AO 108 (Rev. 06/09) Application for a Warrant to Seize Property Subject to Forfeiture

Sealed
Public and unofficial staff access to this instrument are prohibited by court order

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

United States Courts
Southern District of Texas
FILED
May 15, 2025
Nathan Ochsner, Clerk of Court

In the Matter of the Seizure of
(Briefly describe the property to be seized)
The domain names "crypt.guru" and "cryptor.live", held by the domain registry Identity Digital, Inc.

Case No. **4:25-mc-6165**

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the Southern District of Texas is subject to forfeiture to the United States of America under 18 U.S.C. § 1030 *(describe the property)*:

The domain names "crypt.guru" and "cryptor.live", held by the domain registry Identity Digital, Inc.

The application is based on these facts:

See attached affidavit setting out the factual basis for probable cause to believe that certain domain names sought for seizure are subject to forfeiture as property used to sell tools for cybercrime and facilitate unauthorized access to computers as part of various conspiracies and schemes to defraud.

☑ Continued on the attached sheet.

Applicant's signature

Ryan J. Shultz, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: May 15, 2025

Judge's signature

City and state: Houston, Texas

Richard W. Bennett, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

4:25-mc-6164

IN THE MATTER OF THE SEIZURE OF VARIOUS DOMAIN NAMES § § § CASE NO.

4:25-mc-6165

4:25-mc-6166

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, Special Agent Ryan J. Shultz, being duly sworn, hereby declare as follows:

INTRODUCTION

1. I make this affidavit in support of applications for warrants for four domain names, which are held by three different domain registries, VeriSign, Inc., Identity Digital, Inc., and Spaceship, Inc. More specifically, avcheck[.]net is held by VeriSign, Inc., crypt[.]guru and cryptor[.]live are held by Identity Digital, Inc., and cryptor[.]biz is held by Spaceship, Inc. Hereinafter, the identified domains will be collectively referred to as the "SUBJECT DOMAIN NAMES". Seizing the domain names will prevent the use of websites selling services that are used to facilitate cybercrime, as explained below.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") assigned to a cybercrimes squad in the Houston, Texas division. I have been employed by the FBI as a Special Agent since September 2008. As a part of my responsibilities as an FBI Agent, I have attended various classes and trainings. For example, in addition to having completed over 20 weeks at the FBI Academy as a Special Agent, I have taken courses related to computer security, network security, cyber investigative techniques and resources, as well as cyber certification courses.

3. As a Special Agent of the FBI, I am charged with the duty of investigating violations of the laws of the United States, collecting evidence in cases in which the United States is or may be a party in interest, and performing other duties imposed by law. More specifically, I investigate,

among other crimes, cybercrimes involving the unauthorized intrusion into a computer or network and technology-related frauds.

4. The facts in this affidavit come from my personal observations and my training and experience, as well as information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge regarding this matter.

BRIEF SUMMARY

5. "Crypting" is the process of using a type of software to make malware hard for computer antivirus programs to detect, which facilitates computer intrusions. The FBI is investigating an online software crypting syndicate which provides services to cybercriminals to assist them with keeping their malicious software ("malware") from being detected. This Affidavit seeks the forfeiture of certain SUBJECT DOMAIN NAMES because they are associated with websites used to sell cybercriminal services that facilitate the commission of violations of Title 18, United States Code, Section 1030, including unauthorized intrusions into computer systems in order to commit fraud. The United States wishes to seize the SUBJECT DOMAIN NAMES to shut down those websites.

6. This Affidavit describes several websites that provide services that cybercriminals utilize to commit their crimes, including counter-antivirus ("CAV") services. The use of a CAV in conjunction with a crypting service allows a criminal actor to obfuscate malware such that it is no longer detectable by computer antivirus programs, thereby clearing a path for the malware to be utilized for unauthorized intrusions into computer systems. The FBI made undercover purchases (including by an Online Covert Employee operating in Houston, Texas) of some of the services from those websites, analyzed the services to verify that they were designed for cybercrime, and analyzed associated email addresses and other information to determine their association. The

websites information appears in both the English and the Russian languages. As described in detail below, the FBI's investigation and analysis has traced the use of these obfuscation services to known ransomware groups that have targeted both domestic and international victims, including a victim in Houston, Texas.

7. Based on the investigation, the United States seeks to forfeit the SUBJECT DOMAIN NAMES, which the FBI has confirmed are associated with services that facilitate violations of Section 1030. Upon seizure, the website(s) associated with each SUBJECT DOMAIN NAME will be taken down, using the process described in Attachment A, so that criminals can no longer utilize the services.

STATUTORY BASIS FOR FORFEITURE

8. Title 18, United States Code, Section 1030 makes it a federal crime to intentionally access a computer without authorization with intent to defraud, to obtain information from a protected computer, or to traffic in passwords through which a computer may be accessed without authorization.

9. Sections 1030(i) & (j) provide for the forfeiture of "any personal property used or intended to be used to commit or to facilitate the commission" of a criminal offense under Section 1030, including a conspiracy to commit such an offense. As shown below, the SUBJECT DOMAIN NAMES sought to be forfeited are facilitating and are intended to facilitate the commission of criminal offenses in violation of Section 1030.

10. Section 1030(i) explicitly incorporates the procedures of Title 21, United States Code, Section 853 and thereby authorizes the issuance of a criminal seizure warrant under Section 853(f). Section 853(l) provides that U.S. district courts shall have jurisdiction to enter orders without regard to the location of any property which may be subject to forfeiture. Venue for criminal forfeitures lies in the district where a criminal prosecution may be brought. As described

further below, venue would be proper in the Southern District of Texas based upon the law enforcement undercover purchases conducted in the District, as well as a victim of the malware being located in the District.

11. Section 853(f) provides that a court shall issue a criminal seizure warrant if it determines that the property to be seized would, in the event of a conviction, be subject to forfeiture and that a restraining order would be inadequate to assure the availability of the property for forfeiture. Neither a restraining order nor an injunction is sufficient to guarantee the availability of a SUBJECT DOMAIN NAME for forfeiture. By seizing a SUBJECT DOMAIN NAME and redirecting it to another website, the Government will prevent third parties from acquiring the SUBJECT DOMAIN NAME (and accessing the associated websites) and using it to commit or facilitate additional violations of Section 1030.

BACKGROUND ON OBFUSCATION SERVICES

12. A well-known obfuscation tool is a counter-antivirus ("CAV") service. Antivirus software is a computer program that is found on most computer systems and is used to detect malware and prevent it from executing/working on the computer. Typically, antivirus will use different methods to determine if software is considered safe or harmful to a computer. A common technique is to determine the hash value of a computer program and check it against known malware hash values to determine if that computer program is malicious. A hash value is a unique numerical value generated from a cryptographic algorithm that identifies the contents of a program. A hash value is often described as the "digital fingerprint" of a program.

13. A CAV is a type of computer program that aims to defeat the objective of an antivirus program. When used for the purposes of obfuscation, a CAV will use the hash value of a malicious computer program and check it against known antivirus services to determine if that malware gets identified by the antivirus. The CAV will then provide a report to the user of the CAV

to let them know whether the submitted malware was undetectable or detectable by antivirus programs.

14. CAV services do not share submitted samples with legitimate antivirus companies. Legitimate antivirus scanning services distribute uploaded data to the security community, provided the data was detected by at least one antivirus software package. These legitimate services also notify users that, by submitting data to the service, they are consenting to such sharing. Members of the security community can then update their signature databases and blacklisted URLs to better protect customers from infection. CAV services, on the other hand, promise their customers that they will not share samples or URLs with antivirus companies, cybersecurity firms, or computer emergency response teams, thus minimizing the number of antivirus software packages that can detect their customers' malicious products.

15. CAV services are primarily advertised on cybercrime forums. Legitimate antivirus scanning services advertise throughout the internet in order to broaden their exposure and increase their potential clientele base. CAV services, in contrast, are advertised, reviewed, and discussed on forums that cater to cybercriminals, such as those offering access to malware, botnets, hacking services, and other malicious products.

16. CAV services are often advertised in conjunction with other hacking and/or obfuscation tools commonly used by cybercriminals, such as crypting services. Crypting services are used to obfuscate or encrypt malware to make it harder for antivirus programs to detect. Crypting is the process through which cybercriminals encrypt and pack malware to evade the signature-based detection used by antivirus packages. Crypting changes the malware's signature without altering the underlying functionality. The primary goal of crypting when used with malware is to help the malware avoid detection, thereby allowing it to infect a computer system

and carry out malicious activities without being blocked. When crypting is applied to malware, it is given a new hash value and therefore antivirus would not associate it with any known malware in its database.

17. Combining the crypting and CAV tools provides cybercriminals with a higher chance of their malware being executed on their victim's computer systems, thereby increasing the likelihood of victimization. Typically, a cybercriminal will use the crypting tool to change the structure of their malware and then use the CAV tool to determine if the new version of the malware is detectable by antivirus. If the malware is still detectable, the cybercriminal will use the crypting tool again and continue this cycle until it is not detectable by antivirus. Once deemed undetectable, the package can be more successfully deployed to prospective victims.

BACKGROUND ON DOMAIN NAMES AND SERVERS

18. Based on my training and experience and information learned from others, I am aware of the following:

19. Internet Protocol Address: An Internet Protocol address ("IP address") is a unique numeric address used by devices on the Internet. Every device attached to the Internet must be assigned a public IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. An IP address acts much like a home or business street address—it enables devices connected to the Internet to properly route traffic to each other. Devices connected to the Internet are assigned public IP addresses by Internet service providers ("ISPs"). There are two types of IP addresses: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6). An IPv4 address has four sets ("octets") of numbers, each ranging from 0 to 255, separated by periods (*e.g.*, 149.101.82.209). An IPv6 address has eight groups ("segments") of hexadecimal numbers, each ranging from 0 to FFFF, separated by colons (*e.g.*, 2607:f330:5fa1:1020:0000:0000:0000:00d1).

20. Domain Name: A domain name is a string of text that maps to an IP address and serves as an easy-to-remember way for humans to identify devices on the Internet (*e.g.*, "justice.gov"). Domain names are composed of one or more parts, or "labels," delimited by periods. When read right-to-left, the labels go from most general to most specific. The right-most label is the "top-level domain" ("TLD") (*e.g.*, ".com" or ".gov"). To the left of the TLD is the "second-level domain" ("SLD"), which is often thought of as the "name" of the domain. The SLD may be preceded by a "third-level domain," or "subdomain," which often provides additional information about various functions of a server or delimits areas under the same domain. For example, in "www.justice.gov," the TLD is ".gov," the SLD is "justice," and the subdomain is "www," which indicates that the domain points to a web server.

21. Domain Name System: The Domain Name System ("DNS") is the way that Internet domain names are located and translated into IP addresses. DNS functions as a phonebook for the Internet, allowing users to find websites and other resources by their names while translating them into the IP addresses that their computers need to locate them.

22. Domain Name Servers: Domain Name Servers ("DNS servers") are devices or programs that convert, or resolve, domain names into IP addresses when queried by web browsers or other DNS "clients."

23. Registrar: A registrar is a company that has been accredited by the Internet Corporation for Assigned Names and Numbers ("ICANN") or a national country code top-level domain (such as .uk or .ca) to register and sell domain names. Registrars act as intermediaries between registries and registrants. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

24. Registry: A domain name registry is an organization that manages top-level domains, including by setting usage rules and working with registrars to sell domain names to the public. For example, the registry for the ".com" and ".net" top-level domains is VeriSign, Inc., which is headquartered at 12061 Bluemont Way, Reston, Virginia.

25. Registrant: A registrant is the person or entity that holds the right to use a specific domain name sold by a registrar. Most registrars provide online interfaces that can be used by registrants to administer their domain names, including to designate or change the IP address to which their domain name resolves. For example, a registrant will typically "point" their domain name to the IP address of the server where the registrant's website is hosted.

26. WHOIS: WHOIS is a protocol used for querying databases that store registration and other information about domains, IP addresses, and related Internet resources. For example, results from a WHOIS search of a domain would likely include contact information for the registry, the registrar, and the ISP that owns the IP address to which the domain points. Contact information for the registrant of the domain might be provided but is often redacted, masked, or inaccurate.

27. ICQ, WhatsApp and Telegram: ICQ, WhatsApp and Telegram are encrypted instant messaging applications that enable internet users to locate and communicate with one another online.

28. User Agent: A user agent is a software agent responsible for retrieving and facilitating end-user interaction with online web content, including web browsers, email clients, and other standalone software programs.

29. Server: A server is a computer, connected to the Internet, that provides services to other computers. A web server, for example, sends web pages to a user's computer when a user requests those web pages. Customers can connect from their own computers to the server

computers across the Internet. This connection can occur in several ways. In some situations, it is possible for a customer to upload files using a special web site interface offered by a web hosting company. It is frequently also possible for the customer to directly access the server computer through the Secure Shell ("SSH") or Telnet protocols. These protocols allow remote users to type commands to the server. The SSH protocol can also be used to copy files to the server. Customers can also upload files through a different protocol, known as File Transfer Protocol ("FTP"). Servers often maintain logs of SSH, Telnet, and FTP connections, showing the dates and times of the connections, the method of connecting, and the Internet Protocol addresses ("IP addresses") of the remote users' computers (IP addresses are used to identify computers connected to the Internet). Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports.

30. Proxy Server: A proxy server is an intermediary server that sits between a client and a destination server. It acts as a middleman to forward requests and responses between the two. A proxy server is often used by cybercriminals to help conceal their true server IP to prevent being associated with criminal activity.

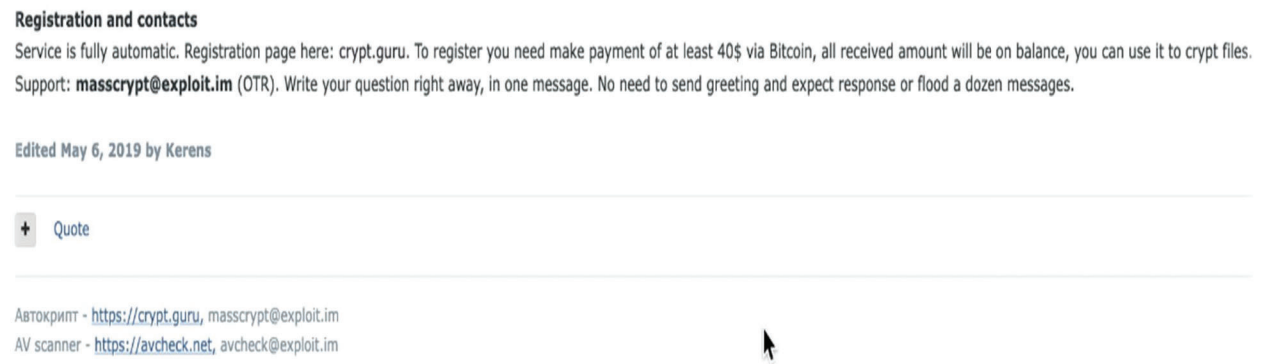
PROBABLE CAUSE

31. It should be noted that in this affidavit, brackets [] were added to website addresses to prevent hyperlinking in the electronic version of this affidavit.

32. The FBI is investigating **crypt[.]guru, cryptor[.]biz, cryptor[.]live, and avcheck[.]net**, or more specifically the actor(s) operating said sites, for potential violations of 18 U.S.C. §371 (conspiracy) as it relates to violations of 18 U.S.C. §1030 (fraud and related activity in connection with computers).

33. In November 2022, a certified FBI Online Covert Employee ("OCE") operating out of Washington, D.C. (hereinafter referred to as OCE #1), was on a website with the domain name of exploit[.]in. According to open-source research, exploit[.]in is a long-running Russian cybercriminal forum. OCE #1 navigated to the section labeled "[Software] – malware, exploits, bundles, crypts", and discovered what appeared to be an advertisement for crypting services. Crypting is the process of using a cryptor, a type of software, to encrypt, obfuscate, and manipulate malware or other files to make them harder to detect by security programs and/or other means.

34. The signature block/area on the above-mentioned exploit[.]in advertisement contained the following websites: https://**crypt[.]guru** and https://**avcheck[.]net**. Based on the websites appearing together, it is reasonable to believe **crypt[.]guru** and **avcheck[.]net** are affiliated and/or operated by the same individual(s). A partial screenshot that includes the signature block is as follows:



35. Furthermore, the aforementioned advertisement on exploit[.]in also contained the following verbiage: "Autocrypt EXE. Single crypts 15$, subscription 40$, API". Based on my training and experience, I understand this to be a point-of-sale advertisement for crypting services. For context, Autocrypt EXE is a reference to automatic protection levied for executable files, while API, Automatic Protection Implementation, automatically implements encryption within the

submitted program source code. Clicking on the advertisement then loaded another website that provided a monetary amount for the listed service. The following information was given by exploit[.]in:

> Price for one crypt
> 15$ - free and unlimited recrypts for 2 hours is available.
> 20$ - time of free recrypts 6 hours.
> 25$ - time of free recrypts 12 hours.
> Autocrypt/Subscriptions – price and features
> 40$ - 1 day, 1 file, unlimited recrypts, 1 replacement original file per day is available.
> 250$ - 7 days, 1 file, unlimited recrypts, up to 3 replacements original file daily.
> 1000$ - 30 days, 1 file, unlimited recrypts, up to 3 replacements original file daily.
>
> If you need to support several files at the same time, then price is added 10$/day for each file after the main file. All files on subscription are automatically scanned and recrypted as soon as appear detects. Each file have API URL, to download clean files to your servers.

A screenshot of the ad follows:

- Crypter is written in C, has no dependencies, it provides maximum execution rate.
- Correct work tested on all versions of Windows, including server OS.
- Any 32-bit exe files up to 10 megabytes, including .NET Framework 2.0 files are supported.
- Average time of crypt is 5-10 sec (including check on https://avcheck.net (https://avcheck.net)).

Prices for one crypt:

15$ - free recrypts for 2 hours are available.
20$ - free recrypts for 6 hours.
25$ - free recrypts for 12 hours.

Autocrypt/Subscriptions - price and features:

40$ - 1 day, 1 file, 1 replacement original file per day is available.
250$ - 7 days, 1 file, up to 3 replacements daily.
1000$ - 30 days, 1 file, up to 3 replacements daily.

If you need to support several files at the same time, then price is added 10$/day for each file after the main file.
All files on subscription are automatically scanned with most popular AV and recrypted as soon as appear detects.
Each file have API URL, to download clean file to your servers.

Important

Free recrypts does not imply any guarantees. If you bought encrypted file, but after a while you can not get FUD - in such cases, no refunds or compensation are provided. At the same time, we are working hard to support FUD 24/7 and we usually cope with this task. Same goes for files on subscriptions.

36. Based on my training and experience, the above reference to files being "scanned with most popular AV and recrypted as soon as appear detects" is a reference to running the crypted

files through a counter-antivirus service ("CAV") in order to scan files to see if they will pass certain antivirus software examination without detection, followed by re-crypting the file if it is detected as malware by the CAV scan.

37. The advertisement went on to state that at least $40 worth of Bitcoin was required to register for the service. Based on my training and experience, Bitcoin is a type of cryptocurrency which is often utilized by criminal actors because of its perceived anonymity and/or potential difficulty to trace to the point of identification of the bad actors if certain techniques are used. In the signature block of the advertisement, two domain names were listed, "https://**crypt[.]guru**" and "https://**avcheck[.]net**" with "AV Scanner" preceding it. Based on this information, it is reasonable to believe that the operator(s) of **crypt[.]guru** are also operating **avcheck[.]net.**

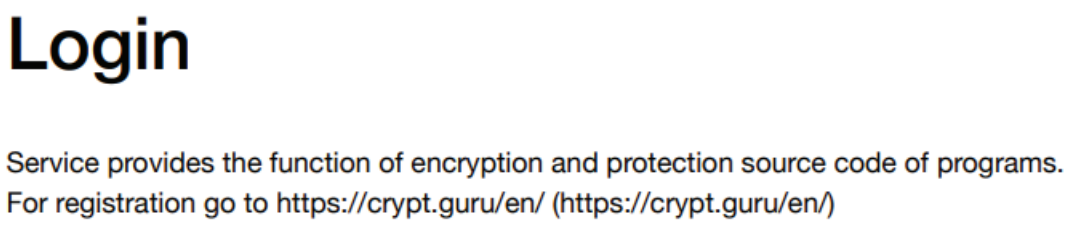
38. In 2023, an FBI employee visited the internet page **crypt[.]guru** and observed both a Russian language page and an English language page. On the English page was an advertisement with similar verbiage to that observed on the exploit[.]in forum as described above.

39. In May 2023, an FBI employee visited **avcheck[.]net** on the internet. On this website, **avcheck[.]net** described itself as an "anonymous high-speed antivirus scantime checker." The website goes on to say, "Scan files with 26 antivirus engines:" The website then appears to list 26 versions of antivirus software, including names such as: "Bitdefender Total Security", "Kaspersky Internet Security", "McAfee Endpoint Protection", "Malwarebytes Anti-Malware", "Sophos Home", "Webroot SecureAnywhere", "Windows 10 Defender", and more.

40. In November 2023, an FBI OCE (hereinafter OCE #2) operating out of Houston, Texas, created an account on **avcheck[.]net**. That same month, the OCE #2 registered an account on **crypt[.]guru** and made a registration payment. Once the registration was completed and the registration fee was paid, OCE #2 was also provided access to **cryptor[.]biz**. In February 2024,

OCE #2 submitted a well-known, open-source tool that can be used for exploit purposes to **cryptor[.]biz** for crypting in exchange for payment in Bitcoin. In a banner positioned at the top of the page, a notice stated: "All files scanned on AvCheck[.]net." OCE #2 was able to crypt the file more than once. Each time the file was crypted, OCE #2 received a notification that the file was "clean" and was provided a link to **avcheck[.]net** with a unique ID for each file.

41. It should be noted that in 2023, an FBI employee accessed **cryptor[.]biz** and according to the website, registration was to be completed at https[:]//**crypt.guru**/en/. This strongly indicates that **cryptor[.]biz** and **crypt[.]guru** were linked sites. A partial screen capture from **cyrptor[.]biz** is displayed as follows:



42. An analysis of the domain name **crypt[.]guru** revealed the public-facing IP address to be 172.67.154.151, which linked to Cloudflare, a company that provides a reverse-proxy for web traffic, among other internet services.

43. In February 2024, the FBI contacted Cloudflare and acquired the true IP addresses for **cryptor[.]biz, crypt[.]guru**, and **avcheck[.]net**. According to Cloudflare, both **cryptor[.]biz** and **crypt[.]guru** were hosted at 45.76.43.161. This further indicates the operation of these two sites are linked. According to Cloudflare, **avcheck[.]net** was hosted at 95.216.37.205, which was geo-located to Helsinki, Finland. Although **avcheck[.]net** is hosted at a different IP address from the other two websites, this does not necessarily mean they are not connected, as single entities can have multiple IP addresses all over the world.

44. A WHOIS IP lookup of IP address 45.76.43.161 indicated it was geo-located to Amsterdam, Netherlands and controlled by Vultr Holdings LLC. Vultr, a cloud service company with servers positioned globally, is headquartered at address 319 Clematis Street, Suite 1004, West Palm, Florida 33401.

45. Hosting companies, such as Vultr, maintain server computers connected to the Internet. Through a variety of possible arrangements, hosting companies sell to customers the right to use their server computers. In some arrangements, a single customer has exclusive control over an entire server. In other arrangements, multiple independent customers share the use of a single server. In these shared-hosting arrangements, individual customers can each upload their own data and programs and can edit and delete their own data, but often have limited access to other users' data.

46. In December 2024, a court-ordered search warrant was executed on the Vultr account associated with IP address 45.76.43.161. An FBI employee analyzed the results of the search warrant and determined that the server was being utilized as a proxy server for IP address 5.45.73.80, which is geo-located to The Netherlands. Within the configuration files observed on the server, their controlled domains were listed as follows:

crypt[.]guru
cryptor[.]biz
cryptor[.]live and
getcrypt[.]shop

That further confirms that all these domains are associated.

47. For clarification, investigation to date has associated each respective domain with the following IP address and geo-location, which would indicate the approximate physical location of the site's dedicated server(s):

Domain	IP Address	Geo-location of Server
avcheck[.]net	95.216.37.205	Finland
crypt[.]guru	5.45.73.80	Netherlands
cryptor[.]biz	5.45.73.80	Netherlands
cryptor[.]live	Unknown	Unknown
getcrypt[.]shop	Unknown	Unknown

It should be noted domain name "getcrypt[.]shop" is not currently sought for seizure because, unlike the other domain names, it is hosted abroad. The domain name is currently inactive.

UTILIZATION OF OBFUSCATION SERVICES BY RANSOMWARE ACTORS

48. The FBI is currently investigating a ransomware variant known as Ryuk Ransomware Group, hereinafter referred to as Ryuk. Ryuk actors utilize a form of malicious software to access victims' computers without authorization, then encrypt the victims' data and thereafter extort virtual currency from them. According to the Cybersecurity and Infrastructure Security Agency ("CISA"), Ryuk first appeared in August 2018 as a derivative of Hermes 2.1 ransomware. Ryuk actors are commonly known to use commercial off-the-shelf products to steal credentials as opposed to developing their own product.[1]

49. Through investigation in collaboration with foreign partners, the FBI determined that Ryuk actors utilize **cryptor[.]biz** as a service responsible for developing and deploying Ryuk. One such actor, who is directly associated with the development of the malware, has been linked to several accounts at multiple counter-antivirus and crypting services. At **cryptor[.]biz**, this actor paid for at least one account on the site since November 2019. The actor then used this account

[1] https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a (accessed on 10/04/2024).

until at least June 2021. This account scanned many files with a naming convention and size similar to known Ryuk samples. For example, on June 22, 2021, the account loaded a file to the site with a name of sp233_multi_for_crypt_x86. A trusted cyber incident response company in the United States identified an identical and unauthorized file found on that same date on the network of a Brazilian construction industry company. The file, specifically identified as Ransom.Win32.RYUK.FAIMDEX, is understood to be associated with the Ryuk ransomware variant.

50. In the interest of the Ryuk investigation, the FBI obtained lawful access to a collaboration server used by a set of actors in the Ryuk criminal enterprise. Upon review of this server, it was revealed that the Ryuk actors had text files and other messages shared amongst the approximately 12-15 users that described the tactics, tools and procedures used to accomplish their ransomware attacks. Within the files and messages were credentials to log into command-and-control servers used to deploy Ryuk, secondary communication accounts, and additional criminal services accounts used to help them successfully encrypt victim networks. Among these credentials were two usernames and passwords that were identified to be used at **cryptor[.]biz**. In addition, a .txt file was found that appeared to give instructions for how to prepare a ransomware sample, which included the same **cryptor[.]biz** credentials in addition to a note about which versions of the ransomware to use for different types of deployments and which versions could be crypted.

51. The use of **cryptor[.]biz** has been identified in several additional investigations within the United States, and law enforcement authorities have identified the service as being associated with at least 37 other investigations spanning 29 different FBI field offices. These investigations have focused on a variety of criminal threats including ransomware, data breaches,

access brokers, malware-as-a-service providers, botnets, remote access trojans and other emerging threat categories.

52. Furthermore, in November 2023, the FBI's Internet Complaint Center received a complaint about a ransomware attack from the representative of a company located in Houston, Texas, hereinafter referred to as "GFI" for confidentiality purposes. The complaint detailed that GFI had been the victim of a ransomware attack which resulted in GFI's computers and backup drives being hacked into and wiped clear of data and/or encrypted by unknown actors. The attackers contacted GFI via a ransomware note and advised that all the data on their servers had been encrypted, thereby making it unavailable without a unique decryption key which would only be provided in exchange for a paid ransom demand. GFI reported noticing the file extension ".ryk" on several files involved in the ransomware attack. The ".ryk" file extension is a known and clear indicator that Ryuk Ransomware was utilized to victimize GFI.

PRESENT DOMAIN STATUS

53. It is noted that at the time of this writing, the domains **crypt[.]guru**, **cryptor[.]biz**, and **cryptor[.]live** are all down and therefore inaccessible to the public. However, investigation has determined that each of the listed domains is still regarded as an owner registered domain that is not for available for purchase and has no recorded lapse in historical registry. This indicates that the domains are very likely still under the control of the actors in question and can be reactivated. The final domain of interest in this matter, **avcheck[.]net**, is still operating in an active status.

54. In my training and experience, when the public at large learns that sites selling cybercrime services have been seized or taken control of by law enforcement and/or cybersecurity experts, those sites become largely ineffective in facilitating further criminal activity and are taken offline. Furthermore, cybercrime actors, as part of operational security, often keep other registered

domains inactive in order to ensure continuity of their online operations in the event that their primary sites are blocked or otherwise taken offline. Therefore, it is still necessary to seize and/or take control of domains regardless of whether they are currently active sites. Such actions serve as a disruptor to the criminal actors in their efforts to pivot their operations to a new and trusted domain.

SEIZURE PROCEDURE

55. The top-level domain for **avcheck[.]net** is ".net." VeriSign, which is headquartered at address 12061 Bluemont Way, Reston, Virginia 20190, currently manages all ".net" domains. Domain names **crypt[.]guru** and **cryptor[.]live** are both managed by Identity Digital, Inc., which is headquartered at address 10500 NE 8th Street, Suite 750, Bellevue, Washington 98004. Domain name **cryptor[.]biz** is managed by Spaceship, Inc., which is headquartered at address 4600 East Washington Street, Suite 300, Phoenix, Arizona 85034. These headquarter locations indicate where each respective domain is registered, as opposed to where their dedicated servers are physically located, as detailed in the table above.

56. As detailed in Attachment A, upon execution of the seizure warrant, the respective registration hosting providers, VeriSign, Identity Digital, and Spaceship, shall be directed to restrain and lock the SUBJECT DOMAIN NAMES, pending transfer of all right, title, and interest in the SUBJECT DOMAIN NAMES to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAMES cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI.

57. In addition, upon seizure of the SUBJECT DOMAIN NAMES by the FBI, VeriSign, Identity Digital, and Spaceship will be directed to associate their respective SUBJECT DOMAIN NAMES to a new authoritative name server to be designated by a law enforcement

agent. The United States Government will display a notice on the websites to which the SUBJECT DOMAIN NAMES will resolve indicating that the site has been seized pursuant to a warrant, as detailed in Attachment A.

58. The only domain name of the SUBJECT DOMAIN NAMES that is still active is the domain name **avcheck[.]net.** With respect to domain name **avcheck[.]net**, therefore, the FBI intends to develop and temporarily maintain an FBI-controlled, spoofed version of the website upon its seizure by the United States Government. The spoofed page will have the appearance of being identical to the real **avcheck[.]net** but will not be functional.

59. Once the spoofed **avcheck[.]net** webpage is staged, which will be completed within hours after seizure of the real domain, users attempting to access the website may attempt to login in accordance with the real site's normal operation. However, after the user either presses the "Enter" key or clicks "Login", users will be directed to an alternate page displaying a message indicating that the desired page is no longer available. Furthermore, users will receive a short series of pop-up messages asking for their permission for things such as accessing their web-based camera or identifying the user's geographical location. These pop-up messages are purely a façade designed as a scare tactic to sow distrust between the users and the administrators of **avcheck[.]net**, as well as similar programs that operate in the same manner.

60. No personally identifying user data will be collected during any portion of the above-described process, to include the login portion, regardless of the user's actions. For example, users attempting to login with their real credentials will receive the same result as a user who inputs false or negative data. Similarly, if a user elects to grant permission to their web-based camera, no additional access will be gained or utilized by the FBI because the pop-up messages are a façade and completely non-functional.

61. After a short period of time, expected to be approximately three days, the spoofed **avcheck[.]net** webpage as described above will be taken down by the FBI and replaced with a page displaying a notice indicating the site has been seized pursuant to a warrant. When this final transition occurs, all of the SUBJECT DOMAIN NAMES will be displaying the same notice of seizure, as well as a hyperlink directing viewers to an applicable press release.

CONCLUSION

62. For the foregoing reasons, I submit that there is probable cause to believe that the SUBJECT DOMAIN NAMES are used in and/or were intended to be used in the facilitation and/or the commission of violations or conspiracies to violate Title 18, United States Code, Section 1030. Accordingly, each of the SUBJECT DOMAIN NAMES are subject to forfeiture to the United States pursuant to Title 18, United States Code, Sections 1030(i) and (j). The SUBJECT DOMAIN NAMES are also subject to seizure pursuant to Title 21, United States Code, Section 853(f).

63. I respectfully request that the Court issue seizure warrants for each of the SUBJECT DOMAIN NAMES, to be executed by the domain registries in accordance with the procedures in Attachment A to each of the seizure warrants.

64. The warrants will be served on each of the three domain registries which control the various SUBJECT DOMAIN NAMES. Because the domain registries will, at a time convenient to them, transfer control of the SUBJECT DOMAIN NAMES to the United States Government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

65. Finally, in order to protect the ongoing investigation, and considering that much of the information set forth above is not otherwise publicly available, I respectfully request that the

Court seal this affidavit and the applications for seizure warrants for 180 days or until further order of this Court.

Respectfully submitted,

Ryan J. Shultz
Special Agent
Federal Bureau of Investigation

Subscribed to and sworn to me by telephone on this 15th day of May 2025, and I find probable cause.

RICHARD W. BENNETT
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A – IDENTITY DIGITAL, INC.

With respect to "**crypt.guru**" and "**cryptor.live**" (SUBJECT DOMAIN NAMES), Identity Digital, Inc. ("Identity Digital"), which is the domain registry for the SUBJECT DOMAIN NAMES, shall take the following actions to effectuate the seizure of SUBJECT DOMAIN NAMES:

1. Take all reasonable measures to redirect the domain names to substitute servers at the direction of the Federal Bureau of Investigation (FBI), by associating the SUBJECT DOMAIN NAMES to the following authoritative name-server(s) or by redirecting traffic from the SUBJECT DOMAIN NAMES to a URL to be designated by law enforcement:
    a. Ns1.fbi.seized.gov;
    b. Ns2.fbi.seized.gov; and/or
    c. Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including email, to Identity Digital.
2. Prevent any further modification to, or transfer of, SUBJECT DOMAIN NAMES pending transfer of all right, title, and interest in SUBJECT DOMAIN NAMES to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAMES cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI.
3. Take all reasonable measures to propagate the necessary changes through the Domain Name System (DNS) as quickly as practicable.
4. Provide reasonable assistance in implementing the terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which the SUBJECT DOMAIN NAMES will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

> "This domain has been seized in accordance with a seizure warrant issued by the United States District Court for the Southern District of Texas as part of a coordinated law enforcement operation and action by:
>
> The U.S. Attorney's Offices for the Southern District of Texas and the District of New Jersey, the Federal Bureau of Investigation, the United States Secret Service, the National Public Prosecutors' Office for the Netherlands, the Finnish Police, and the Dutch National Police."