

Lab 7 Large-scale Incident Handling

1. Source of information
2. Initial investigation
3. Takedown
4. Warning & mitigation
5. Internal worm outbreak: malware capture & analysis, controller identification
6. Case study: hypothetical cyber attack against country X


The main objective of the exercise is to teach students the key information and actions required for the successful resolution of large-scale incidents.

After completion of this exercise, the students should be able to:

- Understand the nature and the consequences of a common large-scale incident;
- Determine the key information required for the successful resolution of such incidents; and
- Coordinate the exchange of information with various authorities.

The exercise is split into four different parts, concerning different types of large-scale incidents. The exercises listed here are intended as examples.


Task 1. Analysing malware

1. Choose a malware URL from URLhaus Database: <https://urlhaus.abuse.ch/browse/>
2. Use Any.Run analysis tool to create virtual machine to analyse malware: <https://any.run/>
3. Study results and upload report for this assignment. 

Another tool to analyse URL or document VirusTotal: <https://www.virustotal.com/gui/>

Another source for sharing malware samples is Malware Bazaar: <https://bazaar.abuse.ch/>

Task 2. Resolving large-scale incident

Read and study the cases of different large-scale attacks. For *Part 1 Large scale phishing attack* answer questions and write your thoughts how to take down this and resolve this incident. 

Home task: Learn elementary networking concepts in "Introduction to networking for complete beginners" course

<https://www.udemy.com/course/introduction-to-networking-for-complete-beginners/>

PART 1 LARGE SCALE PHISHING ATTACK

Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment.

What really distinguishes phishing is the form the message takes: the attackers masquerade as a trusted entity of some kind, often a real or plausibly real person, or a company the victim might do business with.

The attackers spoof their email address so it looks like it's coming from someone else, set up fake websites that look like ones the victim trusts, and use foreign character sets to disguise URLs.

Phishing emails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may:

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice
- want you to click on a link to make a payment
- say you're eligible to register for a government refund
- offer a coupon for free stuff.

That said, there are a variety of techniques that fall under the umbrella of phishing. There are a couple of different ways to break attacks down into categories. One is by the purpose of the phishing attempt. Generally, a phishing campaign tries to get the victim to do one of two things:

Hand over sensitive information. These messages aim to trick the user into revealing important data — often a username and password that the attacker can use to breach a system or account. The classic version of this scam involves sending out an email tailored to look like a message from a major bank; by spamming out the message to millions of people, the attackers ensure that at least some of the recipients will be customers of that bank. The victim clicks on a link in the message and is taken to a malicious site designed to resemble the bank's webpage, and then hopefully enters their username and password. The attacker can now access the victim's account.

Download malware. Like a lot of spam, these types of phishing emails aim to get the victim to infect their own computer with malware. Often the messages are "soft targeted" — they might be sent to an HR staffer with an attachment that purports to be a job seeker's resume, for instance.

Some tell-tale signs of a phishing email include:

- 'Too good to be true' offers
- Unusual sender
- Poor spelling and grammar
- Threats of account shutdown, etc., particularly conveying a sense of urgency
- Links, especially when the destination URL is different than it appears in the email content
- Unexpected attachments

Task 1 Source of information

How you could recognize that the phishing attack is happening?

Example: A phishing URL was reported by a bank, whose customers are being targeted. The CERT team has obtained a URL or URLs pointing to phishing site(s).

Answer:



Task 2 Initial investigation

Next step is to find out: a) if this is not a false alert, b) where the phishing sites are located, and c) how the attack is carried out.

The answers may overlap, so all are included in one step. Questions that can help you find out what is going on:

Are the phishing sites still active or alive? How to check this?

Are they active in all popular browsers or just in a particular one? What about wget? Maybe the phishing site requires a specific 'user agent' field set or another (for example 'referer')?


Where are the phishing sites (logically and physically) located? How to find out? What is the domain and IP address of the www server? To whom does the IP and domain name belong? Who is the host-master? Who is the ISP?

How is the attack being carried out? What technique is used to serve the phishing site? How to check this? Is the fast-flux technique used? Does every IP returned from the dns query lead to a response? Are there other sites on this server (IP)? What about the main page from the phishing URL?

Example:

The domain name resolves to many and various IPs. There is a strong possibility of fast-flux. The IPs belong to different ISPs, perhaps in a different country. There is no 'main page' on the 'server'.

Digression: Why are there so many IPs and why do some of them do not respond? Why do the miscreants use fast-flux? These IPs are probably zombies from some botnet. They are probably desktop-computers infected by special malware. Some of them are simply switched off.)

Answer: 

Task 3 Take down

The next step is to organize the takedown of this site as soon as possible. It is recommended that an attempt be made to try to track down the miscreants and victims of the phishing. Questions for you:

1. How to take down the phishing site? What is the fastest way to communicate with the administrator of the site? From which source can you get contact information?


Example: You could check the who.is database. The fastest way for contacting is by telephone. Many times it is better to send details via e-mail and call to inform that there was a phishing and details were sent via e-mail. Maybe there is an abuse-team or CERT team operating at the ISP? You must take language and time differences into account. In this case it is recommended that another CERT team from that country be involved – you could look one up on the FIRST site, www.first.org.)


2. Is the deletion of the phishing site by the administrator of a compromised site enough?


Where could you search for information about the break-in to the server and the vulnerability? If there could be a vulnerability in the www server or in the PHP scripts or in

the database, etc, where can you find information about suspicious requests, form entries, errors, etc? (**Answer:** inadequate server logs, etc.)

3. How to track down the miscreants? Where can you find some information about them? Where are the drop sites of the miscreants? (**Answer:** you must analyse the source code of the phishing site, as there may be information about where stolen data is sent. Other scripts on the compromised server, as well as server and e-mail logs could be helpful.)

4. Where to find information about victims? 

5. What to do with this information? 


6. Are these steps enough? What about cases, when we were unable to take the site down? 


7. Should law enforcement become involved? 

Answers:

Task 4 Warning & Mitigation

It is strongly recommended that potential victims be warned.

Does the bank know about the phishing? 

Should you write an alert on your webpage? Who should first know about this: the bank or the people reading your site? 

How to alert people who have visited phishing site(s)? Most popular browsers can warn people – how do you get them to do this? In which external services can you report phishing URL(s)? (**Answer:** phishing sites should be reported to Google Safe Browsing, Netcraft (<https://sitereport.netcraft.com>), PhishTank (<https://www.phishtank.com>), Microsoft PhishingFilter (<https://support.microsoft.com/en-us/office/protect-against-phishing-attempts-in-microsoft-365-86c425e1-1686-430a-9151-f7176cce4f2c>) Where else?

Answers:

PART 2 LARGE BOTNET SPREADING THROUGH A NEW VULNERABILITY

Botnet is a collection of internet-connected devices that an attacker has compromised. Botnets act as a force multiplier for individual attackers, cyber-criminal groups and nation-states looking to disrupt or break into their targets' systems. Commonly used in distributed denial of service (DDoS) attacks, botnets can also take advantage of their collective computing power to send large volumes of spam, steal credentials at scale, or spy on people and organizations.

Malicious actors build botnets by infecting connected devices with malware and then managing them using a command and control server. Once an attacker has compromised a device on a specific network, all the vulnerable devices on that network are at risk of being infected.

How to detect botnets: Botnets are typically controlled by a central command server. In theory, taking down that server and then following the traffic back to the infected devices to clean them up and secure them should be a straightforward job, but it's anything but easy. When the botnet is so big that it impacts the internet, the ISPs might band together to figure out what's going on and curb the traffic.

The computers in a botnet are controlled by a central server called a command-and-control server. The command-and-control server sends out periodic instructions to the

computers in its botnet. In some cases, there can be more than one command-and-control server in a botnet. This makes it even more difficult to stop. You may find and shut down one command-and-control server, but the bots will then just receive instructions from another command-and-control server in the botnet.

The existing techniques to detect botnet activity involve firewalls, honeypots, intrusion detection systems (IDS), and sandbox techniques.

Sandbox is an isolated environment on a network that mimics end-user operating environments. Sandboxes are used to safely execute suspicious code without risking harm to the host device or network. Sandboxing is used to test code or applications that could be malicious before serving it up to critical devices. Sandbox produces a number of analytical reports that need to be examined for botnet activity. To observe the impacts of botnet in a test environment, you could allow a variant of it to run rampant in a Sandbox using a Linux/Unix platform.

Honeynet approach is well known by its strong ability to detect security threats, to collect malwares, and to understand the behaviors and motivations of attackers. A honeypot, which comprises honeynet, is a system that lures attackers by pretending to have security vulnerabilities. It is a system that awaits to be attacked. Honeynet consists of more than one honeypot on a network for large-scale network monitoring.

Honeypot is a system that is installed with a purpose to detect abnormal access and it also serves to track down attackers and gather information. To deceive an attacker, a trap is created, as if the attacker had infiltrated into a normal system. And then a bot is caught and analyzed. Based on the analysis results, software disguised as a bot is created and traffic exchanged with the software is analyzed to find a controller or botnet.

The second exercise involves a botnet that spreads through a new vulnerability in a Windows service, available on port 42/TCP.

Task 1 Source of information

The CERT team starts to receive reports about a series of new hacking incidents from its constituency. The first question that can be asked is how the team can get more information about what is going on:

What (open) discussion lists could supply some supporting information?

What public websites could provide extensive information?

What kind of detection systems could the team operate to get more information by itself?

Task 2 Initial investigation

How can the team identify which sources in observed controllers constituency are infected? (Examples: WireShark, Netflow)

In what way could the team obtain a malware sample to verify or discover new controllers? (Examples: honeypots and sandboxes)

Task 3 Takedown

This task concerns the takedown of the controller.

Questions: How could the controller be taken down? What happens if it is in your constituency, or in another ISP in your country, or abroad in the USA, or in China?

What research could be carried out to determine the botnet owner?

How could law enforcement become involved?

Task 4 Warning & Mitigation

A list of infected IPs related to the constituency is obtained.

Questions:

How could the identified IPs be assigned to specific ISPs?

How could contact addresses for CERT or abuse teams of these ISPs be obtained?

How the threat could be contained, especially if taking it down turns out to be impossible?

PART 3 INTERNAL WORM OUTBREAK

Introduction to the hypothetical scenario

The incident that we are going to analyse happens in a hypothetical company called 'Innovative Software'. Figure 1 depicts the diagram of the network.

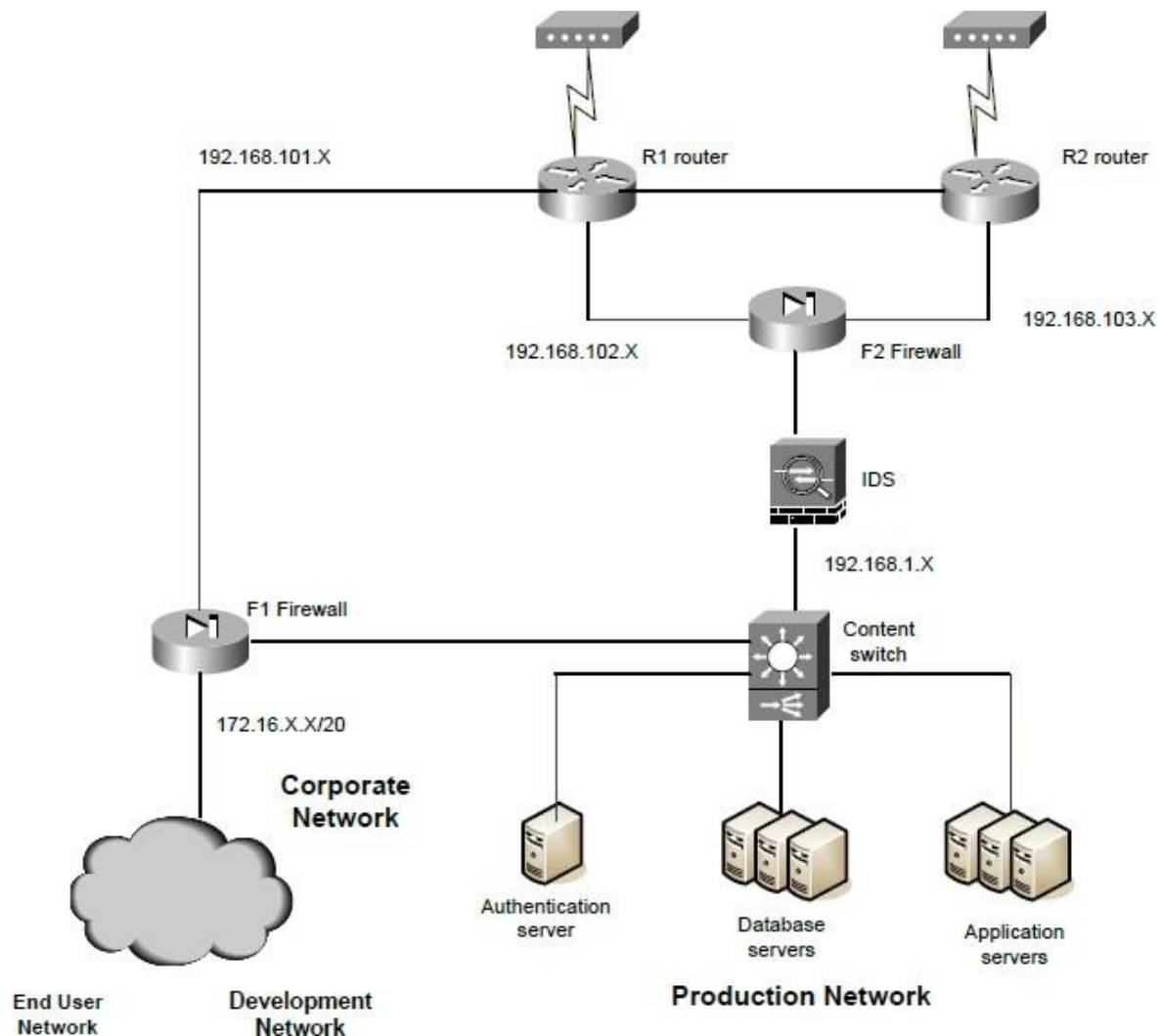


Figure 1: Network map

Innovative Software has two redundant Internet connections from two independent

ISPs. When the network is operating normally, only the connection through router R1 is used. Router R2 is used only in case of problems with the first connection. There are two main networks in the company: Production Network and Corporate Network.

Production Network is supposed to be available externally - for clients using Innovative Software services. Aside from application and database servers there are also authentication servers that allow authentication with advanced credentials using TACACS+ and RADIUS protocols. Corporate Network is divided into two sub-networks - End User Network and Development Network. The distinction is that users from the End User Network cannot reach the Production Network through firewall F1. Development Network is used by the R&D department. The access control lists on both routers and firewalls are configured in a deny-base setup. This means that only necessary traffic is allowed. The access for customers is strictly a web interface so only HTTP traffic is allowed to Production Network through F2 firewall.

We will not analyse the access list thoroughly - entry by entry, as this is not important for the exercise. Moreover, when dealing with the attack performed on a large scale, security specialists often do not know the details of network configuration immediately and have no time to become familiar with it. Therefore being able to estimate possible security flaws based only on general knowledge of the network structure is very important.

Innovative Software has experienced performance problems recently. Investigation of logs on machines in the Production Network revealed that the problem came from sluggish MS-SQL servers that play a critical role in the entire service. Administrators checked to see if there were any recent updates or configuration changes. Nothing appeared to be suspicious so they tried the desperate step of rebooting. At first it looked as if that solved the problems so the administrators sequentially rebooted all of the servers. Unfortunately, it only took minutes for the servers to slow down again to an unacceptable rate of processed requests. Administrators suspected that the network configuration was causing delays. However, running a few pings, traceroutes and DNS lookups at various points on the network did not reveal any problems.

At this point administrators brought up the possibility of compromise. Security engineers were contacted.

Task 1 Possible source of the attack

The Innovative Software network seems to be secured enough. The external firewalls appear to be configured properly, and they do filter traffic to MS-SQL ports.

Estimate where the attack could come from?

Example: The only users that can reach the Production Network are the developers working in the R&D department.

Do the users use MS-SQL servers in the Development Network? Do they have any access to the Internet beside the two firewalled connections? Can R&D employers take their laptops home and bring them back infected with viruses?

Task 2 Type of attack

As it becomes clearer that users from the Development Network could be the source of compromise, further investigation is needed to see if this really is the case.

If a virus came from the development network, as we suspect, then how can you find out more information about the attack, especially the kind of threat you face? Why does the IDS not signal anything?

Example: The first thing that could be done is to check the logs on all the network nodes that could 'see' anything interesting. Logs of neither firewall F1 nor router R1 contain

any useful information. Interesting entries, however, can be found on firewall F2 – a huge amount of denied outbound UDP connections to port 1434 to hosts that appear to be random. This is a clear indication that some type of exploit had compromised the SQL servers. Does the IDS have updated signatures?

It is very important at this point to stop the worm from spreading in the network. We know that firewall F2 stops the traffic, but the original source of attack can still be active and the worm is probably propagating through firewall F1. The following deny statements could be added to the firewall F1 outbound interface (from the 192.168.101 network):

```
deny tcp any eq 1434 any any log
deny tcp any eq 1434 any any log
```

That way you stop the network from propagating the worm and the host that caused infection can be localized through firewall logs.

Next, we should investigate the vulnerability and, especially, try to find out from the controller if the compromised systems are part of a botnet.

Task 3 Malware capture & analysis

Investigate the hosts to which the exploit is trying to connect and try to gain some information from the data that the exploit sends.

Example solution: We may want to separate the exploited server from the production network. To catch the traffic that the exploit sends, it is necessary to set up an environment for the worm to propagate. Such an environment could be a honeypot or sandbox system.

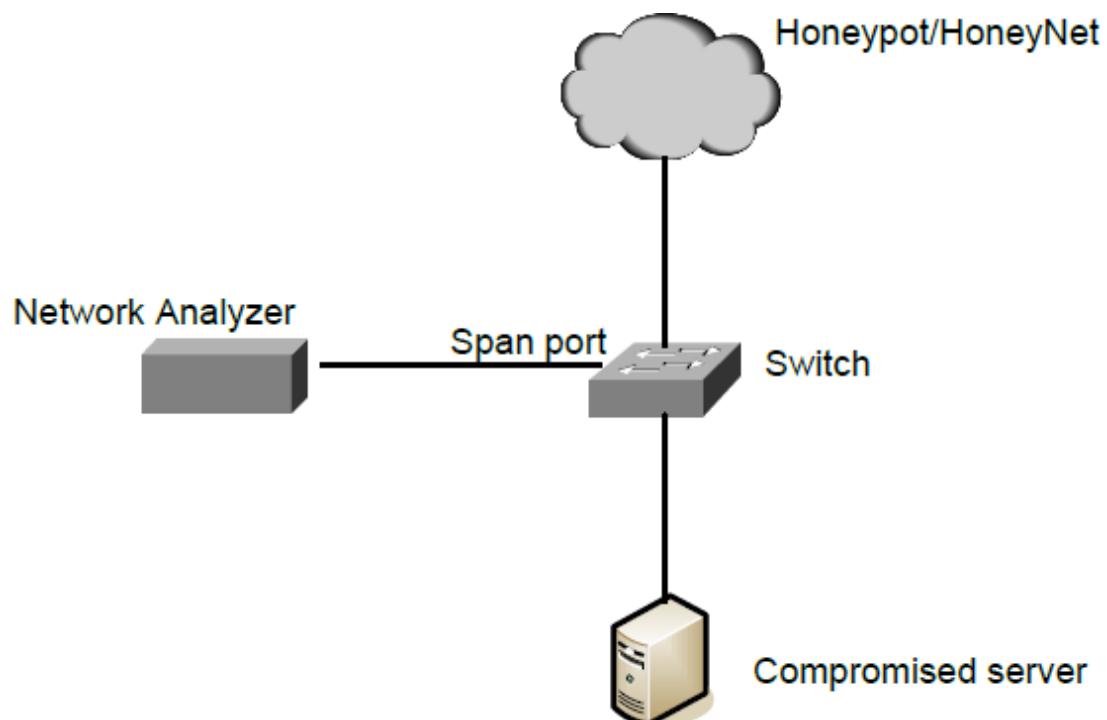


Figure 2: Network map

The network analyser is connected to the switch SPAN port. (Traffic from all other ports is forwarded to the SPAN port.) Due to the network analyser on the SPAN port, all the communications from and to the compromised SQL server can be observed.

You would need a honeypot that emulates the vulnerability used by the worm to obtain

a copy and to understand the infection process.

Task 4 Worm/botnet controller identification

To find out with whom the malware communicates and to try to identify other nodes on the malware network.

Example solution: First of all, you should investigate the range of the IP addresses that are attacked. Do they belong to any particular sub-network or does it look like they are chosen at random? All requests to the DNS server should also be reported. The technique that could be used to catch the URL requests and forward them to a specific IP address is called DNS blackholing. (In this solution the DNS server replies with a preconfigured IP address on specified URLs instead of resolving it.) There is a chance that the worm is actually a botnet and has the address of its controller as a URL rather than an IP address. First of all, IP addresses to which the worm tries to connect often should be considered suspicious. We know that the vulnerable service works on port 1434, so connections to other ports may imply communication with the controller. If no suspicious IP addresses can be found this way, the payload of connections can be analysed. Communication with the controller is different than packets containing exploit payload. So, theoretically, it should be possible to differentiate attack vectors from any other communication. As you have the list of IP addresses, you should check who they belong to. Usually the data you get from whois points to an ISP. In such a case, your role is to notify the ISP of the incident.

We are considering the case of the Innovative Software company network, so the last phase is to secure the network. First of all patches from the vendor should be applied (Microsoft in this case). The second problem is that the network is not secured properly. It should not be possible for the users to connect their laptops (potentially compromised) to the network and have unrestricted access to the production network. There are remedies for this, but they are another large topic which is beyond the scope of this exercise.

PART 4 LARGE SCALE DDoS ATTACKS AGAINST AN ENTIRE COUNTRY

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.

DDoS attacks are carried out with networks of Internet-connected machines.

These networks consist of computers and other devices (such as IoT devices) which have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots (or zombies), and a group of bots is called a botnet.

Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot.

When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become overwhelmed, resulting in a denial-of-service to normal traffic.

Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.

The most obvious symptom of a DDoS attack is a site or service suddenly becoming slow or unavailable. But since a number of causes — such a legitimate spike in traffic — can

create similar performance issues, further investigation is usually required. Traffic analytics tools can help you spot some of these telltale signs of a DDoS attack:

- Suspicious amounts of traffic originating from a single IP address or IP range

- A flood of traffic from users who share a single behavioral profile, such as device type, geolocation, or web browser version

- An unexplained surge in requests to a single page or endpoint

- Odd traffic patterns such as spikes at odd hours of the day or patterns that appear to be unnatural (e.g. a spike every 10 minutes)

This part of the exercise is devoted particularly to developing skills and ideas on handling DDoS attacks.

Task 1 Case study: hypothetical cyber-attack against country X

Example of a hypothetical large-scale cyber-attack that happens to some country X, described below:

This case study describes a hypothetical cyber-attack against country X: Country X is a medium size country with a quite advanced network infrastructure designed to allow consumers, businesses and government to use high bandwidth wire and mobile Internet connectivity. Country X has a substantial (10%) ethnic minority from country Y. Country X has two CERT teams: one ISP CERT and the GOV CERT. In the CERT of the ISP (which is the largest Internet provider in country X) there are some people of nationality Y. The national CERT, the GOV CERT, is a newly established team (three months ago). Country X has no cyber security policy yet. For a couple of years, country X and country Y have been candidates for the Famous International Organization (FIO). One day, country X becomes a member of FIO, while country Y does not. Just after this momentous event, the authorities of country X start to increase discrimination against the minority from country Y. The names of streets (in districts where most of minority Y lives) are replaced with the names in the official language of country X. Shops and schools of country Y are forced to close. Moreover, speaking the language of country Y in offices, shops, and in the streets is forbidden. Subtitles in language Y are eliminated from all TV programs. These government actions are an immediate reason for the start of the conflict. Within a few days, there are a lot of protests by people of nationality Y against these decisions (protest marches, etc.). Almost simultaneously, the conflict in cyberspace begins.

Cyber conflict (Phase I) During the first week, there are the following incidents:

- The government of country X receives millions of e-mails of protest from all over world, so government mail servers go down.
- There are a few cases of defacement attacks targeted against websites of the majority government.
- There are some DDoS attacks against government web servers, so they go off-line.
- Offensive texts in the language of country X are put on some popular country X websites.
- Some content on news portals of country X is replaced with new content in the language of country Y.

Cyber conflict (Phase II) The following week, after some relatively simple incidents, cyber attacks increase. There are many sophisticated and well coordinated attacks. Many of them use large international botnets (a few thousand compromised machines) controlled by five virtual domain name servers (from abroad). DDoS attacks are launched against the critical national information infrastructure of country X:

- Many government sites are overwhelmed by a series of DDoS attacks.
- The computer systems of the largest TV station are attacked and remain unavailable.
- The five biggest banks become unreachable and most banking transactions are paralysed.
- The police network infrastructure is under constant attack.
- Information services, news portals and press agencies are under heavy DDoS attacks.
- On-line shops stop offering electronic services.
- Besides the attacks of botnets, detailed instructions (in many languages) on how to launch attacks and the tools to carry out these attacks, together with 'a list of objectives', circulate on the Internet and are readily available, so even persons not familiar with hacker techniques take part in attacks.

The ISP is overwhelmed, so Internet access is limited. Cyber conflict (Phase III) After two weeks, the attacks continue. There is the beginning of complete information chaos and on-line communication is limited. Most of the important websites and networks (government, information services, police, banks, etc) remain unavailable. GOV CERT comes under heavy DDoS attack.

The task is to develop the defence strategy for country X. The appropriate actions should be proposed for each phase separately.

Is it possible to mitigate (if yes – how?) the particular attacks described in the synopsis?

What kind of measurements would you use for particular attacks?

What kind of response actions could be taken?

What kind of difficulties would you expect to face (regarding attacks, specific procedures)?

Consider the consequences of situations described (eg, disabled on-line news sources), explaining the reasons for the actions proposed, and the potential difficulties (lack of tools, no possibility of control, etc).

What priorities would you assign to the proposed actions in mitigation?

Who do you think should be a coordinator of mitigating actions in country X?

What kind of support can be offered or are you able to offer (as a representative of a CERT team), to country X? How would you organize the support?

What difficulties can occur during the recovery process?

References:

- Russian Invasion of Georgia. Russian Cyberwar on Georgia:
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campaign/2008/556_10535_798405_Annex87_CyberAttacks.pdf
- BCP38, Defeating Denial of Service Attacks which employ IP Source Address Spoofing. Available at <http://www.faqs.org/rfcs/bcp/bcp38.html>.
- <https://safebrowsing.google.com>
- <https://sitereport.netcraft.com>
- <https://www.phishtank.com>
- <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/submit-spam-non-spam-and-phishing-scam-messages-to-microsoft-for-analysis?view=o365-worldwide>
- <https://searchsecurity.techtarget.com/definition/botnet>
- <https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/>
- <https://www.thesslstore.com/blog/largest-ddos-attack-in-history/>
- https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/?utm_referrer=https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

○