN/ (citrix)

The list includes only sites with a revenue of more than 5 million, no gov, no edu, no schools and universities, no CIS, no sites with 2fa, **no empty web entrances**

Not a single line from the list overlaps with my previous lots

The login and password to enter the request + **connect to the PC** in each line were checked!

Each line is a unique domain, there are no duplicates in the list Nothing was torn out or taken away, us, europe, com everything is in place (**us more than 400 lines in the list**)

Work is available through a guarantor at your expense

Start 7000\$ Step 1000\$ Blitz 35000\$

tg <https://t.me/wctrishift>

tox E54D9131BB82D918C341747AC162FDC4F3334F6EE61B72F8A2EFE66411981E098A098C9FF849

Translated exploit[.]in post advertising the mass access brokering event

Source: ZeroFox Collections

Ransomware cartels—which frequently leverage exploit[.]in to purchase access from brokers—are very likely to deem the access sale affordable and to have a potentially high return on investment.

Organizations included in the access sale have an alleged revenue over USD 5 million—a figure that typically satisfies the criterion used by ransomware collectives. No government, education, or Commonwealth of Independent States (CIS)-based entities are included. The targets are all Europe and U.S.-based, with U.S. targets allegedly accounting for more than 400 entries.

The emergence of corporate access checkers on the deep and dark web has driven an increase in bulk access sales in 2023.

- A corporate login checker (such as the Multi Network Checker) was likely leveraged in this instance to verify the list of targets given the high volume of compromised Citrix VPN portals and the claim that the credentials were checked.
- The target list was likely prepared prior to obtaining access and likely based on manual research supplemented by scanning via pentesting tools.

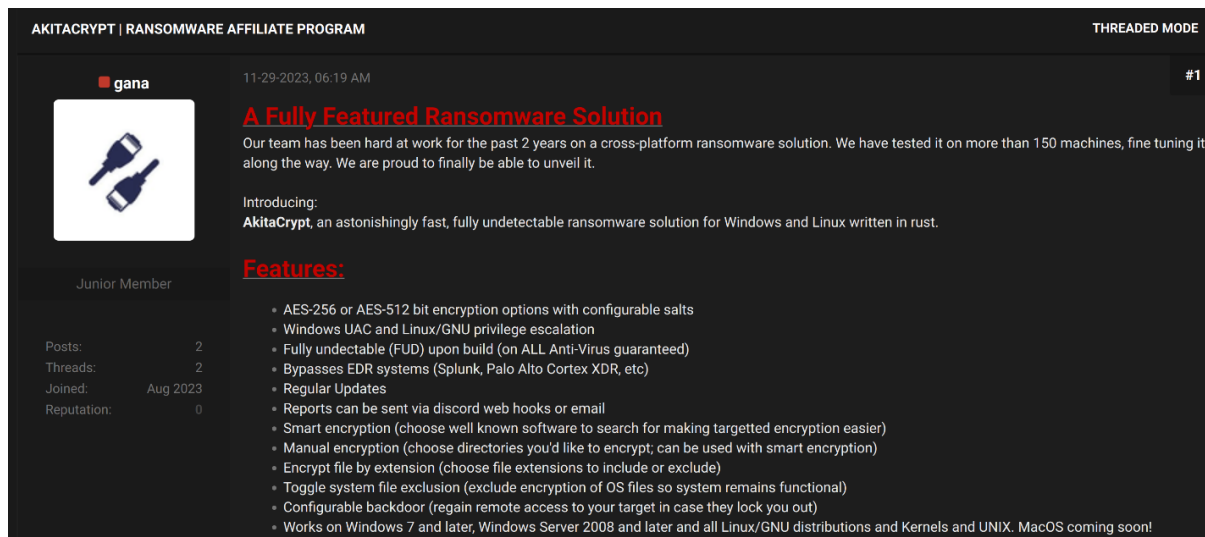
Use of these tools is expected to continue on an upward trajectory as corporate checkers become more readily available to potential attackers.

| New “Akitacrypt” Ransomware-as-a-Service Announced

On November 26, 2023, untested English-speaking threat actor “gana” announced a new Ransomware-as-a-Service (RaaS) offering called “Akitacrypt” on the dark web community BlackForums. The BlackForums platform is operated by actors connected to the “Five Families” hacking group, which consists of ThreatSec, GhostSec, Stormous, BlackForums, and SiegedSec.

The post claims that Akitacrypt is a fully-featured ransomware solution developed and tested privately for two years prior to release. Akitacrypt is allegedly:

- Written in Rust, a programming language becoming increasingly popular amongst malware developers;
- Fast;
- Fully undetectable (FUD), bypassing all antivirus products—including Endpoint Detection and Response (EDR) services; and
- Currently deployable on Windows and Linux operating systems, and—unusually—being developed to have the capability to infect systems running Mac OS.



The screenshot shows a forum post on BlackForums. The header reads 'AKITACRYPT | RANSOMWARE AFFILIATE PROGRAM' and 'THREADED MODE'. The user 'gana' is the author, with a profile picture of a key and a lock. The post is dated '11-29-2023, 06:19 AM' and is the first in the thread. The title is 'A Fully Featured Ransomware Solution'. The text of the post states: 'Our team has been hard at work for the past 2 years on a cross-platform ransomware solution. We have tested it on more than 150 machines, fine tuning it along the way. We are proud to finally be able to unveil it.' It then introduces 'AkiCrypt, an astonishingly fast, fully undetectable ransomware solution for Windows and Linux written in rust.' A 'Features:' section follows, listing: AES-256 or AES-512 bit encryption options with configurable salts; Windows UAC and Linux/GNU privilege escalation; Fully undetectable (FUD) upon build (on ALL Anti-Virus guaranteed); Bypasses EDR systems (Splunk, Palo Alto Cortex XDR, etc); Regular Updates; Reports can be sent via discord web hooks or email; Smart encryption (choose well known software to search for making targetted encryption easier); Manual encryption (choose directories you'd like to encrypt; can be used with smart encryption); Encrypt file by extension (choose file extensions to include or exclude); Toggle system file exclusion (exclude encryption of OS files so system remains functional); Configurable backdoor (regain remote access to your target in case they lock you out); Works on Windows 7 and later, Windows Server 2008 and later and all Linux/GNU distributions and Kernels and UNIX. MacOS coming soon!

Posts:	2
Threads:	2
Joined:	Aug 2023
Reputation:	0

Post advertising the new Akitacrypt RaaS offering

Source: ZeroFox Collections

Affiliates deploying the offering will initially be entitled to 50 percent of the profits of successful extortion campaigns. While this is considerably lower than most Russian RaaS offerings (which typically offer in excess of 80 percent of profits), Akitacrypt affiliates that demonstrate sustained successes will be eligible to work up to receiving as high as 90 percent of profits. To qualify, would-be affiliates must satisfy one of the following specialization requirements by being:

- Initial network access brokers,
- Hobby penetration testers or web application hackers,
- Bug bounty hunters,
- Exploit developers, or
- Insiders with internal access.

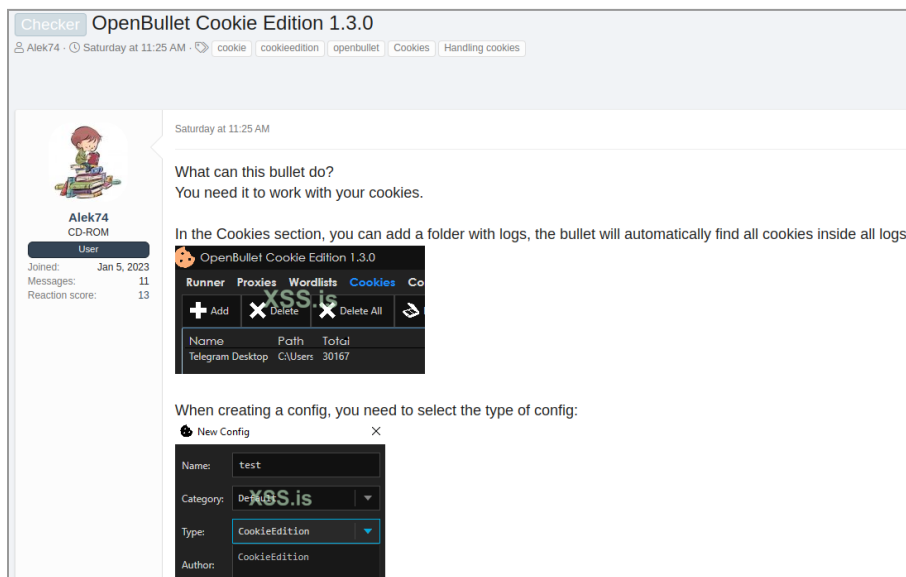
The RaaS model has become increasingly popular outside of the typical Russian-speaking threat actor communities. Historically, English-speaking actors have advertised entrepreneurial ransomware products designed to be used by a single actor or a small team in isolation. However, the RaaS model has gained greater traction within English-speaking communities in 2023.

ZeroFox assesses that if gana's claims around Akitacrypt's technical specifications are legitimate, the strain will very likely achieve considerable success and pose a significant threat to corporate entities worldwide. However, the actor is untested, and therefore the veracity of their claims is difficult to ascertain. Further, although BlackForums is the official home of the Five Families outside of Telegram, it is still not widely regarded as a gathering place for serious brokers because of its low numbers of less-notable forum members.

| Modified OpenBullet Tool for Cookie Parsing

On November 25, 2023, well-regarded Russian-speaking actor "Alek74" announced the release of a modified version of the popular pentesting tool OpenBullet on the dark web marketplace xss[.]is. The OpenBullet tool enables threat actors to attack the servers of a particular entity by checking credentials against various login pages using commands within a specific configuration file. This modified version, dubbed "OpenBullet Cookie

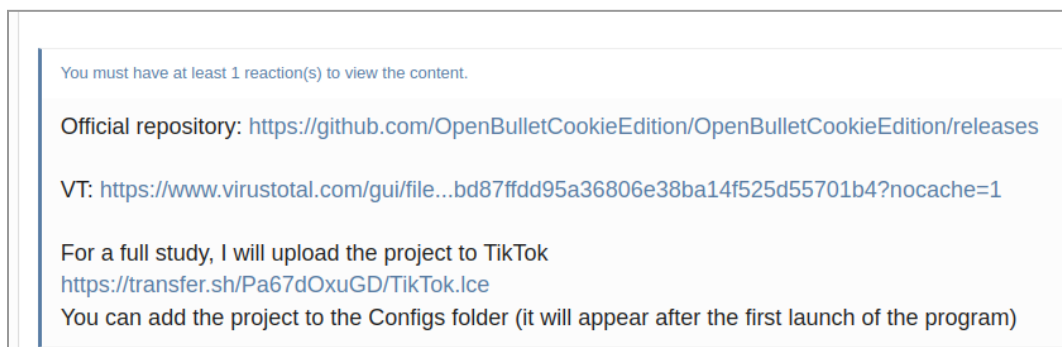
Edition” parses cookies from botnet and infostealer logs and checks them against a list of targets.



Translated post advertising the new OpenBullet Cookie Edition tool

Source: ZeroFox Collections

Alek74 posted full instructions for operating the tool and provided a link to the OpenBullet modification on GitHub. The actor also referred to a download of their OpenBullet Cookie Edition project, which targets TikTok accounts by checking session cookies against them. If a hit is recorded, the attacker can begin integrating the validated cookies into their browser and continue the victim’s session.



Links provided by the actor to GitHub and their project targeting TikTok accounts

Source: ZeroFox Collections

OpenBullet Cookie Edition will likely gain traction on dark web marketplaces, greatly aiding threat actors' efforts to leverage botnet and infostealer logs by streamlining parsing and validation of cookies. It represents a continuation of the trend seen in 2023 wherein bonet and infostealer logs have become a more valuable resource to threat actors than database dumps and combolists containing emails and passwords. While the standard OpenBullet tool leverages email:password lists to attack login portals, the modified Cookie Edition has been adapted to leverage logs, which are now a more valuable and more common resource.

| 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 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 deep and dark web forums.
- Configure ongoing monitoring for Compromised Account Credentials.

| 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%