TLP: GREEN

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

28 AUG 2020

Alert Number

MU-000132-DD

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**. Email: cywatch@fbi.gov

Phone: **1-855-292-3937**

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS/CISA and US Treasury.

This FLASH has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Cyber Criminals Claiming to be Fancy Bear Conduct Ransom Denial of Service Attacks Against Financial Institutions, Other Industries Worldwide

Summary

Beginning 12 August 2020, thousands of institutions in multiple industry verticals across the globe began receiving ransom denial of service (RDoS)[a] extortion emails from cyber criminals claiming to be "Fancy Bear"[b] demanding bitcoin. The emails stated the actors would demonstrate their capability by conducting a small distributed denial of service (DDoS) attack and that a more substantial attack would occur within six days if payment was not received. The DDoS "demonstration" activity varied across institutions with some targeting a single IP address and others targeting multiple IP addresses, as well as variable peak volumes and attack length. Most institutions that reached the six-day mark did not report any additional activity or the activity was successfully mitigated; however, several prominent institutions did report follow-on activity that impacted operations, indicating this is an active campaign. In 2017 and 2019, cyber criminals posing as the Fancy Bear advanced persistent threat (APT) group and other APT groups[c] launched RDoS attacks against companies in the financial sector and demanded a ransom in bitcoin.

[a] RDoS campaigns are extortion-based DDoS attacks motivated by financial gain.

[b] Fancy Bear is also tracked under the following names: APT 28, Sednit, Sofacy Group, Pawn Storm, and Strontium.

[c] The FBI has also observed RDoS activity from the same actors claiming to be Cozy Bear, Lazarus Group, and the Armada Collective.

Technical Details

Beginning on 12 August 2020, the FBI observed a cyber criminal RDoS extortion campaign targeting institutions worldwide in the financial, retail, travel, and e-commerce sectors. The targeted financial institutions received RDoS extortion emails purportedly from Fancy Bear actors that threatened to conduct a 2 terabit per second (Tbps) DDoS attack against each institution unless they paid the actors 20 bitcoin,[d] which is approximately $227,567.20. *See Figure 1*. The email indicated the cyber criminals would demonstrate their capability by conducting a small DDoS attack against an identified Internet Protocol (IP) address and stated a more substantial attack would occur within six days if payment was not received.

> *"If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time. (sic)" - Armada Collective*

The extortion letters also focus on reputation, warning that the pending attacks will do more than just harm infrastructure.

> *"...your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers. [...] We will completely destroy your reputation and make sure your services will remain offline until you pay. (sic)" - Fancy Bear*

Figure 1 – Snippets from the Ransom Note

The DDoS "demonstration" activity varied across institutions, with some targeting a single IP address and others targeting multiple IP addresses, as well as variable peak volumes and attack length. Importantly, most institutions that ignored the demand and reached the six-day mark did not report any follow-on activity; however, at least two institutions experienced multiple attacks, one of which experienced impacts to their operations. Moreover, additional institutions continue to receive the extortion note, indicating the campaign is ongoing.

This activity is consistent with two previous cyber criminal RDoS campaigns in 2017 and 2019 in which a group identifying itself as "Fancy Bear" sent RDoS extortion emails demanding payment of one to two bitcoin – approximately $20,015.70 as of November 2019 – to financial, retail, and e-commerce institutions in locations around the globe, according to cyber security firms. The ransom notes in the 2017 and 2019 were nearly identical to those in the 2020 incidents, and in most cases the extortion email was followed by no DDoS activity or by activity that was easily mitigated.

[d] The FBI has observed ransom demands that vary from five to 30 bitcoin, which is approximately $56,891.80 to $341,350.80.

The observed DDoS attacks were primarily reflective attacks with ranges in peak volume from approximately 28.8 gigabits per second (Gbps) to 200 Gbps. The attack vectors included the following protocols:

Attack Types				
ARMS reflection	CLDAP reflection	DNS flood	DNS reflection	WS-Discovery reflection or amplification
GRE flood	NTP flood	SNMP flood	UDP flood	UDP fragment

Protocols			
UDP	CLDAP	DNS	WS-Discovery
GRE	NTP	SNMP	

The observed DDoS attacks had the following related source to destination ports:

Source Port	Destination Port
3283	80
53	48303
161	49205
3702	53428
28015	5639
27017	10858
41460	4284
50131	54363
32869	38601
46279	31702
40421	6130

Source Port	Destination Port
UNKNOWN	25385
UNKNOWN	19711
UNKNOWN	5678
UNKNOWN	61726
UNKNOWN	61851
UNKNOWN	57203
UNKNOWN	39215
UNKNOWN	56974
UNKNOWN	50070
UNKNOWN	37022
UNKNOWN	33424

Source Port	Destination Port
3285	5327
11139	37762
24210	22409
43598	6561
3284	50129
43068	28766
35421	34228
1072	28740
UNKNOWN	443
UNKNOWN	54005
UNKNOWN	40377

Information Requested

The FBI does not encourage paying a ransom to criminal actors. Paying a ransom emboldens adversaries to target additional organizations, encourage other criminal actors to engage in additional RDOS activity, and/or may fund illicit activities. Further, paying the ransom does not guarantee that an adversary will not attack a victim's network. However, the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report RDoS incidents to your local FBI field office. Doing so provides the FBI with the critical information they need to prevent future attacks by identifying and tracking RDoS attackers and holding them accountable under US law.

Recommended Mitigations

- Enroll in a Denial of Service mitigation service that detects abnormal traffic flows and redirects traffic away from your network.
- Consider throttling UDP packets with lengths greater than 468 bytes that are sourced from known amplification ports, such as: 1-1023, 1194, 1434, 1900, 3074, 3283, 3702, 5683, 11211, 17185, 20800, 27015, 30718, 33848, 37810, 47808. Note that rate-limiting these ports may cause a loss of functionality on production networks; therefore, you should test these changes on a non-production network and advise all customers before deploying this mitigation. Pay special attention to recursive DNS servers, which may need to receive large responses from port 53.
- Actively monitor inbound email traffic sent to executives and the email address(es) associated with your organization's American Registry for Internet Numbers (ARIN) registry for ransom demands, which may be indicative of a forthcoming attack.
- Configure network firewalls to block unauthorized IP addresses and disable port forwarding.
- Create a partnership with your local internet service provider (ISP) prior to an event and work with your ISP to control network traffic attacking your network during an event. The ISP may retain forensic data necessary for law enforcement investigations.
- Ensure all network devices are up to date and security patches are incorporated when available.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP:GREEN**. Recipients may share **TLP:GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP: GREEN** information may not be released outside of the community.

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.