Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 07
Lecture: 20

Another concept called VPN. Now, let us say we talked about a company with 5 branches, 4 branches. So, do you think they will have copies of same data, same servers everywhere? That does not make sense, right? So, they will create a central repository of information, central repository of everything. Now, how do other locations connect to it? So, this is the beginning of a concept called as a private network. This 5 organizations which are parent wise one organization or to be on a one private network. But can that private network be real? Can they lay lines directly from Hyderabad to let us say, Chennai or Mumbai? It is very expensive, right? So, they use internet, but create a tunnel between themselves, a private encrypted tunnel.

So, this whole process is called creating a virtual private network. So, this is the internet. So, there is a node, this is called a VPN server or VPS, virtual private server. So, you identify yourself to the VPS, then VPS will assign you a private IP and make you virtually part of your office network.

So, this office network could be in Delhi, you will be sitting in Chennai. This VPS will assign you a IP as if you are in Delhi. So, you can access all the resources in Delhi, clear? So, now a Chennai office member can participate, deal, access resources in Delhi through the process of VPN. Now, think about from the point of view, hackers perspective. What is VPN to him? Key to the kingdom.

If I can fool the VPN or a VPS server, I am in, nobody will even know, clear? Now, you see how it actually looks like in real life. Correct? The multiple VPN servers connecting each other, this is how all big companies, all big organizations actually look like in cyberspace, correct? The group is as strong as the weakest one in the group. Now, you guys can visualize, where things will be bad, fair enough, clear? Yeah. Now, let us look at the common things. I am sure you guys have seen CIA triad.

So, I would not spend much time on it. Let us quickly look at how a cyber attacker actually attacks, what are the steps involved ? This is no different from a regular commando ride that you see in movies. How many of you have seen Uri? Most of you almost, I think I would expect most of you. Whatever preparations they do, think about this. Have they done enough reconnaissance? You have seen the bird flying all over the

place, that small bird goes and comes.

How much of effort they put in to identify the tunnels, satellite imagery, connecting the dots, that is called? Ok. Then after reconnaissance, they have identified that the best way to get in would be in the night. So, that changes lot of things, correct? They get air dropped in a helicopter which makes very little noise. They do not want to wake them up. So, they get dropped away from the field.

Have you seen the movie? All of you have seen the movie, right? Correct. So, that means, picking right weapons for the fight, which in cyber language means, once you have done your homework, you have identified the cyber assets that are available. So, like in the last example, it could be a VPN, it could be a server, it could be any damn thing. Now, you have to pick a weapon that will be effective against it, correct? Prepare. Then next part, go and shoot.

Works, there is a crack. Now, you got inside, exploit. Now, you have access to the operating system. What will you do now? Will you come back? You want to remain there, do your work. Maybe you come to steal information or maybe you come to destroy the server, whatever it is, you have to deliver your payload and retain access, that is called? Because all these steps are happening from delivery to installation, is happening without your visibility.

You cannot see it as a hacker. They are all happening. Once all this is happened, you get an alert. "Yes Boss, it is done", to the command center. We will see with one more example.

So, that is much more clearer to you. Then you do whatever you want to do. Keep it as a botnet, try to copy the data, try to destroy the server, whatever you feel like. So, broadly they are all called as kill chain, cyber kill chain, clear? Now, we talked about how people generally prepare hacking. So, like we said you know in the initial discussion about ransomware and others, see how people usually try.

This is how most of the cyber hackers do. They randomly pick huge number of email addresses and keep sending payloads, with a hope that some of them will compromise. Then from them what they do? They collect more data from that system because that system is mostly inside a network or could be an email address, you get more leads, then you spread again. You keep spreading. So, over a period of time you will have a large list of vulnerable machines at your command, correct? This is totally unplanned random, probably looks like a spam mail, clear? So, here usually let us say you are looking at a cyber security situation.

Nobody has specifically targeted your company or your organization. It is just going in the flow, you could be one unfortunate victim and I am telling you in my experience lot of big, big companies fall victim to such operations. And then there is a specialized operations. This is cyber espionage. They are hell bent on targeting you and you only, correct? Now here they very focused, launch attack, collect details from one victim first, then expand, expand, expand.

They do not launch operations against everyone. They are fully focused only on those. Now here the weapons are different, tools are different, everything is different. Because in this earlier model, you have a risk of getting exposed. What if you targeted a cyber security researcher? Everything is gone, it simply published two page report.

We will see one report also like that, correct? So, this is more expensive, dangerous and tough also, clear? Of course, these principles we have already discussed. So, what does it mean and all that, yeah. And these are the common terminologies that I am sure you should know. But if anybody wants to clarify anything, please feel free to ask. How many of you know difference between a Trojan and Malware? I am just kidding.

What is the difference between Trojan and Malware? Malware is a general term, if Trojan would be particularly specific. Correct. Takes a payload within a payload. This is a question to ensure how many of you are not sleeping.

Yeah. So, Trojans are one type of malwares. Their primary objective is to give a back door to the attacker, correct? Ransomware and Trojan. Can a Trojan become a ransomware? Yes, it can. Yes, that is the point.

Yes, you should understand. Phishing and spear phishing, what is the difference? Spear phishing is more targeted. Absolutely, phishing is random emails, not really targeted effort, not really focused effort. Imagine someone does lot of research and finds out that I have a daughter who is studying in Doon school, writes an email to me, tries to phish me out, that is spear phishing, which means what do you conclude, Number 1? Attacker is motivated, he only wants you. It is an important input or not? Correct? So, in cyber jargon people do not talk about command and control, they use a very loose word called C2, alright C2.

It is basically C and C. There is also another terminology called C and C, command and control. So, if your machine is compromised, the machine is managed through a command and control. It is again another machine, whose job is to keep taking pings. It keeps asking are you alive? Are you alive? Are you alive? Yes, I am alive. Say this is a command for

you, do this.

Fetch me all the images, fetch me all the files, send huge packets to this computer. So, all that type of stuff. How many of you understand, what is the DOS? Denial of service attack? Please. So, denial of service attack is basically some server is providing some kind of service, the person who is attacking or the hacker who is attacking basically wants that, that service should be denied to all the clients or the customers and this is done by overwhelming that server.

Correct, very true, very true. What is distributed in it? When does it become a distributed attack? The same thing is done from multiple. Very true. So, basically see these are volumetric attacks. So, what happens is whenever you are on a network, you have a limited bandwidth available. When you are running a computer, you can only handle so many connections at a time.

Now the objective is to overwhelm it, so that you are not able to serve your legitimate customers. So, how many have you, have you ever seen this type of attacks before in your lifetime? Yes, the website is simply not responding, that is how you would see it as. So, what is actually happening is the website is serving customers who do not care about it. Correct, this is a very common form of cyber warfare or very simple crude way of settling accounts on the cyberspace, ok. Now you will hear another very common set of concepts like this vulnerability, exploit and payload.

If you do not understand this, you do not understand cyber security effectively. So, it is important that you guys understand these things. So, just look at the example for a moment. This is a bunker buster bomb. Can you see it clearly? See it clearly and who can explain me what is vulnerability, exploit and payload? I need three people to explain.

Anyone else? What is a vulnerability? Here, here, Binod here. Usko pata hai. Vulnerability can be said as a weak link in the security which can be. Absolutely, in this example, what is a weak link? Show me what is example. The thinnest part where the bunker buster is launched, the thinnest part, again the weakness.

Correct. Now does that mean that you are able to exploit always? You need a material with sufficient strength to break through that. That is called exploit. Now that you have gone inside, you need to be able to deliver something which will do your job. I will come with a clear example. How many of you know Microsoft word document exploits? Microsoft word has lot of vulnerabilities.

So, it can allow any hacker to execute arbitrary commands, ok. So, that is a vulnerability.

Someone exploited it. Basically, it can run any command that you say. Someone exploited it to run his own commands which are loaded from an internet server.

Then it became a exploit. What does a command do? Download a Remote Administration Tool and install it. This is the payload. Clear? So, in that, in this example the hacker identified a vulnerability in Microsoft office, weaponized it to create an exploit, so that when you double click it or run it, it downloads the code from a computer that he controls which will install a payload on your machine. Which is the deadliest part in all of this? The payload. Most of the anti viruses try to identify payloads, not the exploits.

Some of them these days also look for signatures of exploit. It is a different matter. But it is a rapidly changing thing. Clear so far? Everybody understands the concepts? Now, like I said payloads, how do they look like? They are pretty simple lower level software.

They give you very good control of the machine. They can be bought for 15, 20 dollars on dark web. There are many people who sell it. If your victim is not really cyber aware, you can make him install it randomly. Simply say, it is a flash update, new app to install, get bonus, Amazon is giving 200 rupees extra, Flipkart has giving 50 percent sale. I am sure all of you have received all those messages.

Those are all prompts to make you install Rats. We did Rat, means a remote administration tool. There was a genuine use of Rats like for example, Team viewer, Ammy admin. These are all genuine tools. People have inspired take inspiration from them and built their own tools.

So, that nobody can detect them. Correct? So, there are many open source tools also like Puppy Rat, Qrat. There are like huge markets where they sell access to a Rat, which cannot be detected by anti viruses. That market is dark web market. So, DarkComet, Atom Logger, all of them. They are sold license because anti virus is also changing every day.

So, the person who is making this Rat has to constantly update, so that it does not, which is why they charge you annual subscription. As long as you keep the annual subscription, your Rat will continue to be alive. Otherwise it will get caught. See the business model? Post Covid use of key loggers sky rockets.

I am sure this is the extent that we all expect, right. Nothing wrong about it. Suddenly lot of people who do not understand how to operate in cyberspace, have access to cyberspace. So, they all most of them, fell victims to this game. There is a huge market in India also.

Just have a look at how a command control panel looks. I will zoom it. Good, good, good. So, this is a special type of a Trojan or malware called a Stealer. It's job is to steal passwords.

Just see it briefly on the screen. So, the stealer name is Vidar, correct. So, what is it stealing? Passwords that you use to log into sites. So, who are the victims? Two victims on the screen. The first victim is from Brazil and second victim is from Lucknow. Based on the IPS, I mean based on the IP, it looks like the Reliance Jio customer probably.

Maybe a mobile guy or a desktop or a broadband guy, we do not know. So, what are the details that the stealer stole? Redbus.

in, grammarly.com, olacabs.com, kesco.co.in, freecharge.in domains are stolen. How did they steal it? Through which application they delivered it? Winrar archive.

zip data. How big is the file? 0.13 MB data, correct. Oh yeah, I am sorry, I just drive it little bit this side, yes. Yes, you can see it the date and time, command control information. You are selling it for who? All those details are here. These are the command control looks like, clear. Yeah, why the hundreds of supply sources like this on the dark web, hundreds, hundreds, hundreds.

Because like I said, it is a easy business, you make once, you can sell as many as you like and people will happily pay you on bitcoins and all that whatever type you like. So, there is a thriving business, it is a huge business on the dark web. If you traverse in the dark web, there are hundreds of forums where people try to sell this to you, cheaper price and all that, all that and you do not know you may be running it, you may become victim, that is also there, correct. And adding to this is constant updates of vulnerabilities which are discovered every day. Every day something or another is discovered and not everything is patched, correct.

Now let us look at one Trojan, so that you guys get a complete idea of how it looks like. So this is a Trojan called Qbot. Qbot basically is part of a first phase random emails, you know they send random emails hope for a target, collect it, put them into a botnet. Then think about how do you monetize the botnet, ok.

See the way it operates. Clearly see it. I will zoom in, zoom in, zoom in, zoom in, zoom in, I will zoom in. This is a phase 1. So, this uses what platform? Ok, I can call it ok. So, it uses an attachment with a zip file.

Why zip file? So, that the email scanners cannot scan. So, you download, you unzip the

file. So, the file that you have scanned which is a zip file and the file that you are running now on your machine are two different things. See the ingenuity, smartness, correct. So, when you open what happens there is a malicious XLSM file, which is in it.

When you open it, what happens? It will execute Macros. Here the vulnerabilities are Macros. Macros are designed by Microsoft to make your life easier, to automate lot of tasks. Now the attacker is exploiting it to do his tasks, on your machine. Clear? What happens to it next? It downloads the malicious DLL file separately, binary separately, there is first stage payload and from the first stage payload it loads the actual Trojan.

After that the, see the stages. Can you see the first level download, second level download, persistence? Now here ransomware and trojans, it depends on how the bot manager wants it to be. Collect some random documents, random emails and then sends it to the master, which is your command control. Now command control looks at sample documents that it received and realizes, oh my god this guy looks like a guy with lot of money.

Let us ransom him. I will place like a random fellow who does not have anything. Let him buy my botnet. I will make him just click random ads, get some advertisement money. You guys can see clearly now, how it all operates. I will show you some emails.

There is a real thing which we, compromised email address, real email. Hello please read this and confirm regards. See the zip file. Now if you receive an email like this from your boss what will you do? Yes sir, I will do sir. Correct? That is what they count on.

Now read this one, another trick, another trick. Please familiar yourself with the attached file and reply here, if you have any questions. Do not call me. Reply here only because if you call me, I will tell you I did not tell you.

Correct? This is how this world operates. Same document again here too. Yeah, now if you look at the malware you can see lot of things are hidden here. Can you see hidden, hidden, hidden, hidden, hidden, hidden? So there are many sheets in the excel, in the excel file which you cannot see. When you open the file it looks like this, enable content, what does it say here, Macros have been disabled. It will force you to enable it.

So it is a clever use of exploit plus social engineering. Background you can see. Sir it is a data pro that you are using. Data pro form.

Yes it is. It is not data pro you do not need data pro for this actually. Ok. But yeah data pro is this one. Yeah. This is data pro. Data pro is a debugger so that you can look at the source code to understand the malicious component more easily.

There are many other tools like Ghidra. Ghidra data pro. Ghidra is released by US intelligence, NSA. It is a good tool but nobody trusts it, but then it is a good tool. Yeah, now we have seen roughly some idea, So far any questions? Nothing now? Clear, everything is clear, super duper? Yeah now, let us look at we have talked about small, small actors. How do you define a cyber attack? Now we look at the serious players in this game.

The serious players are called APTs. APTs are people who run this as a serious business. They have their own motives. They could be government trying to compromise other governments or it could be a group of hackers who are in it to make a lot of money. Because building these softwares, finding bugs, exploiting, weaponizing, targeting is a very, very expensive business. It is not as cheap as it appears to people, correct. So it is basically an attempt to gain unauthorized access to a computer or a system or a network with intent to cause damage.

So broad difference APTs have, some other higher motives which is why they are called, they are advanced and they are persistent, they are after you, they are not going to give up so easily. They do not give up at all and they continue to be a threat. A regular hacker leaves you behind, goes after something else, but APTs do not go. So the most dangerous threats that we look at are advanced persistent threats like another one example of APT group is where India was developing vaccines during corona, all our healthcare companies were relentlessly targeted, to copy the vaccine source code, to copy the vaccine mixtures, formulations and all that. So that is an advanced attack and it is a persistent attack, they did not give up till they get what they want, clear.

Of course, lot of people have lot of motives, we will talk about some of them. The first motive steal data, this is also called as cyber espionage. Second one disrupt and third is destroy. So usually technically we look at cyber attacks in 3 Ds.

The first one is called disrupt. You basically irritate the functioning of any system. Next you degrade, I used to manage 100 customers simultaneously, I can only do 50 because you destroyed two of my servers or you are just doing worse on me, my bandwidth is getting wasted at you. Last one is, so these are the 3 Ds, correct. One recent example we had was the power grid of Mumbai, the Tata power's power grid suddenly came down, nobody had any idea why, I leave it to you to imagine, correct.

Just keep that thought with you. Let us broadly look at what type of attacks that we usually see. These are the types of attacks that we usually see, the top 15 attacks, I am sure all of you will understand something about these attacks, if you don't please ask me.

I have sorry, sorry. Distribution of malware, web based attacks, phishing attacks, web application attacks, spam, denial of service, identity theft, data breaches, insider threats botnets, physical manipulation, damage, theft and loss. How does that happen? Take a USB drive and put it, I will explain in couple of examples also, ransomware, espionage, crypto jacking. What is crypto jacking? Crypto jacking is when you take over other PCs or something to basically start mining for cryptocurrencies.

That is crypto mining, crypto jacking could also mean taking over your wallet directly, clear. These attacks everybody understands now, fair enough. Let us also look at one sample APT group to continue our discussion going back. So, SideCopy is an APT group which probably is affiliated with Pakistan. So, nowadays we see it with lot of Chinese help, naturally expected. So, their malware modules are constantly under development, continuously they evolve, but the code remains are very same, the actors are keeping track of detection, you know you can see that efforts they are trying to change their source code.

So, that no longer this antivirus detects that antivirus detects and they are also smart enough to fool others by trying to copy another probably Indian APT group, by copying that group's tools you want to mislead others. So, this also happens, now this is an application which Government of India developed to prevent people from accessing illegally email accounts of government officials. So, this group started a campaign distributing a malicious version of that application, by saying you seem to be hacked.

So, please download this application and use it henceforth. I will just put a screen on this. So, this is the actual application. So, they started using this similar copy of this application, correct. How do they do it? Here you see this one, I will go back.

Now you have seen this application, mail hyphen gov dot in, how many will notice it. Happily distributed this. So, this was an operation which they worked also.