# UNITED STATES DISTRICT COURT

for the

Southern District of Florida

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

INFORMATION STORED ON A SANDISK FLASH DRIVE BEARING EXTERNAL SERIAL NUMBER BP2310006354W IN THE POSSESION OF THE FEDERAL BUREAU OF INVESTIGATION AT 2030 SW 145TH AVENUE, MIRAMAR, FLORIDA

Case No. 23-6595-HUNT

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A.

located in the SOUTHERN District of FLORIDA, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B.



The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B) / 371 | COMPUTER FRAUD / CONSPIRACY TO COMMIT COMPUTER FRAUD |
| 18 U.S.C. § 1956(h) | CONSPIRACY TO COMMIT MONEY LAUNDERING |

The application is based on these facts:

SEE ATTACHED AFFIDAVIT.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[redacted]
*Applicant's signature*

[redacted], FBI
*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by TELEPHONE *(specify reliable electronic means)*.

Date: 12/11/2023

*Judge's signature*

City and state: FORT LAUDERDALE, FLORIDA

HON. PATRICK M. HUNT, U.S. MAGISTRATE JUDGE
*Printed name and title*

**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF FLORIDA**

| | |
|---|---|
| IN THE MATTER OF THE SEARCH OF INFORMATION STORED ON A SANDISK FLASH DRIVE BEARING EXTERNAL SERIAL NUMBER BP2310006354W IN THE POSSESION OF THE FEDERAL BUREAU OF INVESTIGATION AT 2030 SW 145TH AVENUE, MIRAMAR, FLORIDA | Case No. 23-6595-HUNT |

**SEALED AFFIDAVIT IN SUPPORT OF**
**APPLICATION FOR SEARCH WARRANT**

I, [redacted], being duly sworn, depose and state the following:

## INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since January 2016. I am currently assigned to the [redacted] FBI Miami Division and am responsible for the investigation of crimes with a nexus to computers. Accordingly, I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7). By virtue of my FBI employment, I perform and have performed a variety of investigative tasks, including functioning as a case agent on computer crime cases. I have received training regarding computer technology. I have also received training and gained experience in interviewing and interrogation techniques and participated in the execution of federal search warrants involving the search and seizure of computer equipment.

2. I submit this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the search of a SanDisk flash drive bearing external serial number BP2310006354W in the possession of the FBI at 2030 SW 145th Avenue, Miramar, Florida (the "Flash Drive"), as described in Attachment A, for the seizure of the items described in Attachment B.

3. Based on my training and experience, and the facts set forth in this Affidavit, there is probable cause to believe that individuals affiliated with a ransomware strain known as Blackcat (also known as ALPHV or Noberus, but hereinafter "Blackcat") have violated 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B) (computer fraud), 18 U.S.C. § 371 (conspiracy to commit computer fraud), and 18 U.S.C. § 1956(h) (conspiracy to commit money laundering). There is also probable cause to search the Flash Drive, as described in Attachment A, to seize the public/private encryption key pairs for websites used by Blackcat-affiliated individuals to perpetuate their criminal activity, as described below and in Attachment B.

4. The facts set forth in this Affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation, knowledge obtained from other individuals, review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, this Affidavit does not set forth every fact I learned during this investigation.

## DEFINITIONS

### Ransomware

5. Ransomware is a type of malicious computer software that enables cybercriminals to encrypt victims' computers so that the cybercriminals can demand ransoms in exchange for decrypting the computers. Virtually all ransomware demands require victims to make payment in cryptocurrency, to cryptocurrency addresses controlled by the cybercriminals responsible for the attack. Cybercriminals use cryptographic algorithms to encrypt victims' computer files and the only way to decrypt the data is with the cryptographic key created by the actors.

### Ransomware as a Service ("RaaS")

6. RaaS is a ransomware model in which developers are responsible for creating and updating the ransomware and for maintaining the Internet infrastructure that enables the group's illicit activities. "Affiliates" are responsible for identifying and attacking high-value victim institutions with the ransomware. After a victim pays, developers and affiliates share the ransom.

### The Onion Router ("Tor") and The Tor Network

7. Tor is a free and open-source software for enabling anonymous communication via the Internet. To access the Tor network, a user must install the Tor software. The Tor software protects a user's privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking actual Internet Protocol ("IP") addresses. This

prevents someone attempting to monitor an Internet connection from learning what sites a user visits, prevents the websites a user visits from learning the user's physical location, and allows a user to access sites which could otherwise be blocked. Because of the way Tor routes communications through other computers, traditional techniques to identify a user's or server's IP address are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP address log. An exit node is the last computer through which a user's communications was routed.

8. Within the Tor network, entire websites can be set up as hidden services. Hidden services, like other websites, are hosted on computer servers that communicate through IP addresses and operate similarly to regular public websites. The IP address for a server hosting a hidden service is obscured and replaced with a Tor address, which is a series of algorithm-generated characters, such as "qsrdk7ls8rmqku3f," followed by the suffix ".onion" (pronounced "dot-onion"). A user can only reach these hidden services if the user is using the Tor software and operating in the Tor network. And unlike an open Internet website, it is not possible to determine through public lookups the IP address of a server hosting a Tor hidden service.

9. A Tor hidden service generates its .onion address by creating "public/private keypairs." Public/private key pairs are elements of "asymmetric cryptography." In asymmetric cryptography, one key is used to encrypt the material and the other is used to decrypt it. In the case of Tor hidden services, the public key, which is the .onion address, allows users to access the hidden service and may be

widely disseminated. The private key, which is intended to be kept secret, controls the use of the .onion.

10. Users seeking to visit the site of a hidden service are not able to connect to the hidden service directly. Instead, hidden services broadcast their public keys to "introduction points," which are nodes in the Tor network that facilitate connections between hidden services and their users. There are many possible introduction points in the Tor network. Once the public keys are broadcast, the hidden service will package its public key and information about its chosen introduction points. This package, called a "hidden service descriptor," must be signed by the hidden service's private key. In this way, any entity that has the private key associated with the .onion address can create a new hidden service descriptor with a new set of introduction points.

11. The hidden service descriptor is uploaded to a "distributed hash table." A user who wants to access the hidden service will download the hidden service descriptor associated with the site's .onion address. The user can then send an encrypted message to one of the hidden service's introduction points, which would pass the message along to the hidden service, along with information about a "rendezvous point," another node in the Tor network through which the user and the hidden service can connect.[1]

[1] If a user is using the Tor browser or similar software, this process occurs automatically and is not visible to the user. The user typically will input the .onion address into the browser, and after completing the described process in the background, the browser will display the hidden service's site.

## PROBABLE CAUSE

### The Blackcat Ransomware Group

12. Beginning in or around December 2021 and continuing through the present, cybercriminals have deployed the Blackcat ransomware against victim institutions around the world, including within the Southern District of Florida. These victims include critical infrastructure entities, medical facilities, school districts, law firms, and financial firms. For example, in early 2022, cybercriminals used the Blackcat ransomware to encrypt computers owned by [redacted] in [redacted] Florida. Blackcat uses a RaaS model featuring developers and affiliates (collectively, the "Blackcat Ransomware Group") and is among the most active ransomware organizations worldwide. The FBI previously issued a report identifying known indicators of compromise as well as tactics, techniques and procedures associated with the Blackcat Ransomware Group to assist the public in protecting against attacks.[2]

13. Blackcat attacks usually involve encryption of victim data, which makes that data inaccessible to the victim; theft of victim data; and a ransom demand. If a victim does not pay a ransom, the attackers typically publish the stolen data on a Blackcat-linked Tor site. Consequently, Blackcat victims have paid hundreds of millions of dollars in ransoms and have lost hundreds of millions more in operational and remediation expenses. Due to the global scale of these crimes, multiple foreign law enforcement agencies are conducting parallel investigations.

[2] https://www.ic3.gov/Media/News/2022/220420.pdf

**Blackcat Attacks, Victim Communication Sites, and Leak Sites**

14. Blackcat affiliates commonly gain unauthorized access to a victim's computer network days, weeks, or even months prior to the demand for ransom. During this time, the affiliate surreptitiously elevates their privileges within the network. Once the affiliate has gained sufficient access to the victim network, the affiliate attempts to steal data from the victim network and installs the ransomware to accessible computers on the network.

15. During the encryption process, the victim receives a ransom note containing a unique Tor .onion address through which to communicate with the Blackcat Ransomware Group (a "victim communication site"). The ransom note also references a primary "leak" site Tor address through which the Blackcat Ransomware Group discloses information about victims and the data they have stolen. This primary leak site consists of the main Tor address given to victims and multiple other Tor addresses that facilitate this main address's operation. The primary leak site also links to other secondary leak sites on Tor where stolen victim data are publicly available. The Blackcat Ransomware Group operates these victim communication and leak sites to extort victims into paying ransom and to shame those who chose not to. In furtherance of these efforts, the Blackcat Ransomware Group also maintains, on the primary leak site, a searchable database of victims who have not paid ransoms.

16. Victims who choose to pay ransoms have made hundreds of millions of dollars in ransom payments to cryptocurrency addresses controlled by the Blackcat Ransomware Group. Once ransomware payments are received into cryptocurrency

addresses controlled by members of the Blackcat Ransomware Group, the affiliates and developers launder the proceeds through several cryptocurrency transactions before dividing the proceeds amongst themselves.

17. Blackcat victims, including several in the Southern District of Florida, have reported experiences consistent with the general attack flow described above. Hundreds of Blackcat victims from around the world have reported receiving links to unique victim communication sites and have had their data appear on Blackcat's leak sites.

**Blackcat Panels**

18. In addition to victim communication and leak sites, the Blackcat Ransomware Group also operates password-protected Tor-based web panels (i.e., online interfaces that can control different aspects of a server) that allow its affiliates and developers to communicate, manage, and coordinate Blackcat attacks amongst themselves. Law enforcement worked to make undercover contact with individuals who provided credentials to these panels. Specifically, law enforcement engaged a Confidential Human Source ("CHS") who routinely provides reliable information related to ongoing cybercrime investigations.

19. The CHS responded to an advertisement posted to a publicly-accessible online forum soliciting applicants for Blackcat affiliate positions. A member of the Blackcat Ransomware Group responded to the CHS and asked questions designed to gauge the CHS's technical proficiency with network intrusion. The CHS responded to these questions to the Blackcat actor's satisfaction. The Blackcat actor then provided

the CHS with access credentials to a Blackcat affiliate panel, available at a unique Tor address. The CHS visited this page, confirmed that this was the log-in page for a Blackcat affiliate panel, and accessed the panel.

20. Law enforcement accessed the affiliate panel pursuant to a separate federal search warrant, navigated the panel, and determined how it operates. Affiliates use the panel to manage each ransomware attack on a victim throughout the attack lifecycle, from ransomware deployment through payment and decryption of victim data. After an affiliate logs into the panel using their credentials, they navigate the panel through the vertical menu bar on the left, which displays content on the remaining portion of the panel's webpage depending on what the user is trying to accomplish.

21. At the top of the menu bar is a "Dashboard" button which, when selected, displays information in grid format showing a summary and status of each victim entity. If the affiliate is actively engaging with a victim infected with Blackcat ransomware, they can select the entity using the Dashboard or select the "Campaigns" button in the menu bar. From the Campaigns screen, affiliates can see the victim entity, full ransom price demanded, discount ransom price, expiration date, cryptocurrency addresses, cryptocurrency transactions, type of computer system compromised, ransom demand note, chats with the victim, and more. These features allow affiliates to engage the victim throughout the entire negotiation process.

22. As an example, when a victim is infected with Blackcat ransomware, affiliates will add the new victim to their affiliate panel. Information about the breach

and ransomware will be stored and used when sending a ransom demand note and negotiating with the victim. After the victim contacts the affiliate, a demand price is negotiated, and payment is made, the affiliate panel will show that the unique cryptocurrency address associated with the victim has funds. Once the victim transfers the ransom payment, the victim receives a key with instructions to decrypt any encrypted data.

**Blackcat and the Tor Network**

23. The Blackcat Ransomware Group's victim communication sites, leak sites, and panels have been able to remain online because they are set up as hidden services on the Tor network.

24. For example, users who wanted to access the primary Blackcat leak site on the Tor network would download the descriptor for the public key represented as the Tor .onion address for that site. The users would be able to view the primary Blackcat leak site through a rendezvous point. As noted above, control of a Tor .onion domain depends on a user knowing both the public key—the .onion address—and the private key that typically is kept secret by the user who created the site. However, any individual who also possessed the private key associated with a public Tor .onion address would have the complete public/private key pair and could consequently broadcast a new route redirecting traffic for the .onion site to a different server. Put another way, the individual holding the private key to the primary Blackcat leak site could redirect users to whatever different content they wanted the users to see. In essence, control over the public/private key pairs to a Blackcat-linked Tor site grants

the Blackcat Ransomware Group control of what visitors to that Tor site see.

**Law Enforcement Obtained the Public/Private Key Pairs to 946 Blackcat-Linked Tor Sites**

25. During this investigation, law enforcement gained visibility into the Blackcat Ransomware Group's network. As a result, the FBI identified and collected 946 public/private key pairs for Tor sites that the Blackcat Ransomware Group used to host victim communication sites, leak sites, and affiliate panels like the ones described above. The FBI has saved these public/private key pairs to the Flash Drive.

26. As noted above, each Blackcat victim received a unique public Tor address through which to engage in negotiations. The FBI has conducted extensive and ongoing outreach to victims. This outreach includes a decryption operation using a tool the FBI developed, which the FBI has offered to over 400 victims around the world. The FBI has also identified public Tor addresses associated with victim communication sites and has confirmed that several of these victim communication sites were among the public/private key pairs collected.

27. The FBI also visited the primary leak site the Blackcat Ransomware Group provided to victims during attacks and several additional Tor sites that appear to support the functioning of this primary leak site. The FBI also visited several secondary leak sites, linked from the primary leak site, that hosted stolen victim data that the Blackcat Ransomware Group published for apparent extortion purposes. The FBI has confirmed that the visited sites were among the public/private key pairs collected.

28. The FBI also confirmed that the Blackcat affiliate panel address provided to the CHS in the undercover operation was among the public Tor addresses collected. The FBI also confirmed through reporting from foreign partners that another known Blackcat affiliate panel was among the public/private key pairs collected.

29. The FBI also visited a sampling of the collected public Tor addresses with associated private keys and confirmed that the visited sites were consistent in presentation with known Blackcat victim communication sites, leak sites, and panels. As such, I understand all the public/private key pairs located on the Flash Drive to be associated with corresponding Tor sites the Blackcat Ransomware Group used exclusively to perpetuate its criminal scheme. Although the FBI lawfully obtained a copy of the public/private key pairs contained on the Flash Drive, in an abundance of caution, the FBI is seeking this warrant to produce a segregated copy of the keys to other law enforcement personnel to facilitate further victim protection and disruptive action against the Blackcat Ransomware Group.

30. The Flash Drive is currently in storage at an FBI facility at 2030 SW 145th Avenue, Miramar, Florida, in the Southern District of Florida. In my training and experience, I know the Flash Drive has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Flash Drive first came into the possession of the FBI. Based on my knowledge, training, and experience, I know that electronic devices like the Flash Drive can store information for long periods of time.

31. Based on the above, and consistent with Rule 41(e)(2)(B), the warrant I

am applying for would permit the search of the Flash Drive consistent with the warrant. The search may require authorities to employ techniques, including computer-assisted scans of the entire medium, that might expose many parts of the Flash Drive to human inspection to determine whether it is evidence.

32. The execution of this warrant does not involve the physical intrusion onto a premises because the Flash Drive is already in the FBI's possession. For this reason, there are reasonable grounds for the Court to authorize execution of the warrant at any time in the day or night.

## CONCLUSION

33. There is probable cause for a warrant authorizing the search of the Flash Drive, as described in Attachment A, to seize private keys to Tor sites used by the Blackcat Ransomware Group to perpetuate its criminal scheme, as described in Attachment B.

Respectfully submitted,

[redacted]
Special Agent
Federal Bureau of Investigation

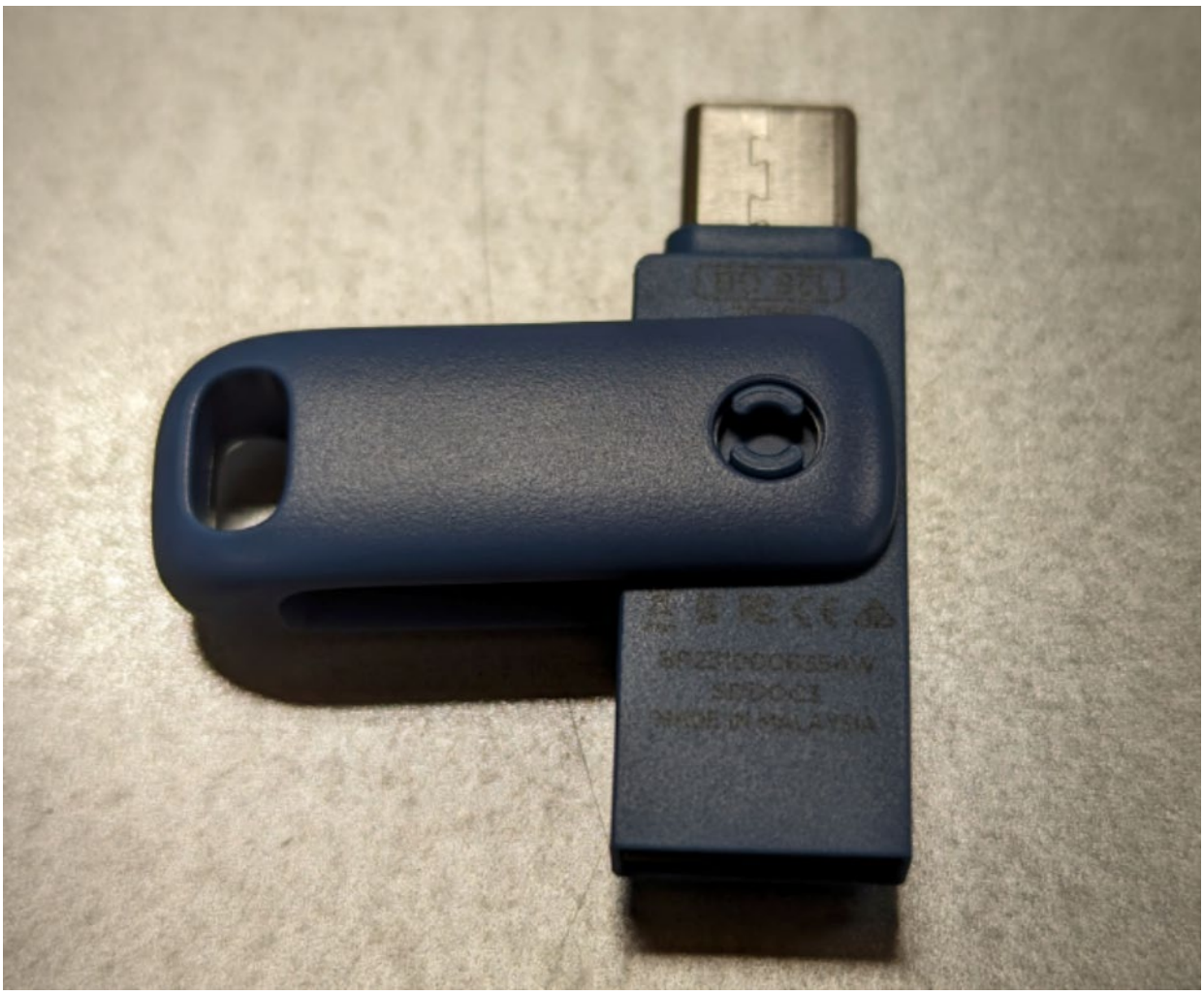
Affidavit submitted to me by reliable electronic means and attested to me as true and accurate by telephone or other reliable electronic means consistent with Fed. R. Crim. P. 4.1 and 4(d) before me this 11th day of December, 2023.

HONORABLE PATRICK M. HUNT
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Thing to be Searched**

This property to be searched is a SanDisk flash drive bearing external serial number BP2310006354W (the "Flash Drive") in the possession of the FBI at 2030 SW 145th Avenue, Miramar, Florida, in the Southern District of Florida. A picture of the Flash Drive is below:



## ATTACHMENT B

## Items to be Seized

All public/private encryption key pairs associated with Tor sites used by the Blackcat Ransomware Group for purposes of effectuating a criminal scheme in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B) (computer fraud), 18 U.S.C. § 371 (conspiracy to commit computer fraud), and 18 U.S.C. § 1956(h) (conspiracy to commit money laundering), including Tor sites hosting and facilitating Blackcat-linked victim communications sites, leak sites, and panel sites.

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

# UNITED STATES DISTRICT COURT

for the

Southern District of Florida

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*
INFORMATION STORED ON A SANDISK FLASH DRIVE BEARING EXTERNAL SERIAL NUMBER BP2310006354W IN THE POSSESION OF THE FEDERAL BUREAU OF INVESTIGATION AT 2030 SW 145TH AVENUE, MIRAMAR, FLORIDA

Case No. 23-6595-HUNT

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the SOUTHERN District of FLORIDA
*(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A.

Certified to be a true and correct copy of the document on file
Angela E. Noble, Clerk,
U.S. District Court
Southern District of Florida
By AARON TIJERINO Deputy Clerk
Date Dec 11, 2023

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B.

Type text here

**YOU ARE COMMANDED** to execute this warrant on or before 12/25/2023 *(not to exceed 14 days)*
❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to DUTY MAGISTRATE JUDGE .
*(United States Magistrate Judge)*

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: December 11, 2023 at 5:15 pm

Patrick M Hunt
*Judge's signature*

City and state: FORT LAUDERDALE, FLORIDA

HON. PATRICK M. HUNT, U.S. MAGISTRATE JUDGE
*Printed name and title*

**Return**

| Case No.: | Date and time warrant executed: | Copy of warrant and inventory left with: |
|---|---|---|
| 23-6595-HUNT | 12 December 2023 @ 1:17 PM | FBI Miami Evidence |

Inventory made in the presence of :
FBI Miami Personnel

Inventory of the property taken and name(s) of any person(s) seized:
A spreadsheet containing 946 Blackcat public/private key pairs.

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 12 December 2023

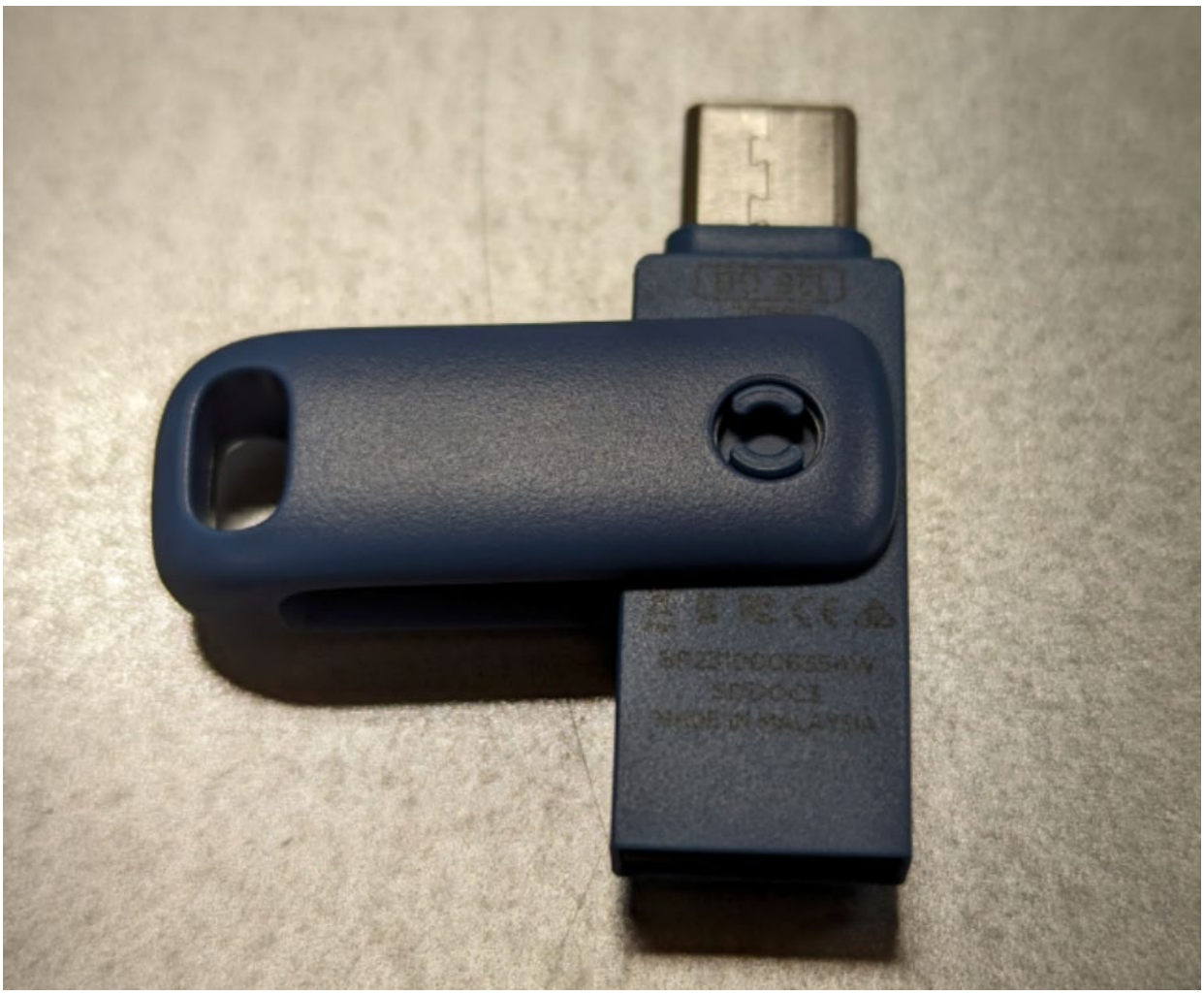
[redacted]
*Executing officer's signature*

[redacted] Special Agent
*Printed name and title*

**ATTACHMENT A**

**Thing to be Searched**

This property to be searched is a SanDisk flash drive bearing external serial number BP2310006354W (the "Flash Drive") in the possession of the FBI at 2030 SW 145th Avenue, Miramar, Florida, in the Southern District of Florida. A picture of the Flash Drive is below:



## ATTACHMENT B

## Items to be Seized

All public/private encryption key pairs associated with Tor sites used by the Blackcat Ransomware Group for purposes of effectuating a criminal scheme in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B) (computer fraud), 18 U.S.C. § 371 (conspiracy to commit computer fraud), and 18 U.S.C. § 1956(h) (conspiracy to commit money laundering), including Tor sites hosting and facilitating Blackcat-linked victim communications sites, leak sites, and panel sites.