From the Security Experts at Corero Network Security

HOW TO HANDLE A RANSOM-DRIVEN DDOS ATTACK

Be Proactive, Not Reactive

STEP-BY-STEP GUIDE

The Rise of Ransom-Driven DDoS Attacks

Ransom-related Denial of Service attacks (RDoS) have been gaining popularity as of late. Recent examples span across industries—from banking and financial institutions, to hosting providers, online gaming services and SaaS organizations.

Unfortunately, when even one, high-profile victim chooses to engage with attackers by paying a ransom, we tend to see an increase in these types of attacks. RDoS attacks have grown in frequency as cyber criminals are constantly on the lookout for more efficient methods to attack systems and obtain profits. When faced with the costs of their business going offline if a successful DDoS attack is launched against them, some organizations may believe that paying a ransom demand represents good value for money.

This approach is playing with fire, and offers no guarantee that an attack will not be launched. Thus, it's important to highlight the danger these attacks pose to businesses and learn how to build a successful defense against them.

The Rising Concern of DDoS Attacks

In an RDoS attack, cyber criminals send a message threatening to carry out a DDos attack, or infect an organization's operational systems with forms of ransomware, unless the payout is received by a certain deadline. Many hackers are motivated by the potential for financial gain and the ease at which such attacks can be performed. Extortion is one of the oldest tricks in the criminal's book, and one of the easiest ways for today's hackers to turn a profit.

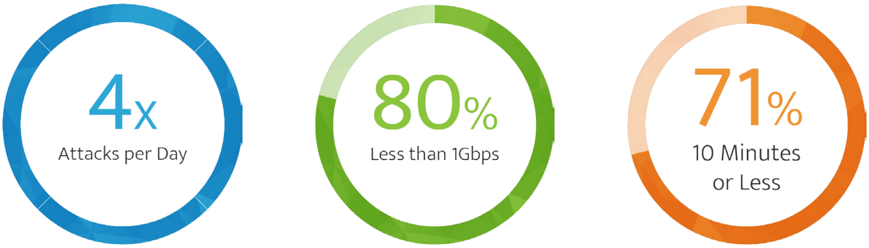
These attacks have become so common that according to a 2016 study, Corero found that 80 percent of European IT security professionals expect their business to be threatened with a DDoS ransom attack during the next 12 months.

When service availability is threatened, the victim company is facing costly implications including revenue loss and reputation damage. Thus, it is not surprising that almost half of IT security professionals (43%) that took part in our 2016 study thought that it was possible that their organization might pay such a ransom demand in the hope of circumventing an attack.

The Links Between Ransom, Ransomware and DDoS Attacks

DDoS attacks are increasingly used as smokescreens for more nefarious network infiltrations, such as ransomware. DDoS attackers are getting more sophisticated; their objective is not only to cripple a website, but rather to distract IT security staff with a low-bandwidth, sub-saturating DDoS attack. Such attacks typically are short duration (under 5 minutes) and low-volume, which means that they can easily slip under the radar without being detected or mitigated by some DDoS protection systems.

Latency and service outages are all tangible outcomes of a successful DDoS attack—ransom related or otherwise. As we know, an attack only requires a few minutes to overrun traditional security infrastructure, such as firewalls and intrusion prevention systems (IPS), offline; in effect, the network doors are wide open. While IT staff scramble to handle the momentary network outages or system slowdowns, hackers can use automated scanning or penetration techniques to map a network and install ransomware.



Corero continues to observe a steady flow of DDoS attack attempts against customers. In Q1 2017, Corero customers experienced an average of four attack attempts per day.

To compound the frequency of DDoS attacks, 80% of attack attempts were less than 1Gbps in volume. The average duration of DDoS attacks is also cause for concern, as 71% of these attacks were 10 minutes or less in duration.

How to Deal with DDoS Ransom Threats: Be Proactive, Not Reactive

Unfortunately, most cyber security solutions focus on recovery from criminal extortion attacks, rather than defeating one. The DDoS mitigation landscape has evolved to deal with these attacks automatically and instantaneously to eliminate the threat to your business. Enterprises should take a more proactive stance when it comes to preventing ransom-related attacks, and one way they can do that is by installing DDoS protection solutions that automatically detect and block even the smallest of DDoS attacks, 24x7. Only then can IT security teams have comprehensive visibility into network incursions.

1. **Recognize DDoS attack activity**

   Large, high-volume DDoS attacks are not the only form of DDoS activity. As discussed, short duration, low-volume attacks are stress testing and finding security vulnerabilities within your security perimeter. Understand your network traffic patterns and look to solutions that identify DDoS attack traffic in real-time, removing the threat immediately.

2. **Document your DDoS resiliency plan**

   These resiliency plans should include the technical competencies, as well as a comprehensive plan that outlines how to continue business operations under the stress of a successful denial of service attack.

   An incident response team should establish and document methods of communication with the business, including key decision makers across all branches of the organization, to ensure key stakeholders are notified and consulted accordingly.

3. **Pair time-to-mitigation with successful attack protection**

   In the face of a DDoS attack, time is of the essence. Minutes or more before a DDoS attack is mitigated is not sufficient to ensure service availability. As you develop your resiliency plan and choose your method of DDoS protection, time-to-mitigation must be a critical factor in your decision-making process.

4. **Do more than check the box**

   Even firewalls that claim to have anti-DDoS capabilities built in have only one method of blocking attacks: the usage of indiscriminate thresholds. When the threshold limit is reached, every application and every user using that port gets blocked, causing an outage. Attackers know this is an effective way to block the good users along with the attackers. Because network and application availability is affected, the end goal of denial of service is achieved.

Conclusion

Today's DDoS attacks are almost unrecognizable from the early days of attacks, when most were simple, volumetric attacks intended to cause embarrassment and brief disruption. Today, the motives behind attacks are increasingly unclear, the techniques are becoming ever more complex and the frequency of attacks is growing exponentially. This is particularly true in light of automated attacks, which allow attackers to switch vectors faster than any human or traditional IT security solution can respond.

The combination of the size, frequency and duration of modern attacks represent a serious security and availability challenge for any online organization. Minutes or more of downtime or latency significantly impacts the delivery of essential services. When you combine these factors, victims are faced with a significant security and availability challenge.

GTT’s DDoS Mitigation Service

GTT’s DDoS Mitigation service is an always-on, managed offering that guarantees protection from DDoS attacks. The service leverages Corero’s next-generation SmartWall platform technology to deliver immediate threat detection, deep packet inspection analytics and filtering of malicious traffic at GTT’s scrubbing centers.

GTT’s DDoS Mitigation is a proactive offering, providing continuous, automated routing of traffic for cleaning, without any outside intervention required. Clean traffic is returned via MPLS IP VPN or a GRE IP tunnel. The service is also available in an on-demand, reactive, near-real-time option for clients that prefer this approach to DDoS mitigation.

The service includes alerting and deep visibility into real-time and historical DDoS threats through a client portal and is backed by stringent response time SLAs, providing peace of mind that DDoS threats are mitigated quickly and efficiently.

About GTT

GTT provides multinationals with a better way to reach the cloud through its suite of cloud networking services, including optical transport, wide area networking, internet, managed services, voice and video services. The company’s Tier 1 IP network, ranked in the top five worldwide, connects clients to any location in the world and any application in the cloud. GTT delivers an outstanding client experience by living its core values of simplicity, speed and agility. For more information on how GTT is redefining global communications, please visit www.gtt.net.

GTT Headquarters
7900 Tysons One Place, Suite 1450
McLean, VA 22102
+1 703 442 5500

corero

gtt