

AO 91 (Rev. 11/11) Criminal Complaint

AUSA: Patrick Corbett
Special Agent: Andrew Sczygielski

Telephone: (313) 226-9703
Telephone: (313) 965-6082

UNITED STATES DISTRICT COURT
for the
Eastern District of Michigan

9

ORIGINAL

United States of America
v.

KONRAD VOITS

Case: 2:17-mj-30327
Assigned To : Unassigned
Assign. Date : 7/5/2017
Description: CMP USA v. SEALED MATTER (SO)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of January 24, 2017 through March 10, 2017 in the county of Washtenaw in the Eastern District of Michigan, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1030(a)(2)(C)	Intentionally accessing a computer without authorization and thereby obtaining information from a protected computer;
18 U.S.C. § 1030(a)(4)	Knowingly, and with intent to defraud, accessing a protected computer;
18 U.S.C. § 1030(5)(A)	Knowingly causing the transmission of a program and, as a result, intentionally causing damage, without authorization, to a protected computer.
18 U.S.C. § 1028(A)	Using the means of identification of another during and in relation to a felony computer intrusion

This criminal complaint is based on these facts:

See attached

Continued on the attached sheet.

SA Andrew Sczygielski
Complainant's signature

Andrew Sczygielski, Special Agent, FBI
Printed name and title

[Signature]
Judge's signature

Sworn to before me and signed in my presence.

JUL 05 2017

Date: _____

City and state: Detroit, Michigan

David R. Grand, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, Andrew Sczygielski, being duly sworn, hereby depose and state the following:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), assigned to the Detroit Field Office-Cyber Division, and have been employed by the FBI since August 2010. I am responsible for investigating cyber-related crimes and have received training relating to cyber intrusions and have managed investigations involving the use of cyber-enabled techniques.
2. The information contained in this affidavit includes facts known to me personally, and to other investigators working similar cyber matters. This affidavit is intended to show only that there is sufficient probable cause for the requested arrest warrant, and does not set forth all of my knowledge about the investigation.
3. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18 United States Code Section 1030, including but not limited to Section 1030(a)(2)(C) (intentionally accessing a computer without authorization and thereby obtaining information from a protected computer), Section 1030(a)(4) (knowingly, and with intent to defraud, accessing a protected computer and obtaining something of value), and 1030(5)(A) (knowingly causing the transmission of a program and, as a result, intentionally causing damage, without authorization, to a protected computer), and Title 18 United States Code 1028A (using the means of identification of another during and in relation to a felony computer intrusion), have been committed by a suspect known to the FBI. The facts and information, necessary to support the application for arrest, are spelled out below.

PERSON TO BE ARRESTED

4. This affidavit is written in support for the Court's approval of an application for a complaint and warrant to arrest the following person: KONRADS

VOITS. Your affiant has reason to believe that VOITS is the individual involved in a criminal computer intrusion.

5. The FBI first encountered VOITS in March 2015, when VOITS called the FBI's Public Access Tip Line, and reported a bomb threat to the National Security Administration (NSA) building in Baltimore, Maryland. VOITS stated he knew someone who had bomb making materials, had made the bombs, and was going to use a vehicle to drive to the front of the NSA building and detonate the explosive. That investigation showed no merit to the threat, and VOITS was subsequently prosecuted by the Washtenaw County Prosecutor's Office for Filing a False Police Report. The investigation also showed VOITS to have made statements indicating he was going to "die in a firefight with law enforcement" if approached by law enforcement. VOITS spent his time in jail in Washtenaw County facilities.

BACKGROUND

6. On March 10, 2017, VOITS was an occupant at 25 Johnson Street, Apartment Number 3, Township of Ypsilanti, Michigan (hereinafter Apartment), and was present during the execution of a search warrant lead by Michigan State Police Officers. The search warrant was predicated on evidence from a State of Michigan arson investigation, of which VOITS was the primary suspect. VOITS was the only person in the Apartment at the time the search warrant was executed.
7. As officers entered the dwelling, VOITS was alone sitting in front of a laptop computer, with minimal furnishings in the Apartment. VOITS was taken into custody, and the screen on the laptop was left open. Investigators observed, then confirmed, that what appeared on the screen of the laptop showed a breach into Washtenaw County's (hereinafter County) internal network. The computer log on the screen showed an internal IP (Internet Protocol) address known to belong to the County domain. VOITS was not authorized to have access to the County's network, and was subsequently charged by the Washtenaw County Prosecutor's Office with a violation

MCL 752.797 (Fraudulent access to computers, computer systems, and computer networks), as well as other charges.

8. Officers obtained additional State of Michigan search and seizure warrants for digital devices seized during the search, including a laptop (System76), four cellular telephones, a hard drive, and a flash drive.
9. Washtenaw County Sheriff's Office requested assistance from the FBI-Cyber Division; the FBI opened a full investigation on April 3, 2017.
10. Forensic analysis of the devices showed a deluge of digital evidence connecting VOITS to the computer intrusion into the County's network.
11. VOITS is currently in the custody of Washtenaw County Sheriff's Office, detained on his state computer charges. He has state court hearing dates on July 6, 2017, and August 2, 2017. Because Washtenaw County, including the Washtenaw County Prosecutor's Office (WCPO), is considered a victim of this crime, the state courts have ordered that the case be reassigned to another prosecuting entity. Through the filing of this complaint, the United States Attorney's Office for the Eastern District of Michigan is agreeing to accept this case for federal prosecution.

PROBABLE CAUSE

12. I was assigned to investigate whether VOITS was involved in committing an unauthorized computer intrusion. I, along with my co-case agent, contacted and met with Washtenaw County Sheriff's Office officials, as well as other State of Michigan investigators, to assess the facts and the extent of the network intrusion.
13. The FBI's investigation to date, has established that VOITS, among other acts, registered a fraudulent website, sent spear phishing emails to County employees, made telephone calls to County employees purporting to be a County IT employee, used a malicious software code to gain access to the network and exfiltrated County data to remote cloud-based servers. While

inside the network, VOITS attempted to alter County data, including moving up the release dates of County Jail inmates, and to view law enforcement sensitive files.

COUNTY INVESTIGATION

14. Between February 14 and 16, 2017, employees of the County received a series of targeted, malicious email messages from a "Daniel Greene," danielgreene95101@gmail.com. The text of the email read, "Hi. You helped me while I was in jail. Is my court record being leaked on the jail website? I am pretty sure these are all my docs (sic) Sincerely, -Daniel". The emails contained a hyperlink attached to the word "website" which pointed to a domain name, ostensibly designed to mimic the appearance of the true County website, www.ewashtenaw.org, replacing the last "w" with a visually similar sequence of two "v's". After querying open source registration databases, the email address associated with the Registrant of the domain name is kaligangbang@protonmail.com. The website was registered on January 24, 2017.
15. Between February 20 and 23, 2017, County employees received telephone calls from someone posing as a specific, and known County IT employee (hereinafter Victim), utilizing telephone numbers 734-436-1838 and 734-961-2225 on multiple instances. Local investigators determined the actual employee, i.e. the Victim, denied making such phone calls, or authorized anyone to do so. Victim's information was entered into the County's system as a victim of identity theft.
16. Per the Washtenaw County Sheriff's Office report, in one instance on February 20, 2017, the caller identified himself as Victim "with IT" and said he was "attempting to assist in updating XJail". The male caller instructed the County employee to open an internet browser and type in the URL "tinyurl.com" and enter the address "tinyurl.com/xjail-08", which was blocked by a County firewall. The caller stated that this was the issue IT had been seeing and possibly the reason for the XJail issues. He then directed the employee to tinyurl.com/xjail-backup-update, which took the employee to a page of code which the caller wanted the employee to save to his/her computer. The call quality was poor and the employee, becoming increasingly suspicious, ended the conversation and hung up.

17. In all, there were at least ten documented attempts of the scam caller between February 20 and 23, 2017, all with a similar theme. The caller identified himself as a County IT employee, then directed the County employees to type a web address into their browsers and download an executable file (.exe) to upgrade the County's jail system. After being convinced the caller did work for the IT department, some employees did type in the web address and at least partially downloaded the .exe file as directed. Others reported it as a scam and informed IT security.
18. On February 28, 2017, VOITS was found by a local Police Officer on the rooftop of the Hands-on Museum in Ann Arbor, Michigan. Apparently, VOITS gained access via a fire escape ladder. On the rooftop, Officers observed the individual, who was positively identified as VOITS, with an open laptop. When asked what he was doing on the rooftop, VOITS claimed he was only trying to get better network reception. Officers issued him a trespass notice and let VOITS go. The museum is located directly across the street from Ann Arbor municipal building, one of the buildings where the suspicious telephone calls were directed.
19. On March 5, 2017, County IT personnel determined that information was being taken from County networks and sent to a www.box.com account. Further investigation showed the account to be associated with email address kaligangbang@gmail.com.
20. On March 6, 2017, a suspicious customer, later determined to be VOITS, entered the Ann Arbor City Hall café. VOITS came in the morning and stayed all day until closing. Throughout the day, the café employee became suspicious and took a photograph of the "customer" from behind VOITS's back. Per Washtenaw County Sheriff's reports, the employee stated the customer was typing "codes and commands". In reviewing the grainy photograph of the computer screen, a person experienced in computer operating systems could surmise the operating system used by VOITS was Linux based. In my training and experience, I know Linux also to support the Kali Operating System, a program used as a network penetration testing tool.

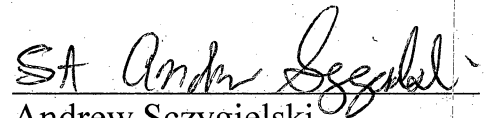
21. Intrusion investigators at this point did not know the true identity of the suspect or the person affiliated with the kaligangbang accounts.
22. On March 10, officers executed the search warrant (see paragraphs 6-8) at VOITS's Apartment. Both Michigan State officers and Washtenaw County Sheriff officers were present. As mentioned earlier, the laptop screen was left open as VOITS was taken into custody. Per Washtenaw County Detective Kevin Parviz, who is also certified in multiple computer related certifications and present at the time of the search, the screen of VOITS's laptop showed a running Kali Operating System, with the username Kaligangbang visible on the screen. Detective Parviz confirmed with an IT administrator that the internal IP address which appeared on the screen belonged to the County's network, indicating an intrusion had occurred.
23. As previously mentioned, numerous cellular telephones were seized during the search of VOITS's apartment. FBI investigation revealed that one telephone was assigned the MSISDN number (telephone number) 1-734-961-2225, one of the same numbers found in the County's call logs and answered by County employees between February 20 and 23, 2017, during which the caller stated he was from the IT Department and needed the employee to assist in upgrading the jail system. Another phone was assigned MSISDN number 1-734-829-9790, and had an email address associated with outgoing calls, janehoffman7348299790@gmail.com. Investigators determined the email address to be associated with an App, downloaded onto the telephone, named Hushed. Investigators learned the Hushed App provides users anonymous telephone numbers which cannot be traced by a recipient, effectively making it a "burner phone". Further investigation shows the account username to be janehoffman7348299790@gmail.com, and to have multiple phone numbers associated with it, including 734-436-1838, the other number used to call County employees. Your affiant also compared County call logs to the telephone numbers associated with telephones found in VOITS's possession and found numerous, matching calls.
24. FBI served Federal search warrants on the domestically located, cloud-based service providers, to include Box.com, Microsoft and Amazon, after it was determined the malicious website directed data to IP addresses associated

with each service. Your affiant is aware the results returned from the Box.com account include the associated email address of kaligangbang@gmail.com. A review of the digital return showed County data on the Box.com server, as well as coding scripts associated with the creation of malicious software. Box.com has verified that the account has been deactivated. The search warrants for the other providers are pending and may still provide VOITS with access to sensitive County personal data and malicious software.

25. The FBI has further determined that VOITS may have used foreign service providers in a similar manner. The FBI is actively pursuing international legal steps to further investigate.
26. Law enforcement did a forensic review of the System76 laptop which was found in the possession of VOITS at the time of the search warrant. The review revealed copious logs, files, digital photographs, and audio files indicating VOITS was the only person associated with the laptop. Screenshots of VOITS's own activity, captured by an application apparently scheduled to automatically capture a screenshot of the monitor, show VOITS's activity in launching code aimed at penetrating the County's network. Screenshots also depict websites visited by the user, which show accounts tied back to KONRADS VOITS. For instance, one screenshot shows the name KONRADS VOITS, attempting to purchase lock-picking tools. A valid credit card number is also visible. Other screenshots depict Virtual Currency accounts associated with the username kaligangbang.
27. In order to remediate the damage caused by the VOITS, the County hired Mandiant Consulting Services, an incident response services company. Mandiant charges \$30,000.00 per month and has been retained since March 2017. The County continues to need the services of Mandiant. County employees have expended numerous hours, both during business hours and overtime, to address this cyber incident.
28. In summary, the facts involving VOITS's social engineering attempts, attempts to test the County network for vulnerabilities, the connected telephone call logs, the search warrant return indicating County data had been exfiltrated, the evidence located on VOITS's laptop, and the laptop

screen showing user kaligangbang at the time of the search warrant, leads your affiant to conclude there is probable cause to believe that KONRADS VOITS, during the time period between approximately January 24, 2017 and March 10, 2017, in the Eastern District of Michigan, committed the offense of computer intrusion and aggravated identity theft in violation of Sections 1030 and 1028A of Title 18 of the United States Code.

Respectfully submitted,



Andrew Sczygielski
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this 5th day of July, 2017.

Date: JUL 05 2017



David R. Grand
Hon. United States Magistrate Judge