Cyber Terrorism: A study and determination of actions after an attack

Jeevan Chandrashekar

Table of Content

Serial number	Content Name	Page No
1.	Introduction	3
2.	The ardit ferizi case	8
3.	Protonmail	15
4.	Conclusion	23

Introduction

In 2015, an average of 85,000 cyber-attacks a month was reported worldwide (Passeri). The US Government alone reported 77,000 attacks, a 10% increase from the previous year (Volz). The estimated annual cost for cyber-crime committed globally has added up to 100 billion dollars (heimdalsecurity.com). The motivations for these attacks vary. Most of them falling into one of the following categories: Cyber Crime, Hacktivism, Cyber Espionage, or Cyber Warfare, with Cyber Crime being the overwhelming majority, accounting for 67% of attacks in 2015 (Passeri). This brings up the question what exactly is Cyber Terrorism? Is every attack considered terrorism? Are only the major attacks considered terrorism? This question is widely debated among experts. The Merriam-Webster's dictionary defines Cyber Terrorism simply as 'terrorist activities intended to damage or disrupt vital computer systems'. This is a very broad definition that leaves a lot to the imagination. Some hackers only want to feed their ego by hacking into a site or system and leave some kind of mark behind, much like graffiti, just to show they can, without causing any serious damage, while others intend to expose confidential information or cripple an entire power grid. Some experts choose a more narrow definition, limiting it to only attacks performed by known terrorist organizations or individuals intending to create damage and mass alarm or panic, excluding the smaller lower level attacks performed by amateurs. One thing all experts can agree on is that cyber-attacks and cyber terrorism isn't going anywhere. The number of attacks and techniques and weapons used for these attacks only increases every year. And with more and more vital resources and information being completely dependent on computer systems, the threat and risk to individual and national security only becomes

graver. Technology seems to advance at a pace that is nearly impossible to keep up with by organizations and, especially, government agencies. By the time an entity can secure the systems they have, the technology has advanced and attackers can obtain it before those organizations even know new tech exists. Because of this, new threats come into existence before existing vulnerabilities have been mitigated.

Cyber Terrorism is not a new trend. Some of the earliest known cyber-attacks began in the 1980's. One of the first known computer viruses was created in 1982. It was created by a 15 year old high school student named Rich Skrenta, who created it as a joke to play on his friends (Jesdanun). The virus was called Elk Cloner and worked by attaching itself to the Apple DOS 3.3 operating system and was spread by floppy disk disguised as a video game, and used a technique known as a boot sector virus. Once the game was launched for the 50th time the virus was released and would copy itself to the computer's memory and displayed a blank screen with a poem about the virus. Once the computer was infected, if an uninfected disk was inserted into the computer the entire DOS along with the virus would copy itself onto the disk allowing it to be spread.

In 1988 one of the first known worms affected the world's cyber infrastructure. Known as the Morris Worm, it spread around computers largely in the US. The worm used weaknesses in the UNIX system Noun 1 and replicated itself regularly. It slowed down computers to the point of being unusable. The worm was the work of Robert Tapan Morris, who said he was just trying to gauge how big the Internet was. He subsequently became the first person to be convicted under the US's Computer Fraud

and Abuse Act (CFAA) (U.S. v. Morris, 928 F.2d 504 (2d Cir. 1991)). He now works as a professor at MIT (www.nato.int).

As the year 2000 approached fear of the Millennium Bug and the potential harm it could do was heightened. With the growing size and popularity of the internet along with the increase of dependency of computer systems by major corporations and banks and government infrastructure, a large majority of the general public were concerned almost to the point of hysteria about the harm this millennium bug could do. The whole thing turned out to be a hoax but the large scale fear that was invoked on the nation and the world and the media coverage that it got was noticed by our advisories and acted as a catalyst for the possibility of a devastating cyber-attack.

Since the year 2000 and the terrorist attacks of The World Trade Center on September 11, 2001, terrorism has continued to increase, particularly cyber terrorism. So much so that the United States Department of Defense charged the United States Strategic Command with the duty of combating cyberterrorism and in 2009 The United States Cyber Command was formed. Cyber-attacks have become and will continue to be one of the largest threats to the nation as well as individuals and corporations. Virtually every record and every piece of data, from the Government's most confidential secrets, to the balance sheets of businesses both large and small, to the communications of emergency response personnel, or the power grid of entire cities, all the way to the last thing an individual searched for or purchased online is stored on a computer network that is vulnerable to being hacked. This fact along with the fact that every day more and more people are learning and creating new techniques to commit attacks makes the threat of a major attack very large. Every day systems and networks

are being attacked. Sometimes these attacks are unsuccessful but sometimes they are. A lot of times a new vulnerability isn't even known until it is successfully exploited by an attacker. It takes a huge amount of diligence and resources to stay ahead of the eight ball when it comes to cyber security. Because of this tons of corporations and agencies are vulnerable. Some organizations don't take cyber security seriously, some have a larger risk appetite than others, and some simply don't have the capital and resources needed to remain secure. Regardless of the reason, successful attacks happen nearly every day and sensitive data is compromised on both large and small scales. In recent years many of these more high profile attacks have been made public by the media, attacks such as the Ashley Madison breach, or the breach on Target in 2013. What you don't hear about are the attacks made on our Department of Defense systems that happen on a daily basis, or the smaller breaches that expose the identities of individuals on a smaller scale. The fact of the matter is that in this day in age it's not a matter of if you or your data will be attacked but when.

Another area of cyber-attacks that never gets much coverage by the media is what happens after the fact. Once an organization gets hacked and their data exposed or stolen, what happens then? What do they do to clean it up or prevent it from happening again? These after attack response actions are critically important to the organization as well as the rest of the cyber world. The actions taken in the period after the attack can be make or break for the organization and should be used to learn from by themselves and other vulnerable parties. The topic is so important that it is common practice and in most cases a standard requirement to have Contingency Plans, and Disaster/Incident Response Plans for your system and network. So that in the case of

an attack you have a plan to recover your data and get your systems back on line in the least amount of time possible. The chances of an incident occurring is so great that having a solid Incident Response Plan should be a major priority for your organization.

In the topics to follow, we will be focusing on these after attack responses. There is a right way and a wrong way to handle an attack, especially an act of cyber terrorism. Some organizations handle it quite well and their techniques can be learned from, while others fail to recover from a cyber terrorist breach and, in many cases, it has been the demise of their business. These poor techniques can also be learned from as an example of what not to do. We will examine two different cases in which attacks occurred and were successful and what the organizations did after the breach. We will compare what they did right or wrong and lay out what we believe to be the most efficient way to respond and recover from an act of cyber terrorism.

THE ARDIT FERIZI CASE

The United States military must lead the way in and how cyber terrorism is defended in this country. The case against Ardit Ferizi is one of the first such cases in which one person was tried and convicted for cyber terrorism. Ardit Ferizi is the Kosovo hacker who helped ISIS by hacking into an online retail business and obtaining detailed military personnel information. He then provided it to ISIL as a hit list which contained information of military and government personnel with the understanding that ISIL would use the personally identifiable information (PII) as information to use to target and kill them. Ardit Ferizi, aka Th3Dir3ctorY, was 20 years old at the time of his arrest and capture. He was a citizen of Kosovo and was sentenced to 20 years in prison for providing material support to the Islamic State of Iraq and the Levant (ISIL), a designated foreign terrorist organization, and accessing a protected computer without authorization and obtaining information in order to provide material support to ISIL.

The time line of this case is listed as such: Ferizi admitted on June 13, 2015 that he gained system level administrator access to a server that hosted a website of a U. S. company that turns out to be the company was victimized. The website contained a database with PII belonging to over 10 thousand names of the company customers, which included military and government personnel. Ferizi was only interested in the PII of the military and government personnel which totaled over 1,300 names. On the exact same day, June 15 2015, Ferizi provided the PII belonging to over 1300 military and government officials to Junaid Hussein. On 11 August 2015, Hussain posted a tweet containing a document with the PII of the 1300 military and government personnel. Ferizi was detained and arrested by the Malaysian authorities on behalf of the U.S. government and was charged of criminal complaint on 6 October 2015.

This case demonstrates how important it is that law enforcement agencies around the world must have strong partnerships to follow and track down cyber criminals around the world. As this case demonstrates, “Cybercrime knows no boundaries and our efforts to dismantle these

operations would be impossible without international collaboration. The FBI will continue to vigorously investigate these crimes and work with our international partners to track down and arrest those who steal from our nation and citizens." This case also says that no matter how a person supports a terrorist group like ISIL, whether on the battlefield or in the cyber world, the FBI will identify, disrupt and bring them to justice for placing the lives of our military and government personnel at risk.

The seriousness of this case goes well beyond a trial and a conviction. The threat to these 1,300 victims goes beyond the release of their private information. They have now been marked as enemies of ISIL. Any ISIL member or sympathizer in the United States looking for a target now has the information belonging to 1,300 individuals who ISIL has specifically marked for attack. The victims have a permanent target on their backs. While the defendant may not have pulled a trigger, he told members of ISIL where to shoot. And the threat to these 1,300 victims has no end in sight. Because ISIL transmitted the PII over the internet, there is no way to know if the risk to these military members, civilian government employees, and their families, will ever end. It is not possible to permanently remove items from the internet, which means the private information of the victims that was released in this case will remain public. We do not know who or how many people downloaded and saved the PII, and when they may republish the information again. What we do know is that ISIL supporters have republished the PII provided by the defendant multiple times since August 11, 2015. These 1,300 victims can never stop wondering whether someone will accept ISIL's command to strike at their necks. One of the victims, a member of the military, perfectly captured this fear in his victim impact statement when he wrote, "I have to live constantly under the threat that someone might actually arrive at my residence and harm me or my family members."

The need for deterrence in the form of a huge punishment is the only thing that might make terrorists think twice about committing cyber terrorism. A bigger sentence is absolutely necessary to signal that the criminal is more than just a hacker, he is a terrorist. Stealing and

taking information to make money or embarrass people is one thing, but stealing it to harm or kill people is a whole different situation. These type of terrorist must be punished significantly to ensure that they know that it is a crime that will be taken seriously. If they know that they will be punished heavily for these types of crimes, they might think twice about engaging in such a crime. Many believe that a sentence of at least 25 years would make such a statement to future criminals thinking about participating in this type of crime.

Ardit Ferizi is a hacker and is fully aware of what he was doing. His skills and intelligence are verified by the fact that he led a group of hackers called the Kosovo Hackers Security (KHS). He demonstrated that he has the character and personality to participate in and commit a crime of this magnitude. Once a person demonstrates this type of behavior, he most likely will continue to participate in this type of crime. The organization that he was in charge of hacked into and stole information from several private and government servers around the world. This crime he and his organization committed was no accident, because it was demonstrated that he was fully aware of what he and the organization he was leading was doing by repeatedly participating in these types of crimes. Ardit Ferizi and his organization repeatedly sought opportunities to support ISIL with information from hacked accounts with government and military personnel.

Cyber Terrorism is a crime. Cyber ransom demands have exploded, with hackers hitting hundreds of businesses every day, encrypting hard drives and turning over the decryption key only once a payment has been made. The FBI estimates such attacks cost individuals and businesses $209 million in the first quarter of 2016.

Cyber Terrorism in the form of ransom attacks has grown extremely fast, said Dan McNemar, director of intelligence at Binary Defense Systems, a Hudson, Ohio-based company that helps defend clients from cyberattack. Yet those hit by the ransom attacks often are reluctant to report them. Companies fear the government will not keep it confidential and they fear what may happen once their shareholders find out.

According to a member of a private company's digital intelligence team, Cyber Criminals capabilities are 1,000 times what they were four years ago, but Daveed Gartenstein-Ross, a counter-terrorism expert at the Foundation for Defense of Democracies, said U.S. government cyber experts are "orders of magnitude better" than Islamic State-linked hackers. Tristan Reed, a security analyst at Stratfor, an Austin, Texas-based global security consultancy, said many issues make it difficult for companies to know whether intruders like the "Albanian hacker" Ardit Ferizi are linked to terrorist groups. Determining the source of an attack or a digital ransom demand requires difficult forensics. But since so much of public infrastructure in the United States is owned by the private sector, including electric utilities, the government and private businesses will find themselves needing to work together more often. "It's actually critical to collaborate," Reed said.

According to the FBI testimonials; although U.S. cyber adversaries' capabilities are at an all-time high, combating this challenge is a top priority of the FBI and the entire government. Thanks to Congress and the administration, the FBI is devoting significant resources to this threat. The FBI partnerships within industry, academia, and across all of government have also led to a dramatic improvement in the United States' ability to combat this threat. The FBI's statutory authority, expertise, and ability to combine resources across multiple programs make it uniquely situated to investigate, collect, and disseminate intelligence about and counter cyber threats from criminals, nation-states, and terrorists. The FBI is a substantial component of the Comprehensive National Cybersecurity Initiative (CNCI), the interagency strategy to protect the United States' digital infrastructure as a national security priority. Through the CNCI, the FBI and their partners collaborate to collect intelligence, gain visibility on our adversaries, and facilitate dissemination of critical information to decision makers.

In addition, as part of the FBI's overall transformation to an intelligence-driven organization, the Cyber Division has implemented Threat Focus Cells, which bring together subject matter experts from various agencies to collaborate and address specific identified cyber threats.

Who is behind such attacks? It runs the gamut—from computer geeks looking for bragging rights…to businesses trying to gain an upper hand in the marketplace by hacking competitor websites, from rings of criminals wanting to steal your personal information and sell it on black markets…to spies and terrorists looking to rob our nation of vital information or launch cyber strikes. Today, these computer intrusion cases—counterterrorism, counterintelligence, and criminal—are the paramount priorities of the FBI's cyber program because of their potential relationship to national security.

How can we as the U.S. combat the threat of Cyber Threats? In recent years, the FBI has built a whole new set of technological and investigative capabilities and partnerships—so they're as comfortable chasing outlaws in cyberspace as they are down back alleys and across continents. That includes:

- A Cyber Division at FBI Headquarters "to address cyber crime in a coordinated and cohesive manner"
- Specially trained cyber squads at FBI headquarters and in each of our 56 field offices, staffed with "agents and analysts who protect against investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud"
- New Cyber Action Teams that "travel around the world on a moment's notice to assist in computer intrusion cases" and that "gather vital intelligence that helps us identify the cyber crimes that are most dangerous to our national security and to our economy"
- Our 93 Computer Crimes Task Forces nationwide that "combine state-of-the-art technology and the resources of our federal, state, and local counterparts"
- A growing partnership with other federal agencies, including the Department of Defense, the Department of Homeland Security, and others—which share similar concerns and resolve in combating cyber crime.

The WHO behind these attacks is a blend. This blend of the criminal actor, the nation-state actor and the terrorist actor, that's going to be the trend over the next five years," said John Carlin, who recently stepped down as head of the Justice Department division that monitors foreign espionage in the United States.

Cyber Attacks have not only caused the FBI to change how they work but the CIA has had changes in their organization also.

But some active clandestine officers of the CIA argue that the intelligence community has grown too reliant on technology, a trend they trace back four decades to the directorship of Stansfield Turner. Satellite photography, remote sensors and communications intercepts have become more sophisticated, but so have encryption techniques and anti-satellite weapons.

More important, they argue, is that technology is no substitute for "penetrations" - planting or recruiting human spies in foreign halls of power.

Today, these current and former CIA officials contend, American policymakers have little insight into the thinking of other country leader's inner circle. Presidents, kings and dictators often don't share their true intentions electronically, putting this valuable information largely beyond the scope of digital spying. The best sources are still people, and these officials believe the agency is not mounting the kind of bold human spying operations it did in the past.

The CIA equivalent involves having the agency's five main directorates - Operations (covert spies), Analysis (trends and prediction), Science and Technology (listening devices and other gadgetry) and Digital Innovation (online sleuthing) and Support (logistics) - provide the personnel needed by each regional mission center.

Andrew Hallman, director of the new Directorate for Digital Innovation, said the CIA has embraced cloud computing as a way to better share intelligence. In a move that shocked insiders and outsiders, the CIA awarded a $600 million contract to Amazon in 2013 to build a secure cloud computing system where multiple CIA databases can be quickly accessed.

For decades, different directorates maintained their own separate databases as a security measure, said Hallman. Some of the applications the agency used were so old - up to 30 years - that the manufacturer was no longer in business.

ProtonMail

ProtonMail is an encrypted mail service. It is protected mail services. They use the combination of public key and symmetric key encryption. It was founded in 2013 at the CERN research facility by Jason Stockman, Andy Yen and Wei Sun. ProtonMail uses client side encryption to protect email information and user data before they are sent to ProtonMail Servers. The service can be accessed through Webmail client or dedicated iOS and Android apps. The servers are located at two locations one is Switzerland and other is European Jurisdiction.

Features:

User must provide login password and mailbox password. The login password is used for authentication, whereas mailbox password encrypts the user's mailbox which contains inbox, outbox, contacts and other user's information. When user tries to login, should provide both passwords to access the account as well as encrypted mailbox and private key encryption. Figure 1, shows when message must be sent message password must be typed. Password is Encrypted and sent to the user. When user must check the mail, password should be typed to decrypt the mail.

Security Level:

ProtonMail has invested in owning and Controlling their own server hardware at several locations within Switzerland. Datacenters are located all over the world. This provides an extra layer of protection by ensuring encrypted emails.

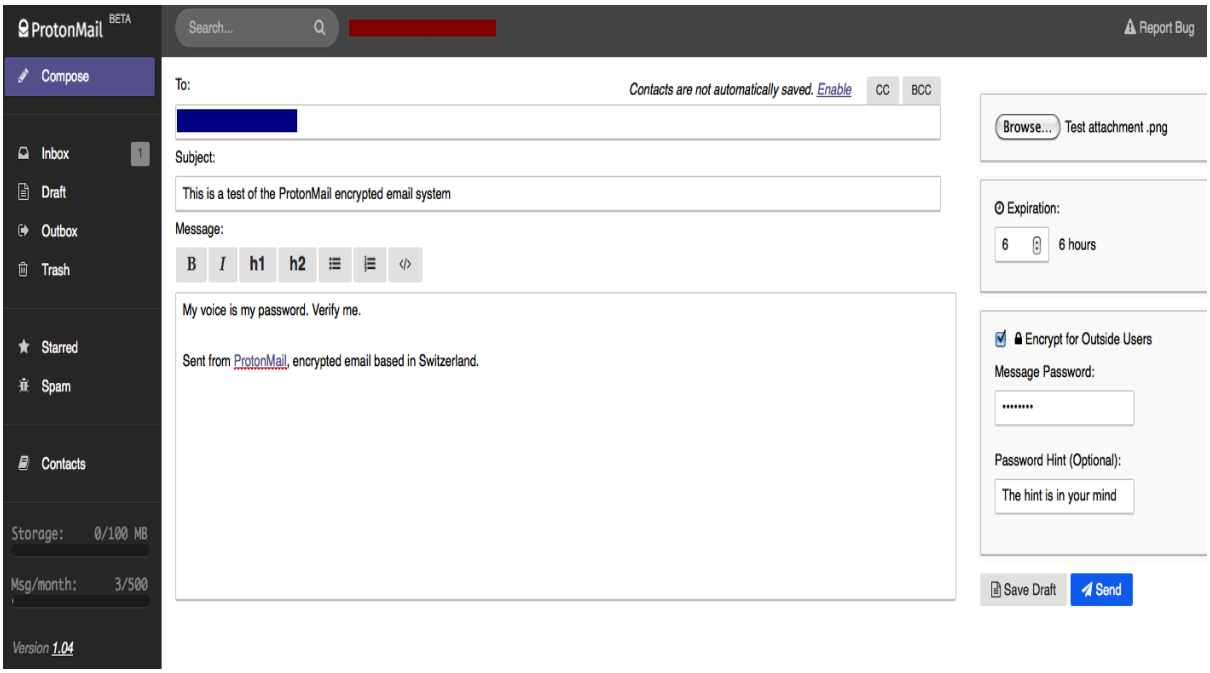

Figure 1

Threat Model in ProtonMail:

ProtonMail team did a good job in providing threat model. Analysis points out 3 attack vectors.

a) Comprised user's machine.

b) Man in the Middle Attacks.

c) Unauthorised backdoor planted by an external attacker on ProtonMail Servers.

There are some more additional threats included.

i) Metadata:

Metadata doesn't protect metadata. It will be a problem when it comes to surveillance. When ProtonMail is used, following metadata is available.

(1) Who you're been writing to.

(2) Email Subject.

(3) When the message was sent.

(4) Message size.

(5) From which IP

(6) Frequency of exchanges.

From these we can tell ProtonMail doesn't perform any better than Gmail, Hotmail, Yahoo etc. SCRYPTMail provides a better design by encrypting both Sender and Receiver side. In addition to that email subject, email content of course.

ii) Code Modification:

The main threat is modification of the application code to leak mailbox passwords. Few modifications in the mailbox can be done.

(1) At server level: By ProtonMail Employee Maliciously or upon court order, either targeted at a specific user or targeting any user.

(2) There are situations where MITM attack comes into the attack.

a) Certification Authority(CA) could be compromised delivering to valid SSL certificate.

b) SSLStrip attack when first time site was visited or computer. HSTS implementations doesn't prevent such attack.

iii) Private Key Theft:

Encrypted key is stored on ProtonMail Servers. Everytime user logs in encrypted key is transmitted to the browser. This opens private key theft at the ProtonMail Servers. Once private key is stolen, brute force attack can be performed on it.

Password Managers:

Not all password managers support ProtonMail Service because they use two passwords. If password manager is used, ProtonMail should try disabling it and enter password manually. If that works then bugs must be reported with describing password manger and computer. So that can make them work with ProtonMail.

Main goal of ProtonMail is to protect against malicious attacks to provide them encryption which is easy to use. When ProtonMail felt, everything was going well large mitigation DDoS attack was done. These attacks made users not to access ProtonMail Services but security was

not breached out. DDoS attacks continued with application and network vectors. Swiss based Servers experienced continuous attacks from different sources: one on a financial quest and the other ProtonMail's central mission. Along with that ransom request to be paid through Bitcoin, which eventually made ProtonMail pay the ransom, to see DDoS attacks combining application and network vectors. Cyber-attacks increased from 16% to 25%. In addition to that hitting ProtonMail, the attackers took down datacenters and several ISP's causing serious damage. Attacks continued but they could not extend the attacks for longer period. Recovering team recovered from these attacks.

Timeline of ProtonMail DDoS Attacks

1) November 4th 2015:

ProtonMail received blackmail email from the Armada Collective. They Blackmail companies for Bitcoin under DDoS attacks. The hacktivise group followed their threat with DDoS attack which took ProtonMail offline for almost 15 minutes.

By morning 11a.m., DDoS attack struct the datacentres. Within few hours' attack took a next level. At 2p.m., the infrastructure of upstream provides and datacentre was assaulted. The attack exceeded 100Gbps which affected routers in few locations such as Zurich, Frankfurt where ISP had nodes. Both datacentre and ISP was brought down and affecting many companies. With so much of intense pressure ProtonMail paid ransom via Bitcoin.

2) November 5-7 2015:

ProtonMail continued to suffer from high volume, unknown source and complex attacks.

3) November 8th 2015:

ProtonMail began working on the solution, the emergency response team came to help and restore the services which were affected.

4) November 9-15 2015:

Attacks continued at a high volume, reached to 50Gbps from 30Gbps. A short 2Gbps UDP spike occurred and was successful in blocking. After few minutes' attack resumed on UDP,

traffic was reached to 70Gbps but was mitigated again. The next day, early morning, one more attack was done at 150Gbps which was identified and thwarted by Radware.

Assessing the ProtonMail DDoS Attacks

Following the ProtonMail DDoS attacks, ProtonMail worked with MELANI, to exchange information with other companies which was also attacked. It became clear that the ProtonMail DDoS attacks occurred in two stages. The first was the volumetric attack targeting the company's IP addresses. The second was a more complex attack targeting weak points in the infrastructure of ProtonMail's ISPs.

Technical details of the DDoS attack:

DDoS attack was performed by two different groups, one of them known as Armanda collective and the other is unknown. It was later found that Armanda Collective was only hitting the datacentres; the second group was hitting datacentre, upstream ISPs and any other infrastructure that was exposed. It is to be noted that the attacks described originated from a large botnet, meaning the requests were generated from large number of computers and/or Internet of Things(IoT) devices.

Following are the kind of attacks:

1) UDP Simple Service Discovery Protocol(SSDP):

UDP flood means sending in a lot of UDP packets and are easy to mitigate. SSDP is a protocol that is used for discovering Universal plug and play (UPnP) networking device such as personal computer, printers, wifi camera, routers etc. A SSDP reflection attack means the attacker sends a small UDP packet to one of the networking device with spoofed IP of victim. Now the networking device will send back the response to victim instead of attacker because the device sees that the request was originated from the victim machine.

2) TCP RST/SYN flood:

A TCP packet has number of flags that can be set. RST and SYN are two of them. A ‘SYN’ flag is set when a new connection is about to start and RST flag is sent when the connection cannot be completed successfully or the port is closed. In this kind of attack, an attacker will send spoofed RST/SYN packets at a high rate. If the packets won’t match existing firewall rules and if the packets don’t match with currently existing session, the firewall will be overwhelmed trying to match the packets to existing session. This will slow down and eventually crash the firewall.

3) ICMP flood:

ICMP protocol is used for error handling purposes. It is used by utilities such as ping and trace route to determine if the server and hops are up. In ICMP flood, an attacker overwhelms the server with large number of ICMP echo requests. An attacker attempts sending large IP packets(larger than 65,536 bytes) using TCP fragmentation. This means, an attacker can fragment the packets and send large packets. When the packets are assembled after they pass the firewall, it overloads the server, thus preventing the server from fulfilling legitimate requests.

4) HTTP Syn attack:

In a syn attack, an attacker sends a probe (known as syn packet) with a request to open a new connection. Then, if the server is listening in a port, it will respond with SYN+ACK packet. Normally, a client would be expected to send back an ACK packet to acknowledge the server’s response. But an attacker waits for timeout in HTTP SYN attack. After an attacker finds out the timeout duration, he will keep sending SYN packets to the server and as soon as timeout is about to happen, he sends in another SYN packet. If this is done from large number of bogus IP addresses, server will be overwhelmed and no new connection can be started.

As mentioned before, Protonmail paid the ransom to the first group in hopes of getting their servers up. That didn't work because the second group wouldn't stop attacking Protonmail. This made them devise their own solution to DDoS. This unique approach makes this case a good example for case study.

Following were the steps taken by Protonmail to overcome the attacks:

1) Close unrequired ports:

Since Protonmail is a mail service provider and requires port 25 for SMTP related purposes, it couldn't use a DNS redirection service to block DDoS attacks. Any ports other than 80 and 443 shouldn't generally be required and should be closed.

2) Isolate datacenter and upstream providers:

Although a costly option, this will force an attacker to target a single IP. This will allow a webmaster to filter the kind of traffic they want to allow at a single location. Attackers can't target uplink providers and datacenter separately, so, there is no collateral damage to your providers.

3) Use a cloud based DDoS protection service:

This is like setting up a sinkhole where all the traffic would be scrubbed and only legitimate traffic will be let in. Isolating your infrastructure and using a scrubbing center(or a cloud based mitigator service) will help in keeping the application up.

Overall, the entire setup costs approximately $100,000 a year. This was possible for protonmail because they raised enough to pay the ransom and implement the protection mechanism in a crowd funding campaign.

Recent developments:

The attack we discussed was about 10 months ago. The volume of this attack peaked approximately 100 Gbps. Recently, there have been more attacks on other internet based services as well. Recent attacks on a DNS provider[5] brought big domains like github, twitter and paypal down momentarily. These attacks peaked at 1 Tbps and had millions of bots

continuously sending bogus traffic. The internet is seeing 10 times larger attack than what was considered a really devastating attack 10 months ago.

IOT consists CCTV cameras, wearable technology, TVs and different devices we tend to attach to internet. Recently, Krebs on security (a security researcher's web site, and also the supply of this info) was hit with a best attack of ~620Gbps. Akamai or the cloud content distribution system (CDN) for Krebs' web site, agency ultimately kicked his web site off their service. (They were providing the service for free and they could no longer do it for free with the sustained attack.)

Now usually, attacks of this size use 'DNS reflection', a technique whereby shopper and business routers equipped with DNS servers misconfigured to permit queries from anyplace on net (and thence malicious requests made of these routers appear to return from a fairly trustworthy source). A comparatively tiny attack of this nature is amplified by crafting DNS queries specified whereas the requests flowing in from a malicious assailant on net, and out from these routers are comparatively tiny (in terms of information size), the request generates a response 60-70 times that size from the server that the queries are ultimately sent to. Therefore, a comparatively tiny variety of broken routers will generate an oversized attack.

However, during this instance, the attack didn't suppose DNS reflection. Instead, it absolutely was principally comprised of requests made of many thousands of little devices.

Conclusion

With the threat of cyber terrorism looming overhead, it is always difficult and costly to keep one eye open or always looking over your virtual shoulder. Despite most organizations' best efforts to act proactively; ultimately, you need a reactive system in place. Security guru Bruce Schneier once said, "A sufficiently motivated, funded, and skilled hacker will always get in" and a group of hackers of this caliber are an even greater threat. However, in order to protect ourselves and those that use our systems, we look at cases such as Ardit Feriz1 and ProtonMail to determine courses of action that ultimately stopped and even brought down some of the hardest hitting attacks in cyber terrorism history.

From those cases, what steps were identified after the attacks begun or what should be in place because of these cases?

1. Law – We understand that laws should be in place to punish those that would attack and deter others.
2. Government or authority collaboration – entities working as one to stop threats,
3. In-system configurations and/or traps for different situations – different cases of attack call for different types of countermeasures
4. Preparation for the worst – security of a system especially after an attack is not cheap or easy and any company should be prepared to deal with both.

On a global scale, one key to tackling cyber terrorism is collaboration of law enforcement entities. By working together, we remove the safe havens that cyber terrorist prey on to protect themselves from persecution. Collaboration of agencies to create a super agency also allows the tracking of terrorist movement from system to system. Just a hacker often groups many to attack one, our defense should do the same to counter their efforts. Without collaboration, hacker such as Ardit Ferizi might not be serving time behind bars.

Another step in the after action plan is law enforcement and harsh punishments for cyber crimes. By instilling fear into would-be hackers, we create an environment for mistakes or even deterring attacks altogether. By adding an authoritative entity into the mix and pushing back against cyber terrorist, they are no longer the big bad wolf everyone should be afraid of.

However, just as we look at outside means of responding to cyber terrorist attack, we also have to look within and at what actions the victim system can take to recover from an attack.