SEALED

FILED
AUG 21 2017
CLERK U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY DEPUTY

ALANA W. ROBINSON
Acting United States Attorney
SABRINA L. FEVE
Assistant U.S. Attorney
California Bar No.: 226590
Office of the U.S. Attorney
880 Front Street, Room 6293
San Diego, CA 92101
Tel: (619) 546-6786
Fax: (619) 546-0831
Email: Sabrina.Feve@usdoj.gov

Attorneys for the United States

UNSEALED PER ORDER OF COURT
8/22/17

**UNITED STATES DISTRICT COURT**

**SOUTHERN DISTRICT OF CALIFORNIA**

UNITED STATES OF AMERICA,

Plaintiff,

v.

YU PINGAN, a.k.a. "GoldSun"

Defendant.

Case No.: '17MJ2970

**COMPLAINT FOR VIOLATION OF:**

Title 18, U.S.C., Section 371 – Conspiracy; Title 18, U.S.C., Section 1030(a)(5)(A) – Computer Hacking; Title 18, U.S.C., Sections 982 and 1030(i) and Title 21, U.S.C., Section 853 – Forfeiture

The undersigned Complainant, being duly sworn, states:

**Count 1**

**(Conspiracy Computer Hacking)**

Introductory Allegations

At all times relevant to this Complaint:

1. Company A was headquartered in San Diego, California, Company B was headquartered in Massachusetts, Company C was headquartered in Los Angeles, California, and Company D was headquartered in Arizona.

2. Defendant YU Pingan was a malware broker in the People's Republic of China ("PRC").

3. An Internet Protocol ("IP") address is a unique series of numbers that identifies computing devices connected to the Internet. Computers use IP addresses to connect to each other on networks and the Internet. Because those numbers can be hard to recall, IP addresses are typically assigned a plain text "domain name" (like amazon.com or uscourts.gov). An automated Internet database system called Domain Name System ("DNS") is used to translate domain names into the actual numerical IP address and to route an internet user to that domain's IP address.

4. The term "dynamic DNS" refers to a system that allows a domain name to update its IP address more frequently or, "dynamically." Typically, dynamic DNS is provided for a fee to paying customers.

5. The term "zero-day exploit" refers to a vulnerability or hole in a computer or software's security that a hacker can exploit. One of the defining features of a zero-day exploit is that nobody but the hacker(s) who use it know about the vulnerability and the means for exploiting it.

6. The term "remote access trojan" or RAT refers to a software program that allows an outside party (such as a hacker) to gain remote control over the computer on which the RAT is installed. The remote access is often called a back door.

7. The term "watering hole attack" refers to a hacker's installation of malicious software ("malware") on legitimate websites frequently visited by employees of entities the hackers are targeting. When users visit the legitimate website, malware is installed on the users' computers. This is akin to a predator waiting to ambush prey at the location the prey goes to drink water.

The Conspiracy

8. Beginning in or about April 2011, and continuing up to and including on or about January 17, 2014, within the Southern District of California and elsewhere,

defendant YU Pinga did knowingly, intentionally, and willfully agree and conspire with other persons known and unknown, including Uncharged Coconspirators ("UCC") 1 and 2, to 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, including a loss of at least $5,000, in violation of 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B)(i).

Manner and Means

9. The objects of the conspiracy were carried out in substance as follows:

a. Defendant YU and co-conspirators in the PRC would acquire and use malicious software tools, some of which were rare variants previously unidentified by the FBI and information security community, including a malicious software tool known as "Sakula."

b. Defendant YU and co-conspirators in the PRC would establish an infrastructure of domain names, IP addresses, accounts with Internet service providers, and web sites to facilitate hacks of computer networks operated by companies in the United States and elsewhere.

c. Defendant YU and co-conspirators in the PRC would use elements of that infrastructure and a variety of techniques, including watering hole attacks, to surreptitiously install or attempt to install files and programs on the computer networks of companies in the United States and elsewhere, including but not limited to Company A, Company B, and Company C.

Overt Acts

10. In furtherance of the conspiracy and to accomplish the objects thereof, the following overt acts, among others, were committed within the Southern District of California and elsewhere on or about the dates set forth below:

a. On April 17, 2011, YU told UCC #1 that he had an exploit for Adobe's Flash software.

b. On July 27, 2011, YU and UCC #2 discussed YU's installation of a RAT on an unidentified company and UCC #2 warned YU not to draw the attention of the FBI.

c. On or before August 7, 2012, a conspirator caused malicious files to be installed on Company A's computer network without authorization.

d. On or before September 18, 2012, a conspirator caused malicious files that took advantage of a zero-day exploit, now known as CVE-2012-4969, to be installed on Company C's computer network without authorization.

e. On or before December 12, 2012, a conspirator caused malicious files to be installed on Company C's web server without authorization as part of a watering hole attack that used Sakula malicious software.

f. On or before January 1, 2013, a conspirator caused malicious files to be installed on Company C's web server that took advantage of a zero-day exploit, now known as CVE-2012-4792, and caused a Sakula variant named "mediacenter.exe" to download to third-party's victims' computers without authorization.

g. On or before June 7, 2013, a conspirator caused malicious files to be installed on Company B's web server that caused a Sakula variant named "mediacenter.exe" to download to victims' computers without authorization.

h. On or before December 3, 2013, a conspirator caused malicious files to be installed on Company A's computer network without authorization.

i. On or before January 17, 2014, a conspirator caused malicious files intended to exploit the zero-day exploit, now known as CVE-2014-0322, to be installed on a server assigned to the IP address 173.252.252.204. These files caused a Sakula variant named "mediacenter.exe" to download to victims' computers without authorization.

All in violation of Title 18, United States Code, Section 371.

## FORFEITURE ALLEGATIONS

11. The allegations contained in Count 1 above are realleged herein and incorporated as a part hereof for purposes of seeking forfeiture of property of defendant YU Pingan to the United States pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(2)(b), and 1030(i), and Title 28, United States Code, Section 2461(c).

12. Upon conviction of the offense in Count 1, YU Pingan shall forfeit to the United States (a) any personal property that was used or intended to be used to commit or to facilitate the commission of the offense; and (b) any property, real or personal, constituting or derived from proceeds obtained directly or indirectly as a result of such offense.

13. If any of the property described above, as a result of any act or omission of defendant YU Pingan cannot be located upon the exercise of due diligence; has been transferred or sold to, or deposited with, a third party; has been placed beyond the jurisdiction of the court; has been substantially diminished in value; or has been commingled with other property which cannot be divided without difficulty, the United States shall be entitled to forfeiture of substitute property up to the value of the property

//

described above, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b) and 1030(i).

All pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(2)(B), 982(b), and 1030(i); and Title 28, United States Code, Section 2461(c).

This complaint is based on the attached Statement of Facts incorporated herein by reference.

Adam James
Special Agent
Federal Bureau of Investigation

Sworn to me and subscribed in my presence this 21 th day of August 2017.

HON. BERNARD G. SKOMAL
U.S. Magistrate Judge

United States of America

v.

Yu Pingan, a.k.a. "GoldSun"

AFFIDAVIT

Adam R. James, being duly sworn, states:

1. I am a special agent with the Federal Bureau of Investigation and have been so employed since July 2010. I am currently assigned to a cybercrime squad in the San Diego Field Division and have been assigned to investigate cybercrimes since December 2010. As a member of this squad, I investigate cybercrimes, such as computer intrusions (commonly referred to as hacking), Distributed Denial of Service (DDoS) attacks, Internet fraud, and the use of malicious code. I have received training in conducting cyber-based investigations, including the FBI's cyber career path training, as well as training covering, among other things, hacker techniques, incident responses, computer forensics, and cyber security. Before joining the FBI, I was an Information Security Consultant who held seven professional certifications related to information security and computer forensics. I have a Bachelor of Science degree in Management Information Systems and a Master of Science degree in Management Information Systems with a specialization in Information Security. Based on this training and experience, I am familiar with the manner in which persons engaged in cybercrimes operate; the manner in which cybercrimes are perpetrated; certain techniques, methods, or practices commonly used by persons engaged in cybercrime activity; and indicia of cybercrime activity. This training and experience forms the basis for opinions I express below.

## Statement of Probable Cause

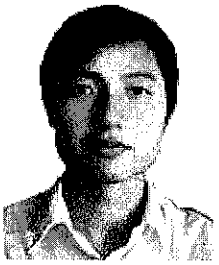
A. *Overview*

2. The FBI is investigating a group of hackers who have compromised the computer networks of U.S. and European companies. Victims of this hacking conspiracy include San Diego-based Company A, Massachusetts-based Company B, Los Angeles-based Company C, and Arizona-based Company D all of which have confirmed to the FBI that hackers accessed their respective networks without authorization. The unauthorized intrusions on Company A continued into the spring of 2014. The unauthorized intrusions on Company B continued into July 2015. The conspiracy gained unauthorized access to Company C's network in or about 2010 and the unauthorized intrusions continued into March 2013.

3. As will be discussed below, the intrusions at all three companies involved variants of an uncommon malicious software tool known as "Sakula." The intrusions also used the overlapping use of other hacking tools, techniques, Internet Protocol ("IP") addresses, email accounts, and domain names.[1] For these reasons, the FBI believes the same group of conspirators was responsible for the intrusions.

4. The FBI has identified one of the conspirators as YU Pingan. For the reasons discussed below, I believe that YU distributed malicious software tools to Uncharged Co-conspirator ("UCC") UCC #1 and that YU knew and agreed that UCC #1 would use these tools in furtherance of a conspiracy to hack U.S. companies. According to YU's C.V., which the FBI seized via search warrant, YU was born on December 16, 1980, lives in Shanghai, China, and his expertise includes computer network security and computer programming. YU's C.V. also included the following picture of himself:

[1] Using IP addresses, it is possible to determine, within limits, the physical locations of such devices. Knowledgeable hackers, however, often hide their true IP addresses and locations through a variety of methods.



5. To date, search warrant results, along with open source research, have also identified "UCC" #1 and #2.

B. *Background Terminology*

6. I use the following terms below:

a. *DNS Service Provider*: When a company or entity wants to register a domain name, it pays a domain name registrar to register that domain name. In addition to registering domain names, domain name registrars typically also provide DNS services, which are akin to serving as the Internet equivalent of a phone operator. To illustrate: when a DOJ employee who wants to access Westlaw types "www.westlaw.com" into his Internet browser, an internal DOJ DNS server first looks up the domain "westlaw.com" in its own internal directory. Typically, an internal DNS server will only have a directory for its own internal domains (*i.e.*, those ending in "usdoj.gov"). The DOJ DNS server can direct internal DOJ queries for DOJ websites without going outside its own DNS server, but to route the DOJ employee's query for an external domain, the DOJ DNS server will go up the chain to its DNS provider. The DNS provider ordinarily has a registry of most domain name assignments, and can point the DOJ server's DNS query to the correct external IP address, such that the DOJ employee would then see the Westlaw homepage open.[2]

---

[2] To use a phonebook metaphor, the DOJ DNS server's query of its DNS service provider would be like if the DOJ employee, needing to call Westlaw, dialed an outside operator, or directory assistance, to find Westlaw's phone number. The DNS service provider, like the operator, has access to a registry, or "phonebook," of registered domain names and corresponding IP addresses. By consulting this registry, the DNS service provider can provide the DOJ DNS server with

b. *Dynamic DNS*: Dynamic DNS, or "DDNS," allows a domain name to update its IP address more frequently or, "dynamically." Borrowing a phonebook metaphor: if the phonebook is published annually and someone moves, his phone number and address will not update until the next year's publication. DDNS is a way to update an IP address faster and sooner. In some instances, DDNS users might have to pay for this additional service if they expect to change a domain name's IP address regularly or frequently. While there are legitimate uses of this service, hackers often use DDNS to distance domain names they control (and that often appear legitimate) from IP addresses that are associated with malicious activity, and to make it more difficult for law enforcement and security researchers to track their hacking activities.

c. *Virtual Private Server*: In general terms, a "server" is a physical computer that processes data for one or more users over a local network or the Internet. An example is a physical computer operated by a popular email service like Google's Gmail, which stores and receives emails for many users who access the server through the Internet. In some cases, a host/operator of a physical server allows others to remotely (e.g., via the Internet) rent or lease part of the server to use as their own, smaller server. These smaller, leasable servers are often called "virtual private servers" (VPS) because "virtual machine" technology is what allows the server operator to run separate, private servers on the same physical server. VPSes are used to host (i.e., store the contents of) domain names, run programs, and store data. One advantage of a VPS is that customers get access to the physical server's resources (memory, storage capacity, processing capability, power source, high-speed access) at low cost; for example, a VPS can be rented for as low as $5 per month, while actually owning and maintaining a dedicated physical server with the same capabilities can be more expensive. A disadvantage of a VPS is decreased security: e.g., the VPS provider who

---

Westlaw's IP address, or "phone number," so that the DOJ DNS server can route the employee's "call" or query.

operates and maintains the physical server could search each VPS or intercept communications to and from the VPS. VPS customers can easily lease the VPS service for short periods (e.g., two to six months). Short-duration VPS is analogous to a disposable phone: it can be used for legitimate reasons, but its inexpensiveness, disposability, and anonymizing features make it very popular with criminals.

d. *Zero-day exploit*: This term refers to a vulnerability in a computer or software's security that hackers can exploit. One of the defining features of a zero-day exploit is that only the people who found and/or use it know about the vulnerability and the means of exploiting it. Consequently, if the same zero-day exploit is used to attack different targets at or around the same time, that tends to indicate that the same person or group is responsible for those attacks. If an exploit is known widely enough that different hackers used it at or around the same time, it would not be a "zero-day" exploit. While it is possible that different hackers could use the same previously-unknown exploit at the same time, that coincidence would be uncommon. The information security community catalogs vulnerabilities and assigns them an identifier that begins with "CVE" and then adds the year, followed by a unique number (e.g., CVE-2017-####). Using this identifier helps to prevent confusion about which zero-day exploit is being discussed.

e. *Remote Access Trojan*: Remote Access Trojan ("RAT") refers to a software program that allows an outside party (such as a hacker) to gain remote control over the computer on which the RAT is installed. The remote access is often called a back door.

f. *Watering hole attack*: A security research company coined this term to describe a particular hacking strategy. Specifically, hackers install malware on legitimate websites frequently visited by hackers' actual targets. When the employees click on links at the compromised website, malware is installed on the target's computer and/or the network the target uses. For example, hackers targeting law firms might

install the malware on a site like Westlaw or Lexis/Nexis. When an employee at firm A clicks on a link on one of those sites, the malware is installed on the employee's law firm computer and/or the firm's network. Depending on the nature of the malware, it may give the hacker remote access to the firm's computers.

C. *The Conspiracy's Unauthorized Intrusions on U.S. Companies*

7. In August 2012, Company A discovered an intrusion into its internal computer networks. Company A identified several pieces of malicious code on its computer networks, including a file named capstone.exe, and provided the malware to the FBI's San Diego field office for review. Company A also provided the FBI with a list of IP addresses and domain names that it had linked to the malicious activity identified on its networks.

8. The FBI analyzed the malicious file capstone.exe and learned that, when run, the malware would call out or beacon to a domain name, capstoneturbine.cechire.com, hosted by a DDNS provider. (A "beacon" is a connection from the victim computer to a computer controlled by the hacker that alerts the hacker to the successful installation of the malware on a victim computer and identifies the victim computer's IP address.)

9. Subscriber records showed that the account that hosted capstoneturbine.cechire.com hosted several other domain names (collectively, ACCOUNT-1). These records also showed that ACCOUNT-1's subscriber listed "Capstone Trubine" [sic] as his/her employer, and the website www.capstonetrubine.com [sic] as the employer's website. Subscriber billing records showed that UCC #1's online e-payment account paid for ACCOUNT-1 (discussed in paragraph 21 below).

10. Based on evidence collected from Company A, the FBI contacted Company C. Company C provided the FBI with copies of its compromised computers. Investigation of the malicious files found on these computers showed that Company C's

public website hosted several zero-day exploits and that these exploits enabled the hackers to use the company's website to stage a watering hole attack. Through this attack, the hackers gained unauthorized access to the computer networks of companies whose employees visited Company C's compromised website.

11. The FBI's forensic analysis of Company C's compromised computers found malicious files that included a file called "frtest.dat." Like the malicious file found on Company A's network (capstone.exe), frtest.dat was programmed to beacon to domain names controlled by ACCOUNT-1. In my opinion, the hackers' use of ACCOUNT-1 to stage attacks on both Company A and Company C, together with the use of a malicious file called "capstone.exe" to hack Company A, indicates that the same hackers are responsible for the two attacks.

12. The intrusion into Company C began in approximately January 2010. In September 2012, malicious files were installed on Company C's web server (the server that hosts the company's website) as part of a watering hole attack that, between September 18, 2012 and September 19, 2012, distributed malicious code to 147 unique U.S.-based IP addresses, using a zero-day exploit now known as CVE-2012-4969. Between May 2012 and January 2013, Company C's web server hosted no less than five variants of Internet Explorer zero-day exploits.

13. No later than December 12, 2012, malicious files were installed on Company C's web server as part of a watering hole attack that, between December 12, 2012 and January 1, 2013, distributed malicious code to 377 unique U.S.-based IP addresses. This attack used the Sakula malicious software ("malware") to compromise networks assigned these IP addresses. At the time of this malicious activity and those described below, Sakula was a new and rare malicious software tool. The only previous use of Sakula documented by the FBI occurred on or about November 21, 2012. This variant is discussed on a public information security blog post available at blog.airbus.cybersecurity.com/post/2015/09/APT-blackvine-malware-sakula (last

accessed August 20, 2017), and the Department of Defense's Cyber Crimes Center ("DC3")[3] also has a copy of the malware variant. For reasons discussed below, seized emails tie YU and UCC #1 to this previously unknown malware. In addition, I believe that the novelty and rarity of this malware is evidence that only a small group of hackers knew of it and that they were working together.

14. No later than January 1, 2013, malicious files were installed on Company C's web server that took advantage of a zero-day exploit now known as CVE-2012-4792. This watering hole attack caused a Sakula variant named "mediacenter.exe" to download to victims' computers.

15. No later than June 7, 2013, malicious files were installed on Company B's web server. Sometime between this compromise and August 23, 2013, additional malicious files were installed on Company B to enable a watering hole attack. These files caused a Sakula variant named "mediacenter.exe" to download to victims' computers.

16. No later than December 3, 2013, malicious files were installed on Company A's computer network. The malware included a Sakula variant that beaconed to a domain that spoofed, or imitated, Company B's name (*i.e.*, oa.[Company B]sen.com). Company A reported that, between December 3, 2013 and December 6, 2013, the conspirators accessed approximately 40 Company A systems without authorization, installed malware on 10 of the systems, stole and used multiple user accounts, and exfiltrated an employee's email account (also known as a .pst file). According to Company A, it has incurred over $5,000 in losses as a result of the December 2013 compromise.

[3] DC3 is a federal cyber center operated by the Defense Department. Its mission is to deliver digital forensics and multimedia lab services, cyber technical training, technical solutions development, and cyber analytics for various mission areas.

17. On December 16, 2013, the FBI looked up the malicious domain, oa.[Company B]sen.com, identified by Company A. The domain resolved to (i.e., was assigned to) the IP address 173.252.252.204. Through open source information, the FBI saw that five other domains were also assigned to this IP address. Those five domains were hosted by a dynamic DNS account (ACCOUNT-3) controlled by UCC #1.

18. No earlier than January 17, 2014, an unidentified conspirator installed malicious files on a server assigned the IP address 173.252.252.204. The files facilitated a watering hole attack intended to exploit the zero-day exploit known as CVE-2014-0322. The malicious files caused a Sakula variant named "mediacenter.exe" to download to victims' computers, which would then beacon to the domain that spoofed, or imitated, Company B's name.

19. In my opinion it would be improbable for unconnected hackers to use the same IP address (e.g., 173.252.252.204), zero-day exploits (e.g., CVE-2014-0322, CVE-2012-4792), malicious files (e.g., capstone.exe, mediacenter.exe), domain names (*e.g.*, oa.[Company B]sen.com and capstoneturbine.cechire.com), and for these malicious domain names and files to keep coincidentally referring to the same small set of victims during an 18-month period. In part for these reasons, I believe that the same group is responsible for the unauthorized intrusions into Company A, Company B, and Company C.

D. *The Conspiracy's Ties to the Unauthorized Intrusions into Company A, B, and C*

20. Based on my training, experience, and knowledge of the case, I believe that the group responsible for the unauthorized intrusions into Company A, Company B, and Company C includes YU, UCC #1, and UCC #2. The evidence upon which I base this belief is easiest to describe by beginning with UCC #1 and his control of dynamic DNS accounts that were central to the hacking conspiracy.

*UCC#1*

21. As mentioned earlier, ACCOUNT-1 is the dynamic DNS account that hosted domains embedded in malware found on the compromised networks of Company A and Company C. An electronic payment account registered to UCC #1 paid for ACCOUNT-1. ACCOUNT-2 hosted multiple domains that included the spoofed domain capstonetrubine.com [sic] and a domain that spoofed Company B. UCC #1's email account, E-3, registered ACCOUNT-2. The dynamic DNS accounts ACCOUNT-3 and ACCOUNT-4 hosted domains that were embedded in malware found on Company B's network, and, as mentioned, five domains assigned to ACCOUNT-3, as well as the spoofed Company B domain embedded in the Sakula malware found on Company A's network, were assigned to the IP address 173.252.252.204 on December 16, 2013. Registration records show that UCC #1 paid for both accounts, that he used his true name to register ACCOUNT-4 on April 25, 2011, and that he used email accounts he controlled (E-3, E-14, and, later, E-21) to register ACCOUNT-3 and ACCOUNT-4.

22. DNS and dynamic DNS accounts like ACCOUNTS-1 through 4 can be a critical part of a hacking conspiracy's infrastructure. For example, in watering hole attacks like those perpetrated on Company C's web server, the hackers do not know which computers are successfully compromised unless the successfully embedded malware beacons and alerts the hackers as to where it has been surreptitiously installed without authorization. Broadly speaking, one way that hackers create such beacons is by embedding "call-back" domain names and/or IP addresses into the malware. Dynamic DNS enables the hackers to quickly and easily re-assign different IP addresses to these call-back domain names, which creates a layer of indirection that obfuscates their illicit activity and facilitates success.

23. ACCOUNTS-1 through 4 controlled scores of call-back domains identified by the FBI, which received beacons from Company A, Company B, Company

C, and many other U.S. and European companies' computer networks. Because these four dynamic DNS accounts were a centralized tool for updating and monitoring malware, I believe that the person or people who controlled these accounts also had control over or access to the malware that beaconed to the domains hosted in these four accounts. In this case, because UCC #1 paid for ACCOUNTS-1 through 4, I believe that he had primary control of the four accounts. Based on seized electronic communications discussed below, I also believe that UCC #1 controlled or directed the deployment of malicious software that beaconed to these dynamic DNS accounts.

24. Seized electronic communications involving a fourth victim, Arizona-based Company D, show that UCC #1 directed UCC #2 to target U.S. computer networks using these dynamic DNS accounts. For example, in 2012, a Company D computer connected to a domain assigned to ACCOUNT-2, which hosted malicious software. The malware, once installed on Company D's network, beaconed to a domain controlled by ACCOUNT-4. The malware included a file called frtest.dat, which was the same file name found on Company C's network. On December 14, 2012, UCC #1 gave UCC #2 an IP address and the username and password for the Company D server assigned to that IP address. UCC #1 told UCC #2 which software commands to use to breach the server and how to package and steal data from it. UCC #1's instructions even included details about how fast to exfiltrate the data, and to go faster only if it was after normal U.S. business hours.

25. Forensic review of Company D's compromised servers showed that the server assigned to the IP address UCC #1 provided to UCC #2 had PlugX malware installed without authorization. PlugX is a common type of malware that was also used to compromise Company A, Company B, and Company C. This PlugX variant included a keylogger function, which recorded both the hacker and authorized user's keystrokes. The keylogger records showed that an unauthorized user bundled and stole files from the server and IP address identified by UCC #1.

*YU's Involvement with UCC #1 and #2*

26. Seized communications show that YU provided malware to UCC #1 and had established this relationship with UCC #1 by April 2011. For example, on April 17, 2011, YU told UCC #1 that he had a version of an exploit for Adobe's Flash software that could work with three different web browsers.

27. YU's relationship with UCC #2 also began no later than April 2011. On April 23, 2011, YU corresponded with UCC #2 regarding malicious software that UCC #2 had sent him. The malicious software was designed to exploit vulnerabilities in the Internet Explorer web browser. UCC #2 said that he and UCC #1 had obtained the software at a meeting in Jiangsu Province. Over the next four days, YU and UCC #2 discussed UCC #1's request that YU provide code capable of exploiting Microsoft Internet Information Server and UCC #1's intention to meet with YU in Shanghai.

28. Seized communications show that YU was warned that he could get in trouble for supplying malicious software and, in particular, that he could get in trouble with the FBI for his involvement in compromising U.S. computer networks. For example, on June 18, 2011, UCC #2 advised YU that an Adobe Flash zero-day exploit attributed to YU had been publicly identified, and, on July 27, 2011, YU and UCC #2 had the following exchange while discussing YU's installation of a RAT (i.e., an unauthorized backdoor) on an unidentified company:

| | |
|---|---|
| YU: | Lost the shell [access to the RAT], but should be able to get it back. |
| UCC #2: | Be careful about security |
| YU: | Um |
| UCC #2: | Don't draw the attention of the FBI.[4] |

29. YU and UCC #1's communications include evidence tying them to the Sakula malware. On or about November 10, 2011, UCC #1 told YU that he had compromised the legitimate Korean Microsoft domain used to download software

[4] This transcription is based on a draft translation from Chinese to English. The term "FBI" however was in the original.

updates for Microsoft products. UCC #1 provided the site http://update.microsoft.kr/hacked.asp so YU could confirm his claim. UCC #1 explained that he could not use the URL to distribute fraudulent updates, but the compromised site could be used for hacking attacks known as phishing.

30. Less than two weeks later, on November 21, 2012, the first Sakula variant known to the FBI was identified. This Sakula variant was configured to beacon to a legitimate Korean Microsoft domain, update.microsoft.co.kr. In my opinion it would be unlikely for multiple hackers to control a legitimate Korean Microsoft domain and be confident enough about its breach to use it for further malicious activities. Rather, I believe that UCC #1 and YU obtained unauthorized access to modify the resolution of Microsoft's valid Korean domain. As a result, they could reassign the domain to IP addresses that they controlled. Using this unauthorized access, they could then embed the otherwise legitimate domain into the early version of Sakula and be confident it would beacon to IP addresses they controlled.

31. Similarly, I believe that the fact that the third-known variant of Sakula was part of a watering hole attack installed on Company C's web server in late December 2012 is also evidence that UCC #1 controlled it and used it in furtherance of the conspiracy to compromise Company A, B, and C.

32. Based on my knowledge of this case, I believe that UCC #1 obtained malware from YU, including Sakula, and that UCC #1 and other conspirators used this malware to compromise U.S. networks with YU's knowledge. I base this belief on the communications described above and on the following:

a. On December 3, 2013, the second Sakula variant known to the FBI was found on Company A. This Sakula variant beaconed to oa.[Company B]sen.com – a domain UCC #1 is believed to have controlled.

b. The FBI and DC3 have collected and analyzed samples of the Sakula malware, including the variation called "mediacenter.exe," discussed above. This

variant used encryption to avoid detection. Through reverse engineering, the FBI and DC3 learned that the decryption key was the word "Goldsunfucker." I believe that "Goldsun" refers to YU because seized emails show that YU used the email account goldsun84823714@gmail.com. Moreover, YU used this account to communicate with UCC #2 and these communications included discussions of UCC #1 and hacking activities. YU also acknowledged to UCC #2 that he used the nickname "goldsun." In my opinion, the decryption key's use of the goldsun nickname is evidence that YU was the distributor of the malware.

c. On or about December 25, 2012, draft translations indicate that YU complained that UCC #1 was using a malicious file "golds7n.txt" to compromise websites and that UCC #1's actions were imprudently implicating YU. This message shows that YU used the "goldsun" nickname and knew that UCC #1 used malicious tools provided by YU in tandem with variations of YU's "goldsun" nickname.

d. YU's providing UCC #1 with the Sakula malware was consistent with their broader transactional relationship. UCC #1 repeatedly obtained malware from YU. For example, on or about March 3, 2013, YU emailed UCC #1 samples of two types of malware: "adjesus" and "hkdoor." The FBI had difficulty deciphering adjesus, but open source records show that it was previously sold as a penetration testing tool (which is what legitimate security researchers call their hacking tools) on the website penelab.com.[5] Part of the coding for the second piece of malware, hkdoor, indicated that "Penelab" had created it for a customer named "Fangshou."[6] Seized communications and open source records show that YU ran the penelab.com website

[5] No later than December 2011, YU used the Penelab website to advertise malicious code named "PENESW-07 ADJESUS域帝" and "PENESW-05 TCPRD骇客之门". The Chinese characters in the malicious code name "PENESW-05 TCPRD骇客之门" translate to the term 'Hacker's Door.'

[6] The relevant part of the code, which is known as a .pdb string reads (emphasis added): "Y:*penelab*\customer*fangshou*\ijuriesa*hkdoor*_srcx64*hkdoor*dll\Release*demo*\x64\Release*demo*.pdb."

(e.g., he used his email address and real name to register it) and that UCC #1 used the nickname "Fangshou."

Conclusion & Request for Sealing

33. At this time, I believe that YU and his coconspirators are unaware of the FBI's identification and investigation of them. Because I believe that premature disclosure of this affidavit could result in flight and the destruction of evidence, I request that it be sealed until further order of the Court.

34. Based on the evidence described above showing that YU provided malware to UCC #1 to maliciously target a discrete group of U.S. companies' computer networks, including the novel and rarely-used Sakula malware, I submit there is probable cause to arrest YU for conspiring to commit fraud in connection with computers, in violation of 18 U.S.C. §§ 371 and 1030(a)(5)(A).

Adam James
Special Agent
Federal Bureau of Investigation

Sworn to me and subscribed in my presence this 21th day of August 2017.

HON. BERNARD G. SKOMAL
U.S. Magistrate Judge