A 2020 VISION FOR SECURITY

LARGE-SCALE DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACKS CONTINUE TO POSE A MAJOR THREAT TO THE INDUSTRY, BUT CARRIERS NEED TO STAY VIGILANT AS THE NATURE OF THREATS CHANGES OVER TIME. NTT HAS ADVICE AND TOOLS THAT CAN PROVIDE A BIG HELPING HAND.

As the end of the decade nears, security remains a key concern for carriers. The second half of the 2010s has been characterised by concerns about the rise of large-scale distributed denial-of-service (DDoS) attacks amid the proliferation of IoT-connected devices.

But while these larger-scale attacks have continued to happen, Michael Wheeler, executive vice president of the Global IP Network at NTT, says a key change in the network security ecosystem in the last 12 to 18 months has been an acceleration in smaller-scale attacks. Some of this activity has been unexpected, he says, reflecting how carriers need to be vigilant in recognising that the threat environment is constantly changing.

"We certainly still see some very large attacks as far as volumes are concerned," says Wheeler. "No one's shocked that volumes are getting bigger; that's just the nature of the internet at this point. The thing we and others in the industry have seen that's a bit less predictable is the higher frequency of very small or shorter-duration attacks."

Such attacks come from various sources, including online gamers, and can last as little as five to 10 minutes. Players can pay for someone to make these attacks via methods such as a credit card or bitcoin, with the aim of simply knocking opponents offline – thus differing from the traditional financial or sociopolitical motivations of DDoS attacks. "It's a very individual-driven approach with a more personal motivation," says Wheeler.

Yet like larger threats, these different types of attack are also being enabled by the proliferation of IoT devices. "There are a lot of devices and a lot of ways in which much smaller-scale attackers can use infrastructure on DDoS-for-hire-type websites," explains Wheeler.

While he says the limited size of this smaller-scale activity means much of it does not have a significant impact on NTT's global IP backbone right now, he emphasises that it's crucial to keep an eye on how it develops over time because continued growth in such attacks may have the potential to eventually cause significant damage if it's not monitored and held in check.

Another issue is that if even random gamers are able to generate these threats, it may open up networks to the possibility of much larger attacks by individuals in future. "If a gamer finds a simple way to marshal a billion devices and generate attack traffic, that may cause problems on a larger scale," says Wheeler.

Dealing with the "ebb and flow"

One challenge in planning ahead to ensure security, he says, is that it's difficult to predict every new type of threat that may emerge – as the rise in activity among gamers has illustrated – and many types of attack tend to "ebb and flow."

"I don't think it's a linear progression in perpetuity," says Wheeler. "Some of this is driven around defences that get created and attacks becoming less effective because certain tools are now available that weren't before. So there's some of that cat-and-mouse game that occurs between the attackers and defenders."

Nonetheless, the fact that NTT has been tracking these events for a couple of decades means the company now has extensive knowledge of what types of tactics it might employ in certain scenarios. Wheeler says the idea is that even if 100-per-cent-foolproof predictions are impossible, the question can still be addressed: "What do we need to do in advance to put ourselves in the best position we can to address this problem?"

A fundamental pillar that props all this up is having the right security team in place, with good prior knowledge of the issues involved so they're not encountering a problem that is completely new to them. NTT again benefits here from its past tracking of events, with its staff having a good idea where to target any future investment in security to maximise the efficiency of attack detection and have a better understanding of threats that might emerge.

"It's critical to have a group of experts that know what they're doing and have experience with this because in my opinion you can't just grab a couple of really sharp people, put them into the security team and expect that they're going to be familiar with how all these things work," says Wheeler.

Over time, the team has continued to track a whole variety of data on threats to help it in future, including everything from attack type and duration to how long mitigation took and the

size of attacks. Customers get round-the-clock access to highly trained engineers at the company's Network Operations Center and detection is additionally aided by the wide span of NTT's Global IP Network, which means staff gain a broad view of potential threats.

Auto-mitigation

Yet though human intervention is critical, NTT has also developed automated tools in-house for proactive threat detection and mitigation that provide robust protection on top.

Among NTT's tools, it is now a year since the company extended its line-up of DDoS Protection Services (DPS) with the addition of its DPS Max offering, providing an even higher level of security than the existing DPS Control, Core and Detect services (see box: NTT's DDoS Protection Services). Wheeler says this has already proved popular among customers, with many newly buying it or migrating to the service from other products.

While including the features of NTT's DPS Core and Detect services, DPS Max's key additional proposition lies in these automatic mitigation capabilities, which are initiated upon the detection of customer-defined attack thresholds. Customers to the service can also request or self-initiate mitigations using a DPS Portal available to them.

In addition, NTT offers "blackholing" services, which can be used to automatically discard all traffic to a certain network or drop traffic from certain geographical locations when a customer is under a large-scale DDoS attack. Wheeler says that even though this blackholing, which is either full or selective, is a more basic approach to mitigation, it allows the customer's network to "catch its breath" while a security team homes in for prevention on a broader level.

"I wouldn't say it's got harder to manage security issues, but it certainly hasn't slowed down," says Wheeler. He adds that threats such as multi-vector and so called "carpet-bombing" attacks can pose more complex problems through combining a variety of attack types or targets, but these haven't necessarily seen a huge rise in volumes.

From a customer perspective, as the complexity of attacks grows, he recommends that companies and organisations have a multi-strategy approach to mitigation – with a combination of selective blackholing, the use of filters to block some applications, and some third-party mitigation for more "intelligent" attacks most likely the best protection.

Collaboration key

Ultimately, says Wheeler, it will take a variety of tools and approaches to continue dealing with threats into the future, but a collective effort from global carriers working together to address industry-wide threats is also key – citing joint initiatives such as RIPE and the Global Leaders' Forum (GLF), of which he is a member.

The GLF's introduction last year of a platform for carriers to share security experiences is now really bearing fruit, he says, with players in the group also unveiling a blockchain initiative earlier this year that should help further improve security.

NTT and other global carriers also learn from situations requiring interactions between operators as bad traffic passes from one network to another, adds Wheeler. "Those real-time interactions can also be very valuable with regard to understanding what's going on and how best to counteract it," he says.

And this need for keen-eyed vigilance is set to continue for the foreseeable future. "With all the IoT-enabled devices out there, the reality is that the potential for attacks gets bigger and bigger every day, and that forces us to consider how we address these issues and get better at it," says Wheeler.

"We're certainly a big proponent of collaborating within the industry and trying to have our teams interact with other folks… There's a long journey ahead, and it's better to be able to do that collaboratively versus independently in a vacuum."

NTT's DDoS Protection Services (DPS)

NTT offers its Global IP Network customers four levels of defence under its DDoS Protection Services (DPS) portfolio, since adding its highest-level DPS Max service last year to its existing Control, Core and Detect offerings.

DPS Control offers an entry-level service for customers that do not require full mitigation assistance, with the ability for clients to block a network from certain types of traffic that they define.

DPS Core is the first level of service for those that want full support for DDoS mitigation and is supported by NTT's Network Security Team – the same team responsible for keeping the company's Global IP Network safe.

DPS Detect adds services such as detection capabilities to help notify customers of potential attacks and client-initiated mitigation via the DPS Portal. It also allows customers to review their detection and mitigation history, and request configuration changes.

Finally, DPS Max provides the highest level of protection, adding automatic mitigation capabilities on top of these other services – with these mitigations based on customer-defined thresholds.

Capacity

Technology doesn't stand still. And nor do we. NTT Communications and the Global IP Network are two of the 28 companies and organizations coming together to form NTT.

We are excited about the journey ahead as the Global IP Network continues to innovate and connect ideas, people and technology to change the world for the better.

Together we do great things

Visit **gin.ntt.net** for more details
Follow **@GinNTTnet** for news and updates on NTT and the Global IP Network
#globalipnetwork #AS2914