WHITE PAPER

Pay Or Else: DDoS Ransom Attacks

neustar

TABLE OF CONTENTS

OVERVIEW

Mention "ransom attack" and most IT security professionals immediately think of ransomware, a virulent kind of malware that, once in a network, can encrypt or block files or even entire systems. The attacker then demands a ransom payment to restore access.

The technique dates back to a 1989 attack launched via floppy disks[1](!). In recent years, however, the attacks have become far more widespread and damaging as more bad actors have created more families of ransomware to exploit ever more vulnerabilities.

But even with all these variations, ransomware attacks all have one thing in common: the malware has to be inserted into a potential victim's network.

Now: No malware required. In recent months, a growing number of extortionists have adopted an approach that doesn't require malware. They simply threaten to shut down your healthy network with a massive Distributed Denial of Service (DDoS) attack at a specified day and time unless you meet their demand and pay them a substantial ransom.

The surge in these DDoS-based ransom threats, known as Ransom Distributed Denial of Service (RDDoS) attacks, is very bad news. While conventional ransomware attacks are still a threat, organizations can take effective preventive action against the malware they require. They can provide user education about phishing and spear-phishing (the most common insertion methods), for example, and employ tools to detect, quarantine and remediate any suspected malware infection.

But RDDoS attacks don't require malware, so these tools are worthless against them – leaving more enterprises more vulnerable to a rapidly growing threat.

A different threat vector makes ransom attacks even more dangerous.

1 "A History of Ransomware: The Motives and Methods Behind these Evolving Attacks," CSO Online, July 27, 2020

THE DDoS RANSOM ATTACK (RDDoS) LANDSCAPE

Extortion threats based on DDoS attacks have been around almost as long DDoS attacks themselves. These first threats were few in number, with a small DDoS attack followed by a protection offer from an "Internet security consultancy" you couldn't refuse.

While DDoS attacks quickly became a perpetual feature of the threat landscape constantly growing larger, more complex and more intense, DDoS ransom attacks did not. In fact, they virtually vanished from the threat landscape until several years ago, when they reappeared. These attacks were conducted in relatively small waves, limited to companies in one or two industries in isolated geographic regions.

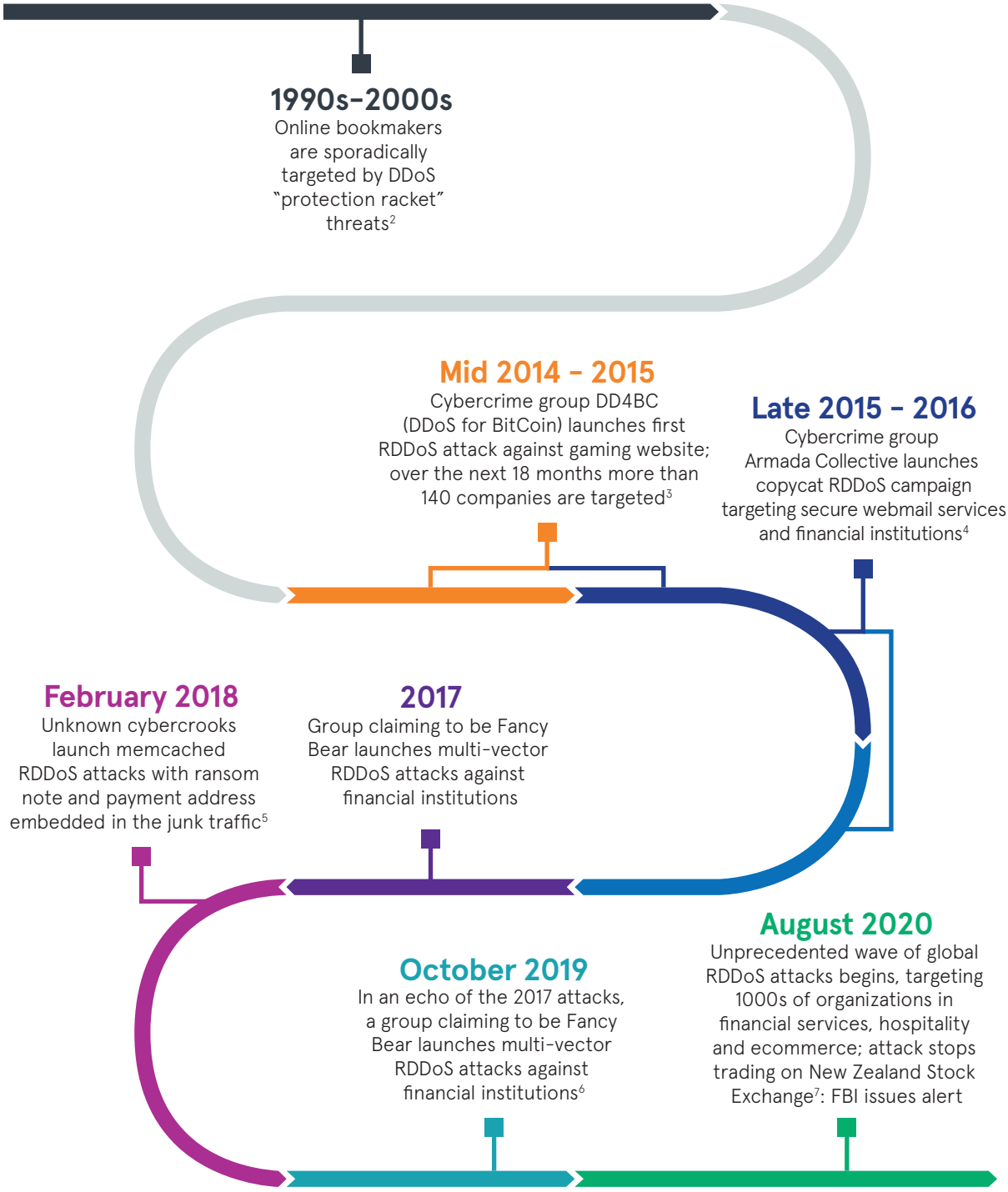
Late in 2020, however, the number of RDDoS attacks exploded. The threats became so prevalent and dangerous that the U.S. Federal Bureau of Investigation (FBI) issued a nationwide alert, calling attention to their scope and intensity.

In addition to the sheer number of attacks, the current wave differs from earlier ones in other important ways:

- They are global in scope. Attacks have targeted commercial organizations everywhere: in North America, Asia and the Pacific, Europe, the Middle East and Africa.
- They span multiple industries. After an initial wave aimed at financial services, attacks have hit companies in technology, business services, hospitality, travel and retail. Neustar's Security Operation Center (SOC) has mitigated attacks against a variety of industries, including recent attacks against sports and gaming companies, large financial service providers and even manufacturers.

In short, your organization is not safe.

RANSOM DDoS ATTACK MILESTONES



2 "DDoS Protection Racket Targets Online Bookies," The Register, November 26, 2001
3 "Ransom Distributed Denial of Service Attacks," Singapore Computer Emergency Response Team, October 2, 2020
4 "Armada Collective: Who Are the Hackers Extorting Bitcoin Ransoms and What Can We Do?", Mary-Ann Russon, International Business Times, September 5, 2016
5 "Powerful New DDoS Method Adds Extortion," Krebs on Security, March 18, 2018
6 "A DDoS Gang Is Extorting Businesses Posing as Russian Government Hackers," Catalin Cimpanu, ZDNet, October 24, 2019
7 "New Zealand Exchange's Massive DDoS Attack: What Went Wrong?" Jeremy Kirk, Bank Info Security, September 14, 2020

ANATOMY OF AN RDDoS ATTACK

This actual RDDoS ransom note, received by one of our clients, includes the key elements that are common to these extortion attacks.

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

Please perform a google search for "Fancy Bear" 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 7 days at Wednesday next week. (This is not a hoax, and to prove it right now we will start a small attack on a few random IPs from [redacted] range 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 (we have all your IPs) 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.

The worst of all, you will lose Internet access in your offices too.

We will refrain from attacking your network a small fee. The current fee is [redacted] 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 enough time for this message to reach somebody from your management 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.

"Fancy Bear"
Stokes fear by claiming to be from a notorious cyber-crime group (others have included Cozy Bear, Lazarus Group and Armada Collective), although experts doubt the real groups are involved.[8]

"New Zealand Stock Exchange"
Established credibility for the attacker by taking credit for a recent, widely reported DDoS attack that successfully froze access to a major financial institution's infrastructure.

"starting in seven days"
Threatens a massive attack on a specific day in the near future, spelling out the dire consequences of a large, successful DDoS attack...

"a small attack on a few random IPs"
...with a small demonstration attack coming much sooner to prove they mean business and can pull it off.

"attacking your network for a small fee"
Spells out the ransom demand you must pay to avoid the attack, typically bitcoin or other cybercurrency worth around $100K to $300K.

"fee to stop will increase"
Raises the stakes by threatening to raise the demanded ransom payment after the attack starts if you don't pay up first.

"never hear from us again"
Promises a happy ending if you pay, preventing the attack, ending the threat forever and preserving your reputation.

8 "A DDoS Gang Is Extorting Businesses Posting as Russian Government Hackers," Catalin Cimpanu, ZDNet, October 24, 2020

WHAT TO DO IF YOU'RE ATTACKED

Finding one of these notes in your inbox is a jarring discovery for even the most seasoned IT professional. Once you get beyond that OMG moment, here's what to do:

1 **Don't panic.**
First, you might not end up facing an attack, as not all cybercriminals actually follow through. Even if they do, it may not be that serious. So far, the DDoS attacks that Neustar clients have faced, following ransom notes, have been moderately sized attacks. What's more, even a massive DDoS attack can be successfully mitigated if you have a plan and a partner with the necessary capabilities.

2 **Don't pay.**
Many RDDoS extortion notes promise that paying the ransom will send the attackers away forever. Don't believe it. You'll simply prove to them that you're willing and able to pay, which could well bring you additional threats in the future.

3 **Contact your DDoS mitigation partner.**
Let them know you've received a threat and tell them the details. If you have partnered with a DDoS mitigation specialist and can forward the actual ransom note, so much the better. They may have insights about the attacker based on either direct experience or industry reporting.

More importantly, if you share the details of the threat, such as when it's expected and how extensive it may be, your provider will be in a much stronger position to successfully mitigate it if it materializes.

4 **Contact the authorities.**
Reach out to the FBI (in the U.S.) or the appropriate cybercrime authority in your country. The 2020 FBI alert about RDDoS attacks specifically recommends that an organization that receives a threat should contact the nearest FBI field office to report it. The more information that can be gathered about these threats, the greater the chance of identifying the attackers and bringing them to justice.

HOW TO BE PREPARED

The key to withstanding a DDoS extortion threat is being ready to withstand a DDoS attack.

That makes a carefully considered DDoS mitigation strategy the most important single precaution your organization can take. After all, when you're prepared for an attack the threat of one is hollow.

Your mitigation strategy should start with an assessment that identifies all infrastructure assets that are at risk from a DDoS attack and their location, as well as your organization's risk tolerance for each of them. This evaluation will help you establish the specific mitigation strategies and service options that will deliver the optimum protection for your network and your needs.

Your DDoS mitigation strategy will almost certainly require an outside partner. DDoS attacks are reaching new heights of intensity and duration; Neustar recently mitigated an attack of 1.17 Tbps, and a different attack lasting almost 6 days. It's almost impossible to withstand such prolonged and intense attacks on your own.

Options in DDoS mitigation range from add-on services offered by your ISP or cloud services provider to DDoS specialists like Neustar, with a fully managed cloud platform dedicated to DDoS mitigation. You can find a more detailed discussion of factors to consider in selecting a provider and configuring your protection here.

Once you have a strategy and partner in place, keep them up to date with your changing network and security infrastructure.

With these preparations in place, even if you do receive a RDDoS threat, you and your security provider can weather it successfully. You will also want to establish pre-emptive protection for the date and time of the threatened attack, extending to segments that might normally be considering high risk; make plans to monitor your assets for performance and availability, and take other prudent steps to mitigate possible harm.

Neustar recently mitigated an attack of **1.17 Tbps**, and a different attack lasting almost **6 days**.

HOW NEUSTAR CAN HELP

You can face an RDDoS attack with complete confidence – as long as you are confident your network is safe and protected from any DDoS attack. The security experts at Neustar support their customers with a comprehensive DDoS solution incorporating five essential characteristics.

1 **Capacity to handle massive volumetric attacks.** Neustar's cloud-based DDoS protection services are anchored by a massive global mitigation infrastructure, built with best-in-breed technologies, with a scrubbing capacity of 12+ Tbps and is IPv6 capable.

2 **Fast response to minimize exposure.** Our always-on cloud-based solution delivers the fastest possible protection, as well as minimal latency thanks to our global platform. Our on-demand solutions provide near-instantaneous protection through automated activation triggered by preset traffic thresholds. And you can create a mixed solution based on prefix to match the needs of your infrastructure.

3 **Protection against application-layer attacks.** Our cloud-based Web Application Firewall (WAF) extends your security protection against this growing attack vector that can target data centers and cloud resources, and requires no additional software or hardware.

4 **Flexibility to meet your security needs.** Tailor your DDoS solution to directly address your risks and tolerance, with options for either always-on or on-demand cloud-based protection, as well as on-premise and hybrid solutions. Choose from DNS or BGP redirection mitigation strategies. Extend your protection to include your VPN traffic – especially important during the pandemic. Leverage direct connections to more than 500 data centers with multiple tier-1 partners to ensure virtually unlimited bandwidth, even during an intense or massive attack.

5 **Specialized expertise on guard and on call 24/7.** Our Security Operations Center is always on duty and always accessible. It is staffed by senior-level DDoS mitigation professionals schooled in best practices and supported by an extensive counter measures library built over more than 15 years of experience.

LEARN MORE

To learn more about how Neustar UltraWAF can support your security needs **click here**, email us at **security@team.neustar**, or call us at **1-855-898-0036** in the US and at **+44 1784 448444** in the UK.

ABOUT NEUSTAR

Neustar is an information services and technology company and a leader in identity resolution providing the data and technology that enables trusted connections between companies and people at the moments that matter most. Neustar offers industry-leading solutions in Marketing, Risk, Communications, and Security that responsibly connect data on people, devices and locations, continuously corroborated through billions of transactions. Neustar serves more than 8,000 clients worldwide, including 60 of the Fortune 100. Learn how your company can benefit from the power of trusted connections at www.home.neustar.

©2021 Neustar, Inc. All rights reserved. All logos, trademarks, servicemarks, registered trademarks, and/or registered servicemarks are owned by Neustar, Inc. All other logos, trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.

WP-SEC-265279-01.27.2021