DoS Attacks? Reporting DoS Attacks are the Key to Fighting Back!

Why is it critical to report a DoS Attack?

(and all other types of attacks)

DoS attacks are not something that can be defended with the “castle” of an organization. Layered defense breaks down when all the walls are attacked. When a castle is under siege, the siege stops from one or two reasons. First the attacker exhaust themselves. Or the castle under attack gets help from an outside source to remove the threat. Organizations who wish to prepare for a DoS attack should prepare to aggressively collaborate with their “allies.” These “allies” include law enforcement, their upstream Service Providers, their vendors, manage security companies, collaborative security groups, professional societies, and a range of other organizations that can be pulled into pushback, disrupt, and mitigate the DoS attack. When asked for help, all of these “allies” require information to help them mitigate the DoS attack, traceback to the source, remediate the tools used for the DoS attack, and possible lead to attribution to who is really behind the attack.

Step back - do you need to hire an expert?

Preparing for DoS is sobering. The materials that will follow look overwhelming. At this point it is natural to think your organization might need to hire an security or DoS expert. As a first step, jumping in and hiring a “security expert” is a mistake. Yes, security expertise should be sought, but that comes later. This first step is for Executive Management to allocate ***time*** for the existing team to focus security. Some of the best people who really know your network can do a range of security work, if you give them time. DoS attacks are not going away. It is best to invest in your existing team, providing them time and leadership to gain the knowledge and skills needed to mitigate and remediate DoS attacks. What's follows is a tool for a team within the organization to focus.

Why is it critical to report a DoS Attack?

How do you stop a baseball bat hitting you? You get out of the way and then stop the person who is swinging the baseball bat.

The essence for stopping DoS attacks are the same. The only way to ***stop*** a DDOS attack is by taking out the person(s) who are launching the DoS attack. Stopping the people launching the DoS attacks is not easy. Attribution is hard. It alway requires international law enforcement action working with private industry to collect a range of information that eventually lead to arrest. But, DoS attribution does happen. Arrest do happen. People who say "DoS attribution cannot be done" is not looking at the evidence.

> ***On 15 and 16 December, law enforcement agencies from Austria, Bosnia and Herzegovina[1], Germany[2] and the United Kingdom[3] joined forces with Europol in the framework of an operation against the cybercriminal group DD4BC (Distributed Denial of Service – DDoS - for Bitcoin) ……***
> (https://www.europol.europa.eu/content/international-action-against-dd4bc-cybercriminal-group)

What is missing is a willingness to drive the investigation to attribution. Many times the investigation would lead to a dead end. Other times the DoS investigation would lead to an inconclusive result. But there are times where the DoS investigation leads to results that become the meaningful arrest. It all starts with the target of the DoS to take action before, during, and after the attacks to report the incident. Without this action, the people launch the attacks, get away, learn lessons from the attack and get better for their next round of attacks.

This document is a collective experience from key DoS investigators in the industry. Many of the contributors wish to remain anonymous. Others are listed as key contributors. All of them have pulled their collective experience together to help craft this work for to help the industry prepare.

DoS Preparation Checklist

There are several good "DoS Preparation checklist" in the industry[1]. Reviewing all what needs to be collected to aggressively collaborate and investigate the DoS attack becomes another item in that checklist. When the internal team uses this document with their existing DoS Reaction plans, they will find new insight and questions. Many gaps for information gathering will be found as conversations happen with the the various vendors, operators, and other parties

Remember, There is no perfect anti-DDOS solution. But with forethought, planning, coordination, and practice any organization minimize the impact of the DDOS attacks. What follows ten essential steps that have proven to help organizations prepare for DDOS attacks.

[1] Recommend a keyword search on "DoS Preparation Checklist" to find several good papers. Several of them will be biased to vendors. These are still valid and should all be used as part of a DoS Preparation exercise.

The fundamental principles you will find in these guidelines is not to panic, DO NOT RUSH TO BUY, and to give your existing team time to invest in your Anti-DDOS Allies.

Step 1 - What services are critical to your business?

A distributed denial of service (DDOS) attack is an assault on a service. What services are essential to your business ("critical" = a direct impact on your business or the mission of the organization)? What are the most business impacting services that are accessible via the Internet? What critical internal services require the Internet to function (i.e. if the Internet stops working will the internal business functions stop)?

One of the most common misconceptions is that everything can be protected from a DDOS attack. Prioritize the most critical services needed for the business or organization's mission. Other non-critical might go down from the director or collateral impact of the DDOS. There is no escaping the reality of a DDOS attack. DDOS attacks can get ugly. Our goal with step 1 is to minimize the anxiety during that attack that trying to restore everything. It is much easier to have internal agreement on the critical services restoration path and work to the plan to keep those services up and to run.

Step 2 - CxO Sponsored Internal "DDOS Workshop."

CxOs worry that their existing team might not be up to the task of defending their network against DDOS attacks. While every organization has knowledge gaps, the people with the best knowledge of the network and services are the existing team. Step 2 for DDOS preparation is to pull together a cross-functional team and have a consultation the "critical services list" and what would happen if there is a DDOS attack. The objective of the DDOS Workshop is to build a list of issues, gaps, and capabilities. It is amazing what existing teams can do if they only get the mandate to spend the time to focus on preparing for a DDOS attack.

Step 3 - Make a list of the potential DDOS Defense Allies.

Defending against a DDoS attack is not a solo affair. The biggest Operators on in the industry collaborate to mitigate DDOS attacks. They collaborate with their competitors. They collaborate vendors. They collaborate with investigators. Collaboration with a group of Anti-DDOS Allies has been the #1 factor for successful DDOS mitigation. So, who are your Anti-DDOS allies? Who would you call? Is it your Internet Service Provider? Is it your equipment vendors? What about law enforcement or the local CERT Team? All of these groups can be your Anti-DDOS Allies if

you spend time and invest in the relationship before the attack. Use the idea provided in this document to make a list of all the potential DDOS Defense Allies. For several of them, you do not need a contract or agreement. For others, they will be part of your ecosystem of vendors and service providers.

Step 4 - Get the Security - Emergency Contacts and "Reach Out."

Who will your team call when a DDOS attack starts? Does everyone on your team know the emails, mobile phones, and IMs of each of your critical Anti-DDOS Allies? Building an emergency contact list is not a new concept. Make sure your operations and security team have all these Emergency Anti-DDOS contacts. This Emergency contact list is an industry Best Common Practice (BCP), but it is surprising that most organizations do not spend the time to build and maintain this anxiety-reducing crisis tool. Practice with the list. Regularly reach out to everyone on the list. E-mail, call, and chat, and practice with the list during tabletop and red/blue team exercises. It is important to make sure each organization is ready to be part of your "DDoS Defense Alliance." This first step to building the confidence they will be willing to help you is to regularly "reach out."

Step 5 - Regular Sync Up Meetings with your Anti-DDOS Allies.

Set up a conference call (or physical meeting) with your new DDOS Defense Alliance members Review your critical services. Explore what can be done together. Exchange intelligence and lessons learned. And when possible, practice. Spend time to explore what information is going to be needed to do the DDOS investigation. Your law enforcement Anti-DDOS allies will help you with the information they need to open a case. In essence, the regular sync up meetings is a vital tool to explore what you can do together and what information needs to be exchanged to facilitate each party's success against a DDOS attack.

Step 6 - Build Anti-DDOS Crisis Communications Plan and Escalation Plan.

Bad things happen to a network. Effective communications with customers, shareholders, staff, and partners are the difference between catastrophe and managed chaos. An internal and

external communications plan should be build before in-depth anti-DDOS architecture and solutions are considered. Build this plan, working with the crisis communications team in the company (or learning crisis communications principles) would all be valuable input for the anti-DDOS solutions that would be considered.

Some peers in the industry joke that organization's do not need to spend millions of dollars on anti-DDOS solutions. All that is required is an effective crisis communications plan that manages the anxiety of customers, shareholders, and the board of directors. They reason why they say this is the witnessing of excellent communications plans during massive DDOS Defense fiascos. The effective crisis communications allowed for quick recovery one the DDOS attack is over. The crisis communications plan would be reviewed quarterly and postmortem after each DDOS incident.

Step 7 - What anti-DoS techniques can be done with what you have right now?

There is a range of simple tools that can be used to build anti-DDOS resiliency into the existing network. All the vendors in the network should be pulled into to have a conversation on “what can be done with what we have now.” Most of them will be pushing new products, but the focus is what can be done now if a DDOS attack starts now.

Step 8 - Practice Practice, Practice.

Anti-DDOS tools only work if everyone knows how to use the tools. Anti-DDOS Alliances are only productive if the Alliance communicates, practice, and work to understand how effectively align their Anit-DDOS response. Regular War Room, Table-top, Red Team/Blue Team, Cyber Range, and other “training exercises” are needed to ensure everyone knows how to use the tools.

Step 9 - How to Report a DDOS Attack - the Collection Exercise.

People who launch DDOS attack do get caught. It takes hard work with a lot of international collaboration. The first steps are the victims of DDOS attacks working with their Anti-DDOS Allies to report the details of the assault. The “How to Report a DDOS” white paper is a tool to

help organizations review and prepare information their Anti-DDOS Allies will need to do their part of the investigation.

Step 10 - What will be done to build a more resilient capability for the future?

Critical services can be built to be highly resilient to DDOS attacks. These architectural principles will be learned over time. Not all of them would be worth the cost, but over time, the organization would learn which are the most beneficial. Ask “which are the top architectural techniques to resist DDOS attacks” during all the conversations with vendors, operators, Anti-DDOS Allies, and other experts.

Where do you report DoS Attack?

Who are your ALLIES?!? Reporting the details about a DoS attack requires trust. That trust can be contractually (i.e. a vendor with a NDA) or it can be mutually gained through experience. The first step in preparing for a DoS attack should be find out who your Allies will be during and after a DoS attack. These “DoS Defence Allies” will shape who to report a DoS attack, what actions will they take when you report the DoS attack, and what follow through will happen to go after the DoS Operators.

There will be multiple parties for which you report the attack. It is advisable to use the same report or reporting tools for all the *DoS Defense Allies*. Mean Time of Response (MTR) is essential during a DoS attack. Some of the information will be used by every organization. Other information will only be used by one of the organizations. But, standardizing your organization’s reporting allows for scaling.

What should be done to Prepare the ***DoS Defense Allies***?

Step 1 - Make a list of the potential DoS Defense Allies. Use the idea provided in this document to make a list of all the potential DoS Defense Allies. For several of them, you do not need a contract or an agreement. For others, they will be part of your ecosystem of vendors and service providers.

Step 2 - Get the Security - Emergency Contacts and “Reach Out. Getting the contact list of all the emergency/security contacts is a BCP. Doing the next step of reaching out, E-mailing, calling, and setting up meetings is the step that is normally missing. It is important to make sure

each organization is ready to be part of your DoS Defense Alliance." This first step of "reaching out" would make sure they are willing partners.

Step 3 - Sync Up Meeting. Set up a conference call (or physical meeting) with your new DoS Defense Alliance member and review what you can do together and what information needs to be exchanged to facilitate each party's success against a DoS attack.

What of some examples for your *DoS Defence Allies*?

Here is a short list to get started:

Upstream Provider - Your upstream service providers are key. They are the path into your organization. The upstream provider is going to use the DoS for their own mitigation, work upstream to the attack to minimize collateral damage, and then to help remediate the attack. The upstream provider is the target's organization's #1 "anti-DoS" collaboration partner. In many ways, they are also a victim of the attack, with the DoS aggregation impacting parts of their network and other customers. The Upstream providers will also be a source of information. Working with them before the DoS attack would help determine what information they can share during the attack.

Cloud Operator and the Cloud's Downstream Providers. Hybrid systems are normal today's networking. That means the target's cloud deployments, the downstream operators that support that cloud, and the interconnects between the cloud are part of the "DoS attack surface" that can be attacked. Given this, the security teams in these cloud operators would be part of an organization's *DoS Defense Allies*.

Law Enforcement - The only way to truly stop a DoS attack is to put handcuffs on the attacker. That requires official law enforcement action. Some might think it is futile to work with law enforcement for DoS attacks which are often transnational. Yet, the only way we will progress is if law enforcement is exercised to act. That action requires preparation before the attack (i.e. knowing who to call) and then reporting the attack. It is highly recommended to reach out to local law enforcement. This helps all parties to scope out each party's capabilities.

Managed Security Service Providers (MSSPs). Managed Security Services are an integral part of today's "resilient architectures." Many of these solutions have Security Operations Centers (SOCs) and Security Incident Teams who are contractually obligated to assist. Take time to prepare the MSSPs before the incident. They have access to some information during the attack, but will need more to get a full scope of the threat.

Hardware, Software, and Solution Vendors. Vendors are the building blocks for "Security Solutions." Most reputable vendors have Security Incident Response teams and Vulnerability Management Teams. Building a relationship with these groups is one element in an overall

response plan. For example, details of a low level “crafted packet” attack that crashes a network element might be linked to an unknown zero day vulnerability. The vendor’s team should be able to help the organization track the issue and deploy appropriate mitigations.

Industry Security Groups. There are many industry groups with established records of trust, working with each other for their collective interest. Some of these groups are trade associations. Others are guarded trust communities focused on specific parts of the threat. Many of these groups have acted collectively to stop DoS attack. The famous 2007 Estonian DoS attack was mitigated through collective industry action by NSP-SEC[2] and the FIRST[3] Communities.

Value of Tabletop Exercises Before the Attack

Image a fire department rolling up to a fire and then trying to figure out how to use the equipment. That is normal for DoS attacks. Organizations wait until the attack before doing any preparation. One preparation tool is to pull in representative from all the allies and run a tabletop exercise. This is a tool used to explore attack situations, how each group would respond to the situation, and how the the groups would work with each other. It is one of the best ways to explore how information would need to be shared, the format of that sharing, and how the information would be used to mitigate and remediate the attack.

How to Report a DoS Attack?

Do not wait until there is an attack to figure out how to report the attack. DoS Attacks cannot be stopped through individual organizational action. Industry wide collaboration is required to remediate the attack and then have a chance to attribute and even put handcuffs on the person(s) doing the attack. This “industry wide collaboration” requires in-depth sharing of information between organizations. Some of this information requires tools to be in place and operational before the attack. Let’s review these tools and ensure that we have detailed understanding of what is needed and why it is needed. We’ll then explore the tools that need to be put in place to collect this information. Lastly, we’ll walk through the policies and legal review that needs to clear the path for “industry wide collaboration.”

What needs to be collected and shared?

The following is the collective list of information that should be collected and then cleared to be shared with the appropriate *DoS Defence Allies*.

[2] NSP-SEC is a informal industry group of service providers who work together to protect each other from DoS attacks and other malicious activities. https://puck.nether.net/mailman/listinfo/nsp-security

[3] FIRST is the Forum of Incident Response and Security Teams. This is a formal membership organization of security incident response teams from all over the world. https://www.first.org/

What?	Why?
Classify the data using the Traffic Light Protocol (TLP). This will shape how the data will be shared during and after the attack.	The Traffic Light Protocol (TLP) is a tool used within the security community to safeguard how information is shared. The first thing the organizations should do is label the information with the appropriate classification. TLP is a global "Industry to Industry" tool that should be used by all parties. For example, a TLP of RED on information shared with the Upstream ISP would means the ISP would not share the information with any other party unless they get explicit permission from the targeted victim. Please review https://en.wikipedia.org/wiki/Traffic_Light_Protocol for more information.
Date of First Observed Attack (including timezone)	This would be the first observed attack. Note that some DoS attack profiles will have precursor attacks that test the target's defenses. Hence, we state that this would be the first *observed* attack. The timezone information should be included to allow for normalization around GMT.
What is the attack type?	There a different types of DoS and Extortion attacks. Some overload with packet flows the saturated the bandwidth. Other overload state tables. Still others target zero day "crash the device" that causes reboots (or other problems). Describe the attack type to the best of your abilities. Not that the attack type might shift over time as the attacker counters defenses put up to mitigate the attack.
Size & Duration of Attack	What is the estimated size and duration of the attack. "Size" would be within the context of the type of attack. bandwidth saturation attacks are different from packet per second (PPS) or state saturation attacks.
What is the impact of the attack?	How is the attack impacting the organization, business, or other function? The attacker would have a objective. There is an intended target. There are also unintended "collateral damage." List out the what is thought to be the intended target and what are collateral impact damage.
Has there been confirmed loss or life impact?	Has the attack caused any documented loss to the business or worse impact to life. The interconnected world will have challenges where the direct or indirect impact of attacks cause human injury. List out the known damages with the understanding that a full scope of the organizational loss can

	only be account for long after the attack during the postmortem.
Source IP Addresses of the Attack	Source address of the attack are valuable. Some people might say “they are spoofed, so it does not matter.” This is not true. The spoofed addresses contain information that can be used to traceback, profile, and gain insight into the attack. In some cases, the source IP addresses will traceback to computers infected with malware. Some SPs are able to take spoofed IP addresses and trace back to the entry ports on their network. They can then work with their peers to continue the traceback.
Source Ports Used for the Attacks	What source ports were used during the attack. Take note that there might be multiple ports in the packets coming from the attacker’s tools. We look for ranges and patterns in the source ports as one type of “fingerprint.”
Destination Ports used for the Attacks	What are the destination ports on the targets for attack Often there will be multiple destination ports targeted.
Logs at beginning and ending of DoS attack	Logs can range from the element under attack (web server, email server, DNS server) to elements around the target (load balancer, routers, switches). They can also include Netflow, firewall logs, IDP/IDS, and other systems.
'Extortion’ demand Email, including Email headers	If there is an extortion E-mail, the full detailed e-mail should be kept and preserved. While many of these are obfuscated, the details from several extortions can be used to gain insight into the extortion.
Any correspondence with or about attackers	Include the whole chain of communications - including the full headers. If there is a chain of Emails corresponding with the extortionist, then that chain of correspondence could provide clues that would help profile the attackers.
Phone call logs and/or recordings	Include the phone logs of attacker who might be calling with threats. There are times where helpdesk and NOCs get called by the attackers. This is where a call logging system is useful.
Details of ransom requested or paid (account identifiers)	Extortion only succeeds if there is a reward to the extortionist. That means money needs to be paid. Tracking the flow of the money is one way tracking the bad guys.
Was there any previous criminal activity before the attack?	Sometimes there will be activity before the attack. Hence, the attack might be linked to a larger criminal activity. Given the difficulty of attribution on the Internet, it would be wise to list out all suspicions of previous criminal activity.

Bitcoin wallet address of subject	Bitcoin is not anonymous. The extortionist must provide details. These details help to gain insight to the attacker.
Bitcoin wallet address of victim if paid and amount	While extortion payment is discouraged, there are times when it happen. If it does happen, details on the victim's Bitcoin details help with the profiling of the extortionist.
Any other information you deemed pertinent	General observations by the victim sometimes offer key "unexpected" insights to the investigators.
IP address that was targeted.	The IP address other see in their attack log may not be the IP address that was actually targeted. The details help find links to other evidence.
PCAPs of the Attack	It would be helpful to have PCAPs of the attack. These full packet captures help to explore the full details of the attack packets, attack sessions, and attack flows. A large PCAP sample would be required to allow for some type of statistical analytics.
Flow Telemetry	Netflow, SFlow, and IPFIX flows are all valuable to understand the attack.
DNS name(s) used if it's an amplification attack	The Fully Qualified DNS Names (FQDNs) of the target are critical to the investigation. These could be the FQDNs used to hit the target(s) Or if the "target" is really a 'reflector' (DNS, NTP, or other protocol) causing 'collateral damage,' then the FQDNs coming into and out of the reflector would be helpful in the investigation. Look for multiple FQDNs. There might be more than one.
What is being done (or was done) to mitigate the attack?	Mitigation impacts the attacker's objective and the impact on the target. List the mitigation technique, when they happened, and the observed behavior is helps to understand the tools, and capabilities of the attacker.
Geolocation Data	Geolocation data can come from unexpected data. For example, where was the target and the upstream entry points? What points did not get attacked? Sometimes the absence of the attack in one location helps to understand the profile of the attack.
Was there any attack precursors before the attack?	DoS Threat Actors will scan, scope, poke, test, and explore the target's network before the attack. These leave "precursors" that, if collected, offers indicators that can be used in the DoS investigation.

What?	Why?
Classify the data using the Traffic Light Protocol (TLP). This will shape how the data will be shared during and after the attack.	The Traffic Light Protocol (TLP) is a tool used within the security community to safeguard how information is shared. The first thing the organizations should do is label the information with the appropriate classification. TLP is a global "Industry to Industry" tool that should be used by all parties. For example, a TLP of RED on information shared with the Upstream ISP would means the ISP would not share the information with any other party unless they get explicit permission from the targeted victim. Please review https://en.wikipedia.org/wiki/Traffic_Light_Protocol for more information.
Date of First Observed Attack (including timezone)	This would be the first observed attack. Note that some DoS attack profiles will have precursor attacks that test the target's defenses. Hence, we state that this would be the first *observed* attack. The timezone information should be included to allow for normalization around GMT.
What is the attack type?	There a different types of DoS and Extortion attacks. Some overload with packet flows the saturated the bandwidth. Other overload state tables. Still others target zero day "crash the device" that causes reboots (or other problems). Describe the attack type to the best of your abilities. Not that the attack type might shift over time as the attacker counters defenses put up to mitigate the attack.
Size & Duration of Attack	What is the estimated size and duration of the attack. "Size" would be within the context of the type of attack. bandwidth saturation attacks are different from packet per second (PPS) or state saturation attacks.
What is the impact of the attack?	How is the attack impacting the organization, business, or other function? The attacker would have a objective. There is an intended target. There are also unintended "collateral damage." List out the what is thought to be the intended target and what are collateral impact damage.
Has there been confirmed loss or life impact?	Has the attack caused any documented loss to the business or worse impact to life. The interconnected world will have challenges where the direct or indirect impact of attacks cause human injury. List out the known damages with the understanding that a full scope of the organizational loss can

	only be account for long after the attack during the postmortem.
Source IP Addresses of the Attack	Source address of the attack are valuable. Some people might say “they are spoofed, so it does not matter.” This is not true. The spoofed addresses contain information that can be used to traceback, profile, and gain insight into the attack. In some cases, the source IP addresses will traceback to computers infected with malware. Some SPs are able to take spoofed IP addresses and trace back to the entry ports on their network. They can then work with their peers to continue the traceback.
Source Ports Used for the Attacks	What source ports were used during the attack. Take note that there might be multiple ports in the packets coming from the attacker’s tools. We look for ranges and patterns in the source ports as one type of “fingerprint.”
Destination Ports used for the Attacks	What are the destination ports on the targets for attack Often there will be multiple destination ports targeted.
Logs at beginning and ending of DoS attack	Logs can range from the element under attack (web server, email server, DNS server) to elements around the target (load balancer, routers, switches). They can also include Netflow, firewall logs, IDP/IDS, and other systems.
'Extortion’ demand Email, including Email headers	If there is an extortion E-mail, the full detailed e-mail should be kept and preserved. While many of these are obfuscated, the details from several extortions can be used to gain insight into the extortion.
Any correspondence with or about attackers	Include the whole chain of communications - including the full headers. If there is a chain of Emails corresponding with the extortionist, then that chain of correspondence could provide clues that would help profile the attackers.
Phone call logs and/or recordings	Include the phone logs of attacker who might be calling with threats. There are times where helpdesk and NOCs get called by the attackers. This is where a call logging system is useful.
Details of ransom requested or paid (account identifiers)	Extortion only succeeds if there is a reward to the extortionist. That means money needs to be paid. Tracking the flow of the money is one way tracking the bad guys.
Was there any previous criminal activity before the attack?	Sometimes there will be activity before the attack. Hence, the attack might be linked to a larger criminal activity. Given the difficulty of attribution on the Internet, it would be wise to list out all suspicions of previous criminal activity.

Bitcoin wallet address of subject	Bitcoin is not anonymous. The extortionist must provide details. These details help to gain insight to the attacker.
Bitcoin wallet address of victim if paid and amount	While extortion payment is discouraged, there are times when it happen. If it does happen, details on the victim's Bitcoin details help with the profiling of the extortionist.
Any other information you deemed pertinent	General observations by the victim sometimes offer key "unexpected" insights to the investigators.
IP address that was hit	The IP address other see in their attack log may not be the IP address that was actually targeted. The details help find links to other evidence.
PCAPs of the Attack	It would be helpful to have PCAPs of the attack. These full packet captures help to explore the full details of the attack packets, attack sessions, and attack flows. A large PCAP sample would be required to allow for some type of statistical analytics.
Flow Telemetry	Netflow, SFlow, and IPFIX flows are all valuable to understand the attack.
DNS name(s) used if it's an amplification attack	The Fully Qualified DNS Names (FQDNs) of the target are critical to the investigation. These could be the FQDNs used to hit the target(s) Or if the "target" is really a 'reflector' (DNS, NTP, or other protocol) causing 'collateral damage,' then the FQDNs coming into and out of the reflector would be helpful in the investigation. Look for multiple FQDNs. There might be more than one.
What is being done (or was done) to mitigate the attack?	Mitigation impacts the attacker's objective and the impact on the target. List the mitigation technique, when they happened, and the observed behavior is helps to understand the tools, and capabilities of the attacker.
Geolocation Data	Geolocation data can come from unexpected data. For example, where was the target and the upstream entry points? What points did not get attacked? Sometimes the absence of the attack in one location helps to understand the profile of the attack.
Was there any attack precursors before the attack?	DoS Threat Actors will scan, scope, poke, test, and explore the target's network before the attack. These leave "precursors" that, if collected, offers indicators that can be used in the DoS investigation.

What's Next?

Once this list of items are reviewed, the hard work begins to explore how the information is collected and how the information will be shared.

Internal Collection Exercise

As mentioned before, while external security expertise might be needed, most of the information collection preparation is best done with the team currently on staff. The collection capability will not be perfect. Gaps are to be expected. The gaps will be an action list that would then shape the DoS Preparation Planning. At this point, the best decision a CxO can make is to clear time for the existing team to run the Internal collection exercise, and build that gaps list of what can and cannot be done.

What gets done during the internal collection exercise? Create a hypothetical DoS attack and then use all the tools within the network to collect the necessary information.

Credits

The following are some of the key people who contributed their experience and help review, add input, and suggestions to this work. Many others anonymous assisted.

Doug Broecker
John Bambenek
Donald Smith
John Schiel
Elliott R. Peterson
Damian Menscher

Need More Help?

If you find your organization needs help and worry about the FUD from the industry, reach out and ask for help. You can reach me at bgreene@senki.org.

==========

➥ ***Barry Greene is Business Development Executive ★ Internet Technologist ★ 25 Year Veteran of Internet Security ★ Emerging Technology Mentor ★ Advisor to Innovative Startups***

➥ ***Barry connects to peers, colleagues, and aspiring talent via Linkedin (www.linkedin.com/in/barryrgreene/). You can also follow on Barry on Twitter (@BarryRGreene) or his blogs on Senki (www.senki.org).***