UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	**SUPERSEDING**
	:	**CRIMINAL COMPLAINT**
v.	:	
	:	Honorable James B. Clark, III
ROSTISLAV PANEV	:	
	:	Mag. No. 24-12254
	:	
	:	**FILED UNDER SEAL**

I, Jacob A. Walker, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

/s/ Jacob A. Walker/AMT

Jacob A. Walker
Special Agent
Federal Bureau of Investigation
Special Agent Jacob A. Walker attested to this Affidavit by telephone pursuant to FRCP 4.1(b)(2)(A).

Sworn to before me telephonically
on September 25, 2024

/s/ Stacey D. Adams/AMT

Honorable Stacey D. Adams
United States Magistrate Judge

Signature of Judicial Officer

ATTACHMENT A

COUNT 1
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers – 18 U.S.C. § 371)

From at least as early as in or around 2019 through at least as recently as in or around February 2024, in the District of New Jersey and elsewhere, the defendant,

ROSTISLAV PANEV,

did knowingly and intentionally conspire and agree with others to commit offenses against the United States, that is:

a. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss to persons during a one-year period from a related course of conduct affecting protected computers aggregating at least $5,000 in value, and cause damage affecting 10 or more protected computers during a one-year period, contrary to Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI), and (c)(4)(B)(i); and

b. to knowingly and with intent to extort from any person any money and thing of value, transmit in interstate and foreign commerce any communication containing a threat to obtain information from a protected computer without authorization and to impair the confidentiality of information obtained from a protected computer without authorization, and a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, contrary to Title 18, United States Code, Section 1030(a)(7)(B), (a)(7)(C), and (c)(3)(A).

In violation of Title 18, United States Code, Section 371.

COUNT 2
(Conspiracy to Commit Wire Fraud – 18 U.S.C. § 1349)

From at least as early as in or around 2019 through at least as recently as in or around February 2024, in the District of New Jersey and elsewhere, the defendant,

ROSTISLAV PANEV,

did knowingly and intentionally conspire and agree with others to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice to defraud, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, and sounds, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Section 1349.

COUNTS 3-15
(Intentional Damage to a Protected Computer – 18 U.S.C. § 1030(a)(5)(A))

On or about the dates set forth below, in the District of New Jersey and elsewhere, the defendant,

ROSTISLAV PANEV,

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and the offense (i) caused loss to persons during a 1-year period from the defendant's course of conduct affecting protected computers aggregating at least $5,000 in value, and (ii) caused damage affecting 10 or more protected computers during a one-year period, described below for each Count, each transmission constituting a separate Count of this Superseding Criminal Complaint:

Count	Approximate Date	Victim
3	October 30, 2021	Victim-1
4	November 13, 2021	Victim-2
5	February 2, 2022	Victim-3
6	December 8, 2022	Victim-4
7	January 16, 2023	Victim-5
8	January 27, 2023	Victim-6
9	February 4, 2023	Victim-7
10	March 19, 2023	Victim-8
11	June 13, 2023	Victim-9
12	August 8, 2023	Victim-10
13	October 27, 2023	Victim-11
14	November 8, 2023	Victim-12
15	May 11, 2024	Victim-13

In violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI), and (c)(4)(B)(i), and Section 2.

COUNTS 16-28
(Extortion in Relation to Information Unlawfully Obtained from a Protected Computer – 18 U.S.C. § 1030(a)(7)(B))

On or about the dates set forth below, in the District of New Jersey and elsewhere, the defendant,

ROSTISLAV PANEV,

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly and with intent to extort from any person any money or other thing of value, transmit in interstate and foreign commerce a communication containing a threat to impair the confidentiality of information obtained from a protected computer without authorization, described below for each Count, each transmission constituting a separate Count of this Superseding Criminal Complaint:

Count	Approximate Date	Victim
16	October 30, 2021	Victim-1
17	November 13, 2021	Victim-2
18	February 2, 2022	Victim-3
19	December 8, 2022	Victim-4
20	January 16, 2023	Victim-5
21	January 27, 2023	Victim-6
22	February 4, 2023	Victim-7
23	March 19, 2023	Victim-8
24	June 13, 2023	Victim-9
25	August 8, 2023	Victim-10
26	October 27, 2023	Victim-11
27	November 8, 2023	Victim-12
28	May 11, 2024	Victim-13

In violation of Title 18, United States Code, Sections 1030(a)(7)(B) and (c)(3)(A), and Section 2.

COUNTS 29-41
(Extortion in Relation to Intentional Damage to a Protected Computer – 18 U.S.C. § 1030(a)(7)(C))

On or about the dates set forth below, in the District of New Jersey and elsewhere, the defendant,

ROSTISLAV PANEV,

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly and with intent to extort from any person any money or other thing of value, transmit in interstate and foreign commerce a communication containing a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, described below for each Count, each transmission constituting a separate Count of this Superseding Criminal Complaint:

Count	Approximate Date	Victim
29	October 30, 2021	Victim-1
30	November 13, 2021	Victim-2
31	February 2, 2022	Victim-3
32	December 8, 2022	Victim-4
33	January 16, 2023	Victim-5
34	January 27, 2023	Victim-6
35	February 4, 2023	Victim-7
36	March 19, 2023	Victim-8
37	June 13, 2023	Victim-9
38	August 8, 2023	Victim-10
39	October 27, 2023	Victim-11
40	November 8, 2023	Victim-12
41	May 11, 2024	Victim-13

In violation of Title 18, United States Code, Sections 1030(a)(7)(C) and (c)(3)(A), and Section 2.

ATTACHMENT B

I, Jacob A. Walker, am a Special Agent with the Federal Bureau of Investigation (the "FBI"). I am fully familiar with the facts set forth herein based on my own investigation, my conversations with other law enforcement officers, and my review of reports, documents, and photographs of the evidence. Where statements of others are related herein, they are related in substance and part. Because this complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

I. SUMMARY

1. U.S. authorities are investigating the LockBit ransomware group, which, since it first appeared in or around January 2020, has ranked among the most prolific and destructive ransomware groups in the world. That investigation has established that the defendant, ROSTISLAV PANEV (PANEV), has provided coding and development services to the LockBit ransomware group since at least as early as in or around January 2022 and has received at least as much as approximately $230,000 in cryptocurrency transfers from the LockBit group during that time.

II. BACKGROUND ON TECHNICAL CONCEPTS

a. Ransomware, Ransomware-as-a-Service ("RaaS"), and TOR

2. Ransomware is a type of malware used by cybercriminals to encrypt data stored on a victim's computer system, leaving that data inaccessible to, and unusable by, the victim, or to transmit data stored on a victim system to a remote computer, or both, in an effort to extort a ransom payment.

3. A ransomware "variant" is a specific type of ransomware developed and operated by cybercriminals. Each ransomware variant generally leaves behind unique artifacts on a compromised system that can allow investigators to determine which variant was deployed on that system. These artifacts might include the particular manner in which files were encrypted, the malware executable, or "payload," executed on the system, or any files saved on the system, such as a ransom note (discussed further below).

4. Cybercriminals often organize themselves into criminal conspiracies centered around the development, maintenance, and deployment of particular ransomware variants. This type of criminal conspiracy is often called "ransomware-as-a-service," or "RaaS." LockBit is one example of a prominent RaaS conspiracy. Other examples of RaaS groups, both historical

and current, include ALPHV/BlackCat, Hive, Conti, Clop, Play, REvil/Sodinokibi, and Babuk.

5. The RaaS model comprises two groups of ransomware perpetrators: developers and affiliates. The developers design the ransomware and then recruit affiliates to deploy it. Developers recruit affiliates through a variety of means, including direct outreach and advertisements posted on online cybercriminal forums. The affiliates, in turn, identify vulnerable computer systems, unlawfully access those systems, and deploy on those systems the ransomware designed by the developers. When victims make ransom payments after successful ransomware attacks, the developers and the affiliates each take a share of those payments in proportions that vary from variant to variant.

6. Many RaaS conspiracies rely on servers, sites, and other resources hosted on the "dark web." The "dark web" comprises internet content that requires specialized software or configurations to access and is intended for anonymous and untraceable online communication.

7. In particular, the Onion Router, or "TOR," network is part of the dark web because it is not publicly indexed on popular search engine websites (e.g., Google). The TOR network attempts anonymity by routing TOR-user communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a "circuit." Because of the way the TOR network routes communications through relay computers, traditional internet-protocol-address-based identification techniques are not effective. The content of a TOR user's communications is encrypted while the communication passes through the TOR network. To access the TOR network, a user must install publicly available TOR software to the user's computer.

8. The TOR network makes it possible for users to operate TOR network websites that are accessible only to users operating within the TOR network, using TOR software (e.g., the websites would not be accessible through commonly used internet browsers). Such websites are called "hidden services" or "onion services." These websites operate in a manner that attempts to conceal the internet protocol address of the computer or server hosting the website. Websites on the TOR network generally bear the suffix ".onion" (rather than ".com" or ".net," for instance) in their URLs.

9. Many RaaS conspiracies operate a TOR site on which to publish data stolen, or "exfiltrated," from victims who refuse to pay a ransom. These sites, often called "data leak sites," are publicly available to any user configured for TOR access. The stolen and victim data published on a data leak site may consist of a company's sensitive intellectual property or financial records or personally identifiable information of the company's customers. Such data

may be used both to the advantage of the criminal and detriment to an individual victim or victim company. For example, stolen personally identifiable information may be used to fraudulently obtain a credit card, line of credit, identification card, or to open a bank account in a victim's name.

10. Many RaaS conspiracies also operate on the TOR network a "control panel," which is a software dashboard made available to affiliates by the developers to both provide that affiliate with tools necessary for the deployment of ransomware attacks and to allow developers to monitor their affiliates' activities. Although the particular functionality provided by the control panel varies from variant to variant, RaaS control panels often allow affiliates, among other things, to generate custom "builds" of the ransomware for particular victims and attacks. In the RaaS context, a "build" is a package containing all the tools necessary to deploy ransomware against a given victim. Although the components of a build vary from variant to variant, a build might contain an executable file containing the ransomware payload for the targeted victim; other files containing scripts or code enabling the deployment of the ransomware payload; or a text file identifying the victim. Builds are frequently generated in a compressed zip file. RaaS control panels also often allow affiliates to communicate with victims for ransom negotiation following successful attacks and to publish data stolen from victims onto that variant's data leak site.

11. Ransomware victims generally become aware that their computer systems have been attacked by ransomware in one or more ways. *First*, a victim might discover that files stored on the system have been encrypted and are inaccessible. *Second*, a victim might discover that the system itself will not operate. *Third*, a victim might discover a ransom note sent by the perpetrators—in a text file saved on the system, for example, or in an email sent directly to the victim from the perpetrators. These ransom notes will generally threaten to either leave encrypted data locked and inaccessible and/or to publish exfiltrated data unless the victim pays an acceptable ransom. The ransom note will generally provide the victim with instructions for making contact with the perpetrators to begin ransom negotiations, often on a TOR chat portal operated by the perpetrators.

12. RaaS conspiracies often publish other messages on TOR sites under their control—sometimes the same sites as data leak sites; at other times, different sites. Such messages might include advertisements for affiliates or general announcements to the public.

13. Additionally, cybercriminals operate a number of forums on the TOR network that allow cybercriminals to discuss and coordinate cybercrime, including the promotion of new cybercriminal ventures, recruitment of associates for cybercriminal ventures, and exchange of malware and technical advice related to cybercrime.

b. Bitcoin, Bitcoin Tracing and Analysis, and Mixing Services

14. Bitcoin is a type of cryptocurrency. Cryptocurrency is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency (such as U.S. dollars) to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Payments or transfers of value made with Bitcoin are recorded in the Bitcoin blockchain and are not maintained by any single administrator or entity. Bitcoin amounts are denoted with the symbol "BTC," much like amounts in U.S. dollars are denoted with "USD."

15. The Bitcoin blockchain is a decentralized, searchable, public ledger that logs every Bitcoin address that has ever received Bitcoin and maintains records of every transaction for each Bitcoin address.

16. Bitcoin is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public address is represented as a case-sensitive string of letters and numbers, 26–35 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address. Users can operate multiple Bitcoin addresses at any given time, with the possibility of using a unique Bitcoin address for each and every transaction.

17. Law enforcement, including U.S. authorities, use commercial services offered by several different blockchain analysis companies to investigate Bitcoin transactions. These companies analyze the blockchain in an attempt to identify the individuals or groups involved in Bitcoin transactions. Specifically, these companies create large databases that group Bitcoin transactions into "clusters" through analysis of data underlying Bitcoin transactions. Thus, these services allow law enforcement to identify Bitcoin addresses that are included in the same transaction, and "cluster" these addresses together to represent the same owner.

18. This third-party blockchain analysis software is widely used by a variety of financial institutions to monitor transactions and implement anti-money laundering protections. The software is also used by law enforcement

organizations worldwide, including by U.S. authorities. This software has been used both in the LockBit investigation and in many unrelated investigations and has led to numerous search and seizure warrants. As such, U.S. authorities have found the information to be reliable. Additionally, U.S. authority computer scientists have independently shown that they can generally use clustering methods to identify Bitcoin addresses and their respective account owners.

19. A cryptocurrency mixing service is a service that intermingles cryptocurrency funds transferred from a sender with other funds before then transferring those funds to the intended recipient, in order to obscure the transfer directly from the sender to the recipient. Mixing services are intended and used to launder criminal proceeds and evade detection by law enforcement of the flows of funds within criminal organizations. They charge a small fee for their service by subtracting a small amount of Bitcoin from incoming transfers before completing the transfer to the recipient.

20. U.S. authorities know that mixing services often conceal the flow of transfers by leaving outgoing funds at a seemingly random and disassociated address on the blockchain and completing the transfer of the same amount of funds from a different seemingly random and disassociated address, making it extremely difficult to follow the flow of funds from sender to recipient on the blockchain alone.

III. THE LOCKBIT RANSOMWARE GROUP

a. Overview

21. LockBit is a RaaS variant and group that first appeared in or around January 2020 and has remained active through the present. As part of their investigation into LockBit, U.S. authorities have tracked LockBit attacks both in the United States and around the world based on multiple sources of information, including victim reports and media reporting.

22. Based on this tracking and other sources of investigation and analysis, U.S. authorities have determined that LockBit has been deployed against at least 2,500 victims around the world, including at least approximately 1,800 victims in the United States. At least approximately 55 of those victims were in the District of New Jersey. Beyond the United States, LockBit's victims have been located in nearly 120 countries around the world, including the United Kingdom, Israel, France, Australia, Germany, Argentina, Kenya, Switzerland, Finland, the Netherlands, Japan, Canada, Spain, Italy, and China. LockBit's victims have ranged from major multinational corporations to small businesses and individuals, and they have included hospitals, schools, nonprofit organizations, critical infrastructure facilities, and government and law-enforcement agencies. Total ransom payments made by

victims have amounted to at least $500 million.[1] Broader losses, including lost revenue and expenses associated with incident response and recovery, have totaled billions of U.S. dollars. LockBit has at times since it first appeared in or around January 2020 ranked as one of the most active and destructive ransomware variants in the world.

b. Structure of the LockBit Group; LockBitSupp; Currently Charged Individuals

23. As with other RaaS groups, U.S. authorities have learned through investigation that the LockBit group comprises developers, like PANEV, and affiliates. The LockBit developers design the LockBit ransomware, maintain the infrastructure on which LockBit operates, and recruit affiliates to join the group and deploy LockBit attacks. The affiliates, in turn, identify vulnerable computer systems, unlawfully access those systems, and deploy on those systems the ransomware designed by the developers.

24. Indeed, LockBit has itself advertised itself as a RaaS developer-affiliate program since it first appeared. For example, LockBit published the following announcement on its dark web-hosted blog site (further discussed below) in or around June 2021:

> **[Ransomware] LockBit 2.0 is an affiliate program.**
>
> Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.
>
> The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.
>
> Unparalleled benefits are encryption speed and self-spread function.
>
> The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.
>
> Brief feature set:
> • administrator panel in Tor system;
> • communication with the company via Tor, chat room with PUSH notifications;

[1] All currency amounts are in U.S. dollars unless indicated otherwise.

> • automatic test decryption;
> • automatic decryptor detection;
> • port scanner in local subnetworks, can detect all DFS, SMB, WebDav shares;
> • automatic distribution in the domain network at run-time without the necessity of scripts;
> • termination of interfering services and processes;
> • blocking of process launching that can destroy the encryption process;
> • setting of file rights and removal of blocking attributes;
> • removal of shadow copies;
> • creation of hidden partitions, drag and drop files and folders;
> • clearing of logs and self-clearing;
> • windowed or hidden operating mode;
> • launch of computers switched off via Wake-on-Lan;
> • print-out of requirements on network printers;
> • available for all versions of Windows OS;
>
> LockBit 2.0 is the fastest encryption so are all over the world. In order to make it clear, we made a comparative table with several similar programs indicating the encryption speed at same conditions, making no secret of their names.

25. Since LockBit's appearance in or around January 2020, one or more individuals using the account names, or "monikers," of "LockBit" and "LockBitSupp" have been used by the LockBit group to publicly promote and speak for LockBit, such as on cybercriminal forums hosted on the dark web, in interviews with and statements to media outlets, and on various messaging platforms. For example, at one point during the LockBit conspiracy, the moniker "LockBitSupp" posted to a cybercriminal forum offering to pay $1,000 to any individual who received a tattoo of the LockBit logo.

26. On May 2, 2024, a grand jury in the District of New Jersey indicted a Russian national, Dmitry Yuryevich Khoroshev, on 26 criminal counts based on Khoroshev's alleged role as the creator and primary developer and administrator of the LockBit group, and as the primary controller of the "LockBit" and "LockBitSupp" monikers. Khoroshev remains a fugitive. U.S. authorities believe that PANEV, a LockBit developer, was subordinate to Khoroshev in the LockBit group.

27. Although the precise number of LockBit affiliates remains unknown, U.S. authorities assess that there are likely at least dozens of either past or current LockBit affiliates—far more than the number of LockBit

developers, including Khoroshev and PANEV. To date, U.S. authorities have charged five individuals as part of their LockBit investigation with being LockBit affiliates, two of whom have admitted their roles as LockBit affiliates in U.S. federal court and are currently awaiting sentencing:

- Mikhail Vasiliev, a dual Russian and Canadian national who has pleaded guilty to his role as an affiliate in the LockBit conspiracy and is currently awaiting sentencing in U.S. federal court in the District of New Jersey.
- Ruslan Astamirov, a Russian national who has pleaded guilty to his role as an affiliate in the LockBit conspiracy and is currently awaiting sentencing in U.S. federal court in the District of New Jersey.
- Mikhail Matveev, a Russian national who is indicted in the District of New Jersey as an affiliate of the LockBit and Hive ransomware groups and a developer of the Babuk ransomware group, presently at large.
- Ivan Kondratyev, a Russian national who is indicted in the District of New Jersey as an affiliate of the LockBit ransomware group, presently at large.
- Artur Sungatov, a Russian national who is indicted in the District of New Jersey as an affiliate of the LockBit ransomware group, presently at large.

c. LockBit Infrastructure

28. U.S. authorities have learned through investigation that Khoroshev and the other LockBit developers, beyond writing and maintaining the LockBit malware code, also maintain multiple infrastructure facilities on the TOR network that enable the LockBit affiliates to deploy attacks.

i. The Control Panel:

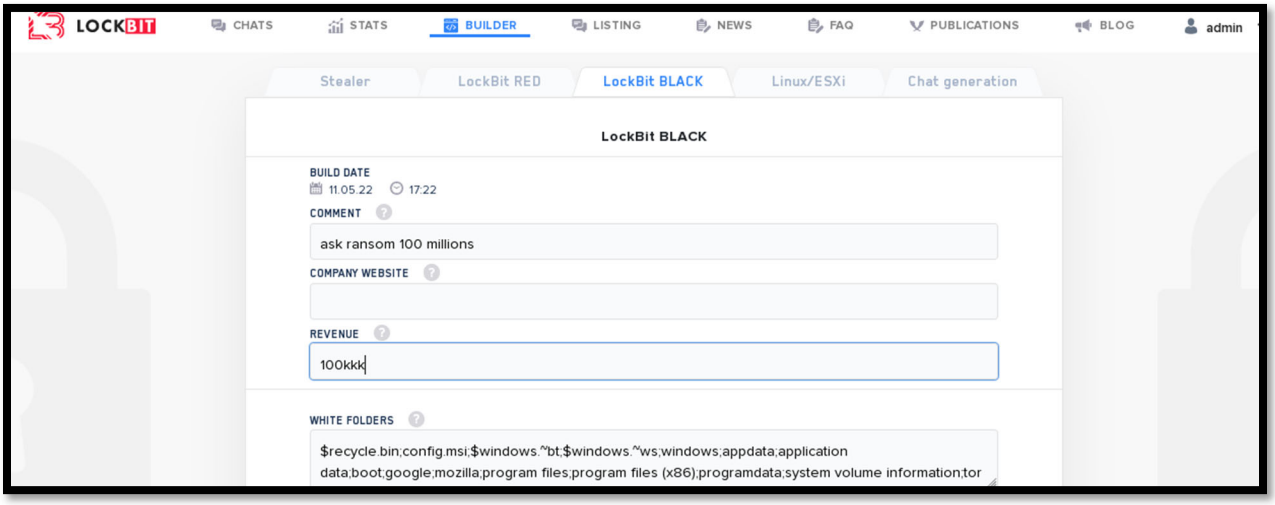
29. As with other RaaS groups, this investigation has shown that the LockBit developers maintain a control panel hosted on the TOR network for their affiliates. For example, at one point during the investigation, U.S. authorities succeeded in gaining access to the LockBit control panel, generating a LockBit build, and deploying that LockBit build within a computer system under the control of U.S. authorities (the "Control Panel Operation").

30. Based on the Control Panel Operation and other investigation, U.S. authorities know that the LockBit control panel allows affiliates, among other things, to develop custom builds of LockBit ransomware for particular victims, a functionality known as the "builder." The LockBit Control Panel also allows affiliates to communicate with LockBit victims for ransom negotiation and to publish data stolen from LockBit victims to the LockBit Data Leak Site.

31. U.S. authorities also know—based on the Control Panel Operation and other investigation—that the LockBit control panel is hosted on the dark web, at a unique .onion TOR domain given to each affiliate by the LockBit developers upon joining LockBit. An affiliate's unique TOR domain for control-panel access requires unique credentials, also provided to the affiliate by the LockBit developers, to access. Thus, the LockBit control panel is not publicly available, and there is no legitimate reason for anyone to have access credentials to the control panel.

1. The LockBit Builder; LockBit Versions

32. The below screenshot depicts the LockBit control panel obtained by U.S. authorities:



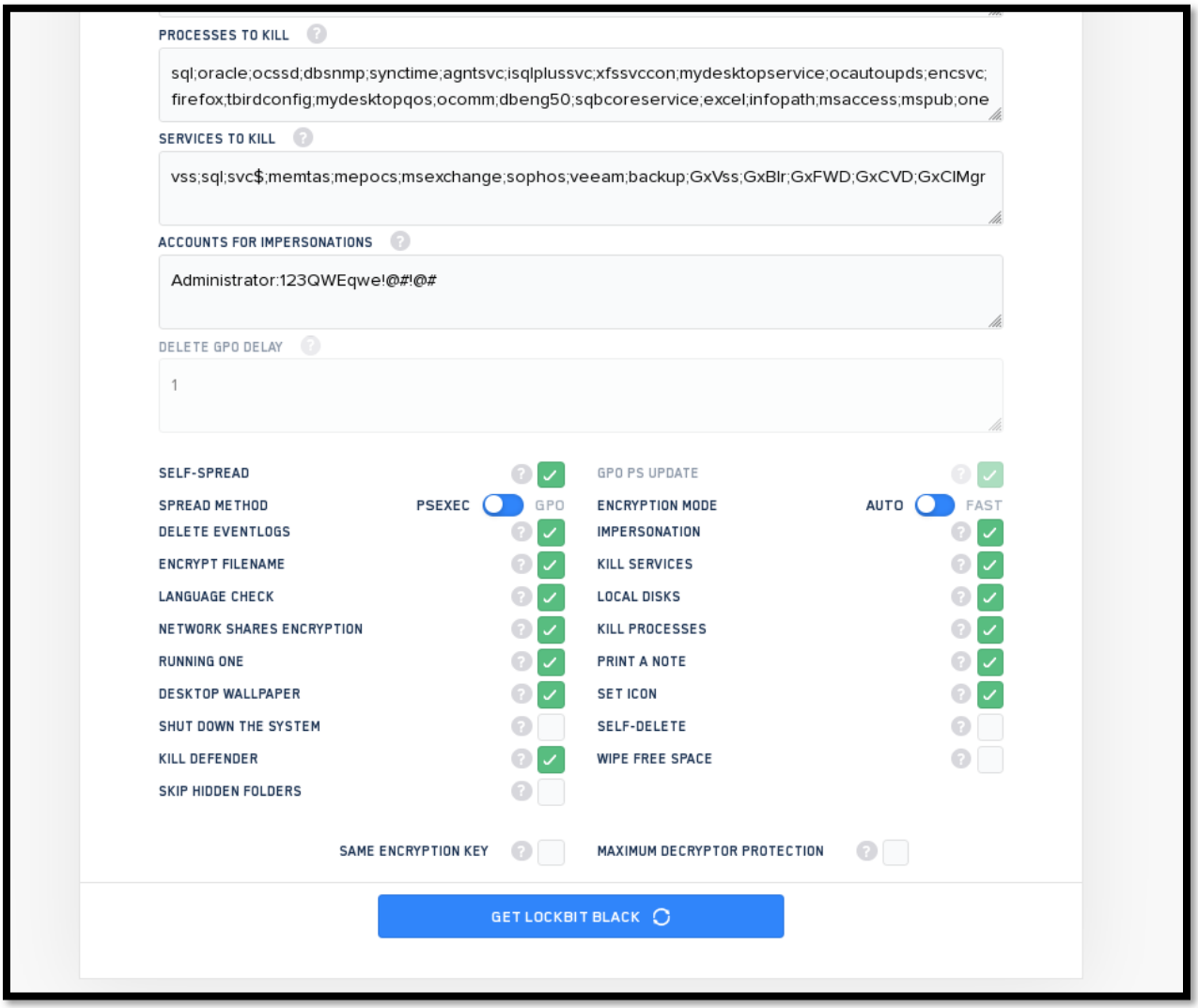
The tabs at the top of the screenshot—"Stealer," "LockBit RED," "LockBit BLACK," "Linux/ESXi," and "Chat generation"—refer to the various versions of the LockBit builder maintained by the LockBit developers. Based on this investigation, including reporting from victims and the cybersecurity community and analysis by computer scientists, U.S. authorities know that the LockBit group has, since it first appeared, provided multiple versions of the builder to its affiliates through the control panel. The LockBit versions have varied and evolved in technical capacity, such as speed of encryption and features offered. The various LockBit versions also allow affiliates to attack victim systems running different operating systems, including Windows and Linux. Moreover, LockBit affiliates can and do generate and deploy builds of multiple versions on the same victim system.

33. The LockBit versions known to U.S. authorities include:

- LockBit, the original version, which first appeared in or around January 2020.

- LockBit 2.0, also known as "LockBit Red", which first appeared in or around June 2021.
- LockBit Linux-ESXi, which first appeared in or around October 2021 and allowed affiliates to target victim systems running Linux and VMware ESXi. ESXi is a technology that allows users to partition physical devices into multiple virtual machines. It is widely used within the computer systems of large enterprises.
- LockBit 3.0, also known as "LockBit Black," first appeared in or around March 2022.
- "LockBit Green" first appeared in or around January 2023.
- U.S. authorities have learned that the LockBit developers are also working on two other builder versions, Proxmox and Nutanix. Both Proxmox and Nutanix are legitimate companies that offer virtualization services and technology; these builders appear designed to target victim computer systems running that technology.

34. The below screenshot is another depiction of the LockBit control panel obtained by U.S. authorities:



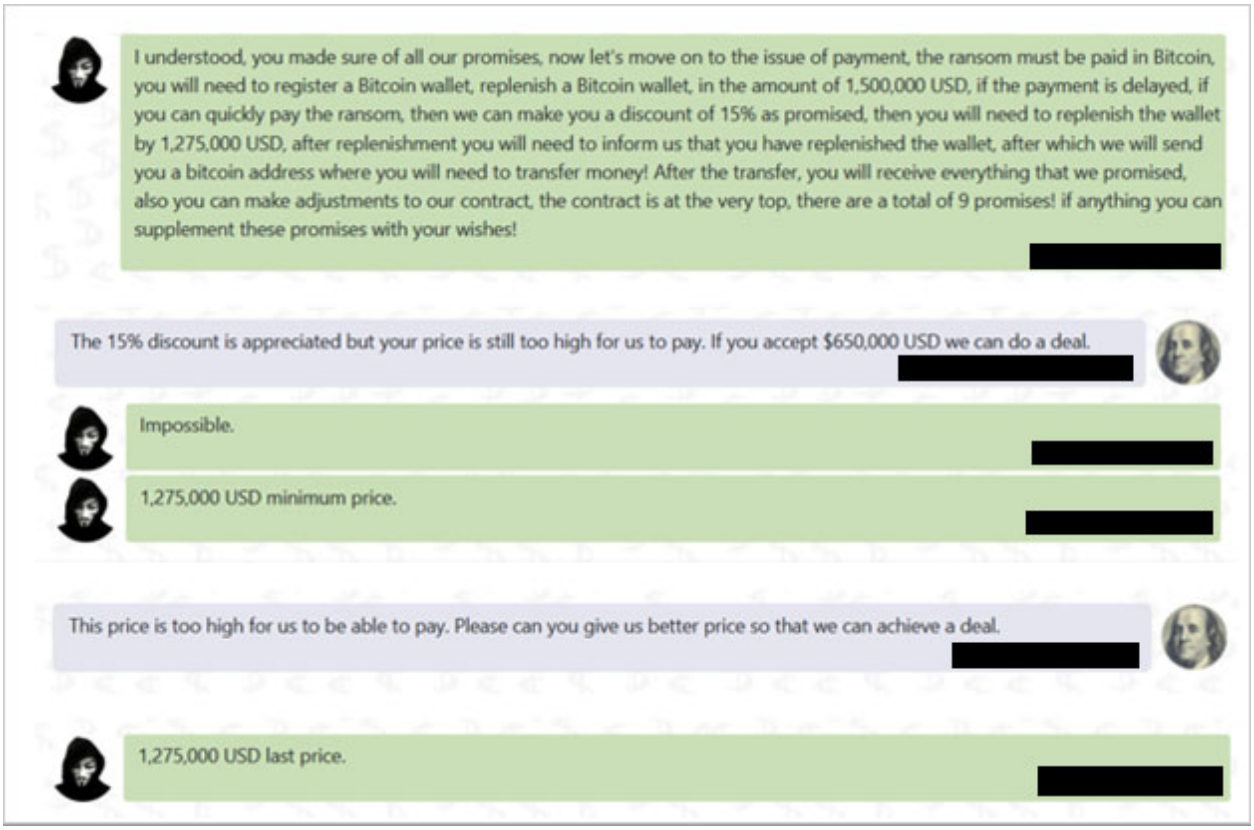
This screenshot illustrates the many technical features made available by LockBit developers to their affiliates, allowing affiliates to customize LockBit attacks for a particular victim based on the characteristics of that victim's system. For example, the "Desktop Wallpaper" feature allows the build, upon execution, to display a ransom message on a victim computer's desktop (further discussed below). And the "Print a Note" feature causes a ransom note to be printed across all printers connected to a victim computer network—a feature that, as explained below, PANEV admitted to developing.

2. The Victim Chat Portal

35. Based on investigation, including victim interviews and reporting and inspection of the LockBit control panel, U.S. authorities know that the

LockBit control panel contains a chat feature enabling affiliates to conduct ransom negotiations with their victims. As further explained below, the ransom notes delivered to LockBit victims contain unique instructions for each victim to access the chat portal and begin ransom negotiations.

36. The below screenshot obtained from U.S. authorities depicts a ransom negotiation conducted within the LockBit control panel:[2]



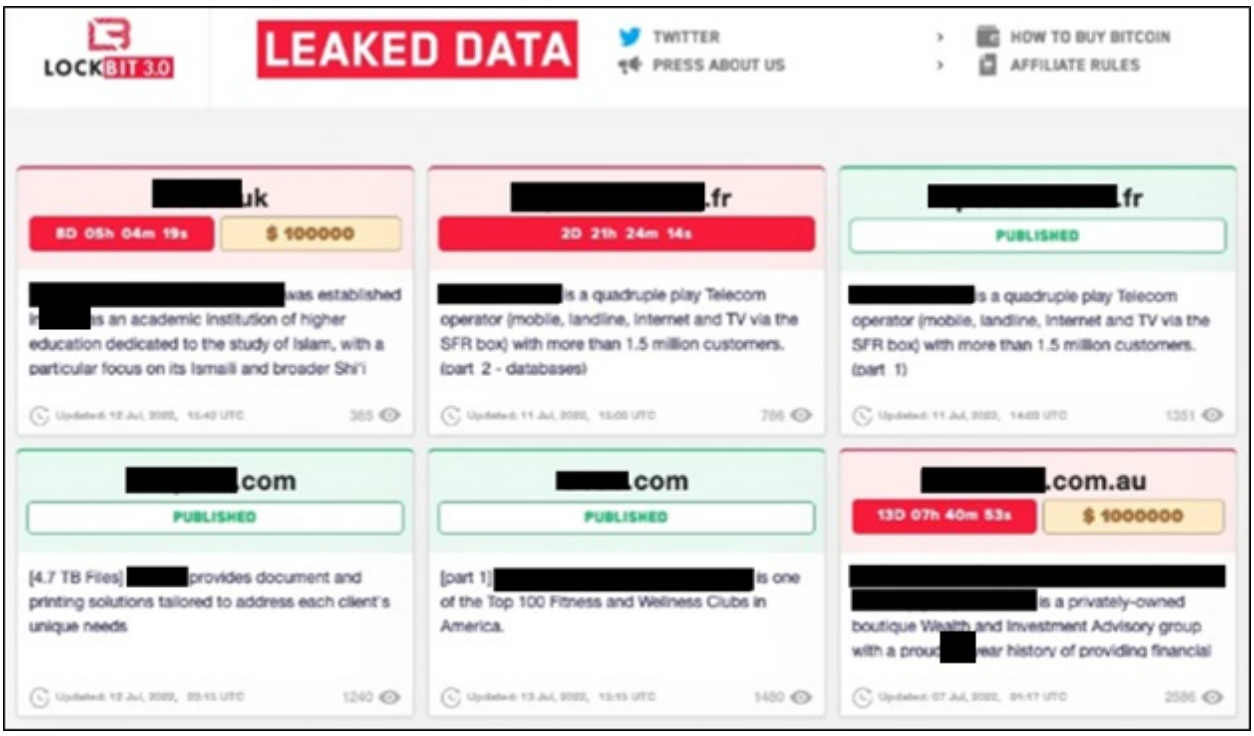
ii. The Data Leak Site:

37. U.S. authorities have learned through investigation that LockBit, like other RaaS groups, maintains a data leak site on the dark web maintained by the LockBit developers. Unlike the LockBit control panel, which requires credentials to access and is made available only to LockBit affiliates, the LockBit data leak site is publicly available and requires only a TOR connection to visit. U.S. authorities have visited and monitored the LockBit data leak site regularly throughout this investigation. Based on that observation and victim interviews, U.S. authorities know that the LockBit data leak site is used to further extort LockBit victims. In some cases, the LockBit group posts only the name and description of victims who have been attacked, along with a timer for that victim to pay an acceptable ransom to avoid publication of that victim's

[2] The dates in this chat have been redacted to protect the victim's privacy.

stolen data. In other cases, generally where ransom negotiations have failed, the LockBit group will then add the stolen data to that post.

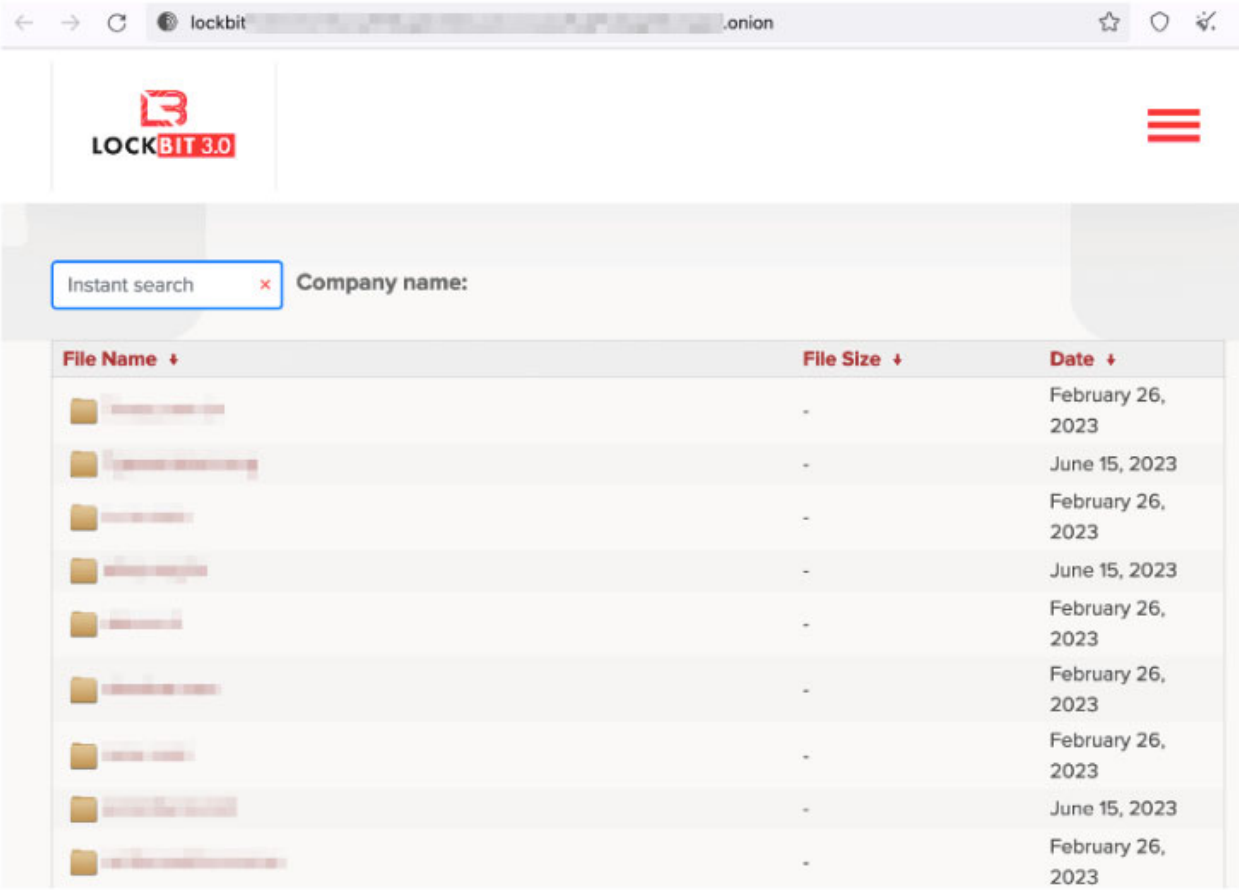
38. The screenshot below, obtained by U.S. authorities, depicts the LockBit data leak site:[3]



39. As this screenshot illustrates, the victim posts in red—accompanied by a timer—signify victims who have been attacked, but have not yet had their stolen data published. The LockBit group uses this tactic to further pressure and extort those victims. The victim posts in green, however—accompanied by the word "Published"—signify victims who have refused to pay a ransom and whose stolen data has been published. These posts generally remain on the LockBit data leak site indefinitely.

40. More recently, U.S. authorities have learned that the LockBit developers have added a search feature to the LockBit data leak site, allowing visitors to that website to search a victim name to find out if that victim has been attacked by LockBit or had its data stolen, as depicted in the screenshot below obtained by U.S. authorities:

[3] The victim names have been redacted to protect victim privacy.



iii. StealBit:

41. The LockBit developers also developed and maintained a tool called "StealBit," labeled "Stealer" on the control panel, intended to complement LockBit by aiding affiliates in storing data exfiltrated from LockBit victims and transmitting that stolen data for posting on the LockBit Data Leak Site. U.S. authorities have determined that the LockBit group has operated StealBit on multiple servers located throughout the world, including servers within the District of New Jersey and in Europe. As discussed below, source code for the StealBit feature was found within a software repository accessed with credentials obtained from PANEV's computer.

d. The February 2024 Disruption

42. In or around February 2024, the LockBit group and infrastructure was severely disrupted by a coordinated operation conducted by law-enforcement agencies in the United Kingdom, the United States, and around the world. At that time, U.K. authorities seized control of the LockBit infrastructure, rendering it practically inoperable and allowing law enforcement to review the data stored on it—including records related to particular LockBit

affiliates, such as those affiliates' victim and attack lists and ransom payment records, including sending and receiving Bitcoin addresses. Moreover, the seized infrastructure contained copies of data stolen from LockBit victims who had paid the demanded ransom, even though the LockBit perpetrators had falsely promised those victims that they would delete the victims' stolen data after the ransom was paid. The data obtained from the seized infrastructure has been reviewed by U.S. authorities, informing and verifying much of the information contained in this Affidavit.

43. After the February 2024 disruption operation, the LockBit group revived its operation and launched new infrastructure. LockBit attacks have resumed since the disruption, although significantly diminished in victim count and reputation compared to the pre-disruption LockBit operation. Among other things, following the February 2024 disruption operation, the LockBit group posted on the LockBit data leak site either fictitious or historical attacks to create the illusion that more victims were being attacked by LockBit than actually were.

e. Course of a Typical LockBit Attack

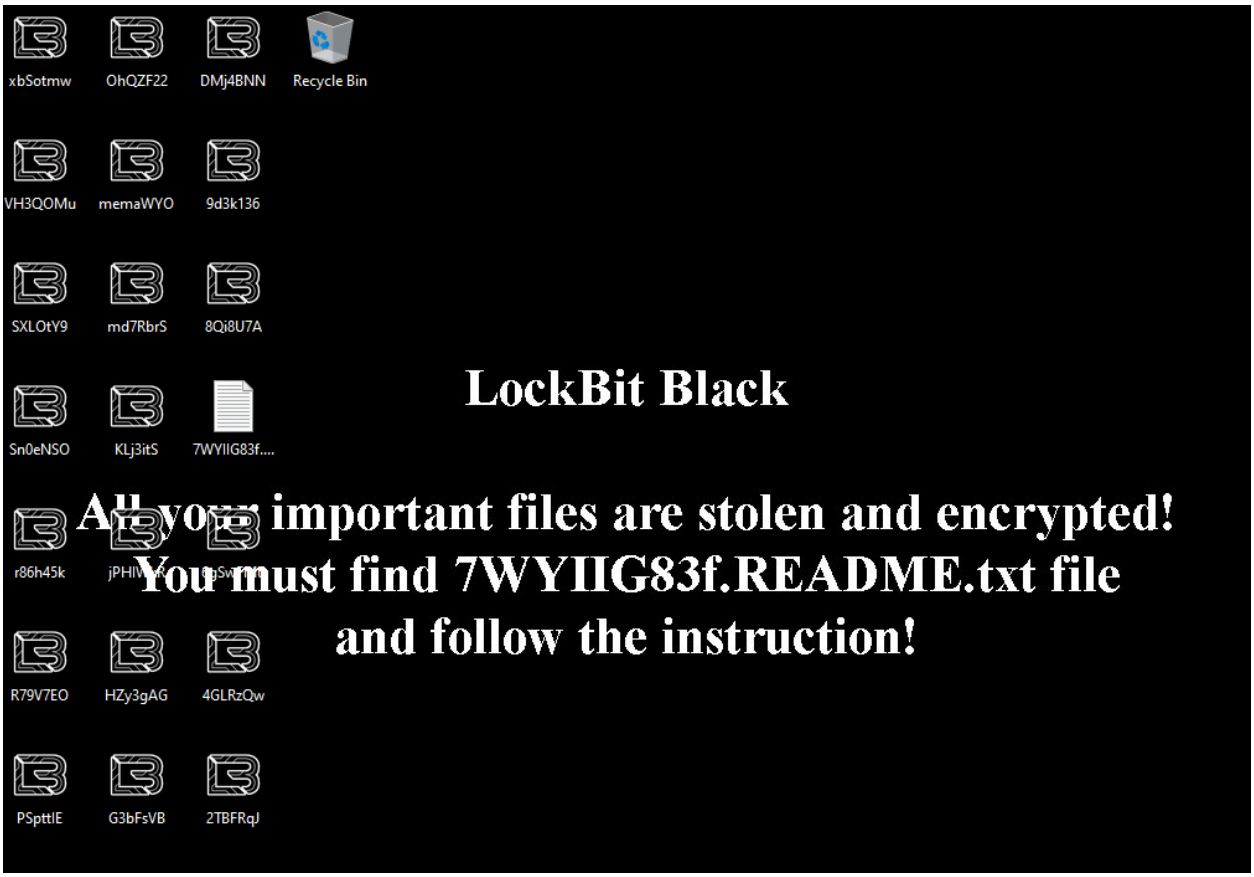
44. Based on victim and witness interviews and other investigation, U.S. authorities have learned how a typical LockBit attack begins and progresses. *First,* an affiliate gains initial access to a victim computer to prepare that system for LockBit deployment. An affiliate might gain initial access through a number of means, including exploitation of newly discovered vulnerabilities in system software, network penetration techniques, the use of stolen access credentials purchased from third-party criminals, and phishing and spoofing attacks. "Phishing" and "spoofing" attacks comprise emails meant to appear legitimate, but actually either contain or link to malicious code, sent to authorized users of a targeted computer system. Once those users are deceived into clicking on a link contained in the email, the malicious code executes, allowing unauthorized access to the attackers.

45. *Second*, once an affiliate establishes "persistent access"—that is, the ability to maintain access to a victim computer system on a consistent basis, while evading detection by the system's owner—the affiliate uses that access to perform reconnaissance on a victim system. That reconnaissance, which can last for weeks or even months before an actual LockBit payload is deployed, allows the affiliate to plan and prepare for an effective LockBit attack—for example, by allowing the affiliate to determine which technical settings within the LockBit builder to activate or omit, as explained above. But because computer systems are monitored by trained information-technology professionals, in order to maintain persistent access, affiliates must use fraudulent means to evade detection from system administrators and avoid being expelled from the system. For example, an affiliate might use the network credentials of an authorized user with high-level permissions, or an

affiliate might deploy a program—called a "beacon"—to illegally monitor system activity that bears a seemingly innocuous process name. LockBit affiliate Mikhail Vasiliev, for example—who, as explained above, has pleaded guilty in U.S. court to his role as a LockBit affiliate—in the reconnaissance phase of multiple LockBit attacks deployed a beacon with the process name "svchost," the name of a standard Microsoft Windows process that would be familiar to any system administrator.

46. U.S. authorities know, based on training, experience, expertise, and the results of this investigation, that achieving both initial access and persistent access, as explained above, intrinsically and necessarily involves the use of fraudulent techniques—that is, techniques intended to deceive the legitimate user or administrator of a victim system. Both initial intrusion into a victim system and the establishment of persistent and undetected unauthorized access on a victim system require the use of any number of fraudulent techniques—for example, the use of stolen access credentials (which deceive a victim computer system into allowing access to someone other than the intended user), or of phishing and spoofing attacks. As a specific example, Victim-2, discussed further below, was initially breached by that LockBit attacker through a spoofed email. As any LockBit member—developer or affiliate—knows, the deployment of LockBit itself, and extortion of a ransom payment after a successful deployment, would not be possible without the use of these fraudulent techniques (in other words, hacking). Indeed, both Mikhail Vasiliev and Ruslan Astamirov—the two LockBit affiliates who have pleaded guilty in open court in the U.S. to their roles as LockBit affiliates—pleaded guilty to the crime of wire-fraud conspiracy and specifically acknowledged, during their plea hearings and under oath, that the use of fraudulent hacking techniques was an intrinsic part of the LockBit operation.

47. *Third,* an affiliate will then, based on this reconnaissance, generate one or more custom LockBit builds within the LockBit control panel tailored to a particular victim system, deploy those builds on the victim system, and execute them. The LockBit payload will then encrypt the data on the victim computer system and allow the affiliate to exfiltrate data. Depending on the technical features of a given build, the payload can also leave encrypted files with the bogus file extension ".lockbit" and leave a message on the victim computer's desktop, as depicted in the below screenshot obtained by U.S. authorities from a LockBit victim:



Notably, the one file depicted in this screenshot that does not bear the LockBit logo—signifying encryption by the LockBit payload—is the ransom note, which appears with an icon signifying a plaintext file.

48. *Fourth,* after a successful deployment of LockBit, the affiliate will seek to begin ransom negotiations with the victim. LockBit affiliates generally do so by transmitting a ransom note to their victims. Upon execution, the LockBit payload will generally create and save on the victim computer a plaintext file, often with an innocuous filename such as "Restore-My-Files.txt," containing a ransom note. Although the particular ransom notes vary somewhat between LockBit versions, all LockBit ransom notes generally include a threat to leave encrypted data unusable and to publish exfiltrated data unless the victim pays an acceptable ransom and instructions for making contact with the LockBit perpetrators. In some LockBit attacks, the LockBit payload will also cause the ransom note to be printed on all printers connected to a victim computer network (a feature that, as explained below, PANEV admitted to Israeli authorities to having developed).

49. More specifically, each LockBit ransom note contains unique identifiers for each victim. For example, each victim is given a unique TOR domain to access to begin ransom negotiations with the attacking affiliate—

which, as explained above, the affiliate conducts through the chat feature of the LockBit control panel. This infrastructure, too, is maintained by the LockBit developers.

50. For example, U.S. authorities have obtained the following copy of the LockBit 3.0 (LockBit Black) ransom note from a LockBit victim:[4]

> ~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~
>
> >>>>> Your data is stolen and encrypted.
>
> BLOG Tor Browser Links: [...]
>
> >>>>> What guarantee is there that we won't cheat you? We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group and we want nothing more than money. If you pay, we will fulfill all the terms we agree on during the negotiation process. Treat this situation simply as a paid training session for your system administrators, because it was the misconfiguration of your corporate network that allowed us to attack you. Our pentesting services should be paid for the same way you pay your system administrators salaries. You can get more information about us on Ilon Musk's Twitter https://twitter.com/hashtag/lockbit?f=live
> >>>>> You need to contact us on TOR darknet sites with your personal ID
>
> Download and install Tor Browser https://www.torproject.org/
> Write to the chat room and wait for an answer, we'll guarantee a response from us. If you need a unique ID for correspondence with us that no one will know about, ask it in the chat, we will generate a secret chat for you and give you his ID via private one-time memos service, no one can find out this ID but you. Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack hundreds of companies around the world.
>
> Tor Browser personal link for CHAT available only to you (available during a ddos attack): [...]

[4] The identifiers in this ransom note have been redacted with "[...]" to protect this victim's privacy and security.

```
Tor Browser Links for CHAT (sometimes unavailable due to
ddos attacks): [...]

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>
>> Your personal Black ID: [...] <<
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>

>>>>> Warning! Do not delete or modify encrypted files, it
will lead to problems with decryption of files!

>>>>> Don't go to the police or the FBI for help and don't
tell anyone that we attacked you.
```

51. *Fifth*, ransom negotiations will commence if victims choose to access the LockBit victim portal. (As explained above, LockBit will sometimes post a victim's name, with a timer, on the LockBit data leak site to pressure victims who do not contact LockBit to do so.) If the parties agree on a ransom acceptable to the LockBit group, LockBit will provide the victims with one or more Bitcoin addresses to send the payment in Bitcoin. U.S. authorities have learned through public LockBit announcements and witness interviews, and confirmed through investigation, that LockBit enforces an 80-percent/20-percent split between affiliates and developers. In other words, the affiliate of a successful LockBit attack retains 80 percent of the ransom payment, and the developers receive 20 percent.[5] In some cases, LockBit provides a victim with two separate Bitcoin addresses and asks the victim itself to send the 80-percent share to one address, and the 20-percent share to the second address. In other cases, LockBit will instruct a victim to pay the entire ransom to one Bitcoin address, from which LockBit members themselves disburse the funds according to the group's internal rules.

52. Once payment is made, LockBit provides the victim with a decryption key, which is meant to allow the victim to decrypt the data encrypted by the LockBit payload, making the victim system usable again. LockBit also promises the victim to delete its copy of exfiltrated data and not post it on the LockBit data leak site. As explained above, however, U.S. authorities have learned through investigation that LockBit frequently retains copies of stolen data despite this promise.

---

[5] In this way, U.S. authorities have determined that Khoroshev, as the creator and primary administrator of LockBit, has received at least approximately $500 million over the course of the LockBit conspiracy, all in payments of the 20 percent developer share.

53. *Sixth*, if victims refuse to pay an acceptable ransom, LockBit will withhold the decryption key and publish that victim's stolen data to the LockBit data leak site, generally resulting in the green "Published" posts on the LockBit data leak site discussed and depicted above.

f. Relevant LockBit Victims

54. U.S. authorities encourage victims to report LockBit and other ransomware attacks to law enforcement, and many victims do so. Victims report LockBit and other ransomware incidents through the Internet Crime Complaint Center, or "IC3," a service operated by the FBI. The IC3 system allows users to provide law enforcement with details regarding a ransomware incident, including ransomware variant deployed and relevant indicators of compromise, or "IOCs."[6] LockBit victims generally know upon being attacked that LockBit is the deployed ransomware variant based on, as discussed above, the ransom note transmitted (which explicitly mentions LockBit) and the victim chat portal (which also specifically mentions LockBit). U.S. authorities also learn about LockBit attacks through the LockBit data leak site, media reporting, and their own investigation. Through these and other means, U.S. authorities have during this investigation learned of and tracked a significant percentage of LockBit attacks.

55. Based on this information, U.S. authorities have learned of the following LockBit victims relevant to this particular investigation. Each of the victims below received a specific LockBit ransom note (either digitally or in printed hard-copy, as described above) stating that the victim's data had been stolen and encrypted and demanding a ransom payment.[7]

1) On or about October 30, 2021, Victim-1, a business in Utah, was attacked by LockBit. After ransom negotiations on the LockBit victim portal, on or about November 2, 2021, the victim paid approximately 18.8768 BTC (or approximately $1.19 million at the time) to a Bitcoin address provided by the LockBit perpetrator. As explained further below, approximately 20 percent of this payment—presumably the developer portion—was transferred on the same date to a Bitcoin cluster controlled by the LockBit developers.

---

[6] Indicators of compromise, or "IOCs," are artifacts and signatures observed on a computer demonstrating an intrusion. Typical IOCs include IP addresses of malicious computers, domain names of attack servers, or unique identifying information of malware files.

[7] Victim names are anonymized to protect their privacy.

2) On or about November 13, 2021, Victim-2, a law-enforcement agency in New Jersey, was attacked with LockBit 2.0. After ransom negotiations on the LockBit victim portal, on or about December 2, 2021, Victim-2 paid a ransom of approximately 1.4928 BTC (or approximately $85,430 at the time) to a Bitcoin wallet as directed by the LockBit perpetrator. As explained further below, approximately 20 percent of this payment—presumably the developer portion—was transferred on the same date to LockBit developers. Victim-2 reported to law enforcement that the method of initial intrusion was via a spoofed email domain.

3) On or about February 2, 2022, Victim-3, a business in Texas, was attacked by LockBit 2.0, which left its computer system substantially inoperable. The victim discovered a ransom note on its system that included the heading "LockBit 2.0 Ransomware" and a link to the LockBit victim portal for the Victim-3 to access and begin ransom negotiations. After those negotiations, on or about February 5, 2022, Victim-3 paid a ransom of approximately 2.8759 BTC (at the time, approximately $120,000) to a Bitcoin address provided by the LockBit perpetrators.

4) On or about December 8, 2022, Victim-4, a business in New Jersey, was attacked with LockBit 3.0, as reported to law enforcement by that victim. After ransom negotiations on the LockBit victim portal, on or about February 9, 2023, Victim-4 paid a ransom of approximately 0.06635025 BTC (at the time, approximately $1,495) to a Bitcoin address provided by the LockBit perpetrators.

5) On or about January 16, 2023, Victim-5, a corporation in Kentucky, was attacked with LockBit 2.0, LockBit 3.0, and LockBit Linux/ESXi. After ransom negotiations on the LockBit victim portal, on or about January 19, 2023, Victim-5 paid a ransom of approximately 239.3676 BTC (at the time, approximately $4,958,574) to a Bitcoin address provided by the LockBit perpetrators.

6) On or about January 27, 2023, Victim-6, a nonprofit organization in New Jersey, was attacked with LockBit 3.0, as reported to law enforcement by that victim. StealBit was also used in the attack to exfiltrate Victim-6's data. Moreover, Victim-6 reported to law enforcement that the LockBit ransom note was printed on printers connected to Victim-6's network.

7) On or about February 4, 2023, Victim-7, a business in New Jersey, was attacked with LockBit 3.0, LockBit Green, and LockBit Linux/ESXi, as reported to law enforcement by that victim. StealBit was also used in the attack to exfiltrate Victim-7's data. After ransom

negotiations on the LockBit victim portal, on or about March 10, 2023, Victim-7 made separate payments, each of approximately 147.978 BTC (at the time, approximately $2,977,571) to two Bitcoin addresses provided by the LockBit perpetrators.

8) On or about March 19, 2023, Victim-8, a business in New Jersey, was attacked with LockBit 2.0, LockBit 3.0, and LockBit Linux/ESXi, as reported to law enforcement by that victim. After ransom negotiations on the LockBit victim portal, on or about March 24, 2023, Victim-8 made separate payments to two Bitcoin addresses provided by the LockBit perpetrators: first (and presumably the developer portion), of approximately 11 BTC (at the time, approximately $308,717.53), and second (and presumably the affiliate portion), of approximately 42 BTC (at the time, approximately $1,178,739.66).

9) On or about June 13, 2023, Victim-9, a school district in New Jersey, was attacked with LockBit 2.0 and LockBit Linux/ESXi, as reported by that victim to law enforcement. StealBit was also used in the attack to exfiltrate Victim-9's data.

10) On or about August 8, 2023, Victim-10, a retirement community in New Jersey, was attacked with LockBit ESXi, as reported by that victim to law enforcement. After ransom negotiations on the LockBit victim portal, on or about August 24, 2023, Victim-10 paid a ransom of approximately 18.9922 BTC (at the time, approximately $495,151.00) to a Bitcoin address provided by the LockBit perpetrators.

11) On or about October 27, 2023, Victim-11, a multinational aeronautical and defense corporation headquartered in Virginia, was attacked with LockBit 3.0 and LockBit Linux/ESXi, which left its computer system substantially inoperable. Victim-11 suffered data exfiltration facilitated by StealBit.

12) On or about November 8, 2023, Victim-12, a major financial institution based in China with operations in New York and New Jersey, was attacked with LockBit 3.0 and LockBit Linux/ESXi. Victim-12 reported to law enforcement that the LockBit ransom note was printed on printers connected to Victim-12's network. Victim-12 also reported to law enforcement that the perpetrators attacked and disabled a Victim-12 disaster recovery facility in New Jersey, impairing Victim-12's ability to resume operations. After ransom negotiations in the LockBit victim portal, on or about November 10, 2023, Victim-12 paid a ransom of approximately 12.024696 (at the time, approximately, $449,075) to a Bitcoin address provided by the LockBit perpetrators.

13) On or about May 11, 2024, Victim-13, a school district in New Jersey, was attacked with LockBit ESXi, as reported by that victim to law enforcement.

IV. ROSTISLAV PANEV AND EVIDENCE OF ROLE AS LOCKBIT DEVELOPER

a. Overview

56. As part of their broader LockBit investigation, U.S. authorities have investigated PANEV and obtained significant evidence establishing PANEV's role as a LockBit developer since at least as early as in or around January 2022 through at least as recently as in or around February 2024. The evidence obtained by U.S. authorities includes the following—

1) Access credentials to the LockBit control panel found on PANEV's computer.

2) Access credentials found on PANEV's computer to a repository hosted on the dark web containing LockBit and StealBit programming source code.

3) PANEV's own admissions to Israeli authorities to having performed coding, development, and consulting work for the LockBit group in exchange for significant payments of Bitcoin.

4) Private messages from in or around January and February 2022 between PANEV and the LockBit administrator on a prominent cybercriminal forum regarding the LockBit builder and control panel—consistent with PANEV's admissions to having performed development and coding work for LockBit.

5) Cryptocurrency tracing conducted by U.S. authorities showing regular payments of approximately $10,000 per month, paid by the LockBit administrator in Bitcoin and laundered through illicit cryptocurrency mixing services, beginning at least as early as in or around June 2022 and continuing through at least as recently as in or around February 2024—consistent with PANEV's admission to Israeli authorities.

6) Other historical evidence, known as "artifacts," found on PANEV's iCloud account reflecting PANEV's familiarity with encryption techniques, ransomware, and LockBit.

This evidence is discussed further below.

b. The August 2024 Operation

57. On or about August 9, 2024, U.S. authorities obtained a criminal complaint against PANEV charging him with one count of conspiracy to commit computer intrusion and extortion and one count of conspiracy to commit wire fraud based on PANEV's role as a LockBit developer (the "August 2024 Complaint"). U.S. authorities based their complaint on the evidence obtained in the investigation at that point, which is discussed in subsections IV(d)-(f) below. U.S. authorities subsequently transmitted a mutual legal assistance request (and ultimately a provisional arrest request) to Israeli authorities based on the same evidence and complaint, in which U.S. authorities requested that Israeli authorities search PANEV's residence and devices for evidence and interview PANEV.

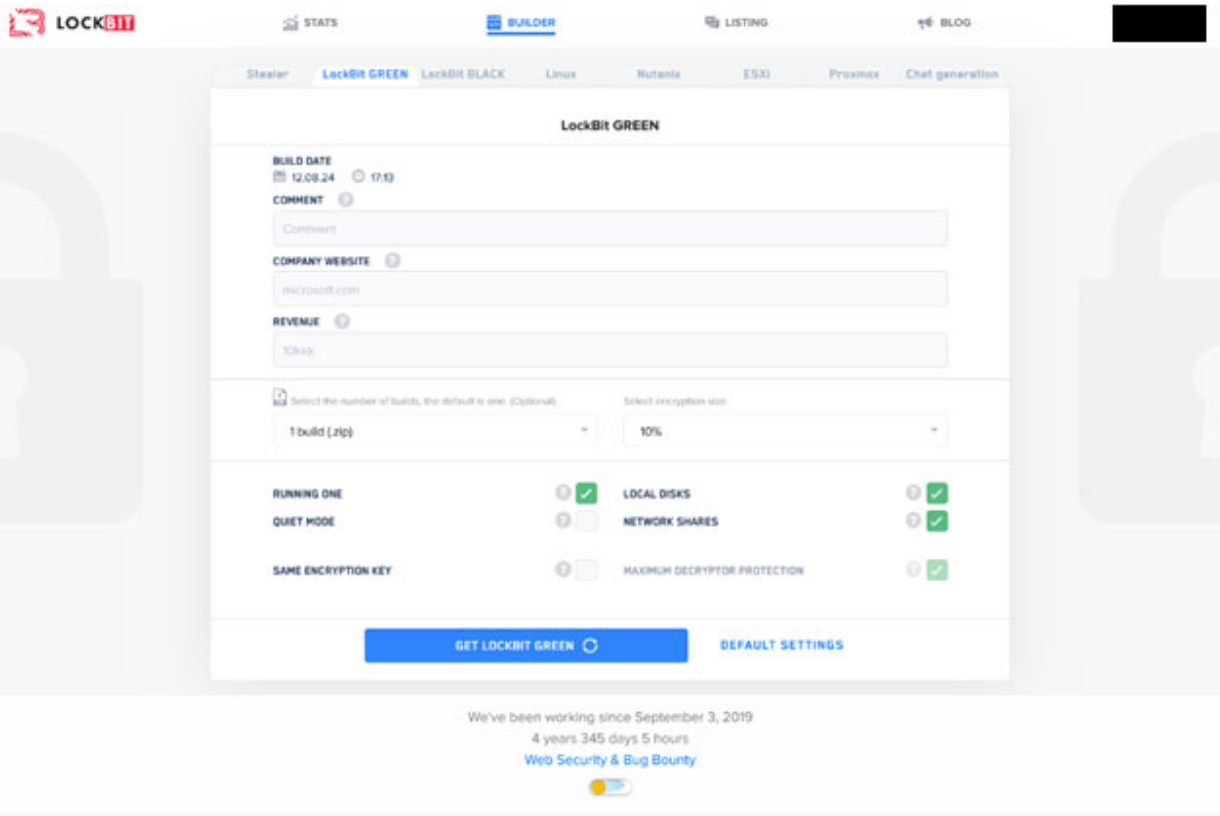
58. On August 12, 2024, pursuant to the U.S. mutual legal assistance request and other authorities, Israeli authorities executed a lawful search of PANEV's residence in Israel (the "August 2024 Operation"). The August 2024 Operation yielded overwhelming evidence further establishing PANEV's role as a LockBit developer—and, specifically, as a developer of code for multiple LockBit builders and other critical LockBit facilities.

i. LockBit Control Panel Access Credentials:

59. During the August 2024 Operation, Israeli authorities obtained PANEV's consent to search a computer in PANEV's custody, per the U.S. authorities' understanding. On that computer, Israeli authorities discovered a certain document (the "Credentials Document") and transmitted it to U.S. authorities pursuant to the U.S. mutual legal assistance request. U.S. authorities have reviewed the Credentials Document. Based on training, experience, and this investigation to date, U.S. authorities believe that the Credentials Document contains a list of access credentials to a variety of remote facilities that they further believe to be connected to the LockBit conspiracy.

60. Importantly, within the Credentials Document, U.S. authorities discovered what they assessed to be, based on training, experience, and this investigation to date, access credentials to the LockBit control panel. On or about August 12, 2024, U.S. authorities then proceeded to access the LockBit control panel with those credentials. That access was successful, and upon accessing that facility, U.S. authorities confirmed that that facility was in fact the LockBit control panel.

61. For example, U.S. authorities took the following screenshot of the control panel accessed with the access credentials found within PANEV's Credentials Document—[8]



U.S. authorities believe, from training, experience, and this investigation to date, that this screenshot depicts the LockBit control panel. The features listed in this screenshot are familiar to U.S. authorities. For example, the Builder tab refers to the "builders" features explained above. The various tabs visible on this screen—LockBit GREEN, LockBit BLACK, Linux, Nutanix, ESXI, and Proxmax—refer to different versions of the LockBit builder offered to LockBit's members by LockBit's developers.

62. Notably, the panel accessed with PANEV's credentials also included a handle to communicate with that LockBit user on "Service-1," a decentralized, end-to-end encrypted messaging platform.[9] Specifically, the listed Service-1 handle was "FUCKFBI" followed by other characters.

---

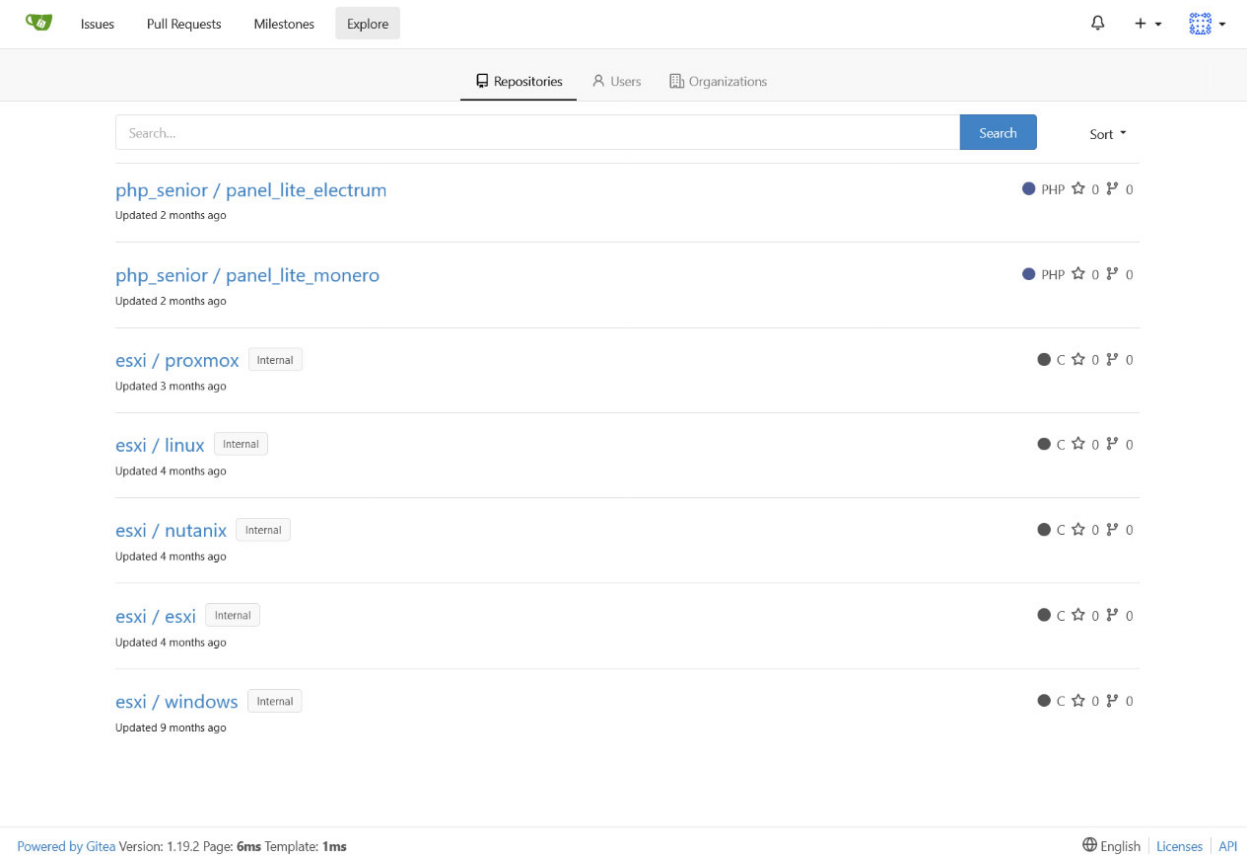
[8] This screenshot has been redacted to protect the integrity of an ongoing criminal investigation.

[9] The name of "Service-1" has been anonymized to protect an ongoing investigation and sensitive law-enforcement techniques.

63. As explained above, U.S. authorities also believe, from training, experience, and investigation to date, that the LockBit control panel is available only to LockBit's members, and not to the general public. U.S. authorities have learned, for example, that new affiliates undergo a vetting process when joining the LockBit group. Only at that time are affiliates given access credentials to the control panel. U.S. authorities themselves, and their international partners, have had to conduct ruses in order to gain panel access through undercover operations. (The screenshot above, taken with PANEV's credentials, appears just as the control panel has appeared to U.S. authorities in other operations in this investigation.) There is no legitimate reason, therefore, for an ordinary member of the public or a non-criminal actor to have access credentials to the LockBit control panel.

ii. Git Repository:

64. Within the Credentials Document, U.S. authorities discovered login credentials for a .onion domain on the TOR network. Pursuant to a search warrant issued by a U.S. court, on or about August 13, 2024, U.S. authorities accessed this domain with these credentials. After doing so, U.S. authorities discovered that the domain hosted a Git repository containing, among other things, LockBit source code (the "PANEV Git Repository"). Git is a free, open-source tool that enables software developers, programmers, and engineers to collaborate on coding projects. Upon accessing and reviewing the PANEV Git Repository, U.S. authorities captured the following screenshot:



65. U.S. authorities, including FBI computer scientists, have reviewed and analyzed the data stored within the PANEV Git Repository. Based on that review and analysis, U.S. authorities determined that the PANEV Git Repository contained the following—

1) Source code for the ESXi, Linux, Proxmox, and Nutanix LockBit builders. "Source code" is text written in a programming language, such as C or Python, that, when translated into machine code, can be executed by a computer. Software developers write computer programs in source code before conversion into machine code. In this way, source code represents the blueprint of a computer program. Therefore, PANEV possessed, within the PANEV Git Repository, the blueprints for multiple LockBit builders—as explained above, these are the tools that generate LockBit payloads.

2) Source code for the StealBit feature. Among other things, the StealBit source code allows an affiliate to either accelerate or decelerate the rate of data exfiltration, presumably to help the affiliate avoid attracting the attention of a system administrator on a victim system. PANEV, therefore, possessed the blueprints not just for multiple LockBit builders, but also for the tool that aided affiliates in exfiltrating, or stealing, victim data.

3) Source code for the Conti ransomware variant, which U.S. authorities believe to be closely related to the LockBit Green version of LockBit.

4) A copy of the LockBit 3.0 ransom note, which was found saved within the folders storing the source code of the ESXi, Linux, Proxmox, and Nutanix builders, as explained above.

66. The review of the PANEV Git Repository by U.S. authorities revealed that PANEV's credentials to that repository—that is, the credentials found within the Credentials Document—are administrator credentials for the repository. In other words, PANEV's credentials allowed the holder of those credentials (here, PANEV) to grant access to some or all of the folders within the repository to other users. Moreover, other users did appear to have access to the repository and to have worked and consulted on the various LockBit-related projects contained there.

iii. Other Artifacts:

67. Broadly speaking, the Credentials Document appears based on analysis by U.S. authorities as a notepad for PANEV's LockBit and other cybercriminal activities. For example, elsewhere on the Credentials Document, U.S. authorities discovered the following text (with English machine-translated from Russian):

```
****** Mask Attack ******
Built-in character sets
?l = abcdefghijklmnopqrstuvwxyz
?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
?d = 0123456789
?h = 0123456789abcdef
?H = 0123456789ABCDEF
?s = "space"!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
?a = ?l?u?d?s
?b = 0x00 - 0xff
```

Based on the heading "Mask Attack" and the technical terms that follow, U.S. authorities believe that this excerpt refers to the execution of cyberattacks. U.S. authorities know, from training and experience, that a "mask attack" is a cybercriminal hacking technique in which cybercriminals attempt to crack the password of an online facility, such as an email account or network credentials, with a targeted brute-force technique. In a simple brute-force attack, a cybercriminal might simply try every possible combination of letters, numbers, and symbols, but that approach is extremely time- and resource-consuming and inefficient. In a mask attack, however, a cybercriminal reduces the number of possible combinations by limiting certain characters based on

assumptions about the victim's behavior. For example, if a cybercriminal knows or guesses that the last 2 characters of a password are numerals—a common practice with passwords—the cybercriminal will, when deploying a mask attack, limit those two characters only to numerals, significantly reducing the number of possible combinations and making the attack faster and more efficient. The "built-in character sets" that follow the "Mask Attack" heading implement this technique. PANEV's familiarity with this technique further demonstrates PANEV's facility with cybercrime and computer hacking techniques, including fraudulent techniques such as these.

68. U.S. authorities also discovered within the Credentials Document the following excerpt (with English machine-translated from Russian):[10]

> [...] [Moniker-1[11]]: the first thing a coder needs to do is this
> fuck off Nutanix
> make green locker stubs with a new note
> make Linux eschi stubs with a new note
> take on Nutanix
>
> When editing a note, keep this in mind: all old blog domains and old links to old chats must be deleted
>
> New main blog domains
>
> http://lockbit[...].onion/
> http://lockbit[...].onion/
> http://lockbit5[...].onion/
>
> here are links to new chats
> lock[...].onion
> lock[...].onion
> lock[...].onion

The portion preceded by Moniker-1 appears to be a message sent to PANEV by that individual. That message appears to contain instructions regarding LockBit development, a conclusion supported by the "lockbit" and "lock" hyperlinks and headings that follow.

---

[10] The TOR domains and timestamp below have been redacted with "[...]" to protect the integrity of an ongoing investigation.

[11] "Moniker-1" has been anonymized to protect the integrity of an ongoing investigation.

69. Moreover, U.S. authorities discovered in the Credentials Document access credentials to "Service-2," a traffic distribution system ("TDS"). Service-2, like other TDSs, enables its users to develop and deploy custom online advertising campaigns, including the ability to push advertisements to websites participating in a given campaign. U.S. authorities know, however, that Service-2 has been heavily used by cybercriminals to engage in malvertising, a form of cybercrime in which online ads are used to lure users to malicious domains, or to deploy malicious code onto the computer of a user visiting a website displaying that ad. U.S. authorities are aware of no legitimate reason for PANEV to possess credentials for Service-2 or any other TDS. PANEV's Service-2 credentials, therefore, further demonstrate PANEV's cybercrime capabilities, including his familiarity with cybercrime techniques involving fraud and deception, such as malvertising.

c. Subsequent Admissions

70. U.S. authorities have been informed that PANEV was taken into custody by Israeli authorities after the August 2024 Operation based on domestic Israeli legal authority. U.S. authorities have been further informed that PANEV agreed to multiple voluntary interviews with Israeli authorities while in custody. Pursuant to the U.S. mutual legal assistance request, Israeli authorities have transmitted reports of those interviews to U.S. authorities, which have reviewed them.

71. Based on that review, U.S. authorities understand that PANEV gave the following admissions to Israeli authorities in an interview on or about August 15, 2024, in sum and substance:

- PANEV admitted that he had communicated with the Forum-1 user LockBit on Forum-1, and later on a separate encrypted messaging platform. PANEV claimed that his correspondence with LockBit began in or around 2019.

- Initially, PANEV claimed, he accepted and performed multiple coding jobs for LockBit in exchange for compensation. Those jobs included, among other things, writing code to disable the Windows Defender antivirus system (presumably, to allow a malware payload, like a LockBit build, to be deployed on a victim computer); writing code to deploy code throughout a network via the Windows Active Directory service; and writing code to print a given text on all printers on a given network (presumably, the LockBit ransom note).

- At some point, PANEV claimed, his relationship with the LockBit group expanded. PANEV acknowledged that he began receiving a regular monthly payment of $10,000 in cryptocurrency in exchange for his

coding and development services—confirming the analysis described below, in Section IV(e), regarding the tracing of Bitcoin from LockBit to the PANEV Exchange-1 Account. At that point, PANEV claimed, the services he provided LockBit came to include writing code for encryption malware and providing technical guidance. For example, PANEV explained that he at one point wrote code to encrypt files on a computer excluding system files—presumably to leave the computer usable to a victim user, but leaving the user's data unusable.

- PANEV claimed—dubiously, in the assessment of U.S. authorities, given the nature of the services he acknowledged providing from the very beginning of his work for LockBit and his own extensive familiarity with computer science, hacking, and cybercrime, as discussed in this Affidavit—that he at first did not realize that the work he was doing for LockBit was unlawful. PANEV admitted, however, that at a certain point, he understood that he was involved with unlawful activity. PANEV admitted that he continued working for the LockBit group, in sum and substance, "for the money."

d. The Forum-1 Messages

72. Before obtaining the August 2024 Complaint, and through investigation, U.S. authorities obtained evidence showing that PANEV exchanged direct messages with Khoroshev on "Forum-1," a major cybercriminal forum hosted on the dark web, using a certain Forum-1 moniker, "Moniker-2."[12]

73. Specifically, U.S. authorities have obtained through investigation records related to a certain user account on "Forum-1," a cybercriminal forum hosted on the dark web, or a portion of the Internet designed for untraceable communication and requiring a special configuration to access. Users of Forum-1 can make public posts and exchange private messages with other Forum-1 users regarding various cybercriminal topics, including promoting cybercriminal products and recruiting others to join cybercriminal ventures. The particular Forum-1 user account in question, "Moniker-2," itself made multiple publicly viewable posts regarding cybercriminal topics, including:

- In or around July 2020, Moniker-2 made a public post titled "Powershell malware." In that post, Moniker-2 wrote:

> Good afternoon,

[12] The actual names of both Forum-1 and Moniker-2 have been anonymized to protect an ongoing criminal investigation and sensitive law-enforcement techniques.

> Where can I find/download the most lively and blazing like a Christmas tree powershell malware samples? Thanks.

In this context, "Powershell" is a tool that allows users to issue program commands from a program's command line. As this post suggests, Powershell is often used by cybercriminals to exploit computer vulnerabilities, evade security software, and conduct cyber-attacks.

- In or around August 2019, Moniker-2 made a resident post titled "Non-resident dropper." In that post, Moniker-2 wrote, in relevant part:

> Hello,
>
> I present to you a service that will allow you to create your own unique non-resident dropper in a few clicks.
> […]
> What the dropper can do:
> 1. Download up to 5 files without attracting the attention of firewalls.
> 2. Organize them into your folders.
> 3. Run payload at a time using command line.
> 4. Self-removal.

In this context, a "dropper" is a type of malware designed to deliver other malware to a victim computer. The reference to "without attracting the attention of firewalls" suggests the use of fraudulent hacking techniques to evade detection by either system administrators or security software.

74. As is relevant to this investigation, Moniker-2 also exchanged private messages with the Forum-1 user with the username "LockBit"—which, as explained above, is known to U.S. authorities to be controlled by one or more other LockBit developers, likely Khoroshev. This investigation has shown that the LockBit user on Forum-1 has, since LockBit first appeared, spoken for the entire LockBit group by, among other things, making LockBit announcements and recruiting LockBit affiliates.[13]

75. The private messages exchanged by Moniker-2 and LockBit are as follows (emphasis added):

---

[13] The "LockBit" username on Forum-1 has not been anonymized.

Approximate Date and Time of Message	**Forum-1 Sender**	**Message (translated from Russian)**
January 31, 2022 at 19:11	LockBit	Hello, where have you disappeared to?
February 1, 2022 at 10:28	Moniker-2	Hello, I got really sick. It is better now. I will get in touch tomorrow.
February 2, 2022 at 12:29	Moniker-2	I wrote into latest [Service-1].[14] It has been silence so far. If I will be needed, I am ready.
February 5, 2022 at 14:39	LockBit	***The builder in the panel needs to be finished urgently.***

76. U.S. authorities believe that the February 5, 2022 message from LockBit refers to core LockBit infrastructure used to commit criminal activity. As explained above, the "panel" is the infrastructure maintained by LockBit developers to enable LockBit affiliates to launch attacks. The "builder" is the programming in the panel enabling affiliates to launch custom-generated versions of the LockBit malware to attack particular victims. U.S. authorities believe, therefore, that this message demonstrates that the user of Moniker-2—as explained below, PANEV—participated and collaborated in the development and maintenance of the core LockBit infrastructure used illegally to commit criminal activity around the world.

77. U.S. authorities have obtained overwhelming evidence that PANEV owned and controlled Moniker-2 at Forum-1 at all relevant times. For instance, U.S. authorities discovered within the Credentials Document evidence of PANEV's control of the Forum-1 Moniker-2 account, proving that PANEV exchanged the Forum-1 private messages with the Forum-1 LockBit user discussed above—

78. *First,* the Credentials Document lists what appear to be access credentials for the Moniker-2 user at Forum-1. (U.S. authorities attempted unsuccessfully to access the Moniker-2 account at Forum-1 with these credentials.)

79. *Second*, the Credentials Document lists access credentials for the same username as Moniker-2 at two other prominent cybercriminal forums.

---

[14] As explained above, "Service-1" is a decentralized end-to-end encrypted messaging platform. Forum-1 users frequently move conversations from the Forum-1 private-message feature to other messaging services, such as Service-1, in this way.

U.S. authorities successfully accessed those accounts with those credentials. In other words, PANEV used the same moniker to register for at least three cybercriminal forums.

80. And *third*, Forum-1 subscriber records for the Moniker-2 user, obtained by U.S. authorities through investigation, show that Moniker-2 registered for that Forum-1 account with a specific email address provided by Onion Mail, an encrypted email provider hosted on the dark web (the "PANEV Onion Mail Account"). The Credentials Document also includes access credentials for the PANEV Onion Mail Account, which U.S. authorities accessed and retrieved with those credentials pursuant to a search warrant issued by a U.S. court. In other words, PANEV owned and controlled the email account used to register the Moniker-2 username at Forum-1, further proving PANEV's ownership and control over that username.

81. Aside from the fruits of the August 2024 Operation, U.S. authorities had, at the time of that operation, developed significant independent evidence attributing Moniker-2 to PANEV. For example, U.S. authorities obtained through investigation other private messages sent on Forum-1 by Moniker-2 in which Moniker-2 provided to other Forum-1 users a separate handle, "Handle-1," to continue communicating on Service-1.[15] Pursuant to a search warrant issued by a U.S. court in or around July 2024, U.S. authorities also obtained records and content stored in PANEV's Apple iCloud account.[16] U.S. authorities have determined through investigation that Handle-1 was accessed from the same IP addresses used to access PANEV's personal Apple iCloud account close in time, examples of which are included below:

[15] Handle-1 has been anonymized to protect an ongoing investigation and sensitive law-enforcement technique.

[16] U.S. authorities confirmed that this iCloud account belonged to PANEV based on, among other evidence, the account being registered to PANEV in his true name and listing an email address U.S. authorities have linked to PANEV, and which PANEV admitted during his interviews with Israeli authorities to owning.

IP Address	Approximate Date and Time of Use by Handle-1	Approximate Date and Time of Access by PANEV Apple account
[...].104	August 29, 2021; 8:30 UTC	August 29, 2021; 8:36 UTC
[...].1	September 8, 2021; 8:20 UTC	September 8, 2021; 8:23 UTC
[...].210	October 13, 2021; 7:10 UTC	October 13, 2021; 6:56 UTC

These instances of IP overlap between Handle-1, which Moniker-2 repeatedly passed in Forum-1 private messages to other users, and PANEV's own iCloud account further proves PANEV's control over Moniker-2 at all relevant times.[17]

e. Payments of Cryptocurrency from LockBit to PANEV

82. As explained above, PANEV admitted to Israeli authorities that he received regular payments of approximately $10,000 per month in Bitcoin from the LockBit group in exchange for his development work. Through blockchain analysis, U.S. authorities have also obtained evidence consistent with PANEV's admission, showing that PANEV, between at least as early as June 2022 through at least as recently as February 2024, received regular payments of Bitcoin that U.S. authorities believe to have originated from the LockBit developers and were laundered through various cryptocurrency mixing services to disguise these criminal payments to PANEV. Those payments, which were iterated in amounts approximating $10,000 per month during this period, total at least approximately $230,000.

i. Identification of Cluster-LockBit and the PANEV Exchange-1 Account:

83. Based on blockchain analysis aided by third-party blockchain analysis software, U.S. authorities have identified a cluster of Bitcoin addresses that they assess to be owned and controlled by the LockBit developers ("Cluster-LockBit"). That assessment is based on, among other things, blockchain analysis showing that the 20-percent developer portion of multiple LockBit ransom payments have been transferred to various Bitcoin addresses within Cluster-LockBit over the course of the LockBit conspiracy.

[17] The August 2024 Complaint also described additional evidence obtained by U.S. authorities showing that PANEV paid for the Moniker-2 account at Forum-1 with funds from a Bitcoin cluster owned and controlled by him. In light of the additional direct and overwhelming evidence of PANEV's control of Moniker-2 obtained through the August 2024 Operation, however, this additional evidence—although valid and accurate—is cumulative.

84. Specifically—[18]

- As explained above, Victim-1, a business in Utah, was attacked by LockBit on or about October 30, 2021. On or about November 2, 2021, Victim-1 paid approximately 18.8768 BTC (or approximately $1.19 million at the time) to a Bitcoin address provided by the LockBit affiliate, ending in "5BC". On or about the same date, 20 percent of that amount—which, based on this investigation, U.S. authorities believe to be the developer portion of that payment—was sent from that address to a different Bitcoin address, ending in "tsz" ("Address-tsz"). Blockchain analysis shows that Address-tsz belongs to Cluster-LockBit.

- As explained above, Victim-2, a law-enforcement agency in New Jersey, was attacked with LockBit on or about November 13, 2021. On or about December 2, 2021, Victim-2 paid a ransom of approximately 1.42928 BTC (or approximately $85,430 at the time) to a Bitcoin address provided by the LockBit affiliate, ending in "tqt". On or about the same date, that address sent 20 percent of that amount—which, based on this investigation, U.S. authorities believe to be the developer portion of that payment—to a different Bitcoin address, ending in "g84" ("Address-g84"). Blockchain analysis shows that Address-g84 belongs to Cluster-LockBit.

85. U.S. authorities have further identified an account in PANEV's name, and bearing PANEV's know-your-customer documents (including PANEV's Israeli driver's license), at a major cryptocurrency exchange, "Exchange-1"[19] (the "PANEV Exchange-1 Account").

ii. Analysis of Bitcoin Flows from Cluster-LockBit to the PANEV Exchange-1 Account:

86. Based on blockchain analysis and review of records obtained from Exchange-1, during the period between June 2022 and February 2024, the PANEV Exchange-1 Account received approximately 30 incoming transfers of Bitcoin from seemingly random and disassociated addresses on the Bitcoin blockchain. Consistent with PANEV's admissions to Israeli authorities, those payments amounted to approximately $10,000 per month during this period. Blockchain analysis also reveals that during that same period, virtually

---

[18] The full Bitcoin addresses involved have been redacted in this section to protect the privacy of the victims and an ongoing law-enforcement investigation.

[19] The name of Exchange-1 has been anonymized to protect that institution's privacy.

identical amounts of Bitcoin were transferred out of the LockBit Cluster, close in time to corresponding transfers into the PANEV Exchange-1 Account, also to seemingly random and disassociated addresses on the Bitcoin blockchain. Those 30 transfers into the PANEV Exchange-1 Account—that is, the transfers corresponding in amount and time to transfers out of the LockBit Cluster—constitute the vast majority of all transfers into the PANEV Exchange-1 Account, showing that this account of PANEV's was used to receive criminal payments from LockBit (in exchange for his criminal services provided to them).

87. As explained below, the transfers of Bitcoin into the PANEV Exchange-1 Account did not originate directly from victims themselves. Rather, U.S. authorities assess, based on the evidence in this investigation, that those transfers effectively constituted salary payments made by the LockBit group from Cluster-LockBit, a Bitcoin cluster under the control of one or more other LockBit developers—likely Khoroshev—which cluster had itself received the 20 percent developer share of LockBit victim ransom payments. In other words, LockBit paid PANEV for his development work in funds extorted from LockBit victims.[20]

88. Consistent with PANEV's own admission to having received regular payments from the LockBit group, U.S. authorities assess that this activity is consistent with the use of cryptocurrency mixing services to launder Bitcoin. For example, the slight differences in the amounts transferred out of the LockBit Cluster and into the PANEV Exchange-1 Account likely reflect the transaction fee charged by a mixing service. Moreover, U.S. authorities know that mixing services often—as with this case—conceal the flow of transfers by leaving outgoing funds at a seemingly random and disassociated address on the blockchain and completing the transfer of the same amount of funds from a different seemingly random and disassociated address, making it extremely difficult to follow the flow of funds from sender to recipient on the blockchain alone. Finally, U.S. authorities are aware of no other legitimate explanation for the significant transfers of cryptocurrency into the PANEV Exchange-1 Account, especially given PANEV's own admissions.

89. More particularly, U.S. authorities have determined the following based on this evidence regarding the pattern of transfers—

90. *First,* between at least as early as in or around June 2022 through at least as recently as in or around February 2024, Cluster-LockBit would

---

[20] Although there is no indication that PANEV received, at the PANEV Exchange-1 Account, funds transferred directly from LockBit victims, U.S. authorities cannot and do not exclude the possibility that PANEV himself had access to, or ownership or control of, either Cluster-LockBit or any other LockBit developer cluster.

transfer a roughly fixed amount of Bitcoin at regular intervals to some other address. Between in or around June 2022 and in or around June 2023, this amount would be roughly $5,000 in Bitcoin (based on the exchange rate at the time of the transaction) transferred every two weeks; beginning in or around July 2023 through at least as recently as in or around February 2024, this amount would be roughly $10,000 in Bitcoin (based on the exchange rate at the time) transferred once per month.

91. *Second,* in at least one instance during the period from June 2022 to February 2024, blockchain analysis shows that this transfer was made to a Bitcoin address known by law enforcement to be controlled by a mixing service. In other instances, however, the funds would be transferred to an unknown and seemingly random Bitcoin address and left there—which is consistent with the operation of a mixing service.

92. And *third*, on roughly the same schedule, the PANEV Exchange-1 Account would receive an incoming transfer of Bitcoin virtually identical, and close in time (sometimes even hours), to the corresponding outgoing transfer from Cluster-LockBit. Those funds would originate shortly before the final transfer to the PANEV Exchange-1 Account at one or more different Bitcoin addresses before being transferred to the PANEV Exchange-1 Account. Those intermediate Bitcoin addresses would be unknown and seemingly random—which is consistent with the operation of a mixing service.

93. A list of all transfers presently identified by U.S. authorities follow below. These transfers and analysis confirm and expand upon PANEV's admission to having earned hundreds of thousands of dollars in cryptocurrency in exchange for extensive development work he performed for the LockBit group.

Approximate Date and Time of Outgoing Transfer from Cluster-LockBit	**Approximate Outgoing Transfers from Cluster-LockBit (in BTC and USD based on exchange rate at time)**	**Approximate Date and Time of Incoming Transfer to PANEV Exchange-1 Account**	**Approximate Incoming Transfers to PANEV Exchange-1 Account (in BTC and USD based on exchange rate at time)**
June 15, 2022; 9:55 UTC	0.23810532 BTC; $4,799.12	June 15, 2022; 21:31 UTC	0.23606914 BTC; $5,221.46
July 1, 2022; 14:48 UTC	0.25972395 BTC; $5,079.18	July 1, 2022; 19:13 UTC	0.25732055 BTC; $4,989.44
July 15, 2022; 03:26 UTC	0.24517995 BTC; $5,019.56	July 16, 2022; 07:57 UTC	0.24279991 BTC; $4,994.17

Approximate Date and Time of Outgoing Transfer from Cluster-LockBit	Approximate Outgoing Transfers from Cluster-LockBit (in BTC and USD based on exchange rate at time)	Approximate Date and Time of Incoming Transfer to PANEV Exchange-1 Account	Approximate Incoming Transfers to PANEV Exchange-1 Account (in BTC and USD based on exchange rate at time)
August 1, 2022; 07:23 UTC	0.21604862 BTC; $5,035.69	August 1, 2022; 14:23 UTC August 1, 2022; 17:11 UTC	0.1095566 BTC; $2,555.88 0.10433217 BTC; $2,420.24
August 15, 2022; 14:20 UTC	0.20691851 BTC; $4,978.68	August 16, 2022; 09:07 UTC	0.2048564 BTC; $4,927.50
September 1, 2022; 15:13 UTC	0.25418984 BTC; $5,022.09	September 1, 2022; 21:12 UTC	0.25187732 BTC; $5,045.26
September 15, 2022; 16:52 UTC	0.25481186 BTC; $5,023.80	September 16, 2022; 09:47 UTC	0.25237826 BTC; $4,971.88
October 1, 2022; 09:28 UTC	0.25962948 BTC; $5,023.27	October 1, 2022; 15:15 UTC	0.25727759 BTC; $4,969.47
October 15, 2022; 01:39 UTC	0.26041434 BTC; $4,995.27	October 15, 2022; 16:08 UTC	0.25798899 BTC; $4,934.88
November 1, 2022; 06:42 UTC	0.24227189 BTC; $4,972.69	November 1, 2022; 16:12 UTC	0.23992533 BTC; $4,898.44
November 14, 2022; 19:13 UTC	0.30059674 BTC; $4,990.72	November 15, 2022; 10:12 UTC	0.29792393 BTC; $5,035.21
November 30, 2022; 22:42 UTC	0.29205396 BTC; $4,993.47	December 1, 2022; 10:21 UTC	0.28950277 BTC; $4,952.46
December 14, 2022; 21:27 UTC	0.281 BTC; $4,978.82	December 15, 2022; 08:52 UTC	0.27851658 BTC; $4,957.97
February 1, 2023; 02:17 UTC	0.21626218; $4,998.81	February 1, 2023; 10:58 UTC	0.21491496 BTC; $4,942.08
February 15, 2023; 11:38 UTC	0.2249735 BTC; $5,004.41	February 15, 2023; 19:46 UTC	0.22346836 BTC; $5,196.75
March 1, 2023; 09:27 UTC	0.20974064 BTC; $4,998.83	March 1, 2023; 15:25 UTC	0.2076142 BTC; $4,944.27
March 16, 2023; 08:45 UTC	0.20311809 BTC; $4,949.81	March 16, 2023; 13:41 UTC	0.20067629 BTC; $4,890.31
April 1, 2023; 15:07 UTC	0.17680419 BTC; $5,017.95	April 2, 2023; 9:30 UTC	0.17483229 BTC; $4,963.70
April 14, 2023; 23:02 UTC	0.16357108 BTC; $4,983.55	April 15, 2023; 08:42 UTC	0.16161208 BTC; $4,919.87

Approximate Date and Time of Outgoing Transfer from Cluster-LockBit	Approximate Outgoing Transfers from Cluster-LockBit (in BTC and USD based on exchange rate at time)	Approximate Date and Time of Incoming Transfer to PANEV Exchange-1 Account	Approximate Incoming Transfers to PANEV Exchange-1 Account (in BTC and USD based on exchange rate at time)
May 1, 2023; 01:15 UTC	0.17046828 BTC; $4,983.53	May 1, 2023; 10:36 UTC	0.16847398 BTC; $4,925.23
May 15, 2023; 19:55 UTC	0.18246869 BTC; $5,008.38	May 16, 2023; 06:12 UTC	0.18075852 BTC; $4,894.07
June 1, 2023; 01:30 UTC	0.18420809 BTC; $5,014.27	June 1, 2023; 07:54 UTC	0.18263693 BTC; $4,902.57
July 1, 2023; 11:00 UTC	0.32831797 BTC; $9,992.99	July 1, 2023; 14:56 UTC	0.32617025 BTC; $9,979.64
August 1, 2023; 05:56 UTC	0.34667626 BTC; $10,133.85	August 1, 2023; 10:01 UTC	0.34381518 BTC; $9,946.89
September 1, 2023; 17:01 UTC	0.38772089 BTC; $9,996.44	September 1, 2023; 19:50 UTC	0.38468427 BTC; $9,854.94
October 1, 2023; 15:16 UTC	0.36866094 BTC; $10,025.94	October 1, 2023; 18:49 UTC October 1, 2023; 21:12 UTC	0.12999459 BTC; $3,522.40 0.23572767 BTC; $6,356.22
November 1, 2023; 08:00 UTC	0.29009913 BTC; $10,004.73	November 1, 2023; 13:46 UTC November 1, 2023; 19:43 UTC	0.12195595 BTC; $4,226.71 0.16573926 BTC; $5,744.14
December 1, 2023; 12:32 UTC	0.26215536 BTC; $10,109.21	December 1, 2023; 19:35 UTC	0.25959235 BTC; $10,074.11
February 1, 2024; 13:06 UTC	0.23750712 BTC; $9,994.03	February 1, 2024; 17:56 UTC	0.23503904 BTC; $10,065.36

f. Artifacts on PANEV iCloud Account

94. As explained above, in or around July 2024, U.S. authorities seized and reviewed PANEV's Apple iCloud account pursuant to a search warrant issued by a U.S. court. That account contained, among other things, a stored backup of an Apple device registered to that account. U.S. authorities discovered the following artifacts saved in memory within that backup—

1) A Google search in or around January 2021 for the phrase "crypto api ransomware."

2) A Google search at an unknown time for the phrase "fsutil file setzerodata windows 7", which appears to be directed to a command for permanently deleting data stored on a Microsoft Windows system.

3) The following phrase, apparently a URL, resident in memory: "https://www.ic3.gov/Media/News/2022/220204.pdfMicrosoft Word - LockBit_2.0_FLASH FINAL - 220204.pdf". This URL appears to have been a link to an FBI LockBit advisory issued to the public in February 2022 (available at: https://www.ic3.gov/Media/News/2022/220204.pdf).

4) The following phrase, apparently a URL, resident in memory: "https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation". In computer science and cryptography, the "block cipher mode of operation" is an encryption algorithm, consistent with ransomware development.

5) A Google search at an unknown time for the phrase "github portable aesgithub portable aes." Github is a popular software development platform. "AES" is an encryption algorithm, again consistent with ransomware development.

6) The following phrase, apparently a URL, resident in memory: "https://core.ac.uk/download/pdf/157830224.pdf". This link points to a paper entitled "No Random, No Ransom: A Key to Stop Cryptographic Ransomware."

7) The following phrase, apparently a URL, resident in memory: "https://www.computer.org/csdl/journal/tq/5555/01/09130140/1159t EuJMJyAnalysis of Encryption Key Generation in Modern Crypto Ransomware". This link appears to a paper entitled "Analysis of Encryption Key Generation in Modern Crypto Ransomware" (currently available at: https://www.computer.org/csdl/journal/tq/2022/02/09130140/1159tE uJMJy).

8) The following phrase, apparently a URL, resident in memory: "https://www.bleepingcomputer.com/news/security/how-malware-gains-trust-by-abusing-the-windows-cryptoapi-flaw/How Malware Gains Trust by Abusing the Windows CryptoAPI Flaw".

95. These artifacts, found within storage on a backup of one of PANEV's devices, confirm PANEV's interest and proficiency in LockBit in particular and in malware development, ransomware, and cryptography more broadly.

96. Artifact (8) in the list above is especially notable, because it demonstrates PANEV's familiarity with the use of fraudulent techniques in cybercrime, and in LockBit in particular. U.S. authorities know from training, experience, and investigation that in or around October 2022, a new common vulnerability and exposure ("CVE") was announced in the Microsoft Windows operating system: CVE-2022-34689, related to a spoofing vulnerability in Windows. Specifically, the Windows CryptoAPI is a Windows tool used to handle cryptography-related functions. Web browsers, for example, use the CryptoAPI tool to validate certificates on websites. The CVE-2022-34689 vulnerability—the same CryptoAPI vulnerability discussed in the BleepingComputer article for which a link was found in PANEV's iCloud storage—allows an attacker to masquerade as a legitimate user or entity in order to gain unauthorized access to a victim computer.

97. Artifact (3) in the list above is also notable, because it demonstrates PANEV's familiarity with the full scope of the LockBit conspiracy, and with the significant prominence and attention that the LockBit group held within the cybersecurity community by that time. The February 2022 FBI LockBit advisory, titled "Indicators of Compromise Associated with LockBit 2.0 Ransomware," provided both a general overview of the LockBit group—similar to the overview provided here—and extensive technical detail regarding IOCs and other features of LockBit attacks. More broadly, however, LockBit has received significant attention both in the general media and the cybersecurity community for virtually its entire existence, as anyone familiar with computer hacking—like PANEV—would have known.

98. Finally, Artifact (5) in the list above—the Google search involving the AES encryption algorithm—is also notable. U.S. authorities have learned through investigation that the AES algorithm has been employed at times by the LockBit group, and that LockBit has at times itself advertised as much in public announcements.