AFFIDAVIT IN SUPPORT OF APPLICATION FOR CRIMINAL COMPLAINT

I, [redacted], being sworn, depose, and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since [redacted]. Since joining the FBI, I have been assigned to a cyber squad that has investigative responsibility for computer intrusion matters. Before joining the FBI, I participated in cyber incident response investigations and have received an industry certification in information technology security. I have been involved in investigations of computer intrusions, mail and wire fraud, and conspiracy, and I have participated in the execution of search warrants in these investigations. I am also an "investigative or law enforcement officer" of the United States, that is, an officer of the United States who is empowered by the law to conduct investigations of and to make arrests for the offenses enumerated in Title 18 of the United States Code.

2. I submit this affidavit in support of a criminal complaint charging Russian national Denis Nikolayevich Obrezko ("OBREZKO"), Cyrillic Денис Николаевич Обрезко, with conspiracy to commit an offense against the United States, to wit, conspiracy to commit unauthorized access to a protected computer, and as a result of such conduct recklessly causing damage, in violation of Title 18, United States Code, Section 1030(a)(5)(B), all in violation of Title 18, United States Code, Section 371.

3. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that OBREZKO conspired to intentionally gain unauthorized access to protected computers, and as a result of such conduct, recklessly caused damage. This intrusion campaign was waged as part of the operations of the Russia-aligned cyber threat actor group known in open-source as Void Blizzard. As described below, there is probable cause to believe, among other things, that OBREZKO facilitated the intrusion campaign by obtaining infrastructure

(specifically, a virtual private server and the purchase of a domain name) that was used to conduct these attacks targeting companies in the United States and elsewhere.

4. The facts described in this affidavit come from my observations and review of records, my training and experience, information obtained from other law enforcement personnel, and information obtained through interviews of witnesses, legal process, court orders, and search warrants. This affidavit is intended only to show that there is sufficient probable cause for the requested complaint and arrest warrants and does not set forth all my knowledge about this matter.

PROBABLE CAUSE

5. Between June and July of 2024, the FBI received two tips with overlapping information from a foreign partner and a U.S.-based private sector partner indicating that several U.S. companies were being targeted by an emerging cyber threat group, later identified as Void Blizzard. In general, and as described in this affidavit, the Void Blizzard activity consists primarily of mass email harvesting across a wide range of U.S. business sectors and industries and appears, based on my training and experience, to be consistent with a large-scale cyber espionage campaign. To date, using information obtained from the initial tips, from apparent victim companies, and from records obtained in response to legal process, the FBI has been able to verify intrusions attributable to Void Blizzard at eleven different U.S. companies, including a company located in Somerville, Massachusetts. This is believed to be only a fraction of the Void Blizzard victims nationwide.

6. During the initial phase of the investigation, the FBI observed threat actor activity involving accounts associated with a U.S.-based provider of proxy services (the "U.S. Proxy Provider"), including proxy servers. A proxy server is an intermediary gateway between a computer and the internet that handles network requests, forwarding such requests to the

destination server and then returning the data to the user. Connection to the U.S. Proxy Provider network requires internet access and a paid subscription.

7. The use of U.S. Proxy Provider accounts to gain unauthorized access to victim accounts was confirmed by multiple victim companies during the investigation. To investigate this activity, the FBI utilized court-authorized pen register and trap and trace devices ("PR/TT") to obtain non-content information associated with U.S. Proxy Provider accounts believed to be used by Void Blizzard (herein, also "threat actor" or "TA"). The information provided by the PR/TT orders allowed the FBI to identify and notify victims whenever a victim host name (or domain) was observed in the netflow data as having communicated with Void Blizzard proxy users. According to the FBI's investigation, the TA would typically connect to the U.S. Proxy Provider network via a publicly-available Virtual Private Network ("VPN") service, becoming effectively anonymous, before signing in to the U.S. Proxy Provider dashboard and selecting a proxy IP address in the general geographic region of a victim in order to circumvent any geo-blocking provisions on the victim's firewall (*i.e.*, security rules that block incoming traffic from certain regions of the world). Once the proxy IP address was selected, the TA would authenticate to the victim's cloud-based environment—usually Office 365—by replaying (*i.e.*, transmitting) a stolen session token to the server.

8. A session token is a unique means of identification, generally a quasi-random alphanumeric string, that can permit a user to maintain access their email or system account without being required to re-authenticate to the server. How the TA obtained these session tokens is still being investigated. Based on my training and experience, they could have been purchased on the dark web, phished using a malicious link, or captured via domain typo-squatting (*i.e.*, a malicious domain that is a slightly-misspelled version of a legitimate domain, such as

"micsroft[.]com"). Regardless of how the session tokens were procured, multiple U.S. victims confirmed that the authentication to specific user accounts was unauthorized and frequently followed by data exfiltration.

9. Among other things, the data obtained from the PR/TT coverage included the timestamp of the connection, the bytes transferred, the client address of the TA connecting to the proxy service, the host domain (*i.e.*, the target victim), the IP address communicating with the proxy IP address (*i.e.*, the victim's IP address), the port number, the proxy IP address, and the request duration. From the victim domain and associated IP address, the FBI was generally able to identify and contact victims. These victims, in turn, would conduct remediation and determine the extent of the unauthorized accesses and resulting data exfiltration. In a few instances when victims confirmed TA activity, the FBI was able to obtain additional proxy IP addresses from logs maintained by the victims. These additional IP addresses were used to identify other accounts at the U.S. Proxy provider being used to conduct similar targeting.

10. Data obtained from the PR/TT orders recorded various Microsoft load balancer IP addresses, which listed the host as outlook.office365[.]com (or some variation thereof), and occasionally identifiable host domain names of the targeted victims. On March 13, 2025, PR/TT data associated with a particular U.S. Proxy Provider account believed to be used by the TA (associated in subscriber information with the email address markrichard1331[@]proton.me) reflected different activity than had been observed during the previous five months of coverage. On that day, the FBI observed activity associated with two apparent victims (a U.S.-based educational institution and a foreign entity) and also what appeared to be general internet browsing activity to include navigation to various Google resources, Cloudflare services, www.crypto[.]com, www.reddit[.]com, and www.intensedebate[.]com, among other activity. The

TA also navigated to the domains [redacted], [redacted], and [redacted]. These latter three domains resolve to private (*i.e.*, publicly non-routable) IP addresses, indicating they are likely an internal resource used by the TA. Open-source Domain Name Server ("DNS") queries associated with these domains identified the related subdomains [redacted], [redacted], [redacted], and others. Based on my training and experience, this activity suggests the TA—while in the process of targeting at least two victims—likely forgot they were connected to the U.S. Proxy Provider server and performed general browsing activity while, at the same time, accessing an internally hosted network. This activity—unauthorized access of user accounts by the TA using stolen session tokens—resulted in changes to the data in each system the TA accessed without authorization.

The [redacted] Domain is Connected to the Russia-Aligned Emerging Threat Group Void Blizzard

11. Through the open-source collection of DNS requests for [redacted], the FBI determined that the [redacted] domain utilized Cloudflare as the authoritative name server for handling network traffic. Cloudflare records associated with the [redacted] domain reflect a login from IP address 193.32.249[.]223 on April 24, 2025, at 13:24:32 UTC. That same day, between 09:25:20 UTC and 14:23:27 UTC, this same IP address was used seven times to access the Cloudflare account associated with email address carriehuff[@]onionmail.org, which records indicate was used to register the domains ebsummlt[.]eu and miscrsosoft[.]com on that same date. Based on my training and experience, because they are close variations of legitimate websites (in this case, the European Business Summit and Microsoft), these appear to be phishing domains. Indeed, during the FBI's investigation, these domains were confirmed by Microsoft to be fraudulent and not associated with legitimate business operations.

12. Separately, on May 5, 2025, at 12:47:57 UTC and 13:33:53 UTC, the IP address 138.199.34[.]154 twice accessed the carriehuff[@]onionmail.org Cloudflare account. This same IP address was also used at 13:22:55 UTC that day to access the Cloudflare account registered to maryoverly[@]onionmail.org, which records indicate registered the apparent phishing domain micsrosoftonline[.]com. The phishing domain micsrosoftonline[.]com has been publicly attributed by Microsoft to the cyber threat group Void Blizzard (VB), whose malicious cyber actions appear aligned with Russian interests based on open-source reporting (screenshot and link below).

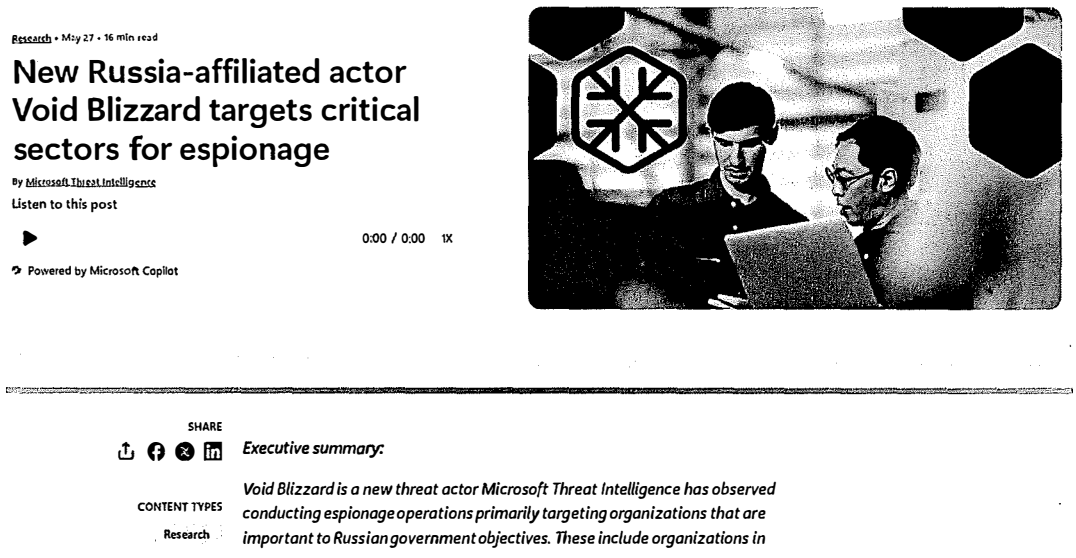


Figure 1 *New Russia-affiliated actor Void Blizzard targets critical sectors for espionage*. Available at https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/. Last accessed October 12, 2025.

OBREZKO Obtained Infrastructure Associated with the [redacted] Domain

13. As discussed above, the [redacted] domain and associated subdomains resolve to private IP addresses indicative of a locally-hosted resource that is *not* navigable via the open internet. Because the TA was connected to the U.S. Proxy Provider service while navigating to this internal resource, the FBI was able to observe that activity through the court-authorized PR/TT even though [redacted] is hosted locally. Based on my training and experience, I believe the network setup for this domain and the subdomains is indicative of an internal network with various tools available to manage data and/or facilitate coordination between additional personnel.

14. As described above, through the open-source collection of Domain Name Server (DNS) requests for [redacted], the FBI determined that the [redacted] domain utilized Cloudflare as the authoritative name server for handling domain name resolution requests. Records from Cloudflare for the [redacted] domain show that it was registered with the email address sharedstaffaccount[@]proton.me on or about May 15, 2024, and that the domain used the services of Let's Encrypt to manage Secure Socket Layer ("SSL") certificates and authentication.

15. Let's Encrypt is a Certificate Authority, which means that it is a trusted third-party that issues and manages digital certificates for authentication and verification purposes. Records obtained from Let's Encrypt for the [redacted] domain listed admin[@][redacted] as the contact email address. Logs of application programming interface (or "API") requests to Let's Encrypt revealed that such requests originated from multiple private IP addresses and some publicly-routable IP addresses, including 172.86.75[.]235. According to open-source WHOIS information, the IP address 172.86.75[.]235 is managed by BitLaunch.io, a cloud-based virtual private server provider.

16. Records from BitLaunch for the virtual private server hosted at IP address 172.86.75[.]235 indicate that it was registered on September 14, 2023, using the email address

robert.pook[@]mailfence.com. According to records obtained from BitLaunch records, the BitLaunch services associated with this account, including the identified virtual private server, were paid for via eight recorded cryptocurrency transactions. One of those transactions occurred on November 7, 2024, and was funded from the cryptocurrency address 0xb4310C702D7b712E65CC911b794B97608686eEcd (hereinafter "0xb431"). The 0xb431 address was originally funded by the address 0x1302312D40Bb5978e250a1A9a3E2a3BDd44cAC2B ("0x1302") on October 11, 2024. The 0x1302 funding address contained a total of ten transactions and two separate cryptocurrency invoices facilitated by BitPay, an online cryptocurrency payment service provider. The invoices were dated April 16, 2024, and June 10, 2024. Based on my training and experience, given the limited number of transactions conducted by the 0x1302 address, it was likely used and controlled by a single individual, as opposed to being an operational address used by a cryptocurrency exchange, reseller, business, or group. A cryptocurrency address operated by such an exchange, reseller, business, or group, would likely contain many more transactions.

17. The FBI was able to obtain records from BitPay associated with these two invoices. Both invoices reflect purchases from the merchant 75 Global, LLC, which operates the Domains4Bitcoins.com website, where users can purchase domain names using cryptocurrency. The June 10, 2024, transaction was performed by a buyer using the email address sharedstaffaccout[@]proton.me and was for the [redacted] domain. As outlined above in paragraph 10, three subdomains of [redacted] were used in close coordination with the targeting of a U.S. educational institution on March 13, 2025.

18. The second BitPay transaction occurred on April 16, 2024, at 17:26:02 UTC. The invoice was viewed on that date via three different IP addresses: 2a03:1b20:6:f011[::]e52e,

172.94.17[.]251, and [redacted]. According to open source WHOIS research, two of the IP addresses – 2a03:1b20:6:f011[::]e52e and 172.94.17[.]251 – are listed as anonymous and as potential hosting providers. (Hosting providers generally store a website's files on a server and make it accessible on the internet.) WHOIS research associated with the third IP address, [redacted], shows that it is neither anonymous, nor a hosting provider, nor a proxy node, and is managed by a Russia-based internet service provider ("ISP") called OOO Suntel. Based on my training and experience and public WHOIS information, I believe the IP address [redacted] is a true, non-anonymized IP address and that OOO Suntel would likely hold subscriber records for the customer assigned that IP address at the relevant date and time.

19. According to the FBI's investigation, on the same day as the second BitPay invoice (April 16, 2024), the [redacted] IP address was used to access a particular U.S. service provider account registered using the email address wisperrrrr[@]gmail.com (the "Service Provider Account"). Additional investigation revealed the [redacted] IP address was used to access the Service Provider Account approximately 1,283 times between September 28, 2023, and February 6, 2025 (*i.e.*, a period encompassing the two BitPay invoice dates). Based on my training and experience and the fact that [redacted] appears to be a true IP address, this long-term, overlapping IP address usage suggests that the Service Provider Account and the wisperrrrr[@]gmail.com email account share a common user, and that this same person accessed the April 16, 2024, BitPay invoice described above in paragraph 18.

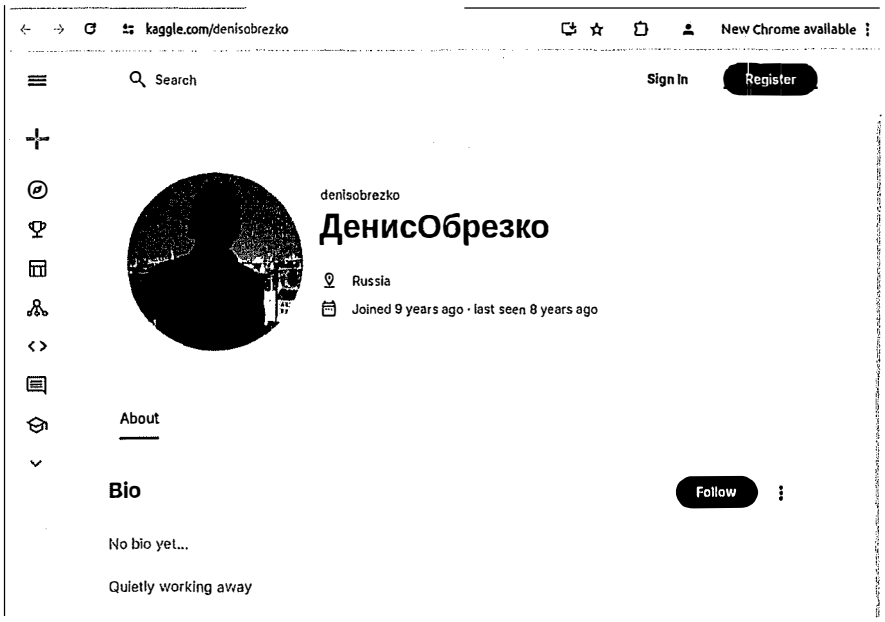
20. Subscriber records from Google associated with the wisperrrrr[@]gmail.com account indicate that it was registered on May 17, 2020, using the name John Peters, the recovery SMS number +79263799902, and the recovery email address w1sper[@]mail.ru. I am aware that +7 is the country code for Russia.

21. According to records from Google, the wisperrrrr[@]gmail.com email address and the SMS number +79263799902 were both used as a means of account recovery for another Google email account, denis.obrezko[@]gmail.com. The denis.obrezko[@]gmail.com email address was registered on August 29, 2016, using the name Денис Обрезко, which translates to Denis OBREZKO.

22. The denis.obrezko[@]gmail.com email address and telephone number +79263799902 were also used to register an X account (formerly Twitter) on September 11, 2016, under the name "DenisOBREZKO," and a PayPal account on February 4, 2020, under the name Денис Николаевич Обрезко, which machine translates to Denis Nikolayevich OBREZKO. In my training and experience, the fact that all the above accounts share the same recovery telephone number suggests that they are controlled by the same user – in this case, OBREZKO.

23. OBREZKO's date of birth is listed in PayPal subscriber records as May 17, 1990. According to a leaked 2023 Russian government database containing information on Russian citizens, a Russian national with the name Денис Обрезко (translates to Denis OBREZKO) and date of birth of May 19, 1990, was associated with the phone number +79263799902.

24. Additional open-source research confirms that Denis OBREZKO is a real person residing in Russia. Through a Google search of "denisobrezko," the following Kaggle (a community site for artificial intelligence and machine learning enthusiasts) account was observed.



25. The same profile picture appears for the Instagram account @wisperrrrr with the name Денис (Dennis) as shown below.

26. Through a Google search using the Cyrillic version of OBREZKO's name, Денис Обрезко, an individual of the same likeness and name was a guest speaker at the Moscow Technical University of Communications and Informatics in 2021 as photographed below (source: mtuci[.]ru).

27. In summary, the IP address [redacted] — believed to be a true, non-anonymized, IP address — was used over a thousand times to access OBREZKO's personal Service Provider Account. The same IP address is connected via cryptocurrency transactions to the purchase of infrastructure used in conjunction with targeting of computer intrusion victims by

Void Blizzard using stolen means of identification (*i.e.*, session tokens). There is probable cause to believe, therefore, that OBREZKO facilitated the unauthorized access to U.S. victim accounts, in coordination with others known and unknown, and who belong to the Russia-aligned cyber threat group Void Blizzard.

CONCLUSION

28. Based on the information described above, I submit there is probable cause to believe Denis Nikolayevich OBREZKO, Cyrillic Денис Николаевич Обрезко, violated 18 U.S.C. § 371. Therefore, your affiant respectfully requests this Court issue an arrest warrant for OBREZKO.

Sworn to under the pains and penalties of perjury,

[redacted]
Special Agent
Federal Bureau of Investigation

Sworn to me via telephone on October 15, 2025.

HONORABLE DONALD L. CABELL
CHIEF UNITED STATES MAGISTRATE JUDGE