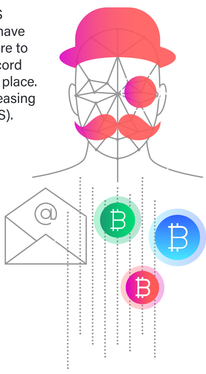
NETSCOUT

Threat Report- Triple Extortion 3

7-Figure Losses from DDoS Attacks Reported by Publicly Traded Company

Although DDoS extortion (aka RDDoS) isn't new, high-profile DDoS extortion attack campaigns sometimes emerge. It's not unusual to have one high-profile DDoS extortion campaign in a year, but it's fairly rare to see two such campaigns in a year. During 2021, however, a new record was established as three high-profile DDoS attack campaigns took place. This also signals that ransomware gangs are laser-focused on increasing the use of triple-extortion attacks (ransomware + data theft + DDoS).



1. The prolific Lazarus Bear Armada (LBA) DDoS extortionist threat actor extended its high-impact attack campaign into 2021, targeting multiple verticals worldwide and exhibiting a high degree of pre-attack reconnaissance to maximize attack efficacy.

2. The Fancy Lazarus DDoS extortionist kicked off a campaign that initially targeted the authoritative DNS servers of wireline broadband access ISPs in the U.K. and Scandinavia by using DNS reflection/amplification attacks, a suboptimal vector when attacking authoritative DNS servers. The campaign was somewhat successful due largely to the unpreparedness of a few network operators; nevertheless, the attacks were mitigated relatively quickly.

3. The third high-profile DDoS extortion campaign of the year was an aggressive series of attacks masquerading as the REvil ransomware group and targeting SIP/RTP VoIP operators. Retail and wholesale VoIP providers in the U.K. were the initial targets, followed by attacks against VoIP operators in Western Europe and North America. Notably, one VoIP wholesaler filed a form with the U.S. Securities and Exchange Commission (SEC) estimating the total cost of the DDoS attack at between $9 and $12 million. Attackers now appear to view DDoS attacks as criminal endeavors in and of themselves — as opposed to one pillar of triple extortion attacks — meaning more-skilled DDoS extortion campaigns should be expected as sophisticated ransomware groups master this tactic.

Ransomware Gangs

In the 1H 2021 Threat Intelligence report, we noted that several different groups conducting ransomware operations have also moved into DDoS attack territory to place greater pressure on victims to pay demanded ransoms. For this report, Palo Alto's Unit 42, a Threat Intelligence partner, created a summary of active and recently inactive ransomware gangs that also use DDoS to extort victims into paying the ransom. The following groups are known to use and have been observed using DDoS as part of their operations.

UNIT 42
BY PALO ALTO NETWORKS

Unit 42 is a premier threat intelligence and cybersecurity consulting organization chartered to identify and resolve the most challenging threats and make the world a safer place.

Avaddon

Avaddon ransomware was first seen in February 2020 and by June 2020 had quickly evolved into ransomware as a service (RaaS). In January 2021, the group evolved again to include DDoS attacks in its extortion repertoire. Despite a successful run, the group inexplicably shut down its operation in June 2021, possibly as a result of political pressure and/or the release of private keys

REvil

Although currently not operational due to a global takedown, REvil was a prominent user of RaaS. With its highly adaptable encryptors and decryptors, REvil provided infrastructure and services for communicating with victims, as well as a leak site for releasing stolen data if the victim refused to pay the ransom. In February 2021, REvil announced that it would begin contacting its victims' business partners and the media to disclose breaches and further extort victims. On March 5, 2021, a REvil spokesperson announced the addition of DDoS attacks, effectively elevating the group's TTPs to include multi-extortion.

BlackCat

One of the newest ransomware groups, BlackCat (aka ALPHV), was discovered in November 2021. Operating as a RaaS, the group quickly gained notoriety for its sophistication and innovation. BlackCat solicits for affiliates in known cybercrime forums by promising to leverage ransomware and give 80 to 90 percent of the ransom payment to the affiliate, with the remainder paid to the BlackCat author. The malware itself is written in Russian and coded in Rust, making it one of the first pieces of ransomware to use it. BlackCat not only encrypts and steals victims' data, but it also then threatens to leak the data via a leak site. Should the victim need additional persuasion to comply with the ransom demand, BlackCat threatens a DDoS attack.

AvosLocker

First seen in summer 2021, AvosLocker is simple but effective ransomware that has utilized triple extortion from the start. AvosLocker operators advertise in underground networks for affiliates with active directory experience, as well as for "access brokers" who potentially could provide access to compromised systems. Affiliates are incentivized with having AvosLocker take care of the extortion and negotiation parts of the process. AvosLocker then uses affiliates to infect a victim, while handling the remaining ransomware process itself. Like some other ransomware groups, AvosLocker operates a leak site to apply additional pressure on victims to pay the ransom. The group has attacked a diverse set of victims in terms of both region and industry.

Suncrypt

Initially appearing in October 2019, Suncrypt was one of the first ransomware groups to launch DDoS attacks. Along with data encryption and theft, Suncrypt extorts its victims by threatening to attack infrastructure or networks. Likewise, further pressure is applied by threatening to expose the breach to employees, stakeholders, and the media should ransom negotiations fail. The group maintains a leak site and promises that it won't expose victim data during the negotiation process. If that process fails, however, Suncrypt leaks victim data and initiates a DDoS attack until negotiations resume.

Despite these recent global efforts, we still face a massive uphill climb to make even a small dent in ransomware activity.

Threat Intelligence Report Issue 8, Findings from 2H 2021

EXPLORE INTERACTIVE REPORT

NETSCOUT

SECIG_017_EN-2201 03/2022