Brandon Harris
Cyber Law
4/2/2025

AFFIDAVIT FOR A SEARCH AND SEIZURE WARRANT

I, Special Agent Bradon Harris, sworn in, states as follows:

I. INTRODUCTION

1. I am a Special Agent for the Federal Bureau of Investigation (FBI) assigned to the Cyber Crimes Division in the Eastern District of Virginia. I work as a Special Agent for 10 years and previously served as a Defensive Computer Network Operator at the National Security Agency (NSA), where I helped to take down threats that posed an immediate risk to our nation's critical infrastructure. I have received specialized training in cybercrime investigations and digital forensics. As part of my duties, I investigate crimes involving hacking and financial fraud.

2. This affidavit is based on a thorough investigation, A review of the case documents, and information given to me by other special Agents, forensic analysts, and partner agencies. This affidavit is being submitted to establish probable cause to support a search and seizure warrant. This affidavit does list collection methods regarding this investigation, as some information is classified and related to National Security.

II. PROBABLE CAUSE

3. This affidavit is meant to support a warrant for 1425 W 49th St, Norfolk, VA 23508, Norfolk, Virginia, and for digital evidence stored on electronic devices, including but not limited to laptops, computers, external storage devices, and phones belonging to Andre BROWN.

4. BROWN has violated several federal laws, including the Computer Fraud and Abuse Act (CFAA)\ and 18 U.S.C. 1343 (Wire Fraud). Specifically, BROWN exploited a vulnerability (CVE-2025-24813) in Apache Tomcat servers used by Navy Federal Credit Union, unlawfully accessing customer data, including email addresses, credit card information, phone numbers, and social security numbers. BROWN then deployed the BlackCat ransomware, developed by Russian threat actors, on the bank's systems, leading to widespread service outages.

III. DETAILS OF THE OFFENSE

5. On March 18, 2025, Navy Federal Credit Union, located at 1140 N Military Hwy Ste 820, Norfolk, VA 23502, detected suspicious activity on its internal network. A Cybersecurity analyst from the bank’s cybersecurity team identified that an unauthorized user had exploited their Apache Tomcat server using a vulnerability known as CVE-2025-24813, a remote code execution vulnerability. The compromised server hosted personally

identifiable information (PII) of thousands of customers and employees.

6. Further analysis determined that BROWN had deployed BlackCat ransomware following the unauthorized access to the Apache Tomcat Server, which encrypted critical bank data and caused Navy Federal Credit Union online services to go offline for approximately 72 hours. The ransomware left a digital note on the affected system's desktop, demanding $5 million dollars in cryptocurrency for decryption keys.

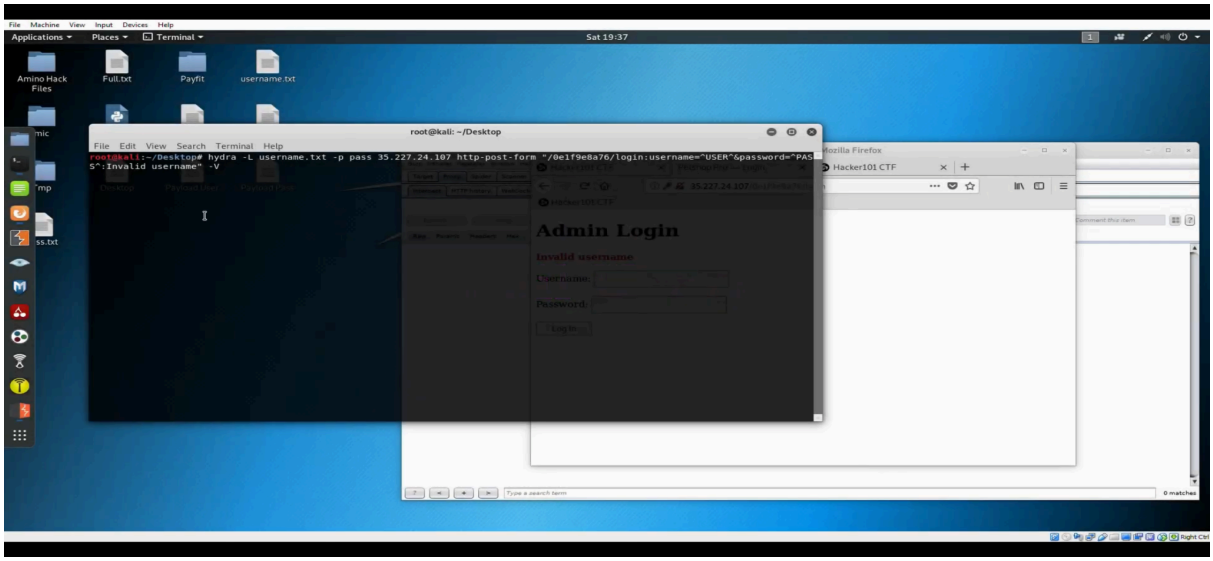
7. On March 19, 2025, Navy Federal Credit Union reported the intrusion to law enforcement. A review of the compromised system logs revealed multiple unauthorized access attempts originating from an IP address linked to a VPN service known for obfuscating user locations. A comprehensive investigation, including subpoenas to the VPN provider, traced the malicious activity to a residential IP address in Norfolk, Virginia, registered to Andrew Brown.

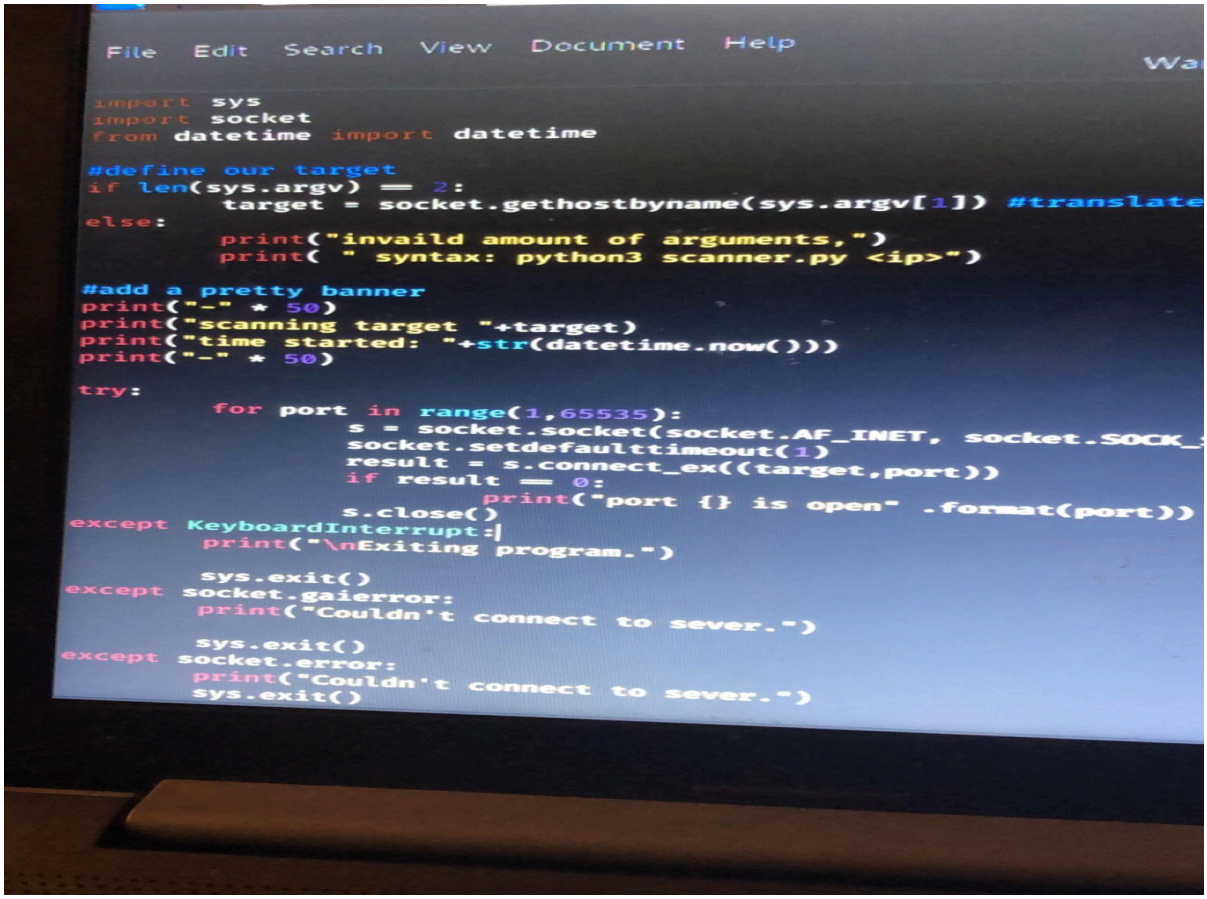
8. Through chat logs obtained from underground forums and encrypted messaging platforms, law enforcement identified BROWN as a member of the ALPHV (BlackCat) ransomware gang. These logs contained conversations where BROWN discussed the attack on Navy Federal Credit Union, including details about the exploited vulnerability, the deployment of ransomware, and negotiations regarding the ransom payment.

9. A confidential informant familiar with cybercriminal forums provided intelligence indicating that BROWN offered to sell stolen PII from Navy Federal Credit Union customers and employees on a dark web marketplace. Samples of the stolen data from the marketplace showed full names and customers' social security numbers and credit information matching the compromised data from the bank’s breach.

10. Surveillance conducted on BROWN's residence at 1425 W 49th St, Norfolk, VA 23508, on March 22, 2025, observed BROWN in his home office engaging in frequent computer and laptop use consistent with cybercriminal activities by running tools associated with malicious activity such as Hydra which is a tool used to crack passwords, and creating a network scanning script in python a programming language that enabled BROWN to remotely access compromised computers. BROWN was also observed using external storage devices to store the exfiltrated data from networks that BROWN had accessed unlawfully.

Digital Evidence Obtained from Investigation “Methods Are Classified”





IV. ITEMS TO BE SEIZED

11. Based on the presented Information, I seek authorization to search the premises at 1425 W 49th St, Norfolk, VA 23508, and seize the following items as evidence, contraband, and instrumentalities of the mentioned offenses:

a. Hard Drives, Computers, USBs, and digital storage devices likely containing stolen data, ransomware payloads, or hacking tools.

b. Mobile phones and other communication devices used to communicate with the ALPHV (BlackCat) ransomware gang and financial transactions of the cryptocurrency payments.

c. Notebooks, Documents, or digital records containing credentials, financial records, or any other information related to the unauthorized access, deployment of ransomware, and sale of stolen information.

d. Any cryptocurrency wallets or transaction records related to payments received from the sale of stolen data or ransomware extortion.

e. Evidence of software exploits, malware, ransomware payloads, hacking tools, or scripts used to compromise the Navy Federal Credit Union system.

V. CONCLUSION

12. Based on my experience and the information outlined in this affidavit, I assess that there is probable cause to believe that BROWN has violated federal law and that evidence of these crimes is located at 1425 W 49th St, Norfolk, VA 23508, Norfolk, Virginia. I ask that the Court provide a warrant allowing the search of the location and the seizure of the items described above.

I declare under penalty of perjury that the information is true and correct

Brandon Harris
Special Agent, Federal Bureau of Investigation
Sworn before me on March 31st, 2025.