

United States District Court

CENTRAL

DISTRICT OF

CALIFORNIA

In the Matter of the Seizure of

(Address or Brief description of property or premises to be seized)

the Internet domain WORLDWIREDLABS.COM

SEIZURE WARRANT

CASE NUMBER: 2:23-mj-1011

TO: Federal Bureau Investigation and any Authorized Officer of the United States, Affidavit(s) having been made before me by FBI Task Force Officer [REDACTED], who has reason to believe that there is now certain property which is subject to forfeiture to the United States, namely (describe the property to be seized)

The Internet domain WORLDWIREDLABS.COM, as described in Attachment A, which is incorporated herein by reference,

which is subject to seizure and forfeiture under 18 U.S.C. §§ 981(a)(1)(A) and (b), 982(b)(1), and 1030(i)(1)(A); and 21 U.S.C. § 853

concerning a violation of Title 18 United States Code, Section(s) 1030(a)(5)(A) and 1956(a)(2).

I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the property so described is subject to seizure and that grounds exist for the issuance of this seizure warrant.

Verisign, Inc. is ordered to redirect the Internet domain WORLDWIREDLABS.COM to substitute servers controlled by the FBI, as set forth in Attachment A.

YOU ARE HEREBY COMMANDED to seize within 14 days the property specified, serving this warrant and making the seizure in the daytime - 6:00 A.M. to 10:00 P.M., leaving a copy of this warrant and receipt for the property seized, and prepare a written inventory of the property seized and promptly return this warrant to the undersigned judicial officer as required by law.

03/03/2023 at 3:11 P.M.

Date and Time Issued

Hon. Rozella A. Oliver, U.S. Magistrate Judge

Name and Title of Judicial Officer

Los Angeles, California

City and State

Rozella A. Oliver

Signature of Judicial Officer

[illegible]

Attachment A

SUBJECT DOMAIN Controlled by Verisign

With respect to the following **SUBJECT DOMAIN**,
WORLDWIREDLABS.COM, Verisign, Inc., located at 12061 Bluemont
Way, Reston, VA 20190, which is the domain registry (the
"Subject Registry"), shall take the following actions to effect
the seizure of the **SUBJECT DOMAIN**:

1. Take all reasonable measures to redirect the
SUBJECT DOMAIN to substitute servers controlled by the FBI, by
associating the authoritative name server for the **SUBJECT DOMAIN**
to the following authoritative name servers:

- (a) ns1.seizedservers.com
- (b) ns2.seizedservers.com
- (c) Any new authoritative name server to be
designated by a law enforcement agent in writing,
including e-mail, to the Subject Registry

2. Take all reasonable measures to propagate the
necessary changes through the Domain Name System as quickly as
practicable;

3. Prevent any further modification to, or transfer
of, the **SUBJECT DOMAIN** pending transfer of all right, title, and
interest in the **SUBJECT DOMAIN** to the United States upon
completion of forfeiture proceedings, to ensure that changes to
the **SUBJECT DOMAIN** cannot be made absent court order or, if

forfeited to the United States, without prior consultation with the FBI or Department of Justice;

4. Provide reasonable assistance in implementing the terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

5. The Government will display a notice on the website to which the **SUBJECT DOMAIN** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text with the potential addition of international partners):

"This Website Has Been Seized

as part of a coordinated law enforcement action taken against the NetWire Remote Access Trojan.

This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant pursuant to 18 U.S.C. § 981(a)(1)(A) and (b), 18 U.S.C. § 982(b)(1), 18 U.S.C. § 1030(i)(1)(A) and 21 U.S.C. § 853, issued by the United States District Court for the Central District of California as part of a joint international law enforcement operation and action by: the United States Attorney's Office for the Central District of California, the Federal Bureau of Investigation, Croatia Ministry of the Interior Criminal Police Directorate, Europol European Cybercrime Center, Zurich Cantonal Police, and the Australian Federal Police"

United States District Court

CENTRAL

DISTRICT OF

CALIFORNIA

In the Matter of the Seizure of

(Address or Brief description of property or premises to be seized)

the Internet domain WORLDWIREDLABS.COM

**AMENDED APPLICATION AND AFFIDAVIT
FOR A SEIZURE WARRANT BY
TELEPHONE OR OTHER RELIABLE
ELECTRONIC MEANS**

CASE NUMBER: 2:23-mj-1011

I, [REDACTED], being duly sworn depose and say:

I am a Task Force Officer with the Federal Bureau Investigation, and have reason to believe that

in the EASTERN District of VIRGINIA
there is now concealed a certain person or property, namely (describe the person or property to be seized)

The Internet domain WORLDWIREDLABS.COM, as described in Attachment A to the affidavit of [REDACTED],

which is (state one or more bases for seizure under United States Code)

subject to seizure and forfeiture under 18 U.S.C. §§ 981(a)(1)(A) and (b), 982(b)(1), and 1030(i)(1)(A); and 21 U.S.C. § 853
concerning a violation of Title 18 United States Code, Section(s) 1030(a)(5)(A) and 1956(a)(2).

The facts to support a finding of Probable Cause for issuance of a Seizure Warrant are as follows:

Continued on the attached sheet and made a part hereof. X Yes No

/s/

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

Sworn before me in accordance with requirements of
Fed. R. Crim. P. 4.1 by telephone

03/03/2023 at 3:11 P.M.

Date

Hon. Rozella A. Oliver, U.S. Magistrate Judge
Name and Title of Judicial Officer

AUSAs Lisa Feldman & Maxwell Coll

Los Angeles, California
City and State

Rozella A. Oliver
Signature of Judicial Officer

[REDACTED]

2. I am familiar with the facts and circumstances described herein. This affidavit is based upon my personal involvement in this investigation, my training and experience, and information obtained from various law enforcement personnel and witnesses, including information that has been reported to me either directly or indirectly. This affidavit does not purport to set forth my complete knowledge or understanding of the facts related to this investigation. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and part only. All figures, dates, times, and calculations set forth herein are approximate.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is presented in support of an application for a warrant to seize the domain name **WORLDWIREDLABS.COM** (the "SUBJECT DOMAIN").

4. This seizure shall be effected by associating the authoritative name server for the SUBJECT DOMAIN name to an FBI-controlled name server, as described in detail in **Attachment A**.

5. The SUBJECT DOMAIN is associated with a corresponding registry and registrar that is each capable of setting the

"authoritative name server" for the SUBJECT DOMAIN. The registry to be served with this warrant is: Verisign, Inc., located at 12061 Bluemont Way, Reston, VA 20190.

III. SUMMARY OF RELEVANT COMPUTER AND INTERNET CONCEPTS

6. The information provided below regarding relevant computer and internet concepts is based on my training and experience and publicly available information:

a. Malware: Malware refers to malicious software written intentionally to carry out annoying or harmful actions. Malware often masquerades as a useful program or is embedded into useful programs, so that users are induced into activating it. Malware includes remote access trojans, computer viruses, and worms.

b. Remote Access: Remote access is the ability to access and control a computer or a computer system from another location by means of a network connection.

c. Remote Access Trojan ("RAT"): A RAT is a type of malware that allows for covert surveillance, allowing a "backdoor" for administrative control and unfettered and unauthorized remote access to a victim's computer, without the victim's knowledge or permission.

d. Commodity RAT: A Commodity RAT is a RAT malware which is sold to others for malicious use.

e. Internet Protocol address: An Internet Protocol address, or "IP address," is a unique numeric address used to

identify computers on the Internet. The standard format¹ for IP addressing consists of four numbers between 0 and 255 separated by dots, e.g., 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. Internet Service Providers ("ISPs") assign IP addresses to their customers' computers.

f. Domain Name: A domain name is a text-based label that serves to identify Internet resources, such as computers, networks, and services, in a way that is easier to remember than an IP address. For example, "google.com" and "cacd.uscourts.gov" are domain names.

g. Domain Name System: The domain name system ("DNS") is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods. The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the "top-level" domain, or TLD. For the example of google.com, ".com" is the top-level domain, and "google" is the second-level domain. In the cacd.uscourts.gov example, ".gov" is the top-level domain,

¹ IP version 4, or "IPv4," is the version of IP most commonly used today, and is the version described above. A newer version of the protocol, "IPv6," wholly different in appearance to IPv4, is sometimes used, but does not pertain to this request, and will not be referred to further.

".uscourts" is the second-level domain, and "cacd" is the third-level domain, with each being a subdivision of the one to its right.

h. Server: A server is a centralized computer that provides services for other computers connected to it through a network. The computers that use the server's services are sometimes called "clients." Server computers can be physically located anywhere. For example, it is not uncommon for a network's server to be located hundreds, or even thousands of miles away from the client computers.

i. Name Servers: Name servers are particular servers which function like a phonebook. Name servers will accept queries for domain names (such as google.com) and return the IP address associated with the domain, much as the name John Doe might be looked up in a telephone book to determine the corresponding telephone number.

j. Registry: A registry is a company responsible for managing the assignment of domains to IP addresses within a top-level domain. For example, the registry for the ".com" and ".net" top-level domains is Verisign, Inc.

k. Registrar: Domain names are usually purchased through a registrar, which acts as the intermediary between the registry and the purchaser of a domain name. Companies such as Namecheap, GoDaddy, and Domain.com are registrars, through which a person can purchase a particular domain name to host a website (among other things). For example, if a person, "Entrepreneur A," wishes to run a website to sell widgets, they might purchase

the domain "widgets-R-us.com" from a registrar like Namecheap, which acts as an intermediary between that customer and Verisign, Inc.

l. Registrant: The individual or business that purchases a domain name is called a registrant. Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Typically, a registrar will provide a registrant with the ability to change the IP address a particular IP address resolves through an online interface. In the example above, Entrepreneur A is the registrant. Once Entrepreneur A purchases the domain widgets-R-us.com, they can host their website anywhere they wish, and the widgets-R-us.com domain will be associated with whatever IP address is assigned to the computer (server) they use to host that website. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

m. WHOIS: WHOIS is a query-and-response protocol that is publicly available and widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name or IP address block. WHOIS query responses provide the contact information for the individual responsible for registering the domain name or the Internet Service Provider ("ISP") which owns the IP block.

n. Passive DNS: Passive DNS is a directory of archived, historical DNS information, which is not available in the DNS directory.

o. Internet Forum: An internet forum is an online discussion site where people communicate with each other, generally relating to a particular topic. Generally, a person on the forum will post a topic or a "thread" and others then post comments to that thread.

IV. APPLICABLE LAW

7. There is probable cause to believe that the SUBJECT DOMAIN is subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 981(b) and (a)(1)(A) because the SUBJECT DOMAIN was involved in one or more violations of 18 U.S.C. § 1956(a)(2) (International Money Laundering), done with the intent to promote the underlying specified unlawful activity, namely 18 U.S.C. § 1030(a)(5)(A) (Unauthorized Impairment of a Protected Computer) as defined by 18 U.S.C. § 1956(c)(7)(D).²

² 18 U.S.C. § 981(b)(3) provides authorization for the seizure of out-of-district or ephemeral assets where, as here, acts and omissions giving rise to forfeiture occurred within the Central District of California. Specifically, that statute provides that "a seizure warrant may be issued pursuant to this subsection by a judicial officer in any district in which a forfeiture action against the property may be filed under section 1355(b) of title 28." 28 U.S.C. Section 1355(b), in turn, allows for the bringing of a forfeiture action in "the district court for the district in which any of the acts or omissions giving rise to the forfeiture occurred." As set forth in the affidavit, acts giving rise to forfeiture occurred in the Central District. Specifically, NetWire RAT malware was transferred to a computer in the Central District of California and was subsequently used covertly by the FBI on test computers.

8. Furthermore, there is probable cause to believe that the SUBJECT DOMAIN is subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. 1030(i)(1)(A) because the SUBJECT DOMAIN constitutes personal property used or intended to be used to facilitate the commission of attacks against unwitting victims for the express purpose of preventing the victims from properly using the Internet, in violation of 18 U.S.C. § 1030(a)(5)(A) (Unauthorized Impairment of a Protected Computer).

9. In addition, the SUBJECT DOMAIN is subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 982(b)(1), and 21 U.S.C. § 853(f), because there is probable cause to believe that a protective order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the property for forfeiture because there is reason to believe that the property is under the control of the targets of this investigation, who cannot reasonably be relied upon to abide by an order to maintain the property in substantially the same condition as it is at the present time, in order to ensure that it will be available for forfeiture. More particularly, providing notice may allow the targets to frustrate further efforts of law enforcement by transitioning their enterprise and infrastructure to jurisdictions beyond the reach of United States law enforcement.

V. SUMMARY OF PROBABLE CAUSE

10. Since 2020, the FBI has been investigating a group of individuals who are operating the SUBJECT DOMAIN, which is an

online marketplace that is being used for the exclusive sale and licensing of the NetWire Remote Access Trojan ("NetWire RAT").

In general, this means that customers pay money to the administrator/s of this website in order to acquire an instance of the NetWire RAT malware and to pay the recurring licensing fee for use beyond the initial year provided. NetWire is the exclusive product for sale on the SUBJECT DOMAIN through a subscription model where users choose between a monthly or yearly subscription license.

11. As described below, the SUBJECT DOMAIN was accessed by the FBI Investigative Team, meaning that a member of the FBI Investigative Team created an account on the website, paid for a NetWire subscription plan, and then downloaded the latest version of the NetWire RAT. Following this purchase and download, a member of the FBI Investigative Team then constructed a customized instance of the NetWire RAT using the product's Builder Tool. This instance of NetWire was built specifically for an isolated FBI lab virtual machine running Windows, used as a victim machine for testing purposes (the "test victim machine").

12. The SUBJECT DOMAIN never required the FBI to confirm that it owned, operated, or had any property right to the test victim machine that the FBI attacked during its testing (as would be appropriate if the attacks were for a legitimate or authorized purpose). In addition, the services provided by the NetWire RAT, described in more detail below, are not consistent with services provided by legitimate remote access services.

Moreover, NetWire has been advertised on Internet hacking forums as a tool for unlawful activities.

13. The SUBJECT DOMAIN accessed by the FBI represents property involved in international financial transactions that promote unlawful activity, specifically computer intrusion. The SUBJECT DOMAIN serves as the marketplace for the purchase of and subscription to the NetWire RAT, and allows users throughout the world, including in the Central District of California, to purchase malware and use it for unlawful purposes.

VI. STATEMENT OF PROBABLE CAUSE

A. The Sole Purpose of the SUBJECT DOMAIN is to Promote the Sale of, and Provide News About, NetWire.

14. On or about August 11, 2020, the FBI Investigative Team visited the SUBJECT DOMAIN and learned the following:

a. The company referenced on the website is World Wired Labs ("WWL").

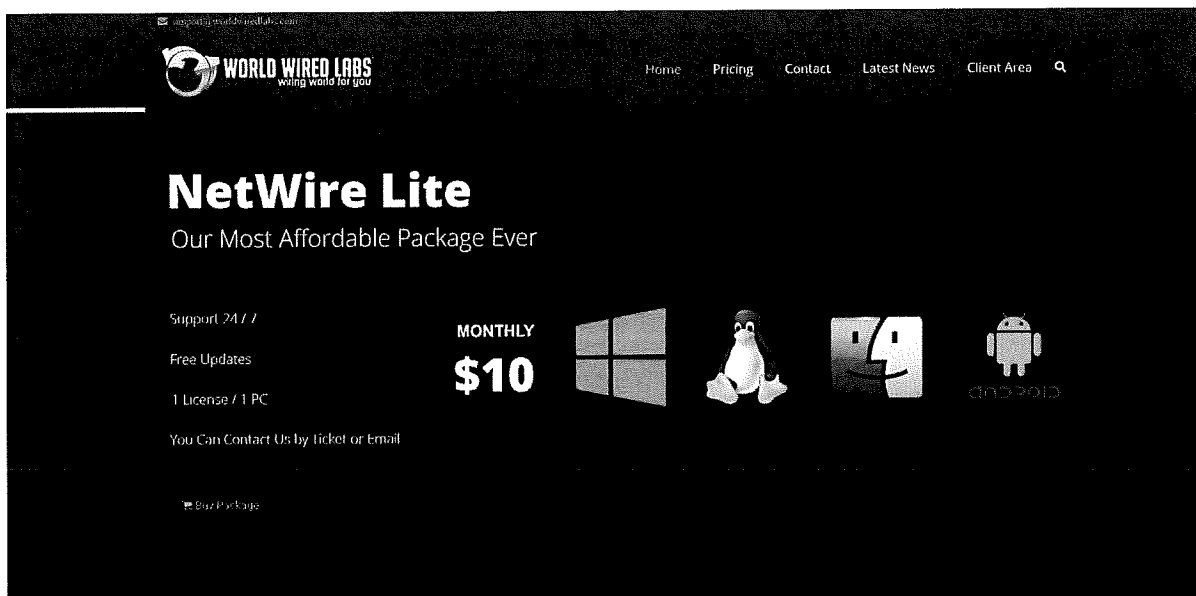
b. NetWire is the only product sold on the SUBJECT DOMAIN. The malware is offered for sale on the SUBJECT DOMAIN through a subscription model where users choose between a monthly or yearly subscription license.

c. According to the SUBJECT DOMAIN, NetWire is a remote access tool that is: "[S]pecifically designed to help businesses complete a variety of tasks connected with maintaining computer infrastructure. It is a single 'command center' where you can keep a list of all your remote computers, monitor their statuses and inventory, and connect to any of them for maintenance purposes."

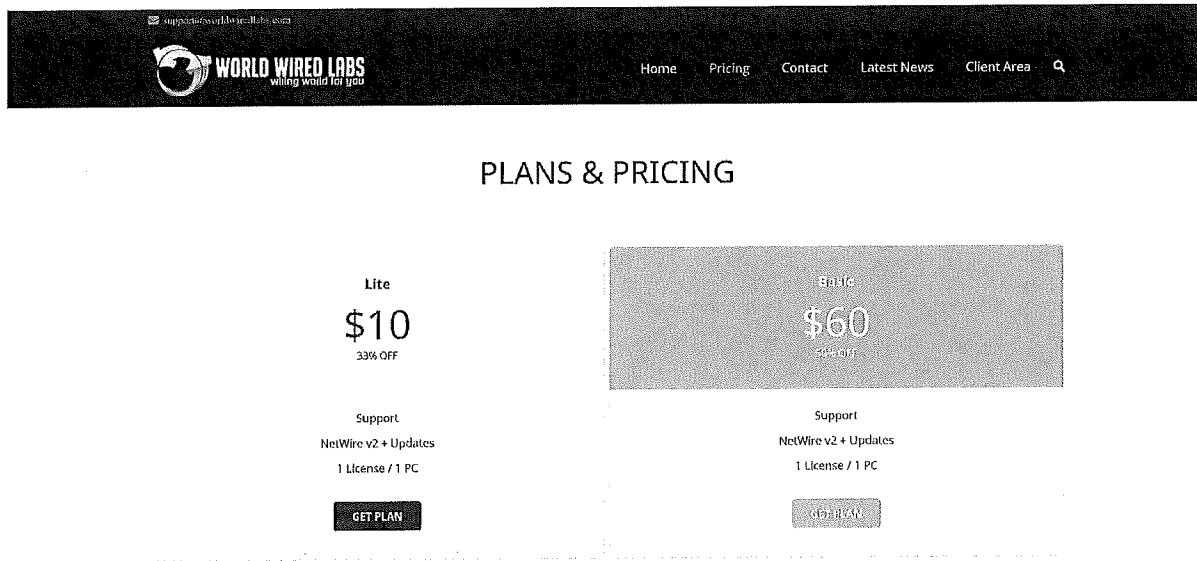
d. Consumers can purchase NetWire in the form of a monthly or annual license, either the "Lite" or "Basic" plan. Each plan gives the consumer access to the latest version of NetWire, including future updates, one license key, and tech support.

15. On March 3, 2023, I visited the SUBJECT DOMAIN for further review. Following this review, I determined that the SUBJECT DOMAIN's sole purpose is to promote the sale of, and provide news about, NetWire. I also took the following three screenshots:

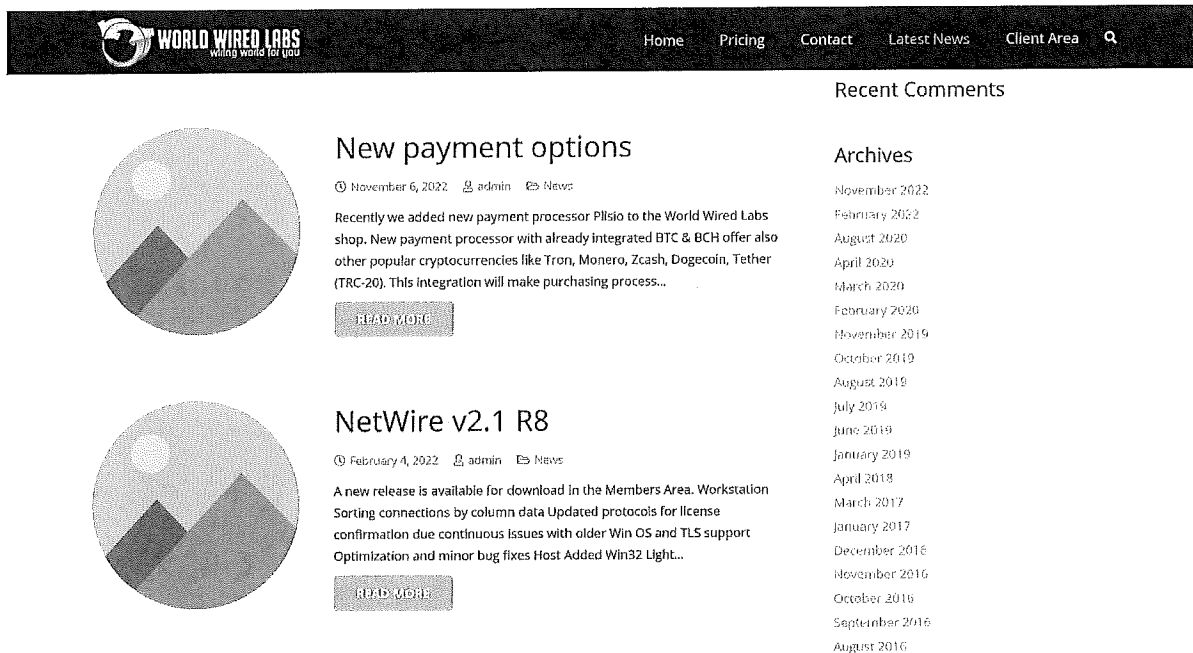
a. Below is a screenshot of the SUBJECT DOMAIN's Homepage, advertising "NetWire Lite" as "Our Most Affordable Package Ever." The links at the top are listed as "Home," "Pricing," "Contact," "Latest News," and "Client Area."



b. Below is a screenshot of the "Pricing" link. After clicking on the link, a page is displayed labeled "Plans & Pricing" which features the only two products sold on the SUBJECT DOMAIN -- NetWire "Lite," which is sold for \$10, and NetWire "Basic," which is sold for \$60.



c. Below is a screenshot of the "Latest News" link. After clicking on the link, a page is displayed listing the latest updates related to the SUBJECT DOMAIN and NetWire:



The screenshot shows the World Wired Labs website. The header includes the logo and navigation links: Home, Pricing, Contact, Latest News, Client Area, and a search icon. The main content area features two articles, each with a circular image of a mountain landscape. The first article is titled 'New payment options' and dated November 6, 2022. The second article is titled 'NetWire v2.1 R8' and dated February 4, 2022. To the right of the articles is a sidebar with 'Recent Comments' and 'Archives'.

World Wired Labs
wiring world for you

Home Pricing Contact Latest News Client Area

New payment options
November 6, 2022 admin News
Recently we added new payment processor Plisio to the World Wired Labs shop. New payment processor with already integrated BTC & BCH offer also other popular cryptocurrencies like Tron, Monero, Zcash, Dogecoin, Tether (TRC-20). This integration will make purchasing process...

NetWire v2.1 R8
February 4, 2022 admin News
A new release is available for download in the Members Area. Workstation Sorting connections by column data Updated protocols for license confirmation due continuous issues with older Win OS and TLS support Optimization and minor bug fixes Host Added Win32 Light...

Recent Comments

Archives
November 2022
February 2022
August 2020
April 2020
March 2020
February 2020
November 2019
October 2019
August 2019
July 2019
June 2019
January 2019
April 2018
March 2017
January 2017
December 2016
November 2016
October 2016
September 2016
August 2016

d. To the government's knowledge, NetWire is only sold on the SUBJECT DOMAIN.

B. NetWire Used by Cyber Actors for Malicious Purposes

16. Despite WWL's marketing on the SUBJECT DOMAIN, based on Internet research and the FBI investigation described below, NetWire is a Remote Access Trojan (RAT) malware used by cyber actors for malicious purposes rather than by businesses as a legitimate tool. Since at least 2016, numerous cyber security companies and government agencies have classified the NetWire RAT as a malicious tool and documented instances of the NetWire RAT being used in criminal activity:

a. On December 7, 2016, the New Jersey Cybersecurity & Communications Integration Cell ("NJCCIC") released a

cybersecurity threat profile on NetWire stating: "The NetWire remote access trojan (RAT) has been widely used by cybercriminals since 2012. In September 2016, SecureWorks researchers observed a new version of NetWire that was scraping card data and using a keylogger that can gather data from devices like USB card readers. The trojan is spread through phishing emails with malicious attachments. NetWire can linger for months or years once it's infected...In early 2016, it was used in attacks against banks and healthcare companies. Victims opened Word documents embedded with malicious macros and the RAT downloaded from Dropbox to infect the user. In 2014, Palo Alto Networks uncovered that Nigerian scammers were using NetWire to remotely control infected systems."

b. On November 28, 2016, in a published research and intelligence report titled "NetWire RAT Steals Payment Card Data," SecureWorks Inc. outlined how "threat actors used a remote access trojan with keylogging capabilities rather than traditional point-of-sale malware." The referenced report was issued in response to an "incident response engagement in September 2016, [where] SecureWorks incident response analysts observed payment card data being collected by a generic remote access trojan (RAT) rather than typical memory-scraping malware."

c. On April 18, 2018, "MITRE ATT&CK" added NetWire to its knowledge base of malware tools. "MITRE ATT&CK" documents how NetWire is used by cyber actors, including keylogging, capture of a victim's screen, and other ways to

discover and collect victim system information. Within the article, MITRE ATT&CK described NetWire as a "publicly available, multiplatform remote administration tool (RAT) that has been used by criminal and APT groups since at least 2012."

d. On February 13, 2019, the NJCCIC released an alert stating, "NetWire RAT Makes a Comeback. The NJCCIC recently detected attempts to install the NetWire remote access trojan (RAT) onto State systems."

e. On April 3, 2019, Proofpoint, Inc., an American enterprise security company, released an article titled "Tax-themed Email Campaigns Target 2019 Filers." Within this article, the Proofpoint Threat Insight Team described NetWire's use in an October 2018 phishing campaign which distributed "thousands of messages with attached Microsoft Word documents. The documents contained macros that, when executed, installed NetWire malware." In this campaign, malicious cyber actors imitated legitimate government agencies including the Australian Taxation Office and the Indian government while utilizing spoofed email accounts from services such as Canada Post, New Zealand Inland Revenue Department. These emails included malicious URLs which downloaded Microsoft Office documents which contained the NetWire RAT.

f. On January 23, 2020, "Trend Micro⁵" published an article titled, "NetWire RAT Hidden in IMG Files Deployed in BEC [Business Email Compromise] Campaign."

g. On March 18, 2021, Cybereason, an American cybersecurity technology company, released an article titled

"Cybereason Exposes Campaign Targeting US Taxpayers with NetWire and Remcos Malware." Within this article, the Cybereason Nocturnus Team outlined their detection of a "new campaign targeting US taxpayers with documents that purport to contain tax-related content, ultimately delivering NetWire and Remcos - two powerful and popular RATs." The Cybereason Nocturnus Team also stated the campaign resembled "another campaign in April of 2020 which also delivered the NetWire RAT."

17. On October 20, 2021, the FBI Investigative Team conducted a review of the NetWire profile created and maintained by the Malware Interactive Hunting Service "ANY.RUN." Within this profile, ANY.RUN describes NetWire as an "advanced RAT - it is a malware that takes control of infected PCs and allows its operators to perform various actions. Unlike many RATs, this one can target every major operating system, including Windows, Linux, and MacOS." In addition to a description of the malware, ANY.RUN also provides a "last seen" tracker which lists the latest instance of NetWire observed as October 20, 2021. ANY.RUN outlines the common tactics, techniques, and procedures (TTPs) of NetWire as distribution in "email phishing campaigns in the form of a malicious Microsoft Office document. The victim must enable macros for the RAT to enter an active state. The macros then proceed to download NetWire, allowing the malware to start the execution process."

C. Online Undercover (Covert) Purchase of NetWire

18. On October 5, 2020, an online covert employee of the FBI ("OCE") purchased a one-year license for NetWire through the

SUBJECT DOMAIN. Six versions of NetWire, including an "experimental version," were available for download. That day, after purchasing NetWire on the SUBJECT DOMAIN, the OCE received the license key and provided it to an FBI-LA Computer Scientist ("CS"), who conducted testing and analysis on October 5, 2020, and January 12, 2021. For this analysis and testing, the FBI-LA CS downloaded the latest version of NetWire, v2.1 R7, on an FBI test computer. On October 5, 2020, after successfully activating the licensing and logging in, the FBI-LA CS began to use NetWire's "builder tool" to create a customized RAT for a Windows computer. The FBI-LA CS then deployed and executed the RAT on an isolated FBI lab virtual machine, which was used as a victim machine for testing purposes ("test victim machine"). Upon successful deployment of the RAT from the FBI-LA CS's computer onto the test victim machine, the FBI-LA CS noted the following features available for use remotely from the lab virtual machine to access the infected test victim machine:

- "File Manager" - remotely access files
- "Process Manager" - view and terminate processes at will
- "Applications Manager" - view and terminate computer applications at will
- "Password Recovery" - for web browsers, messaging, applications, and email
- "Keylogger"
- "Remote Shell" - download and execute commands

- "Screen Capture"

On January 12, 2021, the FBI-LA CS conducted additional testing on various features of the same version/hash of NetWire that was tested on October 5, 2020 and compared them to features that a typical legitimate remote access tool would have (such as one used by an Information Technology Department of a company). During this additional testing, the FBI-LA CS again successfully deployed the NetWire RAT from an FBI test computer (mimicking the attacker's computer) onto a separate FBI isolated virtual machine used a test victim machine ("the infected computer"). The FBI-LA CS's computer displayed a control panel ("the NetWire control panel"), which would be the interface used by an attacker to interact with computers infected with the NetWire RAT. The NetWire RAT then connected to the NetWire control panel to establish a network connection between the attacker's computer and the infected computer. After a successful connection was established, the infected computer was listed under "Connections" on the NetWire control panel. Significantly, the FBI-LA CS confirmed that during the entire time of the connection, there were no visible windows or other indications on the infected computer's screen that would alert the user (victim) to the presence of the NetWire RAT. Even after a successful connection, the user (victim) would not know that the NetWire RAT was actively running on their computer and that their computer was being accessed. The FBI-LA CS noted that a typical legitimate remote access tool would alert the user that their computer was now under the control or being monitored

remotely. After the connection was established, the FBI-LA CS tested the following features offered by NetWire and determined the following:

- "File Manager" - This feature allows the attacker to remotely access and download files from the victim's computer, without the victim user's knowledge. The CS tested this feature by creating a sample text file on the infected computer, which was then able to download from the infected computer through the NetWire control panel.
- "Process Manager" - This feature allows the attacker to view currently running processes on the infected computer as well as selectively closed processes, without the victim user's knowledge. The FBI-LA CS tested this feature by opening "Notepad.exe" on the infected computer and then using the "Process Manager" to remotely force "Notepad.exe" to close.
- "Password Recovery" - This feature retrieves passwords stored on the infected computer in various programs, such as web browsers, messaging applications and email accounts, without the victim user's knowledge. The FBI-LA CS tested this feature by saving an email/password combination for a website on Internet Explorer on the infected computer. The CS then used the "Password Recovery" feature, which found and displayed the saved email/password combination from

Internet Explorer. The FBI-LA CS noted that although dubbed as a password "recovery," this feature is inherently malicious because it remotely extracts plain text credentials without notifying the user. The FBI-LA CS explained that typical password recovery would be done by resetting the password and creating a new password. Thus, the FBI-LA CS determined that the "Password Recovery" feature of NetWire is more akin to credential exfiltration (i.e., password theft).

- "Keylogger" - As the name implies, this feature logs and records all keystrokes input from the infected computer's keyboard, without the victim user's knowledge. The FBI-LA CS tested this by typing phrases on the infected computer into a text document, and then saw the exact keystrokes recorded on the NetWire control panel on a test computer.
- "Remote Shell" - This feature allows the attacker to use the infected computer's "Command Prompt" shell (window) without the victim user's knowledge. The attacker can thus use the command prompt to execute arbitrary commands on the infected computer. The FBI-LA CS tested this feature and was able to execute commands on the infected computer.
- "Screen Capture" - This feature allows the attacker to view the screen of the infected computer at the time of the screen capture, without the victim user's knowledge. The

screen capture feature can also be automated to take screen captures at periodic intervals. The FBI-LA CS tested this feature by taking a screen capture of the infected computer and seeing it displayed on the NetWire control panel.

19. The FBI-LA CS emphasized that in all the features tested above, the infected computer never displayed a notice or alert that these actions were taking place. This is contrary to legitimate remote access tools where consent from the user is typically required to perform specific action on the user's behalf. The FBI-LA CS further noted that legitimate remote access tools will typically inform the user via an alert or notice on their screen that their computer is currently being monitored. The FBI-LA CS concluded that in his opinion, the lack of legitimate features for a remote access tool combined with the fact that NetWire was being advertised on Internet hacking forums such as Hackforums shows that NetWire was designed to be a malicious program rather than a legitimate software tool.

D. Victim Reporting Attack Connected to NetWire

20. On August 11, 2021, the FBI Internet Crime Complaint Center (IC3.gov) received a complaint submission from Victim 1 located in the United States. Within the complaint, Victim 1 advised that on or about March 2, 2021, Victim 1 received notice that 12 client tax returns were rejected. A forensic investigation conducted by a third-party cyber security firm determined that on January 26, 2021, a malicious email

attachment installed a trojan (NetWire) which allowed an unknown third party to log keystrokes and take screenshots of data viewed by two employees between January 26, 2021, and March 8, 2021.

E. Registration Information for the SUBJECT DOMAIN

21. On approximately August 14, 2020, the FBI Investigative Team used a DNS tool to identify the registration information and IP address of the SUBJECT DOMAIN. The search revealed the domain was sold by "Namecheap" and the IP address resolved to the web hosting company "Solar Communications GmbH" located in Zurich, Switzerland, at IP address 46.28.206.174. However, the registration information (including name and contact information) for the SUBJECT DOMAIN was anonymized to protect the privacy of the individual(s) registering the domain. Based on the writer's training and experience, cyber actors frequently anonymize registration information to hide their identity to avoid scrutiny by law enforcement.

22. On approximately November 12, 2020, the FBI Investigative Team obtained subscriber information from Namecheap for the SUBJECT DOMAIN, which revealed the following registrant details:

First Name: Tom
Last Name: Maloney
Street Address: Maloney Rd 45
City: Pristina
State/Province, Zip/Postal Code: PR, 0010000
Country: Albania
Email address: tommaloney@protonmail.ch
Phone number: +381-0385958330

23. Through online research of the registrant address listed above, the FBI Investigative Team determined the registrant address for the SUBJECT DOMAIN does not exist. Given these circumstances, the writer believes "Tom Maloney" is a possible alias for the individual operating the SUBJECT DOMAIN.

F. International Movement of Funds in Relation to the SUBJECT DOMAIN

24. The SUBJECT DOMAIN has one or more essential components that require the international movement, or attempted movement, of monetary instruments or funds with the intent to promote unlawful computer intrusion and proliferation of Remote Access Trojan malware.

25. First, because it is a website which uses a domain, the SUBJECT DOMAIN was registered through an Internet registrar. Here, the registrant had to first determine whether the domain WORLDWIREDLABS.COM was available, and then pay a third party, Namecheap, for the privilege of using that specific domain. This is usually a recurring annual payment of funds. The SUBJECT DOMAIN also requires payments to the registry, Verisign, for the use of the ".com" top-level domain.

26. Second, the website also has to be associated with a server from which it actually operates. Known as "hosting," this means that the prospective website operator would have to either establish their own server or pay a third-party hosting service to operate an Internet-connected server on their behalf.

27. Third, because the SUBJECT DOMAIN is operating as a for-profit enterprise, it needs some manner of accepting

payment. For the SUBJECT DOMAIN, one of the listed payment methods is cryptocurrency. Generally, this means that the website uses a third-party service, such as to allow customers to provide payment directly to the operator's wallet via an accepted cryptocurrency, or to convert fiat currencies (such as U.S. dollars) to cryptocurrency. Because the use of such third-party cryptocurrency payment services also requires payment of fees, usually a percentage of transactions, with each customer payment, a small amount of funds is transferred to the third-party payment service.

28. Fourth, the SUBJECT DOMAIN facilitates the purchase of and subscription to the NetWire RAT. The SUBJECT DOMAIN thus facilitates the transfer of funds from the United States and elsewhere to promote the proliferation of the unlawful Remote Trojan Access malware.

29. Through publicly available information and subscriber records, I verified that the SUBJECT DOMAIN was registered with a United States registrar, Namecheap, and the SUBJECT DOMAIN was hosted in Switzerland. I also verified that the SUBJECT DOMAIN is registered with a United States registry, Verisign, as it is a ".com" domain. In this circumstance, a transaction intended to either pay to register the domain or pay to promote the website's illegal activities necessarily caused a transfer of funds into and out of the United States.

30. Through analysis of the SUBJECT DOMAIN in February of 2023, the FBI Investigative Team also identified that the SUBJECT DOMAIN uses a web hosting automation service,

specifically a U.S. company, WHMCS. On WHMCS's website, whmcs.com, WHMCS describes the business as the following: "An automation platform that simplifies and automates all aspects of operating an online web hosting and domain registrar business." As a result, in this case, a transaction intended to procure website automation and management services from the U.S. company WHMCS necessarily caused a transfer of funds into and out of the United States in order to promote the proliferation of unlawful malware. Based on my training and experience, a website hosted internationally (Switzerland) by a non-U.S. administrator, which utilizes U.S. based services, likely required an inbound payment into the United States.

31. Based on the payments to (1) the registrar Namecheap, (2) the registry Verisign, and (3) the hosting service WHMCS; the acceptance of cryptocurrency for payments; and the SUBJECT DOMAIN's facilitation of the purchase of and subscription to the NetWire RAT, there is probable cause to believe that the SUBJECT DOMAIN was involved in and facilitated the international movement of funds into and out of the United States with the intent to promote unlawful computer intrusion via Remote Access Trojan malware.

//

//

//

//

//

//

VII.

CONCLUSION


32. For the reasons stated above, there is probable cause to believe that the SUBJECT DOMAIN is subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 981(b) and (a)(1)(A) because the website is involved in one or more violations of 18 U.S.C. § 1956(a)(2) (International Money Laundering) and done with the intent to promote the underlying specified unlawful activity, namely 18 U.S.C. § 1030(a)(5)(A) (Unauthorized Impairment of a Protected Computer) as defined by 18 U.S.C. § 1956(c)(7)(D).

33. Furthermore, there is probable cause to believe that the SUBJECT DOMAIN is subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 1030(i)(1)(A) because the SUBJECT DOMAIN constitutes personal property used or intended to be used to facilitate the commission of attacks against unwitting victims for the express purpose of preventing the victims from properly using the Internet, in violation of 18 U.S.C. § 1030(a)(5)(A) (Unauthorized Impairment of a Protected Computer).

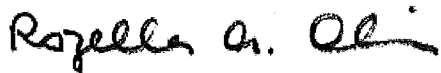
34. In addition, the SUBJECT DOMAIN is subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 982(b)(1), and 21 U.S.C. § 853(f), because there is probable cause to believe that a protective order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the property for forfeiture because there is reason to believe that the property is under the control of the targets of this

investigation, who cannot reasonably be relied upon to abide by an order to maintain the property in substantially the same condition as it is at the present time, in order to ensure that it will be available for forfeiture. More particularly, providing notice may allow the targets to frustrate further efforts of law enforcement by transitioning their enterprise and infrastructure to jurisdictions beyond the reach of United States law enforcement.

/s/


Task Force Officer
FBI

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 3rd day of March __, 2023.



UNITED STATES MAGISTRATE JUDGE
HON. ROZELLA A. OLIVER

Attachment A

SUBJECT DOMAIN Controlled by Verisign

With respect to the following **SUBJECT DOMAIN**,
WORLDWIREDLABS.COM, Verisign, Inc., located at 12061 Bluemont
Way, Reston, VA 20190, which is the domain registry (the
"Subject Registry"), shall take the following actions to effect
the seizure of the **SUBJECT DOMAIN**:

1. Take all reasonable measures to redirect the
SUBJECT DOMAIN to substitute servers controlled by the FBI, by
associating the authoritative name server for the **SUBJECT DOMAIN**
to the following authoritative name servers:

- (a) ns1.seizedservers.com
- (b) ns2.seizedservers.com
- (c) Any new authoritative name server to be
designated by a law enforcement agent in writing,
including e-mail, to the Subject Registry

2. Take all reasonable measures to propagate the
necessary changes through the Domain Name System as quickly as
practicable;

3. Prevent any further modification to, or transfer
of, the **SUBJECT DOMAIN** pending transfer of all right, title, and
interest in the **SUBJECT DOMAIN** to the United States upon
completion of forfeiture proceedings, to ensure that changes to
the **SUBJECT DOMAIN** cannot be made absent court order or, if

forfeited to the United States, without prior consultation with the FBI or Department of Justice;

4. Provide reasonable assistance in implementing the terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

5. The Government will display a notice on the website to which the **SUBJECT DOMAIN** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text with the potential addition of international partners):

"This Website Has Been Seized

as part of a coordinated law enforcement action taken against the NetWire Remote Access Trojan.

This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant pursuant to 18 U.S.C. § 981(a)(1)(A) and (b), 18 U.S.C. § 982(b)(1), 18 U.S.C. § 1030(i)(1)(A) and 21 U.S.C. § 853, issued by the United States District Court for the Central District of California as part of a joint international law enforcement operation and action by: the United States Attorney's Office for the Central District of California, the Federal Bureau of Investigation, Croatia Ministry of the Interior Criminal Police Directorate, Europol European Cybercrime Center, Zurich Cantonal Police, and the Australian Federal Police"