Radware Cybersecurity Alert

Ransom DDoS Campaign: Circling Back

Jan 22, 2021

DDoS Extortions: Circling Back

During the last week of December, 2020 and the first week of January, 2021, Radware customers were targeted by DDoS extortionists for a second time by a global ransom DDoS campaign that **initially started in August**. Organizations received new letters that started with:

> *"Maybe you forgot us, but we didn't forget you. We were busy working on more profitable projects, but now we are back."*

Organizations that received this letter were companies that received threats in August and September of 2020. Analysis of this new wave of ransom letters suggests that the same threat actors from the middle of 2020 are behind these malicious communications.

- Organizations that received these new letters did not respond/pay the ransom demand in the middle of 2020
- Companies that received these new letters were not revealed to the media in August/September of 2020, so only the original threat actor would know these companies
- Radware is confident that the same threat actors that initiated this campaign in 2020 are still active today.

The ransom letter continued:

> *"We asked for 10 bitcoin to be paid at <bitcoin address> to avoid getting your whole network DDoSed. It's a long time overdue and we did not receive payment. Why? What is wrong? Do you think you can mitigate our attacks? Do you think that it was a prank or that we will just give up? In any case, you are wrong."*

Bitcoin Surging

When the DDoS extortion campaign started in August of 2020, a single Bitcoin was worth approximately $10,000. At the time of publication of this alert, it is worth approximately $30,000. This was cited by attackers in this latest round of ransom letters and is representative of the **impact the rising price of Bitcoin is having on the threat landscape**.

> *"We can easily shut you down completely, but considering your company size, it would probably cost you more one day without the Internet then what we are asking so we calculated and decided to try peacefully again. And we are not doing this for cyber vandalism, but to make money, so we are trying to be make it easier for both."*

> *"We will be kind and will not increase your fee. Actually, since the Bitcoin price went up for over 100% since the last time we will temporarily decrease the fee to 5 BTC! Temporarily."*

> *"Yes, pay us 5 BTC and we are gone!"*

> *"You can pay us to the same address we gave you last time or if you need a new one for any reason (privacy, because you have probably forwarded our first email to law enforcement): <new bitcoin address>."*

The message concludes with:

> *"Remember, we never give up. And we always come back, until we are paid. Once paid we are gone and you will never hear from us again - forever."*

The Attack

A few hours after receiving the message, organizations were hit by DDoS attacks which exceeded 200Gbps and lasted over nine hours without slowdown or interruption. A maximum attack size of 237Gbps was reached with a total duration of nearly 10 hours (see Figure 1). The attack vectors used match the original attacks, mainly consisting of UDP fragments, UDP Port 80 and DNS traffic.

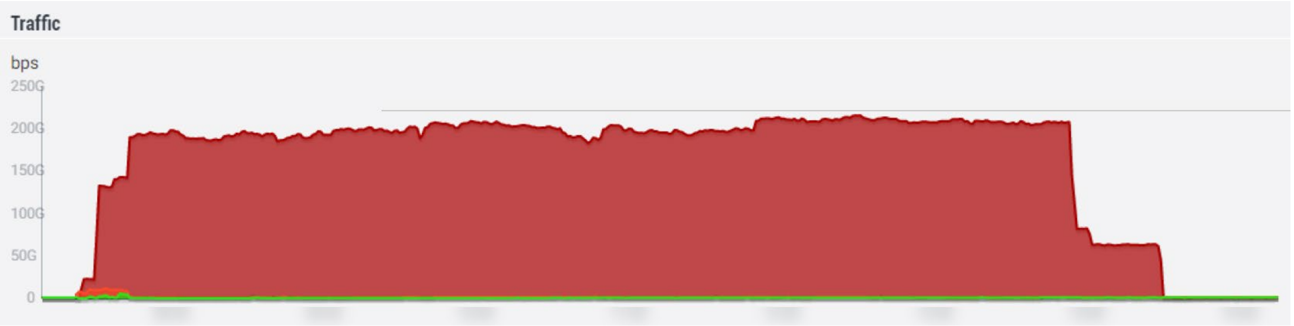

Figure 1

Reasons for Concern

1. Ransom DDoS or DDoS extortion campaigns have traditionally been a seasonal event. They would run annually for a few weeks targeting specific industries/companies before the threat actor(s) would typically give up. The 2020/2021 global ransom DDoS campaign represents a strategic shift from these tactics. DDoS extortion has now become an integral part of the threat landscape for organizations across nearly every industry since the middle of 2020.
2. The threat actors are circling back to previous targets. If your organization received a letter before, there is a high chance you will receive a new letter.
3. The perseverance, size and duration of the attack makes us believe that this group has either been successful in receiving payments or they have extensive financial resources to continue their attacks.

Our Recommendation

Your organization should partner with security experts to protect yourself from DDoS attacks. In addition, Radware strongly advises against paying. There is no guarantee the attacks will stop following payment or

the treat actor won't initiate new attacks after a first payment. Typically, this category of cybercriminal is seeking financial gain. Knowing an organization has succumbed to the threat will lead them to circle back in the future.

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.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate** – using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

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.