Radware Advisory

Ransom Denial-of-Service (RDoS) 2022

Phantom Squad & REvil, Growing Sophistication

May 25, 2022

Over the past several months, Radware has observed a significant increase in DDoS activity across the globe and has been rapidly onboarding new customers in distress. These attacks have ranged from cases of **hacktivism** in Europe and the Middle East to **Terabit DDoS attacks** in Asia and the United States.

However, one of the more concerning trends seen over the past few months has come from ransom denial-of-service (RDoS) groups claiming to be Phantom Squad and REvil. Radware researchers previously alerted about a similar RDoS campaign from a threat group claiming to be **Phanton Squad** in 2017 and more recently covered a campaign about an RDoS threat group claiming to be **REvil**, the notorious ransomware group.

Background

An RDoS campaign is a distributed denial-of-service (DDoS) attack motivated by monetary gain and leveraging extortion as its tactic. Attackers typically start by sending an email or posting on social media threatening to launch an attack on a particular day and time unless a ransom is paid, usually in Bitcoin, by the victim. In some cases, attackers launched a small demonstration attack on the victim's network as evidence that the threat is serious.

RDoS campaigns can be financially rewarding for cybercriminals who can make money for little to no investment. Consequently, several threat actors are now impersonating notorious threat groups and sending out ransom threats, some with no intention of launching an attack, hoping to make a profit.

PHANTOM SQUAD

In 2017, a group claiming to be Phantom Squad, a notable threat group known for launching largescale DDoS attacks in 2015, leveraged its name and emailed ransom letters to thousands of organizations worldwide. At the time, the group was demanding 0.2 Bitcoin (~ $840 US back in the day) under the threat of a DDoS attack. Due to the large number of organizations that received a ransom letter and the low ransom demand, it was quickly determined that the group posing as Phantom Squad could not follow through with their threats. Their objectives were more likely to spread fear and chaos, not drive monetary profit.

```
FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE
DECISION!

We are Phantom Squad

Your network will be DDoS-ed starting Sept 30th 2017 if you don't pay
protection fee - 0.2 Bitcoin @ [redacted]

If you don't pay by Sept 30th 2017, attack will start, yours service going
down permanently price to stop will increase to 20 BTC and will go up 10 BTC
for every day of attack.

This is not a joke.
```

Figure 1: 2017 Phantom Squad RDoS letter

Fast forward five years and Radware is observing signs of either a reemergence of the same fake RDoS threat group or a new threat group leveraging the name and tactics, techniques, and procedures (TTPs) of the former campaign.

On May 22, 2022, a near identical ransom letter from the 2017 Phantom Squad appeared. The only difference between the 2017 letter and the current letter in circulation is the addition of a targeting section, where the threat group provides IP addresses and domain names of their intended targets.

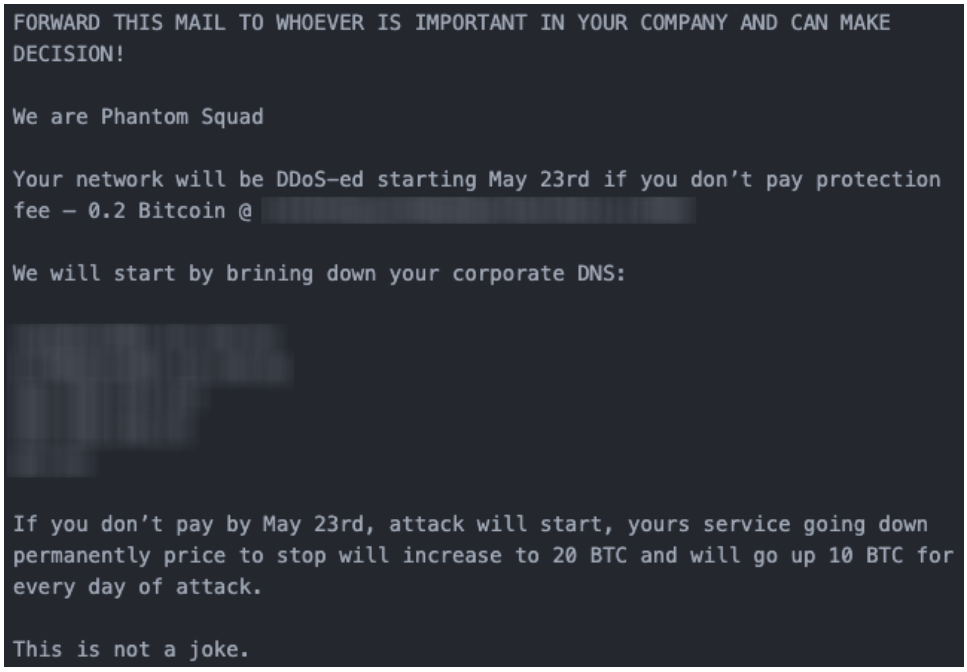

Figure 2: 2022 Phantom Squad RDoS letter

During the 2017 campaign, both the value of the ransom in combination with the total number of victims played a role in determining the threat's validity. In comparison, only one letter has surfaced at the time of writing with no reported or observed outages or demonstration attacks directed at the targeted victims. It is also important to note that the price of Bitcoin has increased significantly over the last five years, resulting in the 0.2 Bitcoin demand now being worth approximately US$6,000 (at the time of publication).

Determining a threat's validity is difficult, but several indicators can be used to determine the risk. Indicators such as how many victims are targeted, how high or low the ransom demand is, and if a demonstration attack was observed. Unfortunately, it is still unknown how many organziations have reveived the current letter in circulation at the time of writing. Radware knows that only one group of victims was targeted and no attacks have been reported. But one suspicious indicator stands out in the current ransom letter: the Bitcoin address.

The Bitcoin address used in the recent ransom letter from the group claiming to be Phanton Squad corresponds to a dormant wallet once **used** during the notorious Wannacry ransomware campaign in 2017. The threat actors behind the current Phantom Squad RDoS campaign are unlikely those who possess this known cash-in/cash-out

wallet address has transacted over 200 times and received an aggregate total Bitcoin value of over $500,000. The current RDoS campaign is likely using the wallet, its transactions and the value to spread fear for yet unknown reasons.

REVIL, THE RDOS GROUP

During one of the many waves of RDoS campaigns in 2021, a group claiming to be REvil targeted several VoIP providers worldwide. At the time, REvil, a notorious ransomware group, had just **returned to action** after disappearing following the Kaseya VSA ransomware attack. The RDoS campaign sparked concern as critical infrastructure was impacted and resulted in an industry-wide warning from Comms Council UK **stating** a "coordinated extortion-focused international campaign by professional cyber criminals" targeting IP-based communication services providers during October 2021. And while RDoS attacks typically were considered lower tier threats that are easy to mitigate, Bandwidth.com **went on record** that the RDoS attacks caused a $700,000 dent in their Q3 revenues and would end up costing them up to $12 million in actual and reputation damages.

During the first quarter of 2022, a renewed campaign of RDoS attacks by a group claiming to be REvil emerged. This time the group is not only sending warning ransom notes before the attack starts, but also embeds the ransom note and demands in the attack payload. The attacks are high-frequency HTTPS GET request floods lasting several minutes and ranging up to several millions of requests per second, targeting online applications and hosts and embedding the ransom message as a readable string in the URL.

Embedding the ransom note in the payload of a DDoS attack is not a new technique. In March 2018, attackers **embedded ransom demands** in the payload of Memcached DDoS amplification attacks. Taking into account that most online applications are logging the URL of GET requests for troubleshooting, leveraging the URL is not a bad technique to get the demand noticed. Whenever a host or website is deteriorating, the first place to look for potential causes are the log files of the server which will be filled with ransom demands.

Attacks leveraging HTTPS request floods with embedded ransom notes by the actor posing as REvil were first **reported** in early March, 2022. During those attacks, the first wave of floods contained a message directed at the web operators of the victim (see Figure 3).

*Figure 3: REvil RDoS note embedded in URL of first wave of attacks (source: **Imperva**)*

As the attacks progressed, the threat group was observed changing the requests' messages to intimidate their victims further. The second wave addressed the CEO of the organization under attack and claimed responsibility for the attacks on service provider Bandwidth.com (see Figure 4).

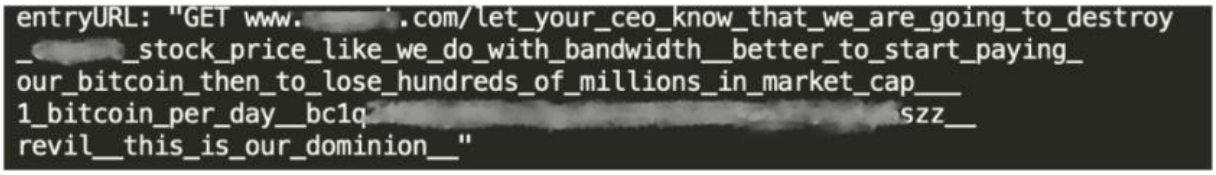

*Figure 4: REvil RDoS note embedded in URL of second wave of attacks targetting the same organization (source: **Imperva**)*

In early May, 2022, Radware was notified of an RDoS attack with a ransom message embedded in the URL, signed with "REvil, this is our dominion" (see Figure 5). The ransom note differs from earlier reported notes. The threat actors seem to be customizing their demands and messages based on the targetted victim.

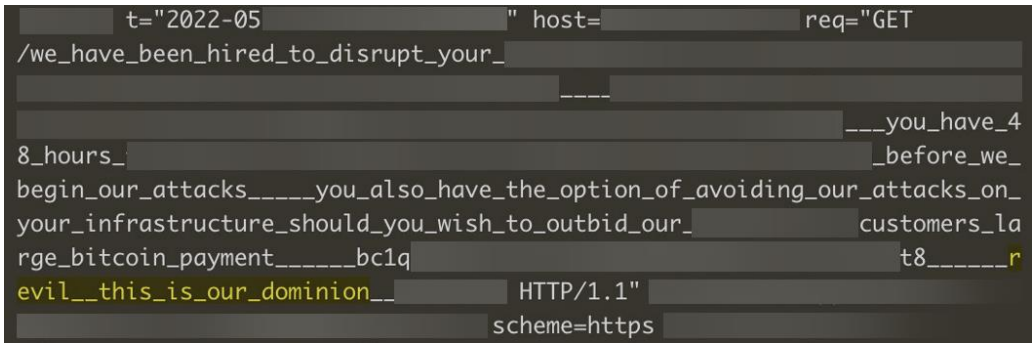

Figure 5: REvil RDoS note embedded in URL and recorded in server log files (source: Radware)

The aggressive attacks lasted several minutes and consisted of millions of HTTPS GET requests per second.

Tactics, Techniques and Procedures

ATTACK VECTORS

Most RDoS threat groups manage their own attack infrastructure. However, some leverage publicly available stresser services to conduct their campaigns. RDoS attacks are characterized by malicious packet floods reaching several hundreds of gigabits per second and leveraging multiple concurrent attack vectors. The attack campaigns are typically persistent and can last for several days of continuous floods for multiple hours per day. Attack vectors used by RDoS threat groups include, but are not limited to:

- UDP Amplification/Reflection
- TCP Amplification/Reflection
- HTTP(S) Request Floods
- Direct path random spoofed UDP and SYN Floods
- Direct path random spoofed TCP-ACK Floods
- GRE IP & ETH Packet Floods

In 2022, Radware has noticed the addition of new techniques and procedures leveraged by RDoS groups. While the typical RDoS attack was generally characterized as a long, network-level volumetric flood, new threat groups

have begun to employ shorter bursts of high rate (rps) encrypted application level attacks with messages embedded in the request URL.

DELIVERY TECHNIQUES

The typical delivery method for RDoS threat groups is email, but there are exceptions. Years prior, threat group XMR Squad ran a ransom campaign using a Twitter account to deliver their ransom notes. The RDoS threat group claiming to be REvil targetting VoIP providers at the end of 2021 also leveraged a Twitter account to pressure their victims by publicly involving the customers of the victims in a bid to force payment.

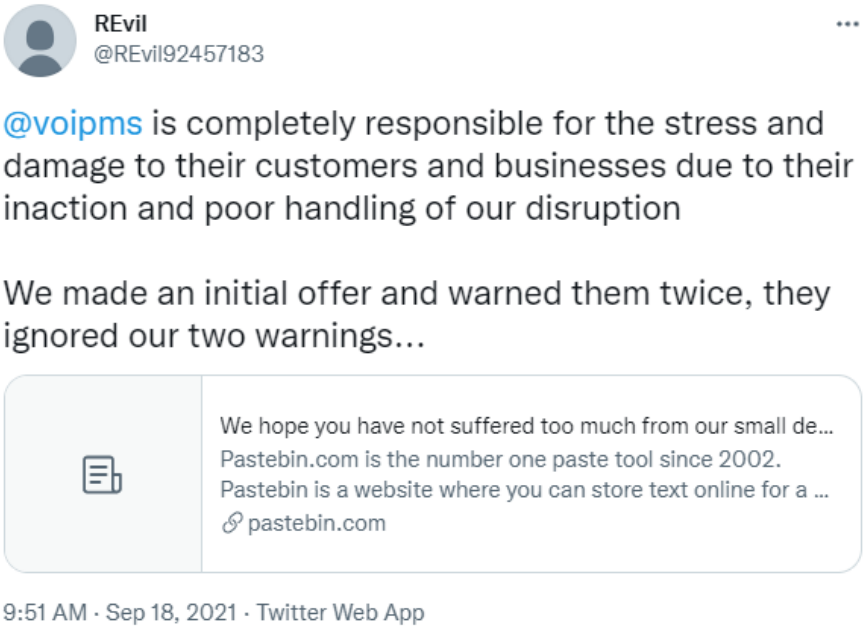

Figure 6: RDoS threat group posing as REvil leveraging Twitter messages to pressure their victims

The same group, months later, was also observed sending ransom notes in the form of an embedded web request. The technique of embedding messages in the payload of DDoS attacks is not new however. One of the first occurrences dates back to 2018, when **Cybereason** observed a threat actor embedding ransom notes in an amplified DDoS attack. At the time, amplification attacks leveraging exposed Memcached servers were responsible for some of the largest recorded DDoS attacks. Cybereason had discovered that those attacks also contained a ransom note in their payload. The ransom note instructed the victims to send 50 XMR to stop the attacks.

TARGETS

The recent extortion letter from the threat group claiming to be Phantom Squad lists a government agency, service providers, and a financial institution as their targets.

- Government
- Service Providers
- Financial Institutions

Reason for Concern

The RDoS threat groups posing as Phantom Squad and REvil appear to be targeting organizations in Europe, the United States and Asia. And while the 2017 Phantom Squad campaign went without actual DDoS assaults, Radware still recommends organizations to stay vigilant.

The group posing as REvil has been observed launching largescale DDoS attacks and using advanced tactics to pressure their victims. Last year, Radware said that RDoS had become a persistent threat, and we do not expect this to change any time soon.

Radware last year also witnessed RDoS threat groups **circling back** to previous victims, demanding for a second time a ransom payment under the threat of a DDoS attack. A few hours after receiving the message, organizations were hit by continuous DDoS floods exceeding 200Gbps and lasting more than nine hours. Due to the persistence, size, and duration of these attacks, Radware believes that the threat group was either successful in receiving payments or had extensive financial resources to fund their long running campaign.

As the RDoS threat landscape continues to evolve, Radware expects to see more largescale, encrypted network and application DDoS attacks leveraged by advanced threat actors in an attempt to force a ransom payment. Over the years, threat actors have become increasingly sophisticated. The recent shift of new tactics and techniques indicates this also applies to RDoS threat actors. Their campaigns continue to present a moderate risk level and potential impact for targets that are not adequately prepared.

Additionally, at the time of writing, the motivations and objectives of the current Phantom Squad RDoS campaign are unclear. It is yet unknown if this is the same group that is circling back after a long pause or if this is a new threat group. However, one thing stands out: the threat actors behind current campaign will most probably not be able to access the ransom payment if one was made.

Recommendation

Radware recommends organizations to partner with experts to protect themselves from the threat of DDoS attacks. In addition, Radware strongly advises against paying ransom demands. There is no guarantee attacks will stop while it creates a precedent for threat actors to circle back to earlier victims they received payment from in subsequent campaigns.

Radware recommends organizations, ISPs and CSPs of any size and vertical to assess the protection of their internet connections and plan against globally-distributed DDoS attacks aimed at DNS servers and attempting to saturate internet uplinks.

On-premise or local DDoS detection and mitigation is adequate for latency-sensitive services and applications. Still, it only protects local infrastructure against attacks below the internet links' capacity. Once attacks grow beyond the bandwidth of those connections, an upstream solution is required to block attacks while allowing only legitimate traffic to the organization.

Large and globally distributed DDoS attacks can only be effectively mitigated by stopping malicious traffic closest to its source and never allowing multiple geographically distributed traffic streams to flock. Globally distributed and anycast protection services are most effective against these kinds of DDoS attacks.

Cloud DDoS services will introduce latency, which can be unacceptable for certain applications and services during normal operating conditions. Hybrid DDoS protection provides the best of both worlds with on-premise protection against all types of DDoS attacks while automatically diverting to a cloud DDoS mitigation service when the attacks risk saturating the internet link. While diverted to the cloud, additional latency will be incurred, but the service will remain available while, in peacetime, there is no additional latency.

More information on different deployment options for different use cases can be found in this **blog**.

Our DDoS response guide outlines steps that allow you to minimize the impact of a DDoS attack and how to recover quickly. Download your guide **here**.

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 Cybersecurity 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 THE RADWARE SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks or learn more about emerging attack types and tools visit **Radware's Security Research Center.** 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.