radware

The Definitive Guide to Ransom Denial of Service

Introduction

Over the years, extortion has evolved from the physical world to the cyber realm through taking computer networks hostage for profit. From ransomware to ransom denial of service (RDoS), threat actors aim to extort money – usually in the form of cryptocurrency – from victims by threatening to degrade networks or encrypt systems and block access to systems until payment is rendered.

Threat actors and cybercriminals leverage RDoS to conduct extortion-based DoS attacks that are financially motivated. By disrupting online services, they can impact the business, productivity and reputation of an organization. Attackers target online resources such as websites, domain name services, web APIs, gaming lobbies, and so on to render online services inoperable and impact an organization's reputation. They can also impact the productivity of organizations by targeting voice, email and remote access in branch offices or from remote workers.

An RDoS attack starts with the attacker sending a private message by email, for example, using a privacy-minded email provider, requesting payment of a certain ransom amount to prevent the organization from being targeted by a DDoS assault. If an organization decides not to pay within a set deadline, the attacker will start a DDoS attack and continue until the ransom is paid. Typically, the ransom demand increases every day the victim refuses to pay. Payments are typically demanded in bitcoin (BTC), with the bitcoin address for payment being uniquely tied to the target and providing the threat actor with a way to track payment.

Normally, a DDoS attack lasts for several hours, will change attack vectors attempting to evade detection and mitigation systems and sometimes reappear several days later after several failed attempts. Throughout the 2020–2021 global RDoS campaigns, attacks ranged from a few hours up to several weeks, with attack rates of 200Gbps and higher.

Continued on next page

Continued from previous page

To add credibility, within the ransom letter, an attacker will often refer to a demonstration DDoS attack, which is a DDoS assault launched prior to the payment deadline that is meant to validate the legitimacy of the threat and can impact services if the victim doesn't have adequate DDoS defenses in place.

Threat actors will sometimes pose as well-known cyber groups, such as nation-state-linked advanced persistent threat (APT) groups or notorious ransomware gangs, to instill additional fear. RDoS groups have called themselves Fancy Bear (the Russian APT), Lazarus (the North Korean APT most renowned for its financial industry focus) and "REvil" (a Russian ransomware group). In older campaigns, threat actors used the moniker Armada Collective or even posed as Kadyrovtsy, a Chechen military group.

When there are ongoing RDoS campaigns, less-capable threat actors leverage this time to run hoax campaigns, sending messages with DDoS threats that are not backed by the infrastructure or the capability to perform attacks. The format of these letters attempts to mimic real threat actors and active campaign messages.

< Prev Next >

The Evolution of RDoS Campaigns

RDoS and extortion campaigns are as old as they are diverse and have evolved over the years, driven primarily by cybercriminal motivations and their modus operandi. Most recently, RDoS campaigns, which have historically been short-term, mostly independent events, have evolved into a persistent addition to the DDoS threat landscape.

Take the global RDoS campaign that began in 2020 as an example. In August of that year, a global RDoS campaign began, with organizations across various industries receiving ransom letters from threat actors posing as "Fancy Bear," "Armada Collective" or "Lazarus Group." These initial letters warned that the victim's network would be the subject of a DDoS attack starting approximately one week after receipt of the letter, with the ability to perform a volumetric attack that peaks over 2Tbps. Initial ransom demands were set at 20 BTC[1].

Attacks were multivector assaults that would typically include various types of UDP Floods, DNS reflection attacks, GRE and NTP Floods and others. These attacks would usually last a few hours, until attacks saw that little to no progress was being made.

At the end of 2020, this campaign entered a second phase, whereby companies were targeted by the same DDoS extortionists for a second time. During this second phase, companies received a different ransom

Watch ***Threat Researchers Live, Episode 14***, to Learn More About RDoS

1 www.radware.com/security/ddos-threats-attacks/threatadvisories-attack-reports/global-ransom-ddos-campaign-targeting-finance-travel-ecommerce

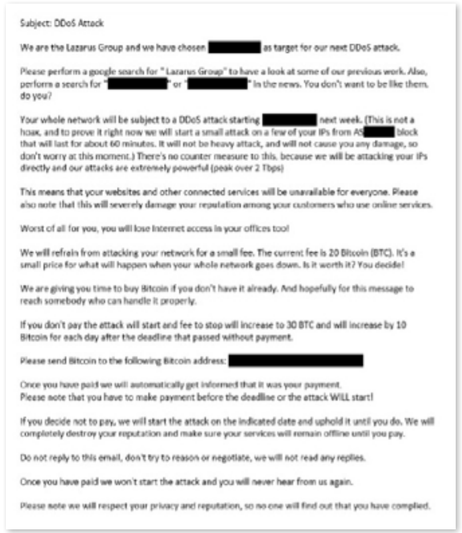
Continued on next page

Continued from previous page

letter (see Figure 2) and were the companies that received threats in August and September of 2020 but did not respond or pay the ransom demand. In addition, companies that received these new letters were not publicly revealed to the media in August and September of 2020. Analysis of this new wave of ransom letters suggested that the same threat actors from the middle of 2020 were behind these malicious communications[2].

The threat actors circled back to earlier targets that did not pay, enabling them to accelerate the campaign by leveraging previous research. These follow-up strikes were typically shorter than earlier threats, leading Radware to believe they were taking this action to accelerate and increase the number of targets while trying to profit from bitcoin's surging value at the end of 2020 and in early 2021.

In the middle of 2021, the campaign evolved yet again through a series of new extortion attempts focused primarily on internet service providers (ISPs) and cloud service providers (CSPs), which reported receiving ransom letters followed by DDoS attacks that impacted their services and availability. Perhaps more important was that DDoS extortion groups began identifying and targeting organizations with unprotected assets. The threat actor(s) targeted only assets protected by cloud protection services leveraging hybrid or on-demand deployment models. Emergency-onboarded organizations leveraging an always-on cloud DDoS protection deployment model did not receive follow-up attacks that could be correlated to the self-proclaimed "Fancy Lazarus" actor. Based on this analysis, it is safe to assume that threat



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!

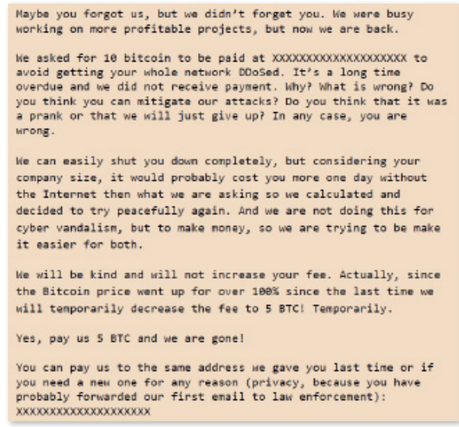
If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

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 letter received by RDoS victims during the 2020–2021 DDoS extortions



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

We asked for 10 bitcoin to be paid at XXXXXXXXXXXXXXXXXXX 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.

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):
XXXXXXXXXXXXXXXXXXX

Figure 2: Sample letter received by RDoS victims during the second phase of the 2020–2021 DDoS extortions

2 www.radware.com/security/ddos-threats-attacks/threatadvisories-attack-reports/ddos-extortions-back

Continued on next page

< Prev Next >

Continued from previous page

actors leveraged Border Gateway Protocol to check for cloud protections in their targets before attempting the DDoS attacks[3].

These service provider–focused assaults also underscore the ability of RDoS threat actors to demonstrate the power and resulting impact of their DDoS attacks by striking unprepared and unprotected targets.

UK-based VoIP operator Voip Unlimited disclosed it was hit by a sustained and large-scale DDoS attack it believed originated from the Russian ransomware group "REvil" following what they described as a "colossal ransom demand." On September 3, after 75 hours of continuous attacks, Voip Unlimited reported a pause in malicious traffic and confirmed a few days later that they did not observe any further attacks[4]. During the same time period, Canadian telephony service provider VoIP.ms announced it became aware of issues preventing customers from accessing its website due to a DDoS attack from a threat actor demanding $4.2 million[5]. The threat actor leveraged Pastebin and Twitter to deliver its ransom demand to Voip.ms. By going public, threat actors increase the pressure on their victims – a tactic used by many of the most notorious ransomware gangs.

And while the threat actors behind these assaults went by the name "REvil," there is no evidence they represent the same REvil ransomware gang that is known to have previously attacked prominent companies.

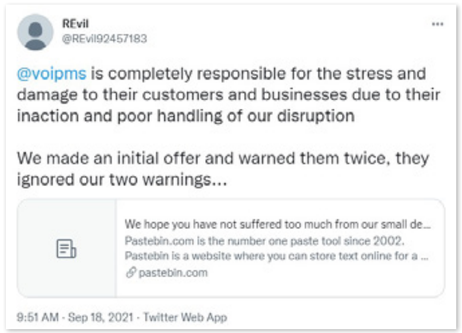
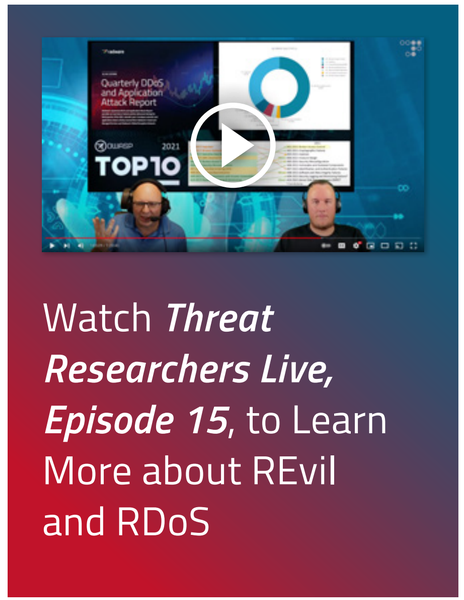


Figure 3: RDoS threat actor posing as REvil delivering ransom note to Voip.ms through Twitter



3 www.radware.com/security/ddos-threats-attacks/threatadvisories-attack-reports/ransom-ddos-update-huntforunprotected-assets
4 www.theregister.com/2021/09/02/uk_voiptelcos_revil_ransom
5 arstechnica.com/gadgets/2021/09/canadian-voip-provider-hitby-ddos-attack-phone-calls-disrupted

< Prev Next >

How to Respond to an RDoS Threat

Don't Pay

Paying DDoS attackers can be damaging on several levels and doesn't guarantee they'll leave your organization alone and/or honor terms. Radware advises against paying a ransom. Moreover, paying a demand potentially "identifies" the target organization as a company willing to pay under threat. Lastly, paying the ransom funds malicious operations, allows threat actors to improve their capabilities and motivates them to continue their campaigns.

Pass the Information On

Many times, DDoS ransom notes are sent "blindly" to the target, using publicly available email addresses. The recipients of these notes are frequently not the relevant stakeholders for network security or IT but, rather, random employees within the target organization. In fact, many ransom notes include instructions to pass this threat on to the relevant people.

As a result, organizations should proactively educate their employees about the existence of RDoS attacks and what to do in case a ransom note reaches them. It is helpful to set up a central email address or contact person for incident handling and explain that all relevant threats should be passed on to them.

Establishing a clear owner and communicating relevant information early and quickly can greatly help the organization to be aware of a ransom note.

Check for a Demonstration Attack

Many ransom notes include the threat of a smaller precursor attack, supposedly to demonstrate the capabilities of the attackers and the viability of the ransom threat.

A demonstration attack can take the form of a small assault that requires checking network logs for traffic spikes indicative of a small-scale DDoS attack. These logs can usually be checked by the organization's network team, security team, ISP or cloud security provider. However, recently, we've seen these attacks take the form of massive,volumetric assaults that can take networks and websites offline.

While it is Radware's recommendation not to pay the ransom in case of attack, evidence of a precursor attack may indicate the viability of the threat and how the target should be prepared. Moreover, it can contain valuable information regarding attack vectors and sources that can be used by your security team and service provider to prepare for any potential subsequent assaults.

Note that evidence – or absence – of a precursor attack does not necessarily mean that an attack will or will not follow. Radware has seen cases where there was no precursor attack despite the threat of one, and other cases where there was evidence of a precursor attack

Continued on next page

Continued from previous page

but a larger attack never followed. Nonetheless, looking for signs of a precursor attack may be a useful indicator as to the seriousness of the threat.

Alert Your Security Provider

Regardless of the severity of the risk, you should alert your security provider to the threat, provide them with the ransom letter and any attack vector data resulting from a demonstration attack and have them jointly monitor attack activity with you. Alerting your security provider can give them time to prepare, monitor your traffic more closely and apply additional security mechanisms, in case they are needed. If you don't already have a dedicated DDoS scrubbing solution, now is a good time to consider deploying one.

How To Prepare for a Ransom DDoS Attack

The best time to prepare for an ransom DDoS threat is before any potential attack occurs. DDoS attacks may come at any time, whether they are accompanied by a ransom demand or not. However, a DDoS ransom note increases the risk and reinforces the need for comprehensive protection against DDoS attacks. Use this threat as an opportunity to apply best practices for DDoS protection.

Continued on next page

< Prev Next >

Continued from previous page

Understand Your Attack Surface

Make a list of all exposed services – such as applications, IPs, servers, data centers and locations – their dependencies and what services are hosted on premise or by a third party. For example, a website or VPN could be dependent on the availability of a DNS service. It's important to know whether that DNS service is hosted by a third-party provider and how secure that provider is from DDoS attacks.

The first step to securing your assets against a DDoS attack is to know what assets you have that need to be secured. Prioritize the list of assets to be protected, and assess which assets are mission critical and which require extra protection. Begin by listing all externally facing assets that could be attacked.

This list should include both physical and virtual assets:

- Physical locations and offices
- Data centers
- Servers
- Applications
- IP addresses and subnets
- Domains, subdomains and specific fully qualified domain names
- Mapping externally facing assets will help you construct a threat surface and identify points of vulnerability

Have a Plan

Formulate and execute a DDoS response plan, with predefined steps of what to do before, during and after a DDoS attack. Such a plan requires a more in-depth evaluation and analysis than can be provided in this guide, but download our guide to understand all aspects of a DDoS response plan:

Be Aware that Comprehensive DDoS Protection Is Critical

Deploy dedicated DDoS protections backed by a leading DDoS protection vendor that has the capabilities and experience for handling the types of large, sophisticated attacks typically associated with RDoS campaigns. Ultimately, the best defense for any RDoS threat is ensuring comprehensive protection is in place before any ransom threat is received. DDoS protection is not a one-size-fits-all proposition, and there are many types of protection options, depending on the characteristics, risk and value of your digital assets.

Continued on next page

Continued from previous page

ON-DEMAND CLOUD MITIGATION SERVICES are activated only once an attack is detected. They require the lowest overhead and are the lowest cost solution, but they require traffic diversion for protection to kick in. As a result, they are best suited for cost-sensitive customers, services that are not mission critical and customers who have never been (or are infrequently) attacked but want a basic form of backup.

ALWAYS-ON CLOUD SERVICES route all traffic through a cloud scrubbing center at all times. No diversion is required, but there is minor added latency to requests. This type of protection is best for mission-critical applications that cannot afford any downtime and organizations that are frequently attacked.

HARDWARE-BASED APPLIANCES provide advanced capabilities and fast response of premise-based equipment. However, an appliance on its own is limited in its capacity. Therefore, these appliances are best used for service providers that are building their own scrubbing capabilities, or in combination with a cloud service.

FINALLY, HYBRID DDOS PROTECTION combines the massive capacity of cloud services with the advanced capabilities and fast response of a hardware appliance. Hybrid protection is best for mission-critical and latency-sensitive services as well as organizations that encrypt their user traffic but don't want to put their SSL keys in the cloud.

Verify DDoS Protection SLAs

Service-level agreements (SLA) are a crucial component of DDoS defenses. It is the contractual guarantee outlining what your DDoS mitigation provider will deliver and their obligation to remedying in case they do not meet those guarantees.

Specifically, there are six critical SLAs that DDoS protection vendors should commit to and that ultimately define a vendor's ability to provide effective protection against DDoS attacks.

< Prev Next >

Conclusion

When it comes to mitigating the RDoS threat, no idiom rings more true than "be prepared." Organizations with comprehensive DDoS protection in place largely diminish the threat to that of internal (employees, response plan, etc.) and external communication (service providers, your DDoS mitigation vendor, etc.).

Be proactive and understand what comprehensive DDoS protection means for your organization if you don't already inclusive protection in place. With strong DDoS protection in place, a RDoS attack has little to no effect on a business's operations.

Prev