



Chinese Businessman Indicted in Vast Hacking Scheme Accused of Infecting Millions of Computers to Sell Access to IP Addresses

Federal prosecutors have unsealed a sweeping indictment against YunHe Wang, a Chinese businessman accused of orchestrating an audacious global hacking operation that infected millions of computers in order to sell access to their IP addresses to cybercriminals.

The Plot: Creating a Black Market for Hacked IP Addresses

According to the indictment, from 2011 to 2022, Mr. Wang and unnamed co-conspirators developed malware that would silently install "backdoors" on mainly residential computers, allowing the perpetrators to commandeer the devices' IP addresses without the owners' knowledge.

Prosecutors say Mr. Wang then sold access to this vast trove of over 19 million compromised IP addresses through his online platform called 911 S5, catering to cybercriminals seeking to mask their identities for nefarious purposes like financial fraud and child exploitation. Customers could allegedly handpick IP addresses by city, state or country.

"The scope and audacity of this operation is striking," said [Prosecutor quote]. "The suspect treated people's home computers as his own personal inventory to exploit for profit."

A Fortune Amassed Through Ill-Gotten Gains

The indictment portrays the 911 S5 service as a gold mine for Mr. Wang, generating over \$99 million in revenue from 2018 to 2022 alone. Prosecutors say he used shell companies and enlisted help from associates to launder the proceeds and invest in luxury real estate, cars and watches around the world.

Among the assets tied to Mr. Wang are a fleet of cars including a Ferrari, a Rolls-Royce and multiple BMWs, along with exclusive properties in Singapore, Thailand, China, the U.S. and elsewhere. Prosecutors are seeking the forfeiture of this sprawling empire of big-ticket items.

Tracing an Elaborate Conspiracy

The indictment offers an inside look at what authorities describe as a sophisticated, multi-pronged scheme.

To distribute his custom malware widely while evading detection, Mr. Wang allegedly employed an array of technical trickery: using encryption services, bundling malicious code with pirated software, and paying affiliates to install it on the sly.

Prosecutors say he focused on infecting computers in wealthy nations like the U.S. to maximize resale value to cybercriminals, claiming the plot ensnared over 600,000 American devices, including hundreds in the Eastern District of Texas where the case is filed.

Cybercriminals then used proxied IP addresses purchased from 911 S5 to conceal their true originating IP addresses and locations, and anonymously commit a wide array of offenses.

These offenses including financial crimes, stalking, transmitting bomb threats and threats of harm, illegal exportation of goods, and receiving and sending child exploitation materials. Since 2014, 911 S5 allegedly enabled cybercriminals to bypass financial fraud detection systems and steal billions of dollars from financial institutions, credit card issuers, and federal lending programs.

READ THE ORIGINAL INDICTMENT ON FOLLOWING PAGES

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

FILED

MAY 10 2023

CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF TEXAS

UNITED STATES OF AMERICA

v.

YUNHE WANG,
a/k/a “Jack Wan,” “Jack Wang,” “Williams
Tang,” “Jack Wong,” “Williams Long,” and
“Tom Long”

Defendant.

Case No. 4:23CR 101
Judge Mazzant

Filed Under Seal

INDICTMENT

THE UNITED STATES GRAND JURY CHARGES:

General Allegations

At all times relevant to this Indictment:

1. Defendant YunHe Wang (WANG), aka “Jack Wan,” “Jack Wang,” “Williams Tang,” “Jack Wong,” “Williams Long,” and “Tom Long,” was a national of the People’s Republic of China and obtained his citizenship by investment to St. Kitts and Nevis.

2. As early as 2011, defendant WANG and others known and unknown to the Grand Jury began developing, and thereafter and throughout the pendency of the scheme, distributed malicious software (malware¹) such as ProxyGate, MaskVPN, DewVPN, and Shine VPN, with the intent to infect residential² computers worldwide—including in the Eastern District of Texas—

¹ As used in this Indictment, “malware” was software designed to disrupt, damage, or help an unauthorized user gain access to a computer or network by bypassing the antivirus software and installing a persistent backdoor. The terms malware and malicious software are used interchangeably in this indictment.

² “Residential proxy services” generally attempt to obtain access to residential computers and IP addresses; however, not all computers and IP addresses available within 911 S5 are residential computers or IP addresses. This is primarily because there are times when computers related to enterprise networks can be found on a residential

with a backdoor³ (i.e., an undocumented way of gaining access to a computer system), allowing WANG to maintain a persistent presence in all the compromised computers.

3. In approximately 2014, WANG created and launched an illicit residential proxy service called “911 S5” through which he sold to customers access to the Internet Protocol⁴ (IP) addresses associated with the network of compromised computers.

4. Defendant WANG used the proceeds received from customers of 911 S5 to purchase property in the United States, St. Kitts and Nevis, Singapore, Thailand, China, and the United Arab Emirates. At various times, defendant WANG resided in some of the properties he purchased in Singapore, Thailand, and China.

5. In addition to 911 S5, defendant WANG owned and operated several companies including, but not limited to, International Media, Ltd., incorporated in the British Virgin Islands; Eternal Code Ltd., incorporated in Singapore; Gold Click Limited, incorporated in the United Kingdom; and Gold Rock LLC and Hard Stone LLC, both registered in the State of Washington.

6. WANG also was affiliated with additional companies including Spicy Code Company Limited, Oasis Capital Company Limited, Hairimo Company Limited, Global Media Company Limited, Cyber Safe Company Limited, and Lily Suites Company Limited, all registered in Thailand.

proxy service network, due to how computers become compromised and the fact that some individuals use their personal devices and both their home and work environments. References to “residential” computers in this Indictment refer to computers included in the 911 S5 residential proxy service, whether they are in fact residential or not.

³ As used in this Indictment, a “backdoor” was a type of malware that negates normal authentication procedures to access a system. Backdoors were used for securing remote access to a computer allowing others to execute code or control the computer remotely.

⁴ An Internet Protocol (IP) address was a unique string of characters that identified a network or a device on the internet. An IP address acts as an identifier and locating protocol for the billions of devices connected to the internet, and an IP address’s exclusivity of use is essential for the internet to properly function. A static IP address did not change and was unique to that client. A dynamic IP address was an IP address that could be reassigned, but only was assigned to one unique client at a time.

7. WANG's companies were shell companies he used to conceal the identity and illegitimate nature of his 911 S5 service and its related proceeds.

8. Customers of 911 S5 used WANG's proxy service to conceal their identities during the commission of cyber-enabled criminal activity worldwide, including bank fraud, loan fraud, credit card fraud, bomb threats, and child exploitation crimes.

9. WANG took measures to ensure that the owners of the compromised computers would not detect or otherwise be aware that their devices had been infected or that their IP addresses were being sold to and used by 911 S5 customers around the world.

10. By such measures, WANG also intended to prevent the Internet Service Providers⁵ (ISPs), financial institutions, and online retailers from detecting whether a particular IP address was being exploited by a 911 S5 customer.

Overview of the Defendant's Criminal Scheme

11. From in or around 2014 until on or about July 28, 2022, WANG operated the 911 S5 proxy service with the intent to sell to customers internet connectivity through intermediary, internet-connected devices, in this case illegally compromised personal residential computers. The owners and/or users of the personal computers did not know that their devices had been compromised, and that other individuals, unknown to them, were accessing and using the IP addresses connected to their devices without their permission, to engage in criminal activities online.

⁵ An Internet Service Provider (ISP) is a company that provides access to the internet to both residential and business customers. ISPs leased to their customers the right to the exclusive use of IP addresses or blocks of IP addresses, either static or dynamic) to enable their customers' access to the internet. A residential ISP leased the right to exclusive use of IP addresses to residential customers. The IP addresses leased by the ISPs were allocated by registries to the ISPs for their right to exclusive use, subject to the terms of the agreement with the registry.

12. WANG and others known and unknown to the Grand Jury developed malware which, when downloaded, would infect the computer with a persistent⁶ backdoor and enable WANG and 911 S5 to access and control the compromised computer and its resources, such as the associated residential IP address. The installed malware would enable the transmission of programs, information, codes, and commands between the compromised computers and servers controlled by WANG and 911 S5. In this manner, the network of compromised computers formed a botnet.⁷ WANG surreptitiously propagated the malware through Virtual Private Network⁸ (VPN) programs; torrent⁹ distribution models run by WANG; and pay-per-install¹⁰ services that bundled WANG's malware with other program files, including pirated versions of licensed software or

⁶ "Persistence" referred to various ways that malware tried to maintain access to a system. Persistence allowed malware to relaunch itself automatically following a predetermined event, such as a device startup, user login, or other events that malware 'listened' for.

⁷ A "bot" was a computer infected with malware without the knowledge of the computer's user and controlled remotely by another individual. For purposes of this Indictment, all "bots" were infected computers, and all infected computers were bots. A "botnet" was an interconnected network of bots.

⁸ A VPN is an encrypted connection over the Internet from a device to a network. Utilizing a VPN service offers users safety, privacy, and anonymity when transmitting data over the internet. VPN services can also mask the location from which a connection originates, but a legitimate VPN service will show that the connection is originating from a VPN server, and not a residential IP address.

⁹ A torrent is a small text file. Torrent distribution or "torrenting" refers to sending and receiving files via a decentralized peer-to-peer file-sharing protocol known as BitTorrent, rather than via a centralized server. This is a particularly useful tool for distributing large media files because the protocol breaks up the file into smaller portions and the user computers share them among each other.

¹⁰ A Pay-Per-Install (PPI) business model was initially used to distribute advertisements, but as used in this Indictment, was a means to spread spyware and malware. PPI was most often used by developers who wished to spread their malware or adware over the internet. The developer would pay a PPI provider to spread his or her malware or adware a certain number of times within a particular geographic area, such as a country or continent. PPI "affiliates" would work with the PPI provider to spread malware or adware, earning money after enabling a certain number of installs. The affiliates received a file—typically malware or adware—from the PPI provider. The affiliates then secreted the PPI-provided file within another program hosted on their site or server, so users who downloaded the program would unwittingly install the malware or adware. The affiliates were paid after the affiliates reached a certain number of installs of the malware or adware received from the PPI provider.

copyrighted materials that were available online for free downloads without authorization of the copyright holder.

13. By distributing the malware and selling the use of the compromised IP addresses, WANG defrauded and deprived the ISPs and the ISPs' residential customers, the computer owners, of their rights to the exclusive use of the IP addresses. The persistent backdoors installed via WANG's malware caused the compromised computers to remain infected indefinitely. Although 911 S5's services ceased operations in July 2022, the unwitting infected computers remain actively compromised and therefore the botnet remains available to be reconstituted into a new illicit proxy service at any time.

14. WANG amassed a worldwide inventory of more than 19 million unique IP addresses that WANG offered to his 911 S5 customers for a fee. This botnet included approximately 613,841 unique IP addresses in the United States. Between on or about August 18, 2018, and July 21, 2022, WANG and 911 S5 exploited approximately 43,884 unique IP addresses in Texas. Between in or about April 2020 through in or about July 2022, WANG's malware infected approximately 346 known computers in the Eastern District of Texas, propagated from downloads of either WANG's ProxyGate, Mask VPN, or DewVPN software.

15. The use of a proxied IP address purchased from 911 S5 enabled a cybercriminal's ability to conceal his or her true originating IP address and location. Cybercriminals have used the 911 S5 service to bypass financial fraud detection systems in the United States and elsewhere and have successfully stolen billions of dollars from financial institutions, credit card issuers and accountholders, and federal lending programs since 2014. For example, in evaluating suspected loss due to fraud against pandemic relief programs, the United States estimates 560,529 unique claims originated from IP addresses exploited and trafficked by 911 S5, with a related loss amount

of approximately \$5,919,590,219.00. Millions more were similarly identified by financial institutions in the United States as loss originating from IP addresses compromised by 911 S5. Cybercriminals around the world also used the 911 S5 service to enable other criminal activity such as bomb threats and child exploitation. Because WANG offered his inventory of IP addresses in such a way that could be filtered by geographic location, cybercriminals using the 911 S5 service were able to select by city, state, zip code, or country exactly the IP addresses through which they wanted to connect to the internet.

16. WANG intended for his malware to be surreptitiously installed and he and others known and unknown to the Grand Jury actively worked to conceal the presence of the malware from unwitting computer owners through illegal encryption services, taking coercive measures to have companies whitelist his malicious software, and other subversive measures.

17. WANG knew that his 911 S5 customers used the service for illegal activity and therefore focused his malware installations on computers in wealthy countries like the United States to make his inventory more valuable to his 911 S5 customers.

18. Between approximately 2018 and in or about July 2022, WANG received more than \$99,000,000 USD from his sales of the hijacked proxied IP addresses through his 911 S5 operation.

Count One

Violation: 18 U.S.C. § 371 (18 U.S.C §
1030(a)(5)(A))
(Conspiracy to Commit
Computer Fraud)

19. Paragraphs one through eighteen are incorporated by reference as if fully set forth herein.

20. From in or about 2011 and continuing through on or about July 28, 2022, in the Eastern District of Texas and elsewhere, defendant WANG did knowingly and intentionally conspire with other persons known and unknown to the Grand Jury to commit an offense against the United States, that is, to knowingly cause the transmission of a program, information, code, and command, and, as a result of this conduct, intentionally caused damage without authorization to a protected computer, and the offense caused loss from the defendant's course of conduct aggregating at least \$5,000 in value to one or more persons during a one-year period, and the offense caused damage affecting 10 or more protected computers during a one-year period.

The Manner and Means of the Conspiracy to Commit Computer Fraud

It was part of the conspiracy and the scheme and artifice that:

21. WANG and others known and unknown to the Grand Jury developed functional VPN software, including ProxyGate, MaskVPN, DewVPN, and Shine VPN, that contained secreted malicious program codes.

22. WANG offered his VPN software for free online and hid the malicious properties from those users that intentionally downloaded what they believed to be a legitimate VPN program.

23. In order to further facilitate the distribution of his malware, WANG and his co-conspirators also caused the malware to be secreted in pirated versions of licensed software or copyrighted materials that computer owners or users could download for free without authorization of the copyright holder, and then spread those files using torrents. In addition, WANG employed Pay-Per-Install services to facilitate the distribution of his malware online.

24. When executed, the malware transmitted codes and commands to the computer that bypassed the virus detection software and altered the computers by installing backdoors onto the

computers without the knowledge or consent of the computer owners or users. Those backdoors allowed WANG and 911 S5 to access and control the internet connected infected computers indefinitely, impairing the integrity and availability of the compromised computers.

25. No matter the method of distribution, WANG's software installed the backdoor-creating malware onto residential, Windows-based computers, without the knowledge or consent of the computer owners or users.

26. From at least in or about 2014 through in or about July 2022, WANG managed and controlled approximately 150 dedicated servers worldwide, approximately seventy-six (76) of which he leased from United States-based online service providers. Using the dedicated servers, WANG was able to deploy and manage applications, command and control the infected devices, operate his 911 S5 service and provide to paying customers access to the proxied IP addresses associated with the infected devices.

27. WANG and 911 S5 further exploited the computers by selling access to the IP addresses assigned to the computers to 911 S5 customers, again without the knowledge or consent of the computer owners or users, and without the knowledge or consent of the Internet Service Provider providing the internet connectivity.

28. Each time a paying customer used a 911 S5-proxied IP address, the 911 S5 service caused data to be transmitted to and received by the internet-connected infected computers, further impairing the integrity and availability of the compromised computers.

Overt Acts

In furtherance of the conspiracy, and to effect the objects thereof, WANG and others known and unknown to the Grand Jury did commit and cause to be committed the following overt acts in the Eastern District of Texas, and elsewhere:

29. In or about May 2014, WANG registered or caused to be registered the official domain for the 911 S5 website, 911.re. WANG also registered or caused to be registered the mirrored domains 911.gg, 911S5.com, and 911S5.org.

30. From in or about 2014 through in or about July 2022, WANG administered the website for 911 S5, which was available to customers around the world, including within the Eastern District of Texas.

31. By in or about July 2022, WANG had infected, or caused to be infected through his malicious software, millions of computers which then made available approximately 19 million IP addresses worldwide to 911 S5 customers. Between in or about April 2020 through in or about July 2022, WANG infected or caused to be infected through his malicious software MaskVPN or DewVPN, approximately 346 computers in the Eastern District of Texas alone.

32. In or about January 2021, WANG and 911 S5 received a Bitcoin payment from a person known to the Grand Jury for the purchase of some proxied IP addresses. In or about April 2021, using the 911 S5 service, the purchaser connected five times through a proxied IP address located in Frisco, Texas, in the Eastern District of Texas, associated with a device, referred to herein as “xxxxEE599,” that previously had been infected with the malicious software MaskVPN without the knowledge or consent of the owner or user of the device.

33. On or about March 16, 2021, WANG infected or caused to be infected with MaskVPN malware a Lenovo ThinkPadX1 laptop, also known as the device xxxxEE599, owned by a Frisco, Texas resident whose initials are “P.W.”

34. On or about November 2, 2020, WANG infected or caused to be infected with MaskVPN malware an Acer Nitro 5 computer owned by a Frisco, Texas resident whose initials are “B.T.”

35. On or about January 25, 2021, WANG infected or caused to be infected with MaskVPN malware an ASUS laptop computer owned by a McKinney, Texas resident whose initials are “J.J.”

36. On or about February 8, 2021, WANG infected or caused to be infected with MaskVPN malware a Toshiba laptop computer owned by a Denton, Texas resident whose initials are “P.A.”

37. On or about February 25, 2021, WANG infected or caused to be infected with MaskVPN malware a desktop computer owned by a Little Elm, Texas resident whose initials are “H.R.”

38. On or about June 8, 2021, WANG infected or caused to be infected with DewVPN malware a Neo Forza computer owned by an Allen, Texas resident whose initials are “L.I.”

39. On or about November 13, 2021, WANG infected or caused to be infected with MaskVPN malware a desktop computer owned by an Allen, Texas resident whose initials are “A.A.”

All in violation of 18 U.S.C. § 371 (18 U.S.C. § 1030(a)(5)(A)).

Count Two

Violation: 18 U.S.C. § 1030(a)(5)(A)
(Computer Fraud)
18 U.S.C. § 2
(Aid and Abet)

40. Paragraphs one through eighteen and Count One are incorporated by reference as if fully set forth herein.

41. Between on or about November 2, 2020, and on or about July 22, 2022, in the Eastern District of Texas and elsewhere, defendant YunHe WANG, aided and abetted by unnamed

co-conspirators known and unknown to the Grand Jury, knowingly caused the transmission of a program, information, code, and command, and as a result of this conduct, intentionally caused damage without authorization to a protected computer, to wit, by and through his malware distribution, WANG compromised or caused to be compromised at least 236 computers in the Eastern District of Texas, and in doing so, made the compromised computers available to 911 S5 customers, and the offense caused loss from the defendant's course of conduct aggregating at least \$5,000 in value to one or more persons during a one-year period, and the offense caused damage affecting 10 or more protected computers during a one-year period.

All in violation of 18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B), and 2.

Count Three

Violation: 18 U.S.C. § 1349 (§ 1343)
(Conspiracy to Commit Wire
Fraud)

42. The allegations set out in paragraphs one through eighteen are incorporated by reference as if fully set forth herein.

43. Between in or about 2011 through on or about July 28, 2022, in the Eastern District of Texas and elsewhere, defendant YunHe WANG, and other unnamed co-conspirators known and unknown to the Grand Jury, did knowingly and intentionally conspire and agree 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 to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce certain writings, signs, signals, and sounds in furtherance of such scheme and artifice, contrary to Title 18, United States Code, Section 1343.

The Object of the Conspiracy and the Scheme and Artifice

44. It was the object of the conspiracy and the scheme and artifice that WANG and others known and unknown to the Grand Jury would develop and spread malware that acquired access to IP addresses worldwide through material omissions, false representations, and false pretenses for the purpose of offering access to and use of the IP addresses to other individuals unknown to the Grand Jury, and that said conduct would result in financial benefit to WANG.

The Manner and Means of the Conspiracy and the Scheme and Artifice

It was part of the conspiracy and the scheme and artifice that:

45. From in or about 2011 and continuing until in or about July 2022, WANG and others known and unknown to the Grand Jury (co-conspirators) developed and administered ProxyGate, MaskVPN, DewVPN, and Shine VPN, among other malware, that would silently install malicious program codes onto primarily residential, Windows-based computers, and those malicious installations would place a backdoor onto the computer without that computer owner's or user's knowledge or consent. That backdoor would allow WANG to access and use that unwitting computer owner's or user's IP address to access the internet without the knowledge or consent of the computer owner or user or the Internet Service Provider.

46. WANG and his co-conspirators distributed the malware in order to build WANG's botnet by transmitting signals and sounds, to wit, the above-described malicious program codes, through interstate and foreign wire communications, from places outside the state of Texas or outside the United States, to other places worldwide, including to at least 346 computers within the Eastern District of Texas.

47. WANG and his co-conspirators took efforts to develop their malware in a way that would avoid detection by antivirus programs. For example, in and around 2019, WANG hired a

co-conspirator known as a “crypter” to develop encryption for WANG’s malware so the malware would avoid detection by antivirus programs, thus facilitating the rapid growth of his botnet.

48. Beginning in and about 2020, WANG transitioned away from his ProxyGate program because it was detected too frequently by antivirus programs. Instead, WANG focused on spreading his MaskVPN and DewVPN malware. WANG also utilized Pay-Per-Install and other services to distribute his malware by secretively bundling it with other seemingly innocuous software programs and files.

49. As of in or about July 2022, WANG had amassed a collection of more than 19 million IP addresses by spreading his malware to computers worldwide. At any given time during the operation of 911 S5, WANG offered access to at least 200,000 of those 19 million IP addresses, on a rotating basis.

50. Throughout the duration of the conspiracy and the scheme and artifice, WANG appropriated the infected computers’ IP addresses and offered them for use, for a fee, through his 911 S5 proxy service. Customers of 911 S5 would pay per connection via cryptocurrency or select credit card payment processors to wallets and accounts controlled by WANG.

51. 911 S5 customers could select the IP addresses to which they wanted to connect by choosing from particular cities, states, zip codes, countries, or ISPs, making it appear that the 911 S5 internet activity was originating from the exploited residential computer rather than the 911 S5 customer’s true location.

52. WANG’s scheme and artifice thus deprived the exploited computer owners of the right to exclusive use of the IP addresses they leased for a fee from the ISPs, and also deprived the related ISPs of the right to exclusive use of the IP addresses allocated and assigned to them, for which they had care, custody, and control.

53. Such conduct also affected at least one financial institution that was insured by the Federal Deposit Insurance Corporation and caused financial loss.

In violation of 18 U.S.C. § 1349.

Count Four

Violation: 18 U.S.C. § 1956(h)
(Conspiracy to Commit
Money Laundering)

54. Paragraphs one through fifty-three are incorporated by reference as if fully set forth herein.

55. Beginning in or about 2018 and continuing to on or about July 28, 2022, both dates being approximate and inclusive, in the Eastern District of Texas and elsewhere, defendant YunHe WANG willfully and knowingly conspired and agreed with others known and unknown to the Grand Jury to commit certain offenses under Title 18, United States Code, Section 1956, namely, to knowingly conduct and attempt to conduct financial transactions affecting interstate commerce, which transactions involved the proceeds of specified unlawful activity, that is, computer fraud, in violation of Title 18, United States Code, Section 1030(a)(5)(A), and wire fraud, in violation of Title 18, United States Code, Section 1343, and knowing, while conducting and attempting to conduct such financial transactions, that the property involved in the financial transactions represented the proceeds of some form of unlawful activity and knowing that the transaction was designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of said specified unlawful activity, in violation of 18 U.S.C. § 1956(a)(1)(B)(i).

Manner and Means

It was part of the conspiracy that:

56. WANG illegally compromised computers and residential IP addresses in the Eastern District of Texas and elsewhere and added those IP addresses to his 911 S5 inventory;

57. WANG received payments, which consisted of proceeds of computer fraud and wire fraud offenses, from customers in the Eastern District of Texas and elsewhere for access to the residential IP addresses WANG made available through his illicit 911 S5 service;

58. WANG avoided directly associating his name with financial institutions in order to conceal the source of his funds, and himself as the true beneficiary of the account activity;

59. WANG directed co-conspirators "J.L." and "Y.Z." to open accounts at various financial institutions and directed J.L.'s and Y.Z.'s cryptocurrency conversion and purchase of real estate for WANG's benefit, all using proceeds of computer fraud and wire fraud offenses;

60. On or about January 24, 2019, while in China, J.L. opened U.S.-based HSBC Bank accounts at the request of WANG, to receive proceeds of computer fraud and wire fraud offenses, while misrepresenting the source of the funds that would be deposited into the account, in order to disguise the nature, source, ownership, and control of the criminal proceeds of the unlawful activity that were subsequently deposited into the account;

61. Between in or about June 2019 and in or about October 2021, J.L. and others helped WANG transfer approximately \$13 million USD of WANG's criminal proceeds through various bank accounts to in order to conceal their source;

62. Between in or about June 2019 and in or about July 2022, WANG, J.L., and Y.Z. made payments to server providers, thereby promoting the carrying on of the Wire Fraud and computer fraud described in Counts Two and Three.

All in violation of 18 U.S.C. § 1956(h).

NOTICE OF INTENTION TO SEEK FORFEITURE

63. The allegations contained in this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to 18 U.S.C. § 981(a)(1)(A) and (C) and 28 U.S.C. § 2461(c), § 982(a)(1), § 982(a)(2)(A) and (B) and § 1030(i). Specifically, the allegations contained in Counts One, Two, and Three of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to 18 U.S.C. § 1030(i), § 982(a)(2), 18 U.S.C. § 981(a)(1)(C), and 28 U.S.C. § 2461(c), and the allegations contained in Count Four of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to 18 U.S.C. § 981(a)(1)(C), 28 U.S.C. § 2461(c), and § 982(a)(1).

64. Upon conviction of one or more of the offenses in violation of 18 U.S.C. § 371, § 1030, and § 1349/1343, as set forth in Counts One, Two, and Three of this Indictment, respectively, defendant YunHe WANG shall forfeit to the United States of America, pursuant to 18 U.S.C. § 1030(i), § 981(a)(1)(C), § 982(a)(2)(A), § 982(a)(2)(B), and 28 U.S.C. § 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the offense or offenses of conviction. Upon conviction of one or both offenses in violation of 18 U.S.C. § 1030 as set forth in Counts One and Count Two of this Indictment, defendant YunHe WANG shall forfeit to the United States of America, pursuant to 18 U.S.C. § 1030(i) any personal property used or intended to be used to commit the offense or offenses of conviction. Upon conviction of the offense in violation of 18 U.S.C. § 1956(h) as set forth in Count Four of this Indictment, defendant YunHe WANG shall forfeit to the United States of America, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), and § 982(a)(1), any property, real or personal, involved in the offense, or any

property traceable to such property. The property to be forfeited includes, but is not limited to, the following:

- (a) 2022 Ferrari F8 Spider S-A Index Mark & Regis. No. SNF2421H, Chassis No: ZFF93LMC000276844
- (b) BMW i8, temporary Thai license plate u-7866
- (c) BMW X7 M50d, Engine No. B57s/G07, Chassis No. LB41418
- (d) Rolls Royce, blue color, Chinese license plate A.5MM59
- (e) One (1) watch: Patek Philippe 5304301R
- (f) One (1) watch, Patek Philippe Grand Complications Self-Winding 5374/300P
- (g) One (1) watch: Audemars Piguet 15416CE Openworked Skeleton
- (h) One (1) watch: Audemars Piguet 26585CE, Royal Oak Perpetual Calendar Openworked
- (i) One (1) watch, Audemars Piguet Royal Oak Jumbo Extra Thin
- (j) Any and all cryptocurrency seized from any electronic device or wallet address attributable to YunHe WANG, including the following offline wallet addresses (only first eight characters revealed):

bc1q05ak	bc1qh3lw	bc1qu5vn
bc1q362n	bc1ql526	bc1qv4kr
bc1q3ael	bc1ql7rn	bc1qw8ev
bc1q49ax	bc1qlfpg	0x6D5ba3
bc1q6w46	bc1qlml	0x6D5ba3
bc1q7hhd	bc1qnykk	bc1qrskw
bc1q7xfq	bc1qnyl4	0xE1D865
bc1q9ua9	bc1qte9r	bnb136ns
bc1qakyc	bc1qtrrf	
bc1qgffx	bc1qtsl3	

- (k) All monies, funds, and credits on deposit at CIMB BANK accounts held in the name of "International Media Ltd.," including account numbers 20007786629 (USD) & 2000778650 (SGD)
- (l) All monies, funds, and credits on deposit at Citibank Singapore Bank account, styled as "WANG YUNHE," account number 0305968543
- (m) All monies, funds, and credits on deposit at Krungthai Bank, including but not limited to account number xxx-x-xx241-4, held in the name of YunHe Wang

- (n) All monies, funds, and credits on deposit up to \$1,796,983.83 USD plus 500,000 Thai Bhat at Krungrsi Bank, account number 628-1-4045-5, held in the name of Yanni Zheng
- (o) All monies, funds, and credits on deposit at Krungsri Bank, account number 628-1-33353-4, held in the name of Spicy Code
- (p) All monies, funds, and credits on deposit at Kasikorn Bank, account number 058-8-23920-9, held in the name of YunHe Wang
- (q) All monies, funds, and credits on deposit up to 680,000 Thai Bhat from Kasikorn Bank, account number 070-8-71460-X, held in the name of Yanni Zheng
- (r) All monies, funds, and credits on deposit at Kasikorn Bank, account number 076-2-77460-7, held in the name of Spicy Code
- (s) All monies, funds, and credits on deposit up to 2,910,000 at Siam Commercial Bank, account number 415-0-79500-4, held in the name of Shigeru Okubo
- (t) All monies, funds, and credits on deposit at Siam Commercial Bank, account number 626-200229-3-840, held in the name of Spicy Code Co., Ltd.
- (u) All monies, funds, and credits on deposit at Siam Commercial Bank, account number 626-200230-8-826, held in the name of Spicy Code Co., Ltd.
- (v) All monies, funds, and credits on deposit at Siam Commercial Bank, account number 626-254368-8, held in the of Spicy Code
- (w) All monies, funds, and credits on deposit at First Financial Northwest Bank, account number 328256, in the name of Hard Stone LLC
- (x) All monies, funds, and credits on deposit at First Financial Northwest Bank, account number 305431, in the name of Gold Rock LLC
- (y) All monies, funds, and credits on deposit at First Financial Northwest Bank, account number 244471, in the name of YunHe Wang
- (z) All monies, funds, and credits on deposit at First Financial Northwest Bank, account number 248842, in the name of Gold Rock LLC
- (aa) All monies, funds, and credits on deposit at First Financial Northwest Bank, account number 244300; in the name of Jingping Liu
- (bb) 1432 E. 47th St., Tacoma, Washington
- (cc) 1434 E. 47th St., Tacoma, Washington
- (dd) 1421. E. 47th St., Tacoma, Washington
- (ee) 1423 E. 47th St., Tacoma, Washington
- (ff) 21 Angullia Park, #27-03 Singapore 239974

- (gg) 366/112 Moo 12, Majestic Residence, Pratamnak, Pattaya, Chonburi, Thailand 20150
- (hh) 17/5 and 17/9 Moo 3, Huai Yai, Bang Lamung, Chonburi, Thailand 20150
- (ii) Centara Azure Hotel Pattaya, 198/31 Moo 9, Nongprue, Banglamung, Chonburi, Thailand 20150
- (jj) 98/272, 31st Floor, Building B, Reflection Jomtien Beach Pattaya, 98/1 Moo 1 Jomtien Beach Road, Najomtien, Sattahip, Chonburi, Thailand 20250
- (kk) 98/273, 31st Floor, Building B, Reflection Jomtien Beach Pattaya, 98/1 Moo 1 Jomtien Beach Road, Najomtien, Sattahip, Chonburi, Thailand 20250
- (ll) 98/274, 31st Floor, Building B, Reflection Jomtien Beach Pattaya, 98/1 Moo 1 Jomtien Beach Road, Najomtien, Sattahip, Chonburi, Thailand 20250
- (mm) 98/86 Unit 45A2. Tower A, Reflection Jomtien Beach Pattaya, 98/1 Moo 1 Jomtien Beach Road, Najomtien, Sattahip, Chonburi, Thailand 20250
- (nn) Ocean Horizon Beachfront Condo Pattaya, No. D-511, 10 224 Moo 2, Na Jomtien, Na Chom Thian, Sattahip, Chonburi, Thailand 20250
- (oo) Ocean Horizon Beachfront Condo Pattaya, No. D-512, 10 224 Moo 2, Na Jomtien, Na Chom Thian, Sattahip, Chonburi, Thailand 20250
- (pp) Wong Amat Tower Club Royal Condominium, No. 2802, Moo 5 223/9 Bang Lamung, Chonburi, Thailand 20150
- (qq) Supalai Mare Pattaya, No. 818/997, Moo 12, 818/15 Thepprasit Road, Pattaya City, Banglamung, Chonburi, Thailand 20150
- (rr) Grand Solaire Pattaya, No. 2531, Thappraya Road, Pattaya City, Banglamung, Chonburi, Thailand 20150
- (ss) Ocean Marina Condos, No. 28D2, Ocean Marina Condos – San Marino, 274 Moo 4, Sukhumvit Highway, Najomthien, Sattahip, Chonburi, Thailand 20250
- (tt) Riviera Monaco Condominium, No. 4001, NaJomtien Soi 4 NaJomtien, Sattahip, Chonburi, Thailand 20250
- (uu) Unit Number: C2 – 201, Heldon’s Estate Hotel & Residences, 95X2+2J4, Newton Ground, St. Kitts & Nevis
- (vv) Dubai Hills Estates, Executive Residence #06-608, Tower A, Dubai, United Arab Emirates
- (ww) The following domains: 911.re, 911.gg, maskvpn.cc, 911s5.net, 911s5.org, 911s5.com, maskvpn.org, dewvpn.com, dewvpn.net, dewvpn.org, dewvpn.co, dewvpn.cc, proxygate.net, shinevpn.net, shinevpn.com, shinevpn.co, shinevpn.org, paladinvpn.com, paladinvpn.org, and cloudrouter.io

(xx) A sum of money equal to the proceeds derived from or obtained as a result of such offense

65. If any of the property described above, as a result of any act or omission of the defendant:

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to 21 U.S.C. § 853(p), as incorporated by 28 U.S.C. § 2461(c), 18 U.S.C. § 981(a)(1)(A) and (C), § 982, and § 1030(i).


All pursuant to 18 U.S.C. § 981(a)(1), § 982, § 1030(i), 28 U.S.C. § 2461(c), and 21 U.S.C. § 853.

A TRUE BILL.

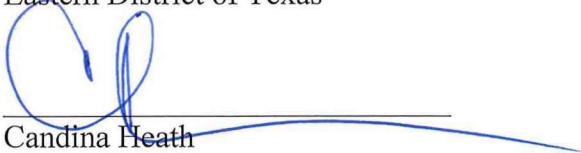


FOREPERSON

DAMIEN M. DIGGS
UNITED STATES ATTORNEY



Camelia Lopez
Assistant United States Attorney
Eastern District of Texas



Candina Heath
Senior Counsel
Computer Crimes Intellectual Property Section
United States Department of Justice

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

UNITED STATES OF AMERICA

v.

YUNHE WANG,
a/k/a "Jack Wan," "Jack Wang," "Williams
Tang," "Jack Wong," "Williams Long," and
"Tom Long"

Defendant.

Case No. 4:23CR 101
Judge Mazzant

Filed Under Seal

NOTICE OF PENALTY

Count One

Violation: 18 U.S.C. § 371, Conspiracy

Penalty: Imprisonment for not more than five (5) years, a fine not to exceed \$250,000, or both fine and imprisonment, and a term of supervised release not to exceed three (3) years.

Special
Assessment: \$100

Count Two

Violation: 18 U.S.C. § 1030(a)(5)(A), Computer Fraud
(Intentionally Causing Damage to a Protected Computer)

Penalty: Imprisonment for not more than ten (10) years, a fine not to exceed \$250,000, or not more than the greater of twice the gross gain to the defendant or twice the gross loss to one other than the defendant, or both fine and imprisonment, and a term of supervised release not to exceed three (3) years.

Special
Assessment: \$100

Count Three

Violation: 18 U.S.C. § 1349, Conspiracy to Commit Wire Fraud.

Penalty: Imprisonment for not more than twenty (20) years, a fine of not to exceed \$250,000, or both fine and imprisonment, and a term of supervised release not to exceed five (5) years.

If the offense conduct affects a financial institution, the maximum term of imprisonment is increased to thirty (30) years, a fine not to exceed \$1,000,000, or both fine and imprisonment.

Special
Assessment: \$100

Count Four

Violation: 18 U.S.C. § 1956(h), Conspiracy to Commit Money Laundering
(Conspiracy to commit 18 U.S.C. § 1956(a)(1)(B)(i))

Penalty: Imprisonment for not more than twenty (20) years, a fine not to exceed \$500,000 or twice the value of the property involved in the transaction, whichever is greater, or both fine and imprisonment, and a term of supervised release not to exceed five years.

Special
Assessment: \$100