IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Lockdown 2.0 and the DDoS Threat

Richard Hummel

Richard Hummel
ASERT Threat Intelligence Lead
NETSCOUT

Biography

Richard Hummel has over a dozen years of experience in the intelligence field and is currently the Threat Intelligence Manager for Arbor Networks' ASERT Research Team, NETSCOUT (https://www.netscout.com). Previously, he served as Manager and Principal Analyst on the FireEye iSIGHT Intelligence's Financial Gain team. He began his career as a Signals Intelligence Analyst with the United States Army. During the course of his service he became certified in Digital Network Intelligence and supported multiple operations overseas including a deployment to Iraq.

After departing from the Army as an enlisted soldier, he began contracting work as a Computer Network Operations analyst in support of the Army. During his tenure as a contractor, he developed many methods and procedures for conducting Cyber Discovery and trained analysts at Army INSCOM HQ's. At FireEye iSIGHT Intelligence, he led a team of technical analysts in the tracking, reporting, and analysis of various cybercrime related malware families.

Keywords DDoS, Lockdown, Cybercriminals, Critical infrastructure, Vulnerability, Defence
Paper type Research

Abstract

No matter how productive you think you have been while working remotely, cybercriminals worked just as hard to exploit every vulnerability that emerged from the pandemic. As we all spent more time online, attackers naturally followed, with a surge in multivector, fast-acting attacks. During the last lockdown, we saw the largest number of Distributed Denial of Service (DDoS) attacks ever in a one-month timeframe. As reported in our own Threat Intelligence Report[1], there were 929,000 DDoS attacks in May alone.

Attackers targeted essential pandemic industries, such as e-commerce, healthcare, and educational services. This also translated on leisure activities. As schools closed, many kids headed online, and we saw online gaming spike. Not surprisingly, we also saw an increase in attacks on broadband networks, which serve as crucial access points to online gaming. In fact, since the advent of the pandemic, monthly attack numbers have been consistently 100,000 to 150,000 greater than those of the previous year.

Unfortunately, it seems clear that many countries are headed into a second lockdown period. With that in mind, what can we learn from attacker behaviour during the first lockdown asks the author of this article?

Introduction – Lessons from the first lockdown

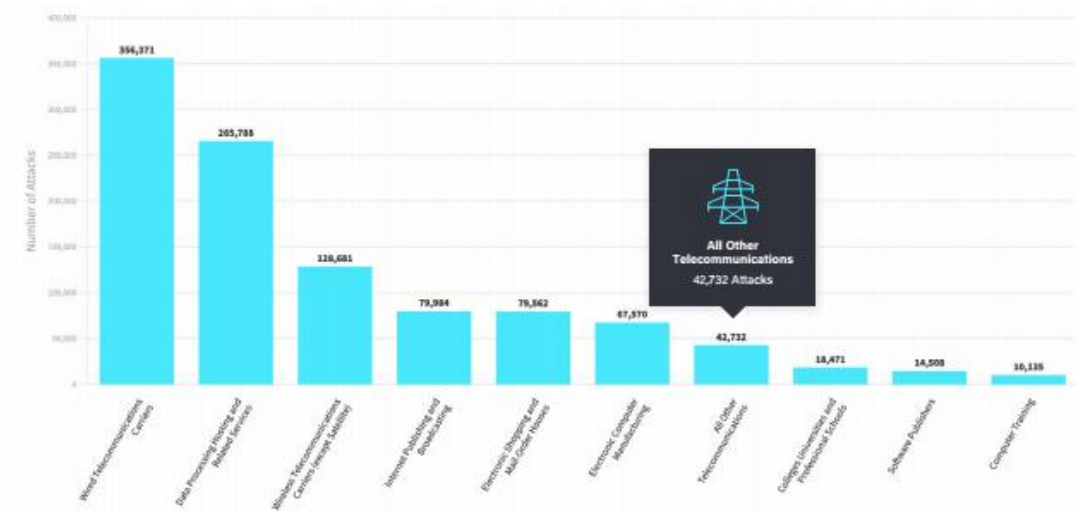
Our NETSCOUT *Threat Intelligence Report*[1] tracks trends in the methods and attack vectors adversaries use to enact DDoS attacks, showing a 25% global increase in attacks in April compared with the first few months of 2020, thus

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

reiterating the narrative that further lockdowns will bring more cyber threats. Based on the trends seen in this timeline, I think it is justified to say that security teams will be met with a substantial number of attacks as second lockdowns settle in.

Figure 1: Top 10 Vertical Industry Targets



Data: Cyber Threat Horizon
Source: NETSCOUT

We can learn quite a bit from the statistics of previous attacks. We saw cybercriminals exploit lockdown measures to their own advantage by significantly ramping up operations to establish DDoS-capable botnets and targeting critical resources such as VPNs. They also shifted to shorter, faster, and more complex attacks, which can be more difficult to defend against. These frequent changes are not surprising, as adversaries constantly experiment with attack methods. Past innovations include increasing the number of vectors, incorporating carpet-bombing to saturate more of a network, and deploying advanced reconnaissance to identify a target's network boundary. They do, however, reflect an impressive ability to react to changing circumstances – the recent trend towards targeting VPNs and upstream service providers is a perfect example.

Industries in the DDoS crosshairs

In late August, the financial sector, along with related industries such as insurance, travel, and even stock market exchanges, came under attack from one of the largest DDoS extortion campaigns we've ever seen. While we cannot say with certainty that the pandemic is their motivation, it does make intrinsic sense. This group, known as Lazarus Bear Armada (LBA)[2], uses the threat of crippling DDoS attacks to extort payment in Bitcoin from victims. Although the financial sector came under attack first, the group has since expanded its focus to include ISPs and healthcare organizations.

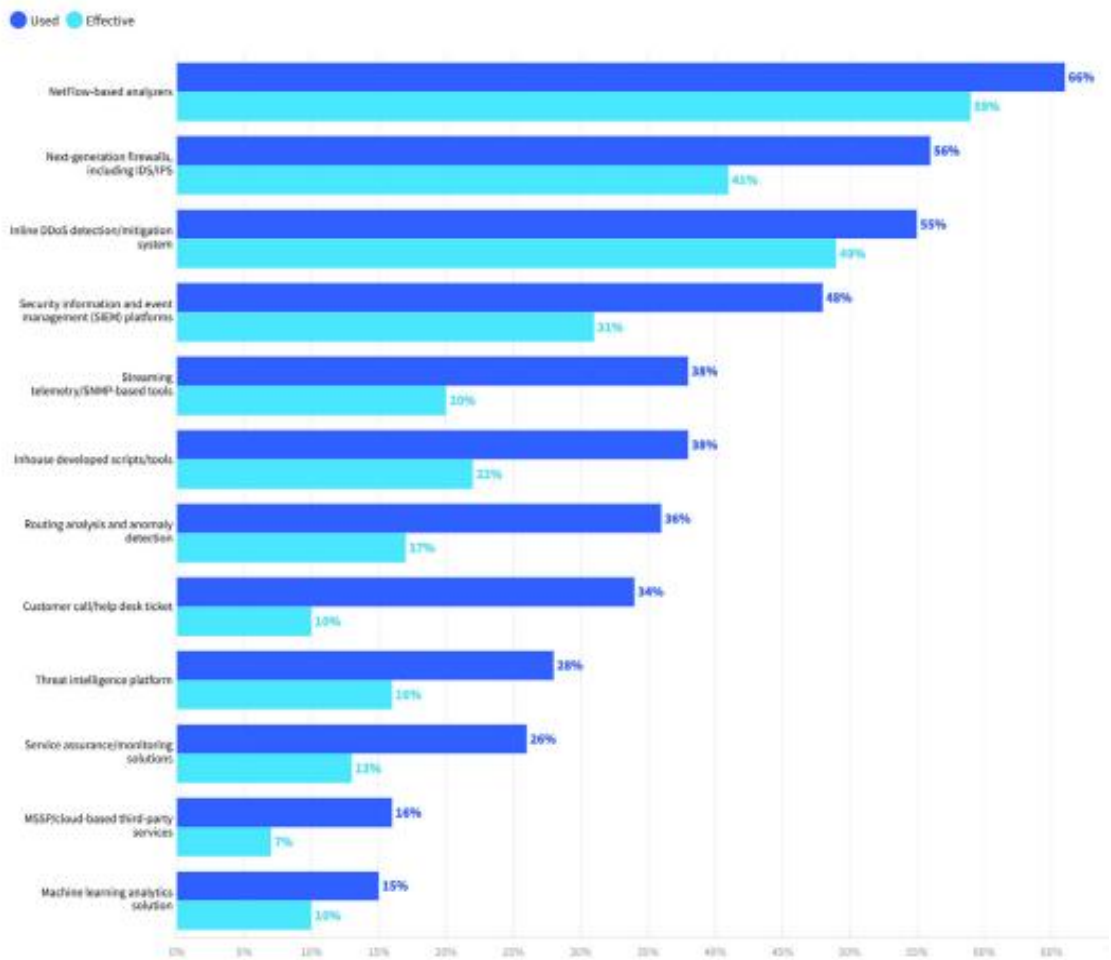
IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

We are also seeing increased attacker focus on specific verticals outside of the LBA campaign. Telecoms, education, and ecommerce have also ranked amongst the most targeted industries. In particular, Ecommerce has seen a huge growth in the frequency of DDoS attacks since last year. As many stores deemed unessential closed their doors during the first lockdown, shoppers inevitably moved even more online than usual. Naturally, the attackers followed.

In the UK, non-store retailers saw DDoS attacks grow 113% compared with the same period in 2019. Similarly, education came under attack when schools moved to a virtual environment. We saw one attack that took down a network in the US, preventing over 170k individuals from accessing the school's online resources. In addition to education going virtual and the majority of the workforce going remote, we also saw a large increase in attacks against broadband networks, and consequently, gaming-related DDoS attacks.

Figure 2: Threat detection tools used verses their effectiveness



Data: Worldwide Infrastructure Security Report
Source: NETSCOUT

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Preparing for lockdown 2.0

Fortunately, DDoS defences also evolve to meet changing DDoS attack tactics and methods. Companies that are prepared with modern defences are more than capable of meeting the challenge posed by online criminals. The key here is the word 'prepare.' The majority of disruptive DDoS attacks succeed by exploiting a lack of preparedness at targeted organizations. We recommend that organizations do the following:

- Implement best current practices for network infrastructure;
- Ensure that application delivery chains are scalable, resilient, and defendable;
- Verify that critical supporting services such as authoritative DNS servers and VPNs[3] are implemented in a secure and defensible manner; and
- Proactively engage DDoS mitigation providers.

In summary

Following trends earlier this year, this lockdown will likely further open the floodgates to a growing range of cyberattacks, including DDoS. This month will be a challenging adjustment for many, and businesses must stay alert to protect invaluable cyber infrastructure as they continue to shift to a digital business model during the global pandemic. By working together as well as with their DDoS mitigation providers, organizations can discourage even the most persistent attackers.

Reference

1 *Netscout Threat Intelligence Report: DDoS in a Time of Pandemic (including the 16th annual Worldwide Infrastructure Security* Report (WISR)), NETSCOUT. Available at: https://www.netscout.com/threatreport

2 Dobbins, R. and Bjarnason, S. (29 December 2020), 'Lazarus Bear Armada DDoS Extortion Campaign - December 2020', NETSCOUT. Available at: https://www.netscout.com/blog/asert/lazarus-bear-armada-ddos-extortion-campaign-december-2020)

3 Dobbins, R. and Modi, H. (20 March 2020), 'Availability in the Time of COVID-19', NETSCOUT. Available at: https://www.netscout.com/blog/asert/availability-time-covid-19