MAZEBOLT

Whitepaper

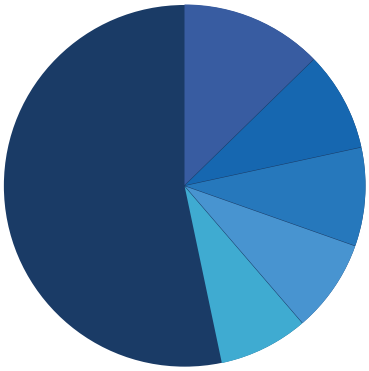
The Anatomy of RDDoS

The New Hybrid Attack Tactic

Table of Contents

Overview

According to the ThreatLabz research team, double-extortion ransomware attacks targeted a diverse range of industries over the past two years.



With the most targeted industries being:

- manufacturing **12.7%**
- services **8.9%**
- transportation **8.8%**
- retail & wholesale **8.3%**
- technology **8%**
- Other various industries **53.3%**

Source: Securitybrief [4]

The year 2020 recorded 10 million DDOS attacks globally, according to the NETSCOUT research that further reports 2.9 million DDoS attacks in the first quarter of 2021, which is a 31% increase from the same time in 2020. Additionally, NETSCOUT's 16th annual Worldwide Infrastructure Security Report (WISR)[1] found that in 2020, distributed denial-of-service (DDoS) extortion attacks grew by a whopping 125 percent. Earlier DDoS attacks caused damaging downtime alone; however, today demanding ransom from targeted companies is flooding the current DDoS threat landscape.

The global pandemic likely contributed to the phenomenal increase in DDoS extortion attacks. Helpnetsecurity website[2] mentions the number of ransomware attacks grew by more than 150%. The eSentire Ransomware Report[3] reveals that in 2021 alone, six ransomware groups compromised 292 organizations. In addition, the Financial Services Information Sharing and Analysis Center (FS-ISAC) announced that in 2020, more than 100 financial services firms were targets of a wave of DDoS extortion attacks conducted by the same threat actor.

Launching Ransomware and DDoS attacks together is a sneaky attack tactic. For example, the well-known extortion gangs are now launching ransomware attacks followed by DDoS attacks on the same targets to cause maximum damage. Even DDoS attackers that are not using ransomware are posing as well-known ransomware groups so they can leverage their reputation to extort money from victims.

> No malware required, easy to launch, and more damaging

Commonly known as RDDoS attacks, the crime involves attackers launching DDoS attacks and threatening to shut down the targeted company's revenue-making channels until the victim agrees to meet ransom demands.

This Whitepaper explains the anatomy of RDDoS attacks and the reasons for their popularity, including suggestions for victims offered by the law and security experts. In addition, the document introduces MazeBolt's patent technology that ensures blocking all DDoS attacks and increasing the overall efficiency of deployed DDoS protection.

[1] NETSCOUT Threat Intelligence Report. Issue 6: Findings from 2H 2020. Available at https://www.netscout.com/threatreport

[2] HELPNET SECURITY. Number of ransomware attacks grew by more than 150%. Available at https://www.helpnetsecurity.com/2021/03/08/ransomware-attacks-grew-2020/

[3] ESENTIRE. Six Ransomware Gangs Claim 290+ New Victims in 2021, Potentially Reaping $45 Million for the Hackers. Available at https://www.esentire.com/resources/library/six-ransomware-gangs-claim-290-new-victims-in-2021-potentially-reaping-45-million-for-the-hackers

[4] Ryan Morris-Reade. Report reveals which industries are most vulnerable to new ransomware attacks. SECURITY BRIEF. Available at https://securitybrief.com.au/story/report-reveals-which-industries-are-most-vulnerable-to-new-ransomware-attacks

A copy of an extortion email sent to Telenor Norway demanding 20 Bitcoin, or $200,000 at the time, in ransom to prevent a cyber-attack.

SOURCE: BLOOMBERG BUSINESSWEEK

We are the Lazarus and we have chosen Telenor 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 "NZX" or "New Zealand Stock Exchange" in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting in in 7 days at Monday next week. (This is not a hoax, and to prove it right now we will start a small attack on your DNS servers 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)

Your network is large so we might not be able to completely shut it down, but we will attack crucial parts and many customers will suffer. We have done our research.

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

We are giving you time to buy Bitcoin if you don't have enough already and enough time for this message to hopefully reach someone from your management.

If you don't pay attack will start, fee to stop will increase to 30 BTC and will increase by 10 Bitcoin for each day after 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 network 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.

A leading mitigation company[18] has published an analysis of extortion emails underlying the patterns of threats. The Company reported that their clients received ransom emails from extortionists who threatened them with crippling DDoS attacks unless they paid between 5 and 10 bitcoins ($150,000 to $300,000). If victims missed the deadline, attackers would increase the ransom amount each day until the victim pays the final amount. The mitigation company further concludes, “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.”

Observing a series of such incidents, investigation agencies have noted a distinctive peculiarity of DDoS extortion campaigns; authorities confirm that attackers had conducted a high-level reconnaissance before sending ransom emails. As a result, the criminals knew of the exact vulnerability points and warned the targeted companies of maximum destruction if they dump the threat emails.

[18] RADWARE. Radware Cybersecurity Alert Ransom DDoS Campaign: Circling Back. Available at https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/ddos-extortions-back/

Why RDDoS Attacks are so Popular

RDDoS Attack is a Low-Effort than Installing Malware

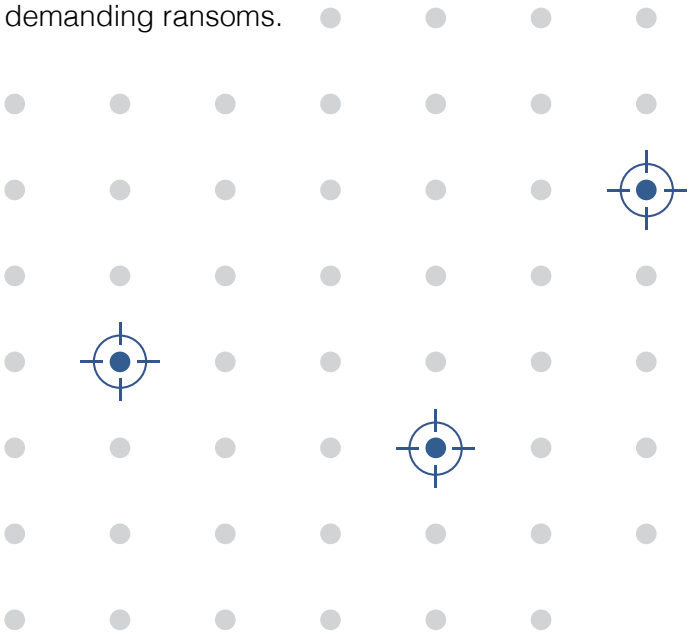
In the report Cyber Threats and Trends: Pandemic Style[19], Neustar mentions one reason for the adoption of DDoS as a ransom vector, as opposed to using malware, is the ease with which such attacks can be carried out. Installing malware in an enterprise's IT infrastructure requires expert skills, due diligence, and creating malicious software programmed for data theft is time-consuming. Launching a DDoS attack, in comparison, is quick and easy with botnets readily available for rent and has the added benefit of being harder to trace back to its origin.

Attackers Motivated by the Surge in Bitcoins

For the past several months, the price of Bitcoin has exploded, making it a newfound formula to getting rich quickly. Consequently, RDDoS attackers are re-prioritizing their demand strategy and returning[20] with massive extortion campaigns in the wake of bitcoin prices surging that continued in Q1 2021.
The hype around digital currency and its prices sparked off when Tesla announced a massive investment in Bitcoin, and it became the preferred currency for cyber ransom. As a result, criminals threaten targeted companies with serial DDoS attacks unless they pay bitcoins in ransom.

RDDoS Used as Smokescreens

Attackers fire low-volume attacks to create smokescreens and distract security officers from a more damaging motive, usually data theft. For example, the Carphone Warehouse websites breach[21], where attackers created junk traffic as a smokescreen before breaking into systems and stealing the personal details of 2.4m customers. The tactic of engaging victims in negotiating ransom can work well as a hidden agenda for attackers to launch a malware attack and steal crucial data. Many times attackers rehearse smaller attacks so they can improve attack techniques, and while doing so, take advantage of demanding ransoms.



[19] NEUSTAR. Cyber Threats & Trends: Securing Your Network Pandemic-Style. Available at https://www.home.neustar/resources/whitepapers/cyber-threats-and-trends-pandemic-style

[20] Felipe Erazo. DDoS Attackers Return With Massive Extortion Campaigns in the Wake of Bitcoin Prices Surging. BITCOIN WEBSITE. https://news.bitcoin.com/ddos-attackers-return-with-massive-extortion-campaigns-in-the-wake-of-bitcoin-prices-surging/

[21] DATA RECOVERY SPECIALISTS, UK. DDoS Attacks as a Smokescreen for Theft. Available at http://www.datarecoveryspecialists.co.uk/blog/ddos-attacks-as-a-smokescreen-for-theft

RDDoS Used to Pressurize Victims

A series of DDOS attacks followed by a major ransomware attack further destroys the victim because its public-facing IPs are now at stake. In such cases, victims feel the pressure of surrendering to ransom demands so they can save their reputation in front of stakeholders, customers, and associates. Brett Callow, threat analyst at Emsisoft[22], who isn't surprised at this new modus operandi, quotes, "DDoS is cheap, easy and in some cases may help convince some companies that speedy payment is the least painful option. The more pressure the criminals can put companies under, the better their chances of extracting payment."

Vulnerable Networks Make It Easy for Attackers

Organizations undergo continuous digital transformation to build modern infrastructure and maintain business continuity. However, during the process of adding software and devices, new vulnerabilities contribute to the network surface risks continuously. As a result, networks remain vulnerable, and attackers exploit them before mitigation systems can identify and block them. Additionally, traditional vulnerability identification tools are time-consuming and inefficient, and therefore, organizations suffer from poor surface risk visibility. Such circumstances make it easier for attackers to overwhelm networks more often and demand ransom because they know that an ongoing business disruption causes serious reputation and revenue damage to the victims. In short, every organization can be a prime target of DDoS extortionists.

[22] Lawrence Abrams. Another ransomware now uses DDoS attacks to force victims to pay. BLEEPING COMPUTER. Available at https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/

Victims are Advised Not to Pay Ransom

When victims receive ransom threats, they prioritize protecting their stakeholders, employees, customers, and associates. On the contrary, law officers advise targeted companies not to pay the ransom because it encourages more attackers to join the extortion crime.

Criminals use DDoS attack tactics to increase pressure on their victims to make them feel there is no choice but to meet their ransom demands. For example, a SunCrypt ransomware affiliate DDoSed a victim's website[23] and threatened to continue until the victim agreed to negotiate the ransom money. Smaller organizations that are already severely affected by a data breach or data encryption cannot survive any further because of business disruption caused by the DDoS attacks and end up paying the ransom.

Extortion gangs promise to stay away from the targets once they meet the ransom demands; however, there is no guarantee that criminals would not return for more money. For example, taking advantage of the bitcoin price-rise, DDoS attackers, in one of their ransom emails, continued increasing the ransom[24] amount by ten bitcoins each day until the victim paid the amount.

In another ransomware attack, Colonial Pipeline paid nearly $5 million in digital currency[25] to recover its data. However, the company found that the process of decrypting its data and turning the pipeline back on again was agonizingly slow, questioning if ransom-paying is even worth it.

By paying ransom, companies do not save the business but make themselves more vulnerable to further damage.

Law officers recommend that organizations deploy a preemptive DDoS Protection to automatically identify and block such attacks before their networks are affected.

[23] Lawrence Abrams. Ransomware gangs add DDoS attacks to their extortion arsenal. BLEEPING COMPUTER. Available at https://www.bleepingcomputer.com/news/security/ransomware-gangs-add-ddos-attacks-to-their-extortion-arsenal/

[24] Lance Whitney. Ransom campaign threatens organizations with DDoS attacks. TECH REPUBLIC. Available at https://www.techrepublic.com/article/ransomware-campaign-threatens-organizations-with-ddos-attacks/

[25] Nicole Perlroth. Colonial Pipeline Paid Roughly $5 Million in Bitcoin to Hackers. THE NEW YORK TIMES. Available at https://www.nytimes.com/2021/05/13/technology/colonial-pipeline-ransom.html

Recommended Mitigations

1. Firstly, maintain a list of all public-facing services and prioritize those that need immediate DDoS protection.

2. Deploy a hybrid mitigation service that includes cloud and on-premise components, detecting abnormalities in your traffic flow and cleaning malicious DDoS traffic before directing it to your network.

3. Pay special attention to the fact that some of the mitigation systems implement rate-limiting techniques; those methods are false-positive prone and may affect production networks.

4. Choose advanced mitigation solutions that include Anomaly Behavioral Based Detection and intelligence on active and unknown threats.

5. Simultaneously, look out for DDoS Protection services offered by the local internet service providers (ISPs) to detect and control volumetric attacks.

6. Ensure an Emergency Response Plan that employs a team of security experts readily available to handle sudden threat outbreaks.

7. Additionally, organizations must ensure all network devices, software, firmware are up to date and vulnerability patches are fixed continuously.

The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) has listed additional mitigation techniques in the Advisory - DDOS Attack Types and Mitigation Strategies[26].

The Missing Link

Mitigation Solution Alone Cannot Stop DDoS Attacks

Despite deploying the best-of-breed mitigation systems damaging DDoS attacks are still bringing down networks! Although a mitigation solution is well designed to block DDoS attacks, it only reacts when it's perfectly configured on a network level and an IP address level to the underlying network it's protecting. As vulnerabilities occur in continually changing networks, security personnel must configure DDoS mitigation settings manually for each separate network.

Additionally, organizations rely on their SLAs to work automatically and fully protect their networks from DDoS threats. However, SLA's are relevant only if the deployed DDoS protection identifies the attack; if not, organizations will have to handle damaging downtime. Moreover, identifying false positives is sometimes challenging, and the time taken to detect a DDoS attack is enough to create a damaging impact upon the target.

As a result, the industry has witnessed successful DDoS attacks despite companies deploying the most intelligent and advanced mitigation solutions.

Organizations need real-time visibility of their networks to close the vulnerabilities before attackers can exploit them. However, many times, organizations do not have the insights on vulnerability points that are susceptible to a potential DDoS attack. Therefore, they are likely to be unprepared to block the attacks.

[26] NJCCIC. DDOS Attack Types and Mitigation Strategies. OFFICIAL SITE OF THE STATE OF NEW JERSEY. Available at https://www.cyber.nj.gov/this-is-security/ddos-attack-types-and-mitigation-strategies

An Immediate Call to Action

Fix All Vulnerabilities BEFORE an Attack

DDoS attacks are successful because attackers are able to exploit vulnerabilities before security personnel and mitigation solutions can identify and block them. In addition, since many open channels are not detected in real-time, vulnerabilities remain unblocked, and DDoS attacks successfully bypass the most robust mitigation solutions. Therefore, organizations must regularly identify vulnerabilities, reconfigure mitigation policies, and revalidate remediation - ALL without disruption or downtime.

MazeBolt's RADAR™ Technology
DDoS Simulation on Live Environments with No Disruption

RADAR™, MazeBolt's transformative technology, is the only 24/7 automatic DDoS attack simulator on live environments with ZERO downtime/disruption. Mitigation solutions are more effective when deployed with RADAR™. RADAR™, compatible with all mitigation solutions, automatically detects, analyzes, and prioritizes the remediation of DDoS vulnerabilities across the network.

RADAR™ simulates a "Full DDoS Attack", where each attack simulation is designed to trigger DDoS security mechanisms (detection & blocking). These security mechanisms by function are expected to get triggered when such a specific type of DDoS attack is being simulated. Suppose the security mechanisms do not get triggered during an attack simulation, in that case, it means a real DDoS attack will not be mitigated automatically when an attacker uses such a DDoS attack vector, causing damaging downtime.

RADAR™ can detect over 9000 vulnerabilities a month on specific production systems, all **without any disruption or manual intervention.** Companies can avoid downtime and protect their networks against all DDoS attacks by deploying MazeBolt's RADAR™ without replacing their existing mitigation solutions.

By adding RADAR™, organizations will increase the efficiency of deployed mitigation solutions by performing continuous simulations, detecting real-time vulnerabilities, reconfiguring their policies, and re-validating remediation, all with no downtime, thereby ensuring smooth business continuity.

Simulating DDoS attacks is a crucial necessity to visualize and react to vulnerabilities identified in your deployed DDoS protection, which helps maintain business continuity. Performing ongoing, non-disruptive attack simulations against production systems is the only way to assess your DDoS protection level in peace-time and ensure that it can **automatically block attacks in real-time** when the need arises.

Conclusion

Companies who have been victims of RDDoS attacks relied on their deployed DDoS mitigation alone to block DDoS attacks automatically; however, their networks were easily overwhelmed and, in some cases, even breached. The RDDoS is a powerful attack tactic to create pressure on the organizations until they end up paying the ransom. Ransom related DDoS attacks are only becoming more popular, and attackers are targeting both small and large companies across wider industry segments.

Companies suffer from DDoS attacks because all mitigation solutions work after an attack is detected. As a result, deploying a preemptive approach such as continuously simulating DDoS attacks is crucially essential to identifying and blocking new and ongoing vulnerabilities. However, simulating attacks is only effective when performed continuously and on live environments.

MazeBolt's RADAR™ simulates DDoS attacks on live environments without any disruption to the business. The transformative technology detects DDoS vulnerabilities non-disruptively and continuously and lowers the vulnerability level to 2% and below.

Because RADAR™ requires no disruption to production services, remediation and immediate validation of fixes to prioritized vulnerabilities is made possible. In conclusion, all DDoS attacks, including those taking the shape of extortion can be blocked before the attack launched, only if organizations deploy MazeBolt's RADAR™ as part of their DDoS Protection.

Request a DEMO

More about RADAR™

MazeBolt is an innovation leader in cybersecurity and part of the DDoS mitigation space. Offering full DDoS risk detection and remediation. Working with any mitigation system to provide the ultimate DDoS protection coverage. Supporting organizations in avoiding downtime and closing DDoS vulnerabilities before any damaging attack happens.

CONTACT US: INFO@MAZEBOLT.COM I WWW.MAZEBOLT.COM