Radware Cybersecurity Alert

2020 Ransom DDoS Campaign Update

October 14, 2020

RADWARE AND THE **FBI** WARNED IN AUGUST ABOUT A GLOBAL RANSOM DDOS CAMPAIGN TARGETING FINANCIAL INSTITUTIONS AND OTHER INDUSTRIES WORLDWIDE. RADWARE HAS WITNESSED AN INCREASE OF NEW EXTORTION LETTERS FROM ORGANIZATIONS ACROSS THE GLOBE.

A New Wave of Ransom Letters

Since middle of August, Radware has been receiving letters sent to several organizations by actors posing as 'Fancy Bear', 'Armada Collective' or 'Lazarus Group'. The letters are sent to a generic email address and do not always immediately reach the right person in the organization. In some cases, letters were received by subsidiaries or branches in the wrong country.

The letters from 'Armada Collective' were an earlier outlier and used different language compared to letters from the same period and more recent extortion letters from actors posing as 'Fancy Bear' and 'Lazarus Group'. The latter are consistent in their use of the English language, matching up paragraph by paragraph. The letters have been improved since the start of the campaign by fixing some typos, rephrasing some actions for better clarity, and press coverage of earlier DDoS attacks that impacted financial organizations have been added to instill more fear.

All the letters Radware received from different organizations across the world indicate that 'Lazarus Group' is the sender when the target is a financial organization. **Intel417** recently reported that criminals posing as Lazarus Group threatened Travelex, a British foreign exchange, with a DDoS attack unless it paid 20 bitcoins.

The moniker 'Fancy Bear' is leveraged only for Technology and Manufacturing targets. The actors seem to have a preference of APT depending on the vertical they are trying to convince to pay a ransom.

APT38, Lazarus

The APTs have been chosen carefully by the actors and do follow a certain logic. 'Lazarus', also referred to as 'APT38', or 'BeagleBoyz' by the Department of Homeland's Cybersecurity and Infrastructure Security Agency (CISA), has been attributed to attacks targeting mostly financial institutions and is believed to have close ties with the North Korean government.

Just last week, the CISA published a warning **'FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks'**. The title of alert AA20-239A leaves little to the imagination and attributes new attacks to 'Lazarus Group' as it **ramped up its efforts** to raise money for its sponsor, the North Korean government. Via numerous campaigns targeting organizations in the cryptocurrency space and financial sector, the cash-strapped nation hopes to raise funds for its **missile program**.

While 'Lazarus' targets organizations in the finance industry, DDoS is not a tactic typically used by the group to get funds. It resorts to malware frameworks and compromised payment networks and servers.

APT28, Fancy Bear

'Fancy Bear', also known as 'APT28' or 'Sofacy Group', is a Russian cyber espionage group and believed to have close ties with the Russian military intelligence agency GRU as sponsored by the Russian government. 'Fancy Bear' was **blamed for the DNC hacks** back in April of 2016. The group typically targets government, military, and security organizations. Fancy Bear is **thought to be responsible** for the cyberattacks on the German parliament, the French television station TV5monde, the White House, NATO, the Democratic National Committee, the World Anti-Doping Agency, the Organization for Security and Co-operation in Europe and the campaign of French presidential candidate Emmanuel Macron. The group promotes the political interests of the Russian government and among others, their tactics include zero-day exploits, spear phishing and malware drop websites disguised as news sources to compromise targets.

"Fancy Bear" typically does not resort to DDoS tactics and typically doesn't target technology or manufacturing organizations unless they are associated with government or political institutions and are seeking to infuse political influence or chaos, and not for financial gain by extortion.

A Small Price to Pay

The extortion letters sent by the Ransom DDoS group warn that the recipient's network will be subject to a DDoS attack starting in about a week from the sending of the letter. On the date of sending, a small attack on the victim's IPs of the ASN number mentioned in the letter is done to prove the legitimacy of the threat but promises not to cause any damage to not worry the victim. They claim there are no counter measures to their attacks and to have the ability to perform volumetric attacks that peak over 2Tbps.

The initial ransom demand is set at 20 BTC (about $230,000 USD at the time of writing) and will increase by 10 BTC for each day not paid, over which time they will uphold the attack.

There is no way to communicate with the blackmailers, so there is no option to negotiate and the only way to get a message through is by sending BTC to the bitcoin address mentioned in the letter. Every victim has a unique bitcoin address to track payments. If payment is not met by the deadline set by the extorters, they send a follow up message noting that they did not find any ransom payments at the bitcoin address and that this must be a mistake on the victim's side. As they are not bluffing or trying to make quick money, they prefer payment over destruction while giving the victim a "second chance to reconsider before going down for good."

Subject: DDoS Attack

We are the Lazarus Group and we have chosen [redacted] as target for our next DDoS attack.

Please perform a google search for " Lazarus Group" to have a look at some of our previous work. Also, perform a search for "[redacted]" or "[redacted]" in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting [redacted] next week. (This is not a hoax, and to prove it right now we will start a small attack on a few of your IPs from AS[redacted] block that will last for about 60 minutes. It will not be heavy attack, and will not cause you any damage, so don't worry at this moment.) There's no counter measure to this, because we will be attacking your IPs directly and our attacks are extremely powerful (peak over 2 Tbps)

This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers who use online services.

Worst of all for you, you will lose Internet access in your offices too!

We will refrain from attacking your network for a small fee. The current fee is 20 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already. And hopefully for this message to reach somebody who can handle it properly.

If you don't pay the attack will start and fee to stop will increase to 30 BTC and will increase by 10 Bitcoin for each day after the deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address: [redacted]

Once you have paid we will automatically get informed that it was your payment.
Please note that you have to make payment before the deadline or the attack WILL start!

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

Do not reply to this email, don't try to reason or negotiate, we will not read any replies.

Once you have paid we won't start the attack and you will never hear from us again.

Please note we will respect your privacy and reputation, so no one will find out that you have complied.

Figure 1: Sample ransom letter, based on the more recent letters but anonimized by retyping the message, changing fonts, altering line breaks, and redacting identifying information

How to React

The threats should be taken seriously but should not concern organizations that have adequate DDoS protection. If you lack protection and receive a letter, find a capable partner to assist you in taking mitigation measures so that follow up attacks do not impact your organization and disrupt your business.

All of the organizations that got in touch with Radware and received an extortion letter matching the sample letter above have seen follow through attacks. The size of the attacks is adapted to the size and attack surface of the targeted organization. Attacks have ranged from a couple of gigabits per second up to hundreds of Gbps. In some cases, peaks were reaching 300Gbps (not the announced 2Tbps) but still devastating for most organizations and combine multiple attack vectors.

The attack vectors include ARMS reflection, CLDAP reflection, WS-Discovery reflection, GRE Flood, NTP Flood, UDP and UDP fragment floods, combined with TCP SYN, TCP out of state, DNS reflection and ICMP floods. Attacks typically last for a couple of hours until the attackers see they are not making progress.

In some cases, we have seen the attackers change tactics and aim their attacks at the DNS services of the victims. The DNS service is often hosted outside of the organization by dedicated providers and some are left without protection. It is important to verify security measures to protect DNS services because simply disrupting the name resolution can be as impactful as a direct attack on the service itself.

Do Not Pay

These threats should be taken seriously, but the attacks are not at a level of complexity or amplitude that they cannot be mitigated when adequate protections are in place. Radware advises organizations to not pay the ransom demand. There is no guarantee blackmailers will honor the terms of their letter. Paying only funds future operations, allows them to improve their capabilities and motivates them to continue the campaign.

FURTHER INFORMATION AND RESOURCES

- **Radware Threat Researchers Live** - Ep4 - The DDoS for Hire Threat Landscape
- **FBI FLASH** - Alert Number MU-000132-DD - Cyber Criminals Claiming to be Fancy Bear Conduct Ransom Denial of Service Attacks Against Financial Institutions, Other Industries Worldwide
- **Radware Threat advisory**: Global Ransom DDoS Campaign Targeting Finance, Travel and E-Commerce
- **Intel471**: Criminals posing as Lazarus Group threatened Travelex: 20 bitcoin or we launch a DDoS
- **How to Respond to a DDoS Ransom Note**

EFFECTIVE DDOS PROTECTION ESSENTIALS

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further **network and application protection** measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

LEARN MORE AT DDOS WARRIORS

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit **DDoSWarriors.com**. Created by Radware's **Emergency Response Team (ERT),** it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.