Intelligent DDoS Protection
Use cases for applying DDoS Intelligence to improve preparation, detection and mitigation
Introduction

With the average distributed denial-of-service attacks (DDoS) sending traffic floods of more than 40 Gbps, organizations need every advantage possible to prevent disruption of critical online services that drive their business. Time is of the essence during a DDoS attack. The longer it takes to detect and mitigate the attack, the greater the impact and cost. Depending on the industry, surveys indicate a single DDoS attack can cost an organization as much as $2MM per day.¹

This paper details how DDoS Intelligence can be consumed to shorten the DDoS attack window and minimize the impact of attacks on operations. It will highlight opportunities to make defensive measures and procedures more effective by applying real-time intelligence gathered from DDoS botnets and attacks.

“*We have discovered a clear knowledge gap around the Denial of Service attacks in use today and the defenses needed to maintain availability. There is an all too common belief that the defenses that protect against run of the mill network and application attacks will stand up to a DoS. That’s just not the case.*”
— Mike Rothman, Analyst and President of Securosis³

Common DDoS Mitigation Measures

Many organizations, especially those that have experienced severe DDoS attacks, have made investments to more effectively defend their business operations. Investments are commonly made in three areas:

1. Resilient, distributed network infrastructure
2. DDoS mitigation providers
3. Specialized anti-DDoS network security appliances

Resilient, distributed network infrastructure

Often, improving the resiliency of the network is the first step taken by organizations concerned about DDoS attacks. This is accomplished by upgrading capacity and infrastructure components to handle or offload spikes in traffic due to DDoS floods. In many cases, organizations have infrastructure in place that can be re-architected and distributed to better handle DDoS traffic. Existing network components and security appliances such as firewalls can offer some protection against DDoS attacks. In other cases, additional investment may be needed to build out network capacity and incorporate controls that can provide a higher degree of DDoS resiliency.

DDoS mitigation providers

Many organizations subscribe to DDoS mitigation services. During an attack, DDoS mitigation providers work to diminish the impact by blocking attack traffic upstream before it reaches the network. This is commonly accomplished by re-routing the traffic through high capacity networks equipped with specialized “scrubbers” that filter out malicious network traffic with varying degrees of granularity.
"Organizations that have a critical Web presence and cannot afford relatively lengthy disruptions in online service should employ a layered approach that combines multiple DOS defenses."

– Avivah Litan, Vice President and Distinguished Analyst at Gartner

**Specialized anti-DDoS appliances**

Organizations may also deploy specialized anti-DDoS network security appliances in their own environment. These appliances provide capabilities to detect and block DDoS traffic with higher granularity, extending visibility and control to application-layer activity. This is useful against more advanced DDoS attacks that attempt to evade more common mitigation measures.

As with cyber security in general, multiple defensive layers offer the best assurance for minimizing the impact of a DDoS attack. Any security layer has limitations to allow for legitimate activity. Having more layers helps to minimize these limitations and provide better coverage across possible attack methods and vectors. A layered approach also affords multiple opportunities to stop the attack should any one layer not be sufficient, which is a concern with today’s high volume DDoS threats. **Figure 1** illustrates the common components of a layered DDoS mitigation approach.

**Figure 1: Components of layered DDoS mitigation**
How DDoS Intelligence Fits

DDoS threats continue to grow in both flood volume and attack sophistication as attackers seek to overcome mitigation measures, saturate resources and disrupt service availability. In several cases, attacks have succeeded in taking down public-facing online services in spite of the targeted organizations having made major investments to avoid disruption.

**Figure 2: Advanced DDoS attacks still disrupt services.**

PhishLabs DDoS Intelligence helps reduce this risk by providing real-time information and actionable intelligence about DDoS threats that can be used to:
- Proactively insulate against likely attacks
- Detect and respond to attacks faster
- Take the right mitigation steps to avoid further downtime

At a high level, PhishLabs DDoS Intelligence can include:
- IP addresses of bots and Command and Control (C2) servers
- Current and historical DDoS attack data
- Bot and C2 configurations
- Attack methods and commands

PhishLabs DDoS Intelligence does not replace investments in DDoS mitigation measures. The more mitigation layers in place, the more DDoS Intelligence can be applied to proactively improve resiliency. For organizations that have made significant mitigation investments, DDoS Intelligence should be evaluated as a force multiplier that helps existing investments perform beyond their current level of effectiveness.

For those organizations that have yet to implement DDoS mitigation measures, DDoS Intelligence can provide the information needed to accurately evaluate risk and make the best mitigation investments to minimize the impact of attack.
As illustrated in Figure 3, PhishLabs DDoS Intelligence works with and improves existing mitigation controls to enhance resiliency against DDoS threats.

Figure 3: Enhancing mitigation measures with DDoS Intelligence.
The DDoS Attack Process

Understanding the process behind DDoS attacks allows for stronger defensive strategies and tactics. In general, DDoS attacks follow the process outlined below with variations depending on the attacker’s capabilities and objectives.

Phase 1: Prepare
Before the attack is launched, several preparations must be made. Threat actors plan their attack, identify the target and conduct reconnaissance to find services vulnerable to DDoS.

Sources capable of generating the desired flood traffic are enlisted. This is accomplished by renting capacity from botnets for hire and “booter” networks, or manually by building a network by compromising PCs and/or web servers and installing DDoS botnet software.

Once the botnet is established, members are configured to contribute to the attack. In some cases, this entails installation of specialized tools to Command and Control (C2) servers and bots. Testing is performed to validate flooding capabilities and the effectiveness of attacks against target services.

Phase 2: Launch
Once preparations have been made, attack commands are issued to the botnet to commence sending DDoS flood traffic to targeted services.

Depending on the attack method and botnet composition, the attack may take minutes or hours to reach peak flood traffic. As the attack ramps up, botnet infrastructure is monitored to verify anticipated traffic volumes and attack execution.

Phase 3: Adapt
Throughout the duration of the attack, targeted services are monitored to determine if the attack is impacting performance and availability. If targeted services regain normal operation during the attack, indicating successful mitigation of flood traffic, the attack may be altered and new attack commands sent to counteract mitigation.

How often this process repeats depends on the persistence and capabilities of the threat actor. Determined DDoS attackers may cycle through multiple times before ceasing the attack.
The DDoS Defense Process

The best outcome from a DDoS attack is to mitigate the attack traffic without service disruption. As described previously, it is best to take a layered approach to mitigation. However, effective defense against DDoS attacks calls for more than mitigation measures.

DDoS protection requires a strategic process entailing proactive preparation, fast detection and surgical mitigation. The high-level process outlined below describes the steps needed to minimize the impact of DDoS attacks.

Phase 1: Prepare
All organizations operating high-value online services should evaluate their risk of being targeted by a DDoS attack. This includes online banking, e-commerce transactions, social media, or any service requiring the user to provide sensitive financial or personal information. The evaluation should determine services likely to be targeted, the impact of disruption and the likelihood of attack.

Attack methods should also be researched to identify likely attacks and how those attacks cause denial-of-service conditions. Different attacks may require distinct preparations to prevent or mitigate impact. Testing may be included to determine if the organization is vulnerable to attack seen in the wild.

High-value services should be hardened to improve resiliency against likely DDoS attack methods. Depending on the attack method, hardening can be accomplished by removing vulnerabilities, increasing capacity or implementing additional defensive layers.

It is also a best practice to implement block lists to block traffic from known botnet IP addresses. While they may not be as useful if attack sources are spoofed, or in reflective attacks (where botnet IPs are not the source of the inbound traffic), block lists are an effective layer of defense for other DDoS methods.

Figure 5: The DDoS Defense Process
Phase 2: Detect
Time is of the essence during a DDoS attack. The faster the attack is detected, the sooner mitigation steps can be completed to minimize downtime. If DDoS traffic is detected early as it is ramping up, it may be possible to avoid service degradation altogether.

Once an attack has been detected, it needs to be analyzed to determine the best mitigation steps. For successful mitigation, defenders need to know:

- The vulnerability targeted for exploitation
- The type of DDoS attack (volumetric, protocol, application layer, business logic, etc.)
- Sufficient traffic detail to scrub the malicious traffic without affecting legitimate traffic

Phase 3: Mitigate
After detecting and analyzing an attack, action can be taken to mitigate the DDoS threat. Mitigation layers discussed previously are used in this phase to block, filter and scrub malicious traffic to minimize the volume reaching the target and preserve capacity for legitimate users.

It is important to note that the effectiveness of mitigation depends greatly on the preparations made beforehand and the ability to detect DDoS traffic early in the attack progression.

After mitigating a DDoS attack, it may also be in an organization’s interests to pursue shutdown of the botnet. For example, if a botnet is a persistent threat that relies on compromised hosts; organizations may work with hosting providers, ISPs and law enforcement to reduce the botnet’s footprint and attack capacity.
Applying DDoS Intelligence

PhishLabs provides DDOS Intelligence services that can be applied to all phases of DDoS defense to improve resiliency and protection. As displayed in Figure 6 below, PhishLabs DDoS Intelligence allows the DDoS defense process to be more attuned to the attack process, focusing defensive efforts on the most relevant threats and attack methods.

**Figure 6:** Using DDoS Intelligence to align defenses with attacks.

Using DDoS Intelligence to Prepare
PhishLabs DDoS Intelligence provides valuable insight into botnet activities and capabilities. This insight streamlines research into the DDoS landscape, answering two key questions:

- What is the likelihood of being attacked?
- What attack methods are most likely?

DDoS Intelligence answers these questions via access to rich information on real-time and historical DDoS attacks globally. DDoS Intelligence provides a view of attacks against other organizations and the attack methods being used by both PC-based botnets and “booter” networks.

This intelligence streamlines defensive preparation by providing the real-world DDoS visibility needed to fully prepare for likely attacks as illustrated in Figure 7.
Figure 7: DDoS Intelligence streamlines and focuses preparation efforts.

Determine risk of attack
Via the PhishLabs DDoS Intelligence Portal, clients have detailed visibility into DDoS botnet activity, including organizations being targeted and attacked. Using the Portal, organizations can view botnet families and their history of attacks. This real-world data can be used for more granular assessments of attack likelihood so that preparations can be made with a focus on specific botnet threats. Figure 8 below is a screenshot of DDoS botnet family tracking.

Figure 8: DDoS botnet family tracking.
Research DDoS methods
PhishLabs DDoS Intelligence provides the attack code distributed to DDoS botnets, illuminating targeted services and the specific methods being used to cause denial-of-service conditions. This information is available for all DDoS attacks on-demand via the DDoS Intelligence Portal, allowing clients to quickly understand the methods currently being used by active botnet families. Figure 9 below is a screenshot of attack code provided via the Portal.

Assess vulnerability
The attack code provided can be applied to proactively assess the environment for resiliency against likely attack methods. This includes testing services for vulnerabilities that would be exploited if targeted by a DDoS attack, as well as testing the effectiveness of mitigation measures in place.

Harden environment
With intelligence on likely attack methods and DDoS botnet capabilities, several steps can be taken to harden the environment prior to attack. Where possible, vulnerabilities in services can be remediated. Block lists of botnet IPs and domains can be applied to proactively block DDoS traffic and recognize attacks sooner. Mitigation measures can be optimized for more effective filtering of attack traffic.

Plan response procedures
Understanding the most likely attack sources and methods illuminates gaps in DDoS response planning. Response plans can re-assessed to become more focused, streamlined and up-to-date. Testing exercises can be refreshed with current real-world DDoS attack scenarios.

Figure 9: DDoS attack code sample.
Using DDoS Intelligence to Detect
Most organizations rely primarily on monitoring activity in their own environment to detect threats. DDoS attacks are detected once traffic reaches a certain threshold, initiating procedures for analysis and mitigation. PhishLabs DDoS Intelligence changes this with real-time visibility into external DDoS botnet activity. Using DDoS Intelligence, organizations can detect attacks earlier in the progression and begin mitigation before services are impacted.

Confirm attacks
When a new attack is targeting a DDoS Intelligence client, a Flash Analysis alert is sent to them. This alert details traits of the attack and can be used to rule out alternative causes of the abnormal traffic flow prior to mitigation.

Pictured in Figure 10 below, Flash Analysis alerts highlight the targeted IP and summarize the attack method in addition to providing the attack code.

```
From: ddoe-intel
Sent: Thursday, May 02, 2013 1:18 PM
To: REDACTED
Cc: REDACTED
Subject: New REDACTED attack code
Importance: High

Security Team,

We have detected attack code targeting the following IP used by <BANK>:

-x.x.x.x

During a period of 1000 seconds, it initiates multiple HTTP requests on ports TCP/80 and TCP/443 and sends UDP packets to port 53. The code can be found at the end of this message.

Please contact us on info@phishlabs.com if you have any questions.

***Begin code sample***

```|alm|=trim('x.x.x.x');
|spp|=trim('53-80-843');
|ddd|=trim('1000');
|ssst|=trim('1000');
|rrtt|=trim('1390-1420');

$ar_por=expode('|$ppp|');
$ar_paks=expode('|$ppps|');

if(file_exists("stext.txt"))
{
    $ffp=fopen("stext.txt", "r");
    $rrr=fread($ffp,8);
}
```

Figure 10: Sample Flash Analysis alert.
Determine mitigation

With the context provided by PhishLabs DDoS Intelligence, new attacks can be quickly analyzed to determine potential severity and the best path for mitigation. Additionally, DDoS Intelligence allows clients to understand the current and historical capabilities of the attacking DDoS botnet. This can be used for a more complete mitigation plan that anticipates likely attack adaptations. Figure 11 below is a screenshot of DDoS botnet activity reporting, which can be filtered by targets, botnet families, attack types and time ranges.

Figure 11: DDoS botnet activity reporting.
Using DDoS Intelligence to Mitigate
PhishLabs DDoS Intelligence can be applied to all layers of mitigation measures to block, filter and scrub malicious traffic. The following mitigation measures benefit from DDoS Intelligence:

- Network infrastructure controls such as switches and routers
- Security appliances such firewalls and Intrusion Prevention Systems (IPS)
- Cloud-based anti-DDoS services
- Specialized on-premise anti-DDoS appliances

Filter malicious traffic
PhishLabs DDoS Intelligence provides detailed attack information that can be applied to filtering tools before and during attacks. Clients have access to continuously updated lists of botnet IP addresses, URLs and ASNs that can be readily fed into mitigation measures for proactive blocking of DDoS threats. Figure 12 displays botnet enumeration within the DDoS Intelligence Portal. Block lists are available via API for tight integration with mitigation measures.

![Figure 12: Sample bot enumeration list.](image)

Flash Analyses and attack code samples provide granular detail on specific attack methods that can be used in mitigation measures for more effective filtering. By reviewing this intelligence, clients can quickly understand how the attack is intended to create denial-of-service conditions and implement additional network-layer filtering (cloud or premise) or application-layer filtering (cloud or premise). See Figures 9 and 10 in prior sections for examples of Flash Analysis and attack code provided with DDoS Intelligence.
**Pursue shutdown**
PhishLabs DDoS Intelligence provides key data to support the shutdown of attacking botnets should an organization seek to pursue those efforts. DDoS botnets commonly consist of compromised PCs or web-servers. The enumeration of bot and C2 servers, provided with DDoS Intelligence, can be used to remove compromised hosts from the botnet, reducing its numbers and attack capacity. This intelligence is especially useful in reflection attacks, where the true source IPs cannot be determined by analysis of inbound attack traffic.

Additionally, PhishLabs DDoS Intelligence details the exploits used to compromise vulnerable hosts and add them to the botnet. This intelligence can be used in conjunction with shut down efforts to harden hosts and prevent re-infection.

**Conclusion**
As the paper details, there are multiple use cases in which intelligence on DDoS botnets can be applied for more effective protection against DDoS attacks. PhishLabs DDoS Intelligence can be applied proactively to strengthen resiliency and detect attacks earlier in their progression. It can also be used during attacks to improve all layers of mitigation measures. Using DDoS Intelligence prior to and during attacks shortens the window of time between detection and mitigation, minimizing the potential impact to targeted services.

Overall, PhishLabs DDoS intelligence is an effective way to improve security posture against DDoS attacks. Organizations should consider incorporating DDoS Intelligence into their defensive strategy to ensure alignment with current DDoS threats and to enhance the effectiveness of defensive measures already in place.
About PhishLabs

PhishLabs is the leading provider of cybercrime protection and intelligence services that fight back against online threats and reduce the risk posed by phishing, malware, distributed denial of service (DDoS) and other cyber-attacks. The company fights back against cybercrime by detecting, analyzing and proactively dismantling the systems and illicit services cybercriminals depend on to attack businesses and their customers. With a fixed-fee service model that ensures alignment with client goals, the company partners with businesses to decrease attacks, reduce online fraud and prevent the loss of customer trust.

PhishLabs DDoS Intelligence

PhishLabs DDoS Intelligence delivers the real-time insight organizations need to rapidly assess and counter DDoS attacks so that critical services remain online and functional. PhishLabs monitors and enumerates PC-based botnets and webserver-based “booter” networks to provide real-time intelligence on imminent DDoS attacks. When an attack command is sent, we immediately alert the targeted client and provide crucial intelligence including the attack commands, attack scripts, bot IPs and capabilities of the DDoS botnet.

To learn more about PhishLabs DDoS Intelligence, download the service brief.

@phishlabs
www.linkedin.com/company/phishlabs

Contact Us:
info@phishlabs.com
+1.877.227.0790
References:

1 Prolexic, “Prolexic Quarterly Global DDoS Attack Report 1Q13”

2 Neustar, DDoS Survey: Q1 2012

https://securosis.com/research/publication/defending-against-denial-of-service-dos-attacks