



Brief

The Underground Economist: Volume 4, Issue 14

B-2024-07-31a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web

July 31, 2024

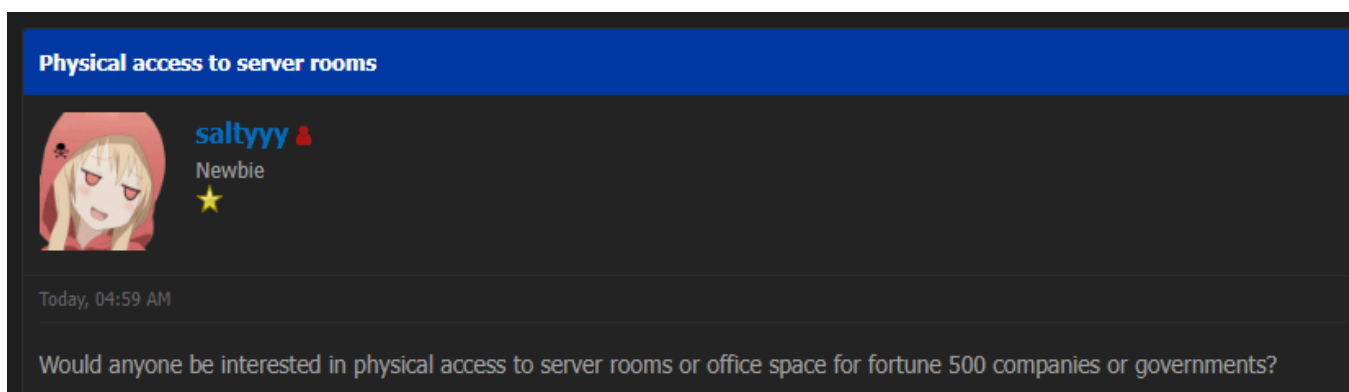
Scope Note

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 July 31, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 14

| Dark Web Forum Hosts Discussion over Usability of Physical Access to Commercial Office Spaces

On July 18, 2024, an untested actor named “saltyyy” posted in the dark web forum Omniforums (to which they had recently registered), attempting to ascertain if their peers had interest in procuring physical access to commercial office spaces. While not specifically stated, saltyyy implied that they were able to offer physical access to server rooms and office spaces that host digital infrastructure belonging to Fortune 500 companies and government entities.

**Saltyyy Omniforums post**

Source: ZeroFox Intelligence

Other forum participants questioned the usefulness of such access, stating that both physical security measures such as cameras and electronic badge readers and digital

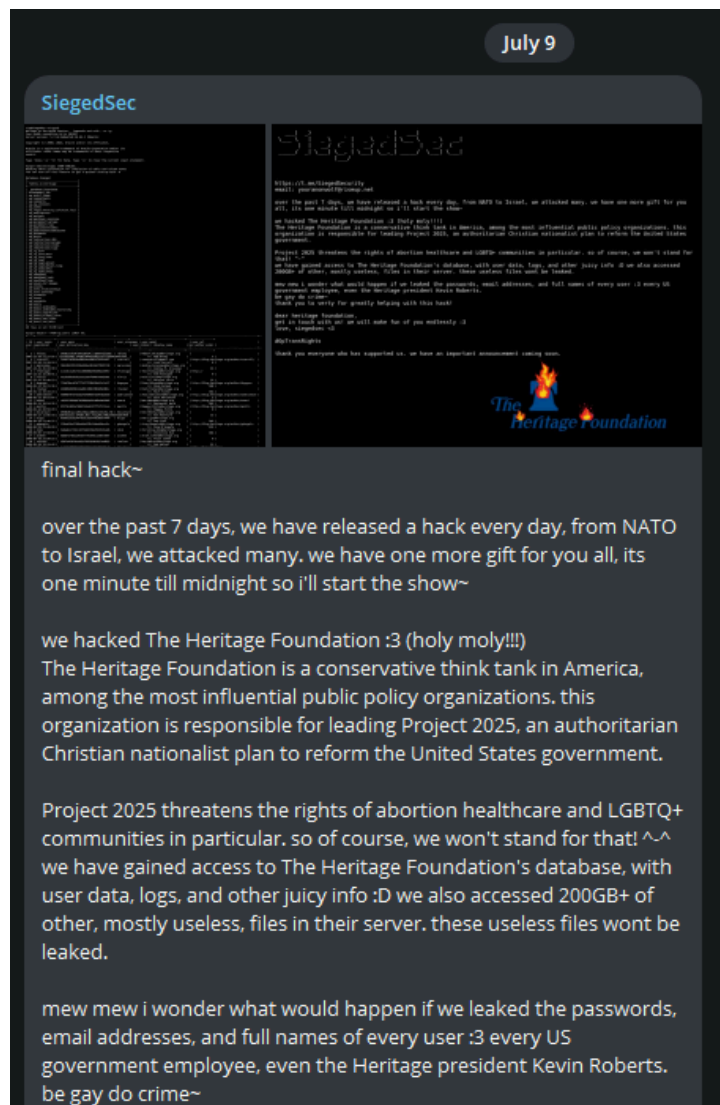
security measures like encryption and privilege restrictions would prevent any exploitation from taking place.

While this post is unlikely to represent an imminent threat, it highlights the diverse techniques, tactics, and procedures (TTPs) that threat actors are willing to explore, develop, and monetize in order to facilitate malicious cyber activity. It also accentuates the necessity for organizations to adopt comprehensive security protocols that address the growing convergence of physical and cyber threats. These threats are likely to be exacerbated in the coming years as organizations adopt increasingly diligent cybersecurity measures, resulting in threat actors seeking alternative means of gaining malicious access.

| SiegedSec Announces Disbandment Following Breach of Think Tank Institute

On July 9, 2024, hacktivist collective “SiegedSec” announced their alleged success in breaching a network associated with The Heritage Foundation, claiming to have stolen over 200GB of data that includes passwords and personally identifiable information (PII). In the announcement, SiegedSec revealed their stance on The Heritage Foundation-led conservative initiative known as “Project 2025”, which the actor describes as “an authoritarian Christian nationalist plan to reform the United States government.”

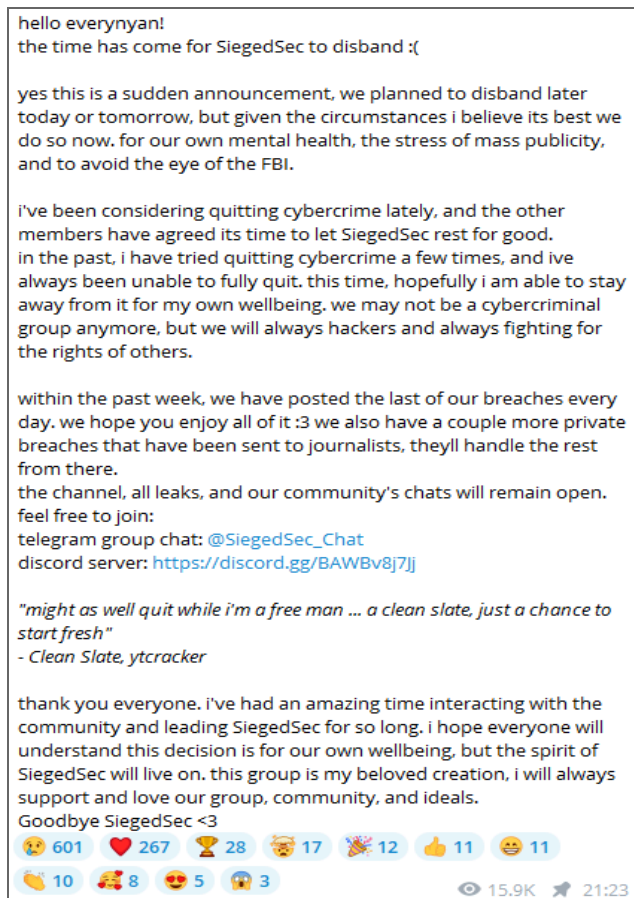
- SiegedSec is a hacktivist group that was first observed in approximately April 2022 and often refer to themselves as the “gay furry hackers.”
- The group was initially a member of “The Five Families”, a unified hacker collective that has conducted financially, ideologically, and politically motivated attacks against organizations across the globe.
- Since its inception, SiegedSec has conducted data theft and disruption attacks against organizations promoting what the group has deemed to be “right-wing” political agendas. Targets have included several U.S. state governments, as well as legal, scientific, and religious institutions. In April 2024, SiegedSec announced its intent to target churches, media establishments, and other entities it perceives to be infringing on the rights of transexual individuals and communities.



SiegedSec Telegram post announcing The Heritage Foundation breach

Source: ZeroFox Intelligence

The next day, SiegedSec revealed alleged correspondence with a senior representative of The Heritage Foundation, providing insight into the nature of their conversations. This was followed by a Telegram post announcing SiegedSec's disbandment, with law enforcement scrutiny and mental health among the cited reasons. Given the intense and threatening nature of the previously revealed conversations between SiegedSec and The Heritage Foundation, there is a likely chance that they contributed to SiegedSec's alleged decision to cease operations.



SiegedSec Telegram post announcing their disbandment

Source: ZeroFox Intelligence

Notorious threat actor "IntelBroker" re-published the leaked information to the hacking forum BreachForums on July 11, 2024. This is very likely to significantly expand the reach and accessibility of the information and increase the likelihood of it being leveraged in social engineering, spam, or blackmail activity.

| New Extended Validation Code-Signing Service Advertised

On June 30, 2024, untested actor "enryu" advertised a new extended validation (EV) code-signing service on the primarily Russian-speaking dark web forum Exploit. According to the advertisement, illicit validation certificates can be purchased that allow

malicious webpages to bypass security protocols such as SmartScreen, Windows User Account Control, and Windows Defender, as well as some AV software provided by third parties such as Kaspersky, Avast, and Malwarebytes.

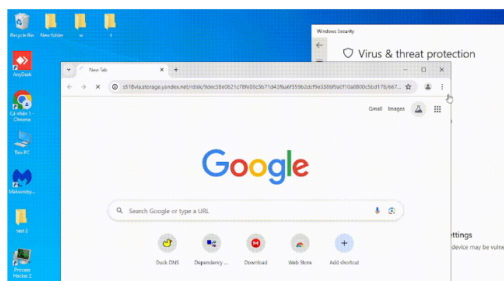
- Compared to SSL/TLS-encrypted web pages certified with domain validation (DV) or organization validation (OV) certificates, those with EV provide a higher level of verification security assurance.
- EV-certified web pages often offer the interacting end user visual reassurance, such as the requested URL being preceded by a green padlock and the organization's name. They are also much less likely to trigger alerts from the operating system or third-party security software programs. Both of these translate to higher levels of endorsement and subsequent end user trust.
- Enryu's orders are allegedly completed within 24 hours and available to a single buyer only. This is a faster turnaround than that offered by many competing services, which typically range between two and five days.

EV CODE SIGNING CERTIFICATES VALID

With code signing, users can trust the software they are downloading, and need not worry about downloading malware onto their computer. A code signing certificate issued by a trusted certificate authority.

What is EV Code Signing?

- Instant bypass of SmartScreen filter, no reputation required
- Makes UAC trusted
- Signed software inspires more trust in the user, which significantly increases conversion
- Bypass of some antiviruses based on signature detection



Exploit post advertising new EV code-signing service

Source: ZeroFox Intelligence

According to enryu, a single certificate costs USD 500, with other options of "one week" and "one month" advertised for USD 1,500 and USD 2,900, respectively. While it is not specified what these services relate to, is it likely the length of time for which a certificate is valid.

If this is the case, enryu's service is slightly more expensive than others observed by ZeroFox, which typically charge between USD 1,500 and USD 3,000 for a single certificate valid for one year, depending on the certificate authority. There is a roughly even chance that enryu's higher price is due to the ability to bypass additional security protocols.

Certificates in stock or on order

- Certificates by pre-order: production time 24h
- Discussion of wholesale orders
- Certificates are sold strictly to one person. Fresh and unused

Bypass ALL AV

 **Features**

- ♥ Bypass Windows Defender
- ♥ Bypass Kaspersky
- ♥ Bypass MalwareBytes
- ♥ Bypass Avast
- ♥ Bypass 360 Safeguard
- ♥ Bypass Avira
- ♥ Bypass Baidu
- ♥ Bypass AVG
- ★ Memory Injection
- ★ Encryption
- ★ (ETW) Bypass
- ★ (AMSI) Bypass
- ★ Virtual Machine Bypass
- ★ Stable

Contacts

TG Channel: https://t.me/Baphomet_Crypter
Owner: @Baphomet_AV

Exploit post advertising new EV code-signing service

Source: ZeroFox Intelligence

Illicit validation certificates offer cyber threat actors the ability to augment a wide array of malicious activities, such as the deployment of disruptive malware to target networks, enhanced social engineering attacks, or data theft resulting in operational disruption, extortion, or fraud. To enable this, threat actors attract victims to malicious web pages by leveraging techniques such as SMS and email phishing, domain spoofing, and—if the web page is able to establish a positive reputation—search engine optimization (SEO) poisoning.

- Threat actors almost certainly seek to leverage illicit validation certificates in as many separate, lucrative attacks as possible to justify their price tag. However,

they are sought after and often revoked by certificate authorities, web browser vendors, and threat researchers.

- EV-certified web pages do not implicitly enable hosted files that are downloaded by the end user to bypass the same security protocols. There is a roughly even chance that downloaded files will be scrutinized by security software regardless of their originating location.

Given the versatility offered by initial network access, services such as these are very likely to appeal to a wide range of threat actors with varying intents and motivations, leading to their continued development, competitiveness, and innovation.

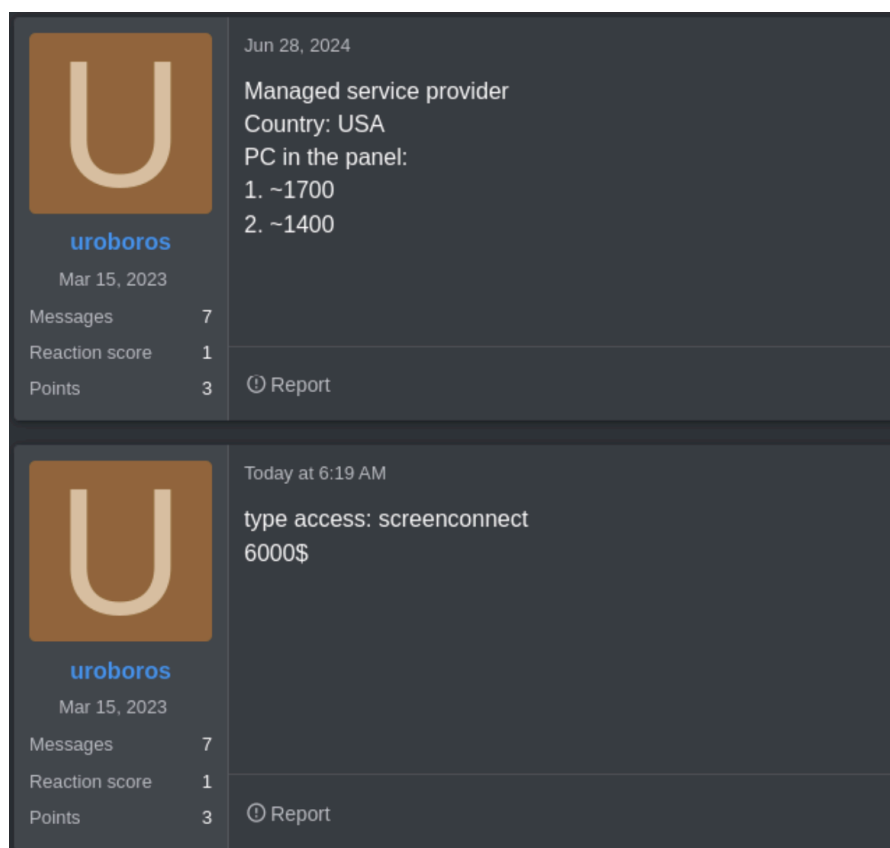
| Positive Reputation Actor Advertises Access to Managed Service Providers

On June 28, 2024, a positive reputation threat actor named “uroboros” advertised network access to two U.S.-based managed service providers (MSP) in the primarily Russian-speaking dark web community RAMP. According to the post, the first organization has 1,700 “PC” in their administration panel, and the second has 1,400. This very likely refers to the number of network endpoints contained within the victim networks that can be illicitly accessed—likely via a remote monitoring and management (RMM) tool. Although not initially advertised, uroboros updated the post on June 10, 2024, to include an asking price of USD 6,000.

- The next day, uroboros also advertised network access with admin rights to an Israeli-based organization with an alleged annual revenue of USD 30 million. The advertisement is very likely reflective of a continued interest in Israel-based targets amongst both financially and ideologically-motivated threat actors.
- Much of uroboros’ positive reputation almost certainly originates from a single RAMP post in May 2023 advertising network access to two U.S.-based companies with alleged annual revenues of USD 2.6 billion and USD 1 billion. The advertisement also included a zero-day vulnerability targeting a commonly-used virtual private network (VPN) provider.

MSPs are very likely considered potentially highly lucrative targets by financially-motivated threat actors, such as R&DE collectives. Successful network intrusion would likely enable access to networks belonging to the MSP's client organizations, leading to the compromise of multiple organizations simultaneously. This threat is exacerbated by the implicit trust underlining MSP-client relationships, as it increases the likelihood that the threat actor would be able to leverage enhanced access or administrator rights.

If data is successfully exfiltrated, the threat actor would likely have the opportunity to exploit both the victim organizations and the MSP, a tactic commonly observed in attacks targeting organizations containing vast quantities of third-party data.



Uroboros RAMP post advertising MSP network access

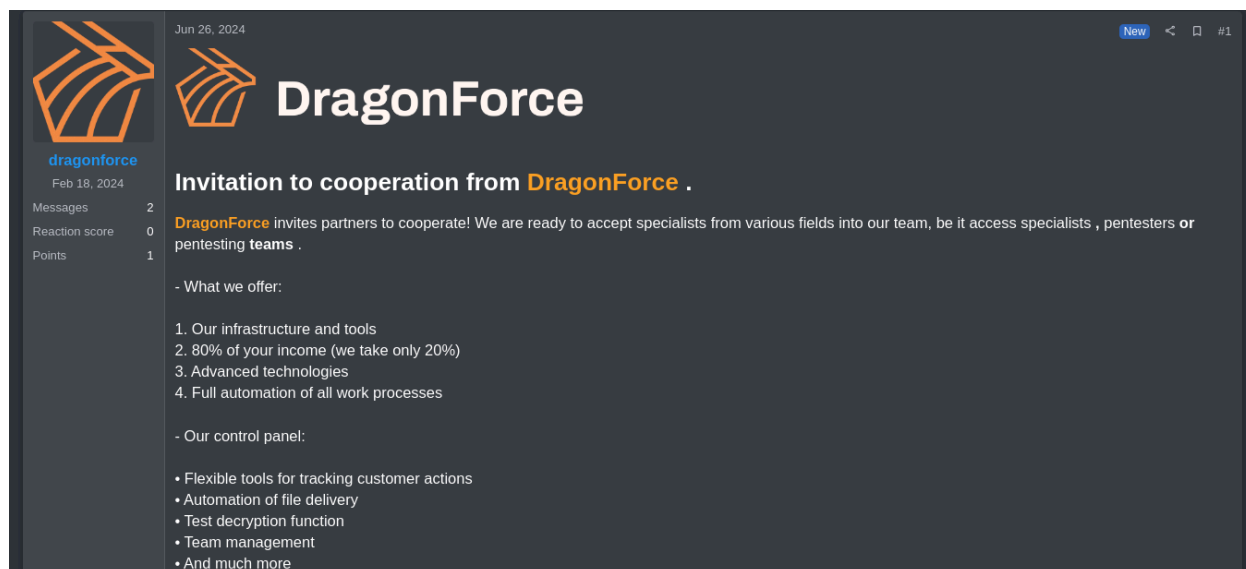
Source: ZeroFox Intelligence

| Ransomware Services Gain Traction in Dark Web Forums

In June 2024, two ransomware and digital extortion (R&DE) collectives advertised their intent to attract additional affiliates with posts in the primarily Russian-speaking dark web forum RAMP. The two outfits—which are unlikely to be related—both specified their need for various specialists, almost certainly alluding to their intent to expand capabilities and increase operational tempo.

On June 26, 2024, untested actor “DragonForce” advertised collaboration opportunities to individuals or “teams” able to carry out penetration testing, as well as other unspecified “specialists.” The post likely attracted significant attention as an update (posted on July 4, 2024) outlined several stringent requirements that potential affiliates must possess, one of which is to demonstrate a potential victim has an annual revenue above USD 5 million.

- DragonForce has conducted extortion attacks relatively consistently since approximately December 2023, averaging nine per month up to July 2024. Their most frequently targeted industries are manufacturing, construction, and retail, with the majority of victim organizations located in North America and Europe.
- DragonForce has been observed leveraging the LockBit 3.0 ransomware builder, leaked in approximately Q3 2022. The collective leverages a double extortion technique, encrypting and exfiltrating targeted data.



Jun 26, 2024

dragonforce

Feb 18, 2024

Messages 2

Reaction score 0

Points 1

DragonForce

Invitation to cooperation from **DragonForce** .

DragonForce invites partners to cooperate! We are ready to accept specialists from various fields into our team, be it access specialists , pentesters or pentesting teams .

- What we offer:

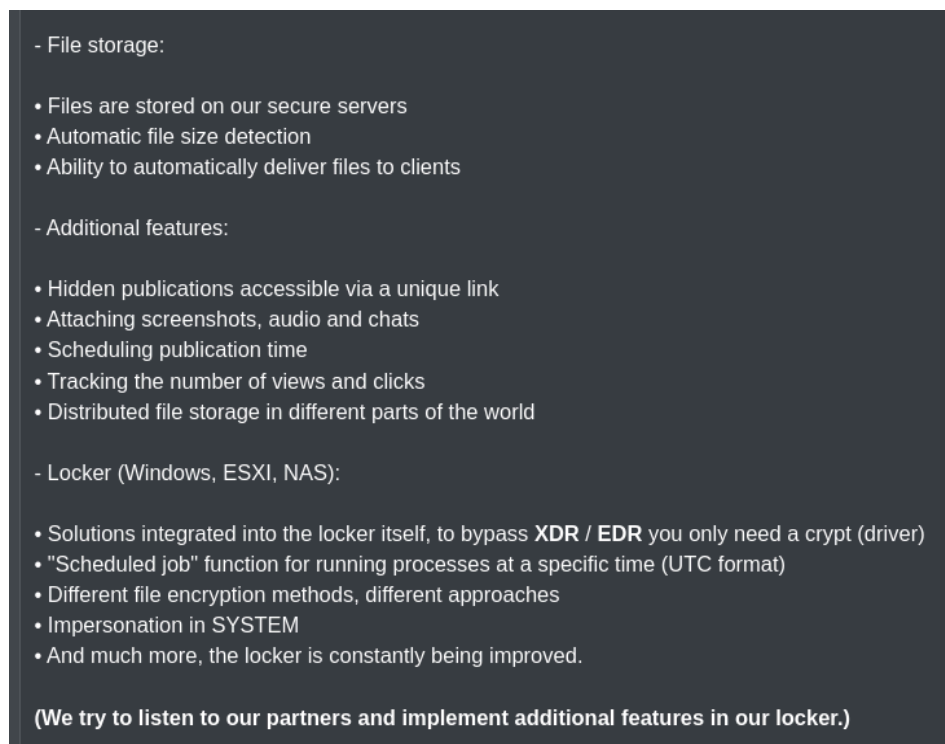
1. Our infrastructure and tools
2. 80% of your income (we take only 20%)
3. Advanced technologies
4. Full automation of all work processes

- Our control panel:

- Flexible tools for tracking customer actions
- Automation of file delivery
- Test decryption function
- Team management
- And much more

DragonForce RAMP post seeking affiliates

Source: ZeroFox Intelligence



- File storage:

- Files are stored on our secure servers
- Automatic file size detection
- Ability to automatically deliver files to clients

- Additional features:

- Hidden publications accessible via a unique link
- Attaching screenshots, audio and chats
- Scheduling publication time
- Tracking the number of views and clicks
- Distributed file storage in different parts of the world

- Locker (Windows, ESXI, NAS):

- Solutions integrated into the locker itself, to bypass XDR / EDR you only need a crypt (driver)
- "Scheduled job" function for running processes at a specific time (UTC format)
- Different file encryption methods, different approaches
- Impersonation in SYSTEM
- And much more, the locker is constantly being improved.

(We try to listen to our partners and implement additional features in our locker.)

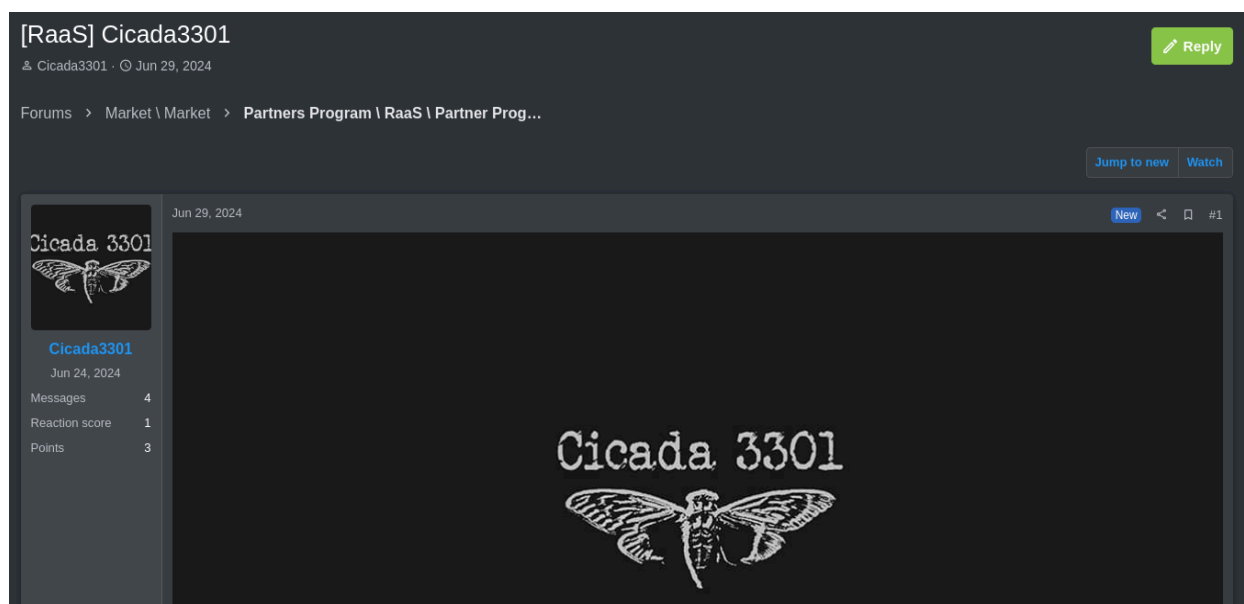
DragonForce RAMP post advertising features available to affiliates

Source: ZeroFox Intelligence

DragonForce described their service as state-of-the-art, listing many features that would be made available to prospective affiliates. Many such features appear to enhance the usability of the internal environment, such as a comprehensive administration panel and customer support options, as well as bolster security, such as globally-dispersed digital infrastructure.

Despite the announcement originally being posted in Russian, DragonForce did not include the typical warning against targeting entities within the Commonwealth of Independent States (CIS). However, there is roughly even chance that this is implied given that the advertisement was posted in the Russian-speaking community RAMP.

On June 29, 2024, positive-reputation actor “Cicada3301” advertised a new Ransomware-as-a-Service (RaaS) under the same name and announced their search for pentesters and “access advertisers” (very likely synonymous with initial access brokers) with which to affiliate.



Cicada3301 RAMP post advertising new RaaS

Source: ZeroFox Intelligence

In addition to many of the features generally expected from modern RaaS operations—such as fast and secure encryption and an ability to operate offline—Cicada3301 also claims its RaaS is compatible with all versions of Microsoft

Windows from 7 onwards, as well as Linux distributions. The advertisement specifically states that attacks against CIS targets are prohibited.

```
Welcome to Cicada3301!

We are recruiting partners to work in our affiliate program:
- Penetrators.
- Access advertisers.

General information :
- Work in the CIS countries is strictly prohibited.
- The affiliate program commission is 20% of the total payout amount.
- To participate in the affiliate program, you must pass a mini-interview.
- A wallet for payments is provided in the chat. For amounts over 1.5 million USD , two wallets are provided: yours and ours.
- It is strictly forbidden to transfer access to the panel to third parties, except in cases agreed with support.

LOCKER :
- The locker is written in Rust from scratch. - ChaCha20 + RSA
is used to encrypt files , which supports full file encryption, as well as encryption of only some of its parts. Modes:

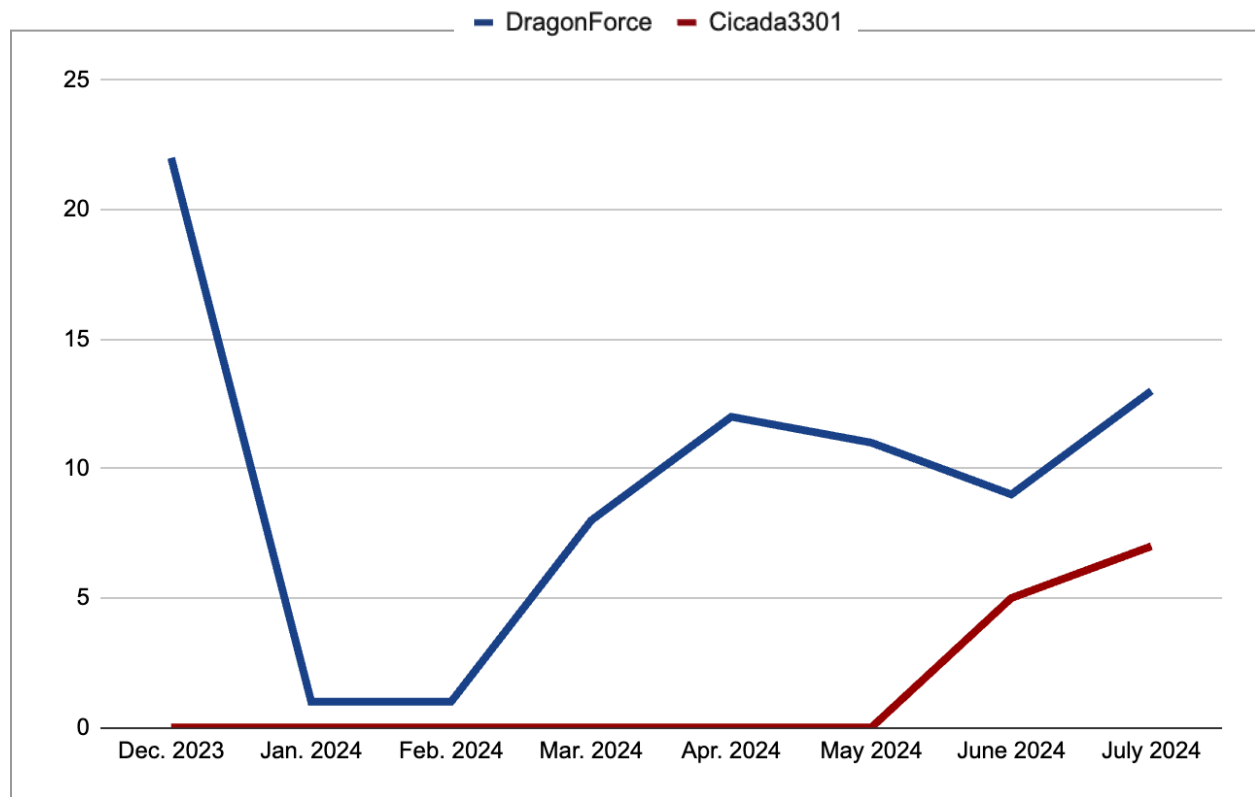
    Full : full file encryption.
    Fast : fast file encryption 15 blocks of 1 MB .
    Auto : Automatic selection of encryption parameters, optimal for files.
Encryption parameters can be configured individually when assembling the locker.
- The locker operates offline, without requiring an internet connection.
- The locker runs on all versions of Windows , starting with Windows 7 , as well as on Linux , ESXi and NAS .
- File encryption occurs in multithreaded mode.
- The locker supports network mode, which allows parallel scanning of the local network.
- It is possible to encrypt files, folders and partitions at specific points.
- The locker supports impersonation, which allows you to run the program under different credentials.
- Before starting work, the locker terminates the specified processes, stops and deletes the specified services.
- Before encryption, the locker mounts hidden drives.
- Before encryption, the recycle bin is emptied, shadow copies and operating system restore points are deleted.
- A text note with instructions is left in each folder where files were encrypted.
- The locker has a list of exceptions for system file extensions and directories that do not need to be encrypted.
- Stopping VM ESXi/Hyper-V .
- The note is stored in encrypted form, the locker can be launched only if there is a key that decrypts the note.
- Delayed start of the locker using a timer, which is optimal for "mining" the network.
```

Cicada3301 RAMP post advertising features available to affiliates

Source: ZeroFox Intelligence

DragonForce and Cicada3301 are both very likely credible and adept RaaS operations capable of posing a threat—primarily to Western organizations. Their manifestation in the wake of significant disruption affecting prominent R&DE outfits in early 2024 very likely reflects an intent to capitalize upon a perceived market gap and affiliates of various specializations that are seeking new opportunities. The innovative features advertised very likely attempt to appeal to prospective partners and affiliates—particularly those centered around ensuring secure operations. Given the likely relative abundance of

available affiliates, RaaS operators will very likely continue to employ highly selective recruitment processes.



DragonForce and Cicada3301 attacks observed by ZeroFox

Source: ZeroFox Intelligence

| Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- 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.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web forums.
- Ensure social media accounts are configured with organic security features, such as phishing-resistant multi-factor authentication and complex, unique passwords.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

| 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%