Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

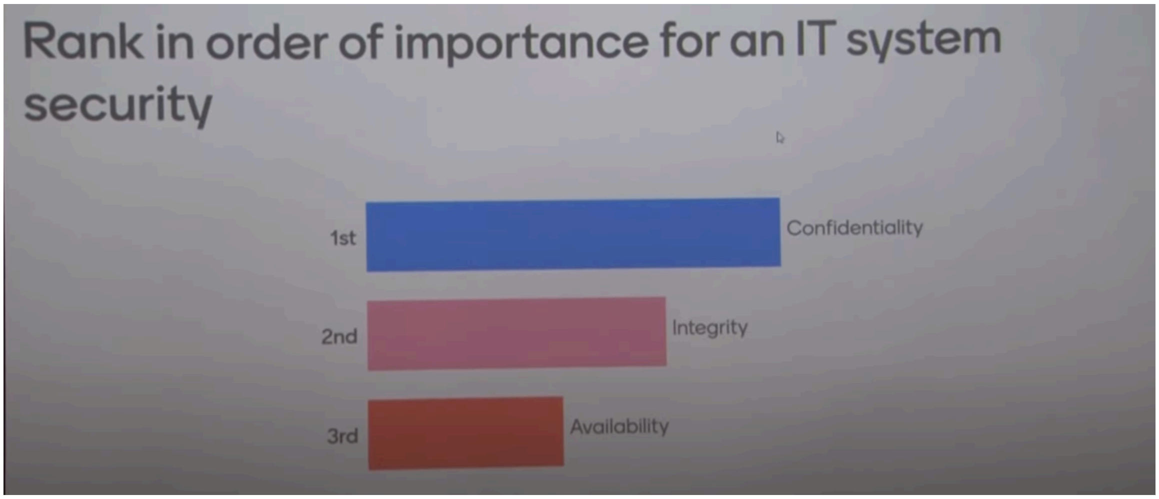
Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

Lecture 03

Understanding Cyber Kill Chain - Delivery, Exploitation and Installation

So today we are continuing with the Lockheed Martin cyber kill chain that we started yesterday. And we only could go through two of the seven stages, the reconnaissance and weaponization. And we'll talk about the next five stages hopefully today. But before that, again, we want to go to menti.com and try this. Okay, so you have the code today, 21312349.


Rank in order of importance for an IT system security

So this question is: rank in order of importance for IT system security. What is more important, confidentiality, integrity, and availability? So again, you can push on your screen to give importance, okay. Okay, so what we're seeing is that confidentiality that is data privacy is given more importance, data integrity that no unauthorized modification of data has happened is given the kind of second rank and availability that is if it is a system that is providing a service It should be available as the users need. So which means that if it is a web service, it should not be down more than so often.

If it is a service that you are using internally, for example, your email system, it should not be down more than so often. So that's the availability. Now the reason why I put this question here is last night I was reviewing a draft regulation for the power system in the country. And in that, the objectives of the regulation was written as confidentiality, integrity, and availability, and the non-repudiation. That is, if somebody has done some modification or done some excess, they should not be able to say that it was not me.

So that's non-repudiation. So when I looked at that, I said, well, We are talking about power system operators. We are talking about a generation company that generates electricity either through thermal energy or through other kinds of energy or solar or maybe nuclear or hydro. Or there are transmission companies which carry power in very high voltage transmission lines from the generation location to the distribution locations. Or there are distribution companies like Kesco in Kanpur or UPPCL in Lucknow, etc. who are actually getting power from generation companies through transmission companies and then giving that power to your houses or local factories and so on. Now these companies, if you say that the goal of cybersecurity measures in these companies is confidentiality, integrity, availability, and non-repudiation, doesn't mean anything, right? So the goal of a power system company is actually to provide something to their customers. For example, a generation company's goal is to provide generated electricity to the customers. In this case the customers are actually the distribution companies and distribution companies the transmission companies are delivering that electricity as and when needed to the distribution companies and distribution companies are delivering electricity to the customers, end customers. And they have a certain service level agreement which is based on, some of them are based on actual regulation. Like you have to, in India you cannot give 50 hertz power.

You have to give India at 50 hertz. I think the US is 60 hertz. So you have to have a certain frequency. You have to have a certain voltage level. You have to have a certain quality of power.

So you cannot have voltage dropping all the time. In rural places, sometimes there are distribution companies where the power distribution actually is pretty bad quality. You have the bulbs flickering and all kinds of low voltage, so this kind of stuff. But that is not what the customers expect. So if you ask me what the goals of cybersecurity rules or regulations are for such companies, I would not say confidentiality, integrity, availability, or non-repudiation.

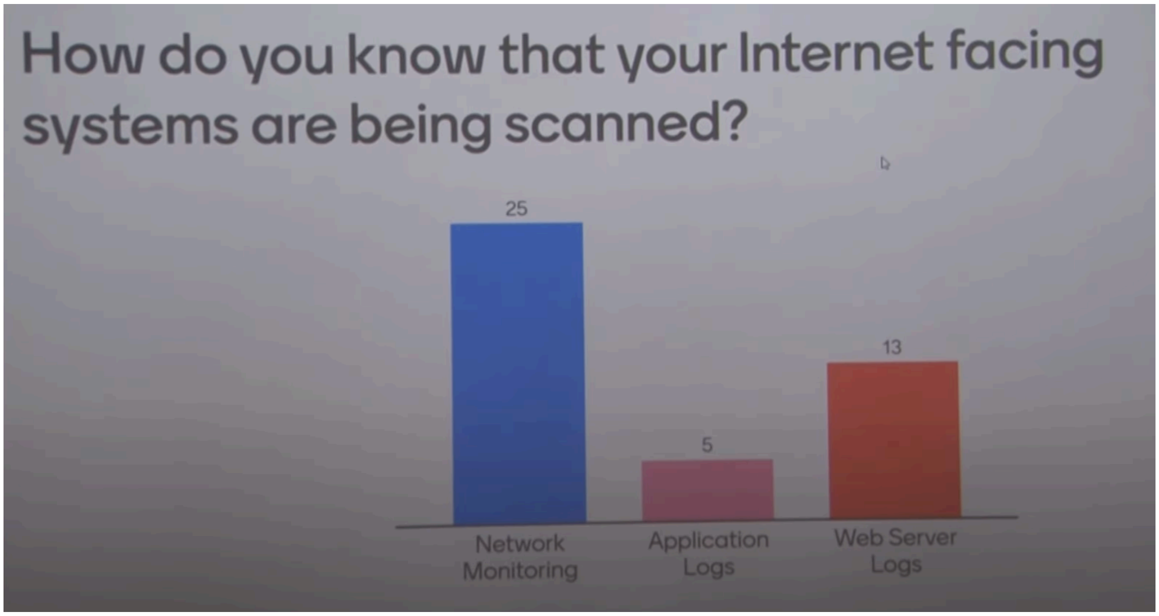
I'll say that I should be able to withstand cyber attacks, and still provide these services as promised to my customers, right? So whatever is the level, a service level agreement or whatever is the regulation, like, you know, what is the frequency level? Frequency cannot, like, exactly, frequency may not be exactly 50 hertz, but it cannot go more than, you know, 0.304 hertz. The excursion cannot be too long because that will basically disturb the entire grid, right? And then I should also make sure that whatever disturbance happens due to a cyber attack on me should not cascade to my customers or the other interconnected components. So that should be the objective. Now to fulfill these objectives, I may have to make sure that I maintain the integrity of the information that flows through my control systems.

I should have my control system available, that is the control like generator control or whatever control is being used to make sure that the electricity is generated at the right frequency, right voltage, the voltage is maintained through the transmission system, there is no loss, power loss through the transmission system, all that control. has to be protected from cyber attackers to change the information that flows from sensors to the controllers and controllers to the actuators. So putting this confidentiality, integrity, availability as my goal of cybersecurity rules and regulations make no sense. So it should always be based on what is my business. So if I say, why should I do the cybersecurity of IIT Kanpur, right? So if I say because I want to maintain confidentiality, integrity, availability, then the question will come of what, right? Not everything has to be confidential.

There is a lot of information that is not confidential. Not everything's integrity change will affect us. Not necessarily that everything has to be available 100% of the time. So I have to say what is my business? and what is my service and what quality of service I have promised to my customers. And my goal would be to maintain that functionality and quality performance when a cyber attack happens.

And to do that, I may have to do something about protecting certain databases, protecting certain services, protecting some data that moves through the network from servers to clients or server to server, network devices to servers, et cetera. And I should have the availability based on what I have promised to my customers. If I have promised that 99.9999% of the time this service should be on, then I have to do that irrespective of how I do it, like whether it's an availability part of the system or it's the confidentiality or the integrity part of the system. So I think that this is very important to understand because many times when you ask somebody, What is cybersecurity? They say that **cybersecurity is the ability to maintain confidentiality, integrity, availability, and non-repudiation.**

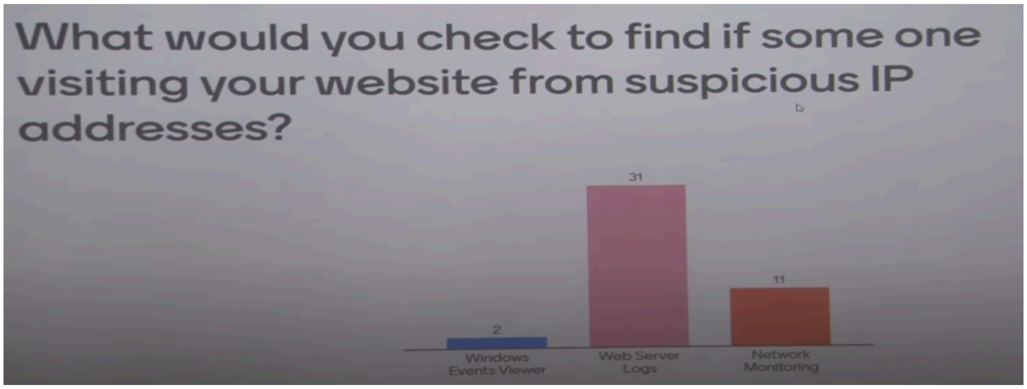
That's a common definition of cybersecurity. But when it comes to practical cybersecurity, It's not by saying these things make very little sense without knowing what services are you offering and what performance of that service you have promised and how to maintain that promise without being affected by cyber attack. So all your efforts, using firewalls, using antivirus, using endpoint security, using network monitoring, using strong authentication, everything will be in service to what you have promised as service quality and service availability to others, right? So that's why I put this question just to see.


How do you know that your Internet facing systems are being scanned?

Now the second question is, how do you know that your internet-facing systems, like your web server, maybe your email server, FTP server, or any web application that you are running, how do you know that your internet-facing systems are being scanned by sending packets to it and looking at the response to those packets and making inference from the responses? Okay, so remember that not every internet facing system is web service, right? You may have an SSH service running which is internet facing. Your VPN might be running.

You may have a FTP running. You may have many other services that may be running. A web service is one of them. So web server logs will only give you things that happen to the server web servers or attempts to connect to the web server or attempt to send HTTP messages to the web servers. That's what you will get from the web server logs.

So if somebody's sending TCP SYN packets or somebody's sending PING, you won't get that in the web server, right? So that will only be visible if you have network monitoring. So if your network monitoring will give you that kind of information.


What would you check to find if some one visiting your website from suspicious IP addresses?

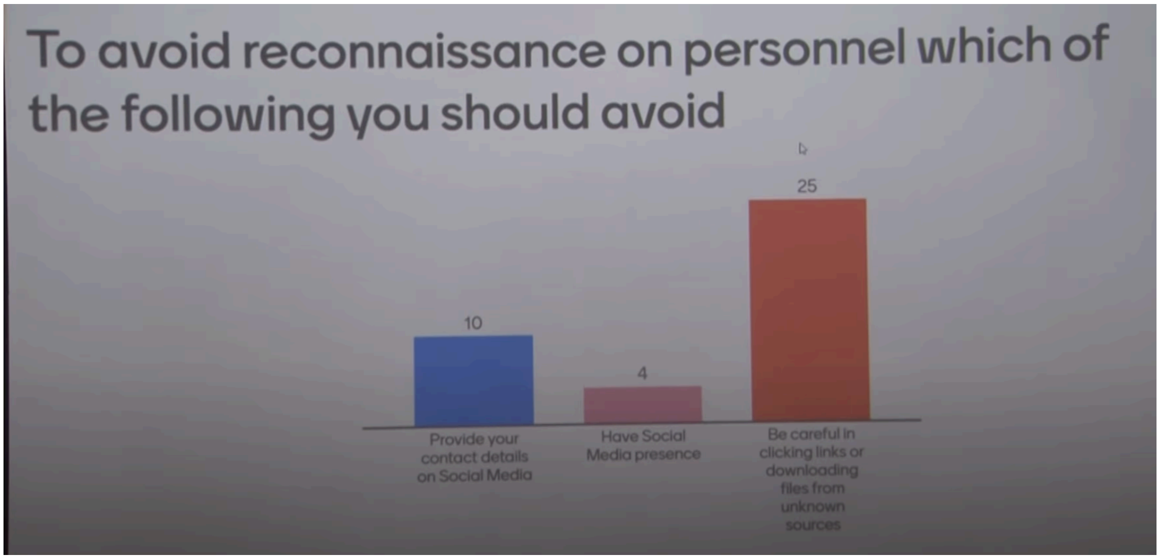
Okay, so next one, what would you check to find if someone is visiting your website from suspicious IP addresses? Okay, so how do you know whether somebody is visiting your website? Well, they will certainly make TCP connections to port 80 or port 443, right? But you do not have to necessarily do network level information. In your web server log, you will get a GET request, right? HTTP GET request. So from the HTTP GET request, you can get that information, right? So you do not necessarily, you can get the information from network monitoring as well, but you do not necessarily have to go that far.

So depending on what you are looking for, you have different logs. And network monitoring is actually, of course, we should have network monitoring for every infrastructure, but if you cannot afford network monitoring, because network monitoring means that you have to actually have a pretty fast you know, packet capture because network monitoring basically mirrors the port through which the network traffic comes and then sends that data to a system where you actually process the packets and get intelligence out of it, like where the packet is coming from. You may sometimes have to coalesce a certain number of packets to actually see what it is. It may be a file, it may be malware and things like that, which is rather expensive. So, if you cannot afford network monitoring for this particular problem statement that I want to see who all are connecting to my website, web server lock should suffice, right? But network monitoring will also give you that information and more information.

Yes? So, well, that depends. So, for example, there is an abuse DB database. that you can always check an IP against. See whether that IP is already listed as malicious. There could be other threat analysts who can actually collect their own set of IP addresses which they have seen in the past doing certain activities.

You could also see whether, like if the IP is not VPN based or Tor based, then it could also show you the country by going to WHOIS database or IP location database so you can find whether it's coming from a country where you are not expecting traffic from. So suspicious is actually a relative term right, what is suspicious to me may not be suspicious to you right so but every company has their own threat intelligence to figure out what they will count as suspicious and what they will ignore. But by ignoring, they might make a mistake, but there is only so much information they have. So that is the way it is. So you don't want to be doxxed.

You know the term doxxed? So when somebody is upset with you, they put up your home address, your personal mobile number, maybe your personal email, et cetera, et cetera, your location on social media or internet so that other people can go and bother you, right? So that is called doxxing, right? Now, most of the time, by going to social media, we dox ourselves, right? If you go to my LinkedIn or Facebook page And if you really want to know a lot of things about my whereabouts and where I'm going and all that stuff, you can figure a lot. So the question is, now as yesterday we said that the reconnaissance, one way of doing reconnaissance is to find an employee or user inside the organization. and use some kind of this phishing email or phishing message on their WhatsApp, et cetera, to actually hook them, and then you do get into the foothold into the system. So if you don't want that to happen, if you have this issue how do you avoid this? Now, I have three choices.



To avoid reconnaissance on personnel which of the following you should avoid

Provide your contact details. You should not provide your contact details on social media. or should not have social media presence. And the third is be aware and do not click on links or download pictures, et cetera, from unknown senders. Now, so cybersecurity is always about a trade-off, trade-off between usability and security, right? Sometimes when we make things very secure, for example, two-factor authentication, We actually make it very difficult for many users. Some users are okay with two-factor, very easy for them.

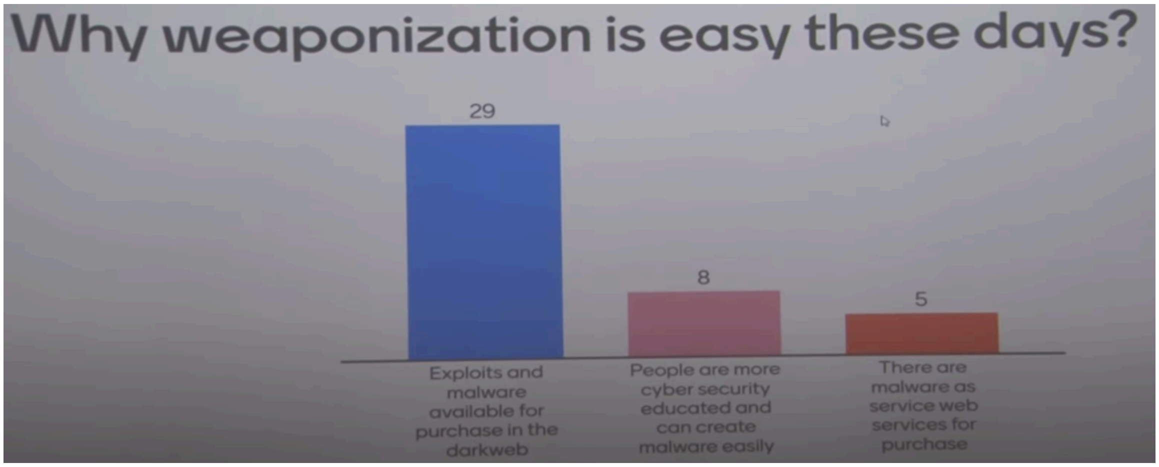
For some people, it may be difficult. So usability versus security. So you have to figure out the risk versus benefit. So if you keep the two-factor authentication off, then you are taking a lot of risk. Now if your system that you are trying to protect by having two-factor authentication does not have too much impact on you, even if it gets compromised, then you can get rid of two-factor authentication and take the risk.

So every organization or every individual has an acceptable risk. So risk is never zero. So anything we do on the digital realm has risk. The question is how much risk can you tolerate? So if you can tolerate a risk, suppose you have a second phone, and that phone you do not do banking or any such things, then you can take a lot of risk on that phone. But the phone on which you are doing your internet banking, UPI, et cetera, you will always have a screen lock and all that stuff because you want to have As a trade-off between usability and security, you will have security on that one because the risk is higher there.

The other phone that you only use for video games or something, you may actually take more risk. So the risk of being compromised versus the usability is always a trade-off. So in this case, for example, most people would like to be on social media, have connections, either in LinkedIn kind of connections or the social Facebook, Instagram kind of connections, whatever, most people would like that. So their best option is to be extremely careful because be prepared to be doxxed on those platforms and then you will get a lot of spam and a lot of phishing emails or phishing messages.

So you have to be extremely careful. So this is what is called risk mitigation by putting in controls. So we cannot always get rid of the risk. So we mitigate the risk by putting in controls. And controls, often people think that controls means firewalls and endpoint security, et cetera. Controls could also be a methodical habit or process, a process that everybody has to go through.

So this is a control. So the one that you have, 27 of you have chosen, this is actually a risk mitigation by exerting a control. So by not being on social media, that is another type of control, but there maybe your benefit is too low. The trade-off is too much, right? If you are not at all on social media, then your chances of getting doxxed reduces drastically. So that's a good control, but that control may not be good enough as a trade-off. So as a trade-off, it is better to have a control that more or less will give you the chance of avoiding any kind of compromise. But for that you have to have some kind of control of your own behavior, right? So all these things will come later when we talk about risks and then how to mitigate risk with controls, some of the controls are technical controls and some of the controls are process level controls. So this is an example of a process level control. Do not trust any email without doing due validation.



Why weaponization is easy these days?

Now the last question I have for today is why is it easy to weaponize these days? If you find a vulnerability, anybody, any person not even having any education in cybersecurity or computer science can do weaponization. Okay, so those who are choosing that people are more cybersecurity educated and easily write malware, I wouldn't say that, right? Because writing malware is like after, don't think that after finishing this class, you will be writing malware.

You won't be able to write malware by doing this class or even doing the other classes in cybersecurity. So we are not teaching. malware design in this institute. But it is easy to learn if you want to learn.

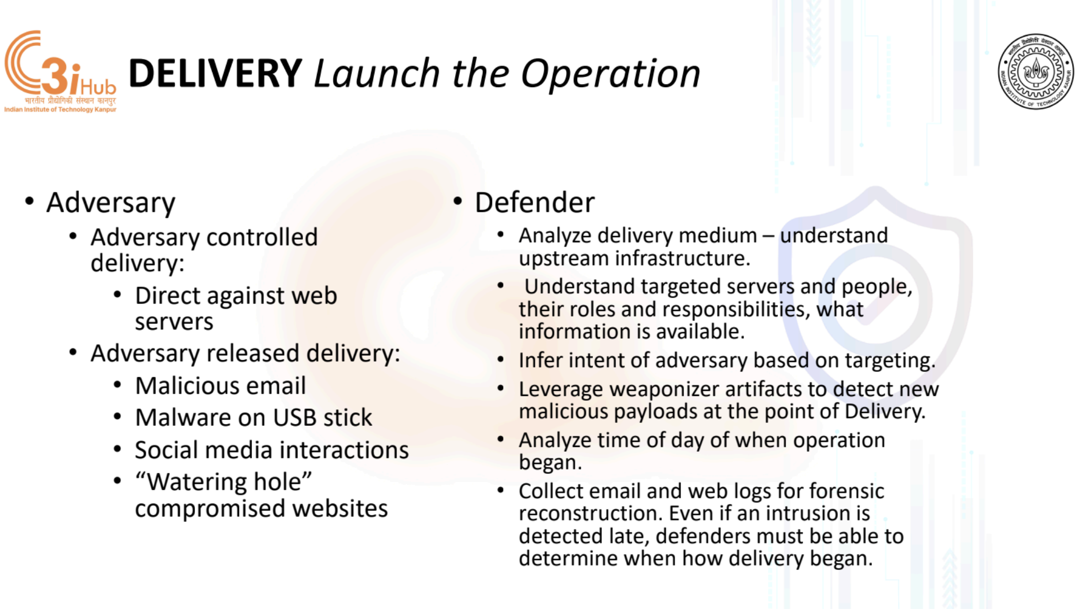
There is a lot of material on the web. So that's not the issue. But that's not the overwhelming reason. Maybe in some of the cases, people are writing their own malware. But in most cases, they're purchasing exploits and malware on the dark web. And the third one, which got very little support, is also a case, right? So ransomware as a service is very common.

So you actually go and tell a ransomware service platform that here are the IP addresses, and here I want the ransomware to be used there to exploit, and the money is kind of divided, right? So whatever money the attackers get, some part goes to the platform vendor, right? So that is also common. So weaponization has become easy. Now what is the implication of that to us? We are good people, right? We are the defenders, right? And we are talking about attackers. So since it's easier for attackers, the job for us gets harder, right? And also the risk goes up, right? So risk, as we'll see later, the risk is based on threats and vulnerabilities and the impact. So the threat here is increasing, right? So the threats are easy to come up with and threats are easy and vulnerabilities are often not patched.

So together, it's a deadly combination for us and therefore we have to work harder for security. Okay, so now going back to the main lecture, So reconnaissance we already talked about. That is how they find how to get into your system. And if you are a defender, you always have to make sure you continue to watch the logs, watch the network and so on to see efforts of reconnaissance. And that will keep you, you know, raise your posture, your cyber security posture.

When you see a lot of reconnaissance activity, then you know that it's time to up the game for defense. So, for weaponization we talked about how they figure out how to, what malware to use or whether to use phishing or whether to directly exploit an internet facing service and so on. And as a defender, if a weaponization happens and you get affected, you have to have an ability to do forensic afterwards so that you are prepared for next time, right? So what is written on the defender side is after actually, the weapon that was created has been detonated on you, and you're trying to learn from it by doing cyber forensics for the next time. You don't necessarily say, well, this did not affect me too much. Only two unimportant machines got affected, so I just cleaned them up.

I will rebuild the system or whatever, and then I am happy, right? No, you have to do very detailed forensics to figure out how this happened. So you have to also do a forensic analysis of the root cause. What path was taken by the attacker, whether it was by exploiting a service, a vulnerability in an internet-facing service, or is it through phishing, or some kind of social engineering, or somebody brought in some kind of USB stick and plugged it in by not knowing, or knowingly, and launched a malware into the system. All this stuff has to be analyzed and used as some kind of preparation for bettering your cybersecurity posture. Okay, so, and also this malware's metadata and analysis can tell a lot about it.



DELIVERY *Launch the Operation*

- Adversary
  - Adversary controlled delivery:
    - Direct against web servers
  - Adversary released delivery:
    - Malicious email
    - Malware on USB stick
    - Social media interactions
    - “Watering hole” compromised websites
- Defender
  - Analyze delivery medium – understand upstream infrastructure.
  - Understand targeted servers and people, their roles and responsibilities, what information is available.
  - Infer intent of adversary based on targeting.
  - Leverage weaponizer artifacts to detect new malicious payloads at the point of Delivery.
  - Analyze time of day of when operation began.
  - Collect email and web logs for forensic reconstruction. Even if an intrusion is detected late, defenders must be able to determine when how delivery began.

You can also tell who might be behind it by looking at the time of the day when the actual launch of the attack happened, because that will tell you which geographical region the attack might be from, right? So this kind of information has to be collected if you are affected. So the third stage is delivery. So you have figured out how to get in, you have figured out what payload to deliver, but you have to now deliver the payload, either by exploiting one of the vulnerable services or by doing some kind of social engineering like phishing email or phishing messages and so on. There are also other kinds of tricks like watering hole attacks. So what you do is that you create some kind of a buzz in social media or in some other forum.

There are also Telegram channels or WhatsApp channels, chat rooms, where you say that, oh, this is a very good website, you are getting a big discount there. So a lot of people go there. and everybody gets affected. So this is called a watering hole attack. So you might have seen, many of you might have seen that sometimes you will see on social media some kind of a post that kind of says that Mukesh Ambani doesn't want you to know how he is going to make money and then picture and stuff gives him Bitcoin or something, right? So many people will think that really Mukesh Ambani said something or Amitabh Bachchan or somebody and then you go in there and you think that this is a new site, it will tell you how to make money and all that stuff and then you get affected, right? So this kind of watering hole is very common.

So you have to, once that happens, as a defender, you have to figure out what was the delivery medium, how it was delivered, and then you also have to see who were targeted. For example, the Ukraine power grid attack that happened in 2015, they actually did phishing of high-level executives And the high-level executives, one of the high-level executives of the company, distribution company, Ukraine's distribution company in Kyiv, clicked on the link and then got affected by malware. Then the malware actually did a lateral movement into other machines and found a bunch of VPN credentials. These VPN credentials are sent back to its command and control servers. And using that VPN, they got into the actual power system operations network.

And then they actually not only changed the power system operational network, at the same time, they actually disabled the UPS. And then turned off all the computers. So even UPS not being there, It was actually, you know, you could not have any power. It was turned off right away.

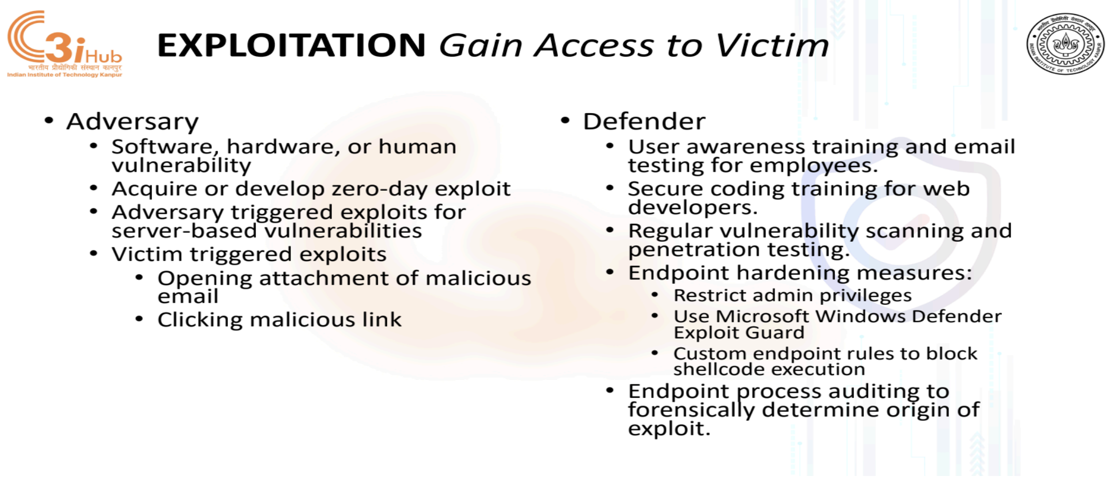
And that's how the operation happened. So who is targeted is important. Like is it random targeting or is it very specific targeting? Is it a spear phishing or regular phishing, right? So that you have to know. Then from these things, you have to understand the intent of the adversary. Why is the intent of the adversary very important? Because if it is a script kiddie who is just playing around, it's less of a problem. If it is a hacktivist, then it's a little bigger problem, but it may not be as big a problem if it was a nation state, you know, advanced persistent threat group.

They have deep resources, they have deep knowledge, and that means that you are at a big problem, right? So figuring out the intent of the adversary and who the adversary is by looking at the time of the day, et cetera, is very relevant and important. And then you collect information from the forensics. Now, if you look at this paper, I already posted the paper also. If you look at this paper, they are not talking about proactive defense, they are talking about after the incident happened, what I should do as a defender to prepare for the next time, right? So of course, you can also learn from other organizations which got attacked, not you, and you can get all this information on how that happened, and then accordingly also raise your cybersecurity posture. So it does not necessarily have to happen to you to learn how to defend.

So in the US, they have these things called information sharing and analysis centers, ISACs. So for every sector, they have an ISAC. For example, they have an ISAC for finance, BFSI sector, banking and finance sector. They have an ISAC for ICS, industrial control systems.

They have an ISAC for the oil and gas sector and so on. So ISAC is information sharing, so all the organizations who are members of the ISAC, if an attack happens on them, they share that information about root cause, forensic information and so on, so that all the other organizations that are part of that ISAC also learn from there, right? Unfortunately, in India, the ISACs are not active. There are some ISACs, but they're not very active because organizations are very, very reticent about not sharing information. In fact, in India, the main problem is that when an attack happens to a company, they hide it. And by hiding that, they are not helping the other banks. If a bank gets attacked, the other banks should know what happened, how it happened, and so on.

But very little information comes out. But this sharing is very important in order for us to actually learn from the adjacent organizations. So now we are in the third stage, right? So reconnaissance, weaponization, now delivery. So the attacker has now delivered the first payload through phishing or whatever. So now, The delivery of the payload does not necessarily mean that the attack will take place because somebody has to click on the link or somebody has to turn on the malware or launch the malware by double-clicking on it or something. Unfortunately, this is not fully true anymore because there are also something called zero-click attacks.



EXPLOITATION *Gain Access to Victim*

- Adversary
  - Software, hardware, or human vulnerability
  - Acquire or develop zero-day exploit
  - Adversary triggered exploits for server-based vulnerabilities
  - Victim triggered exploits
    - Opening attachment of malicious email
    - Clicking malicious link
- Defender
  - User awareness training and email testing for employees.
  - Secure coding training for web developers.
  - Regular vulnerability scanning and penetration testing.
  - Endpoint hardening measures:
    - Restrict admin privileges
    - Use Microsoft Windows Defender Exploit Guard
    - Custom endpoint rules to block shellcode execution
  - Endpoint process auditing to forensically determine origin of exploit.

So I don't know if you've heard of Pegasus. Pegasus was a malware, very infamous malware from an Israeli company, NSO. So they figure out, they put a lot of money into researching, figuring out exploits, especially in mobile systems, mobile like iOS or Android, or some of the applications that come with this Android or iOS and try to find out a vulnerability that nobody else has found yet. So these are called zero-day vulnerabilities. Because a white hat hacker or a responsible hacker will do a responsible disclosure. As soon as they figure out there is an exploit, they will go to the company and say that look, here is an exploit, here is a vulnerability you have and it can be exploited this way.

Please fix it. The companies usually, especially companies which have a large user base like WhatsApp or iOS or Android, et cetera, take this very seriously. They immediately test for it and then try to fix it. And when they fix it, they dispatch an update. So you always get an update from iOS or Android, et cetera. if the hackers do not even tell the company, and the company also continues to do research finding vulnerabilities, but maybe some vulnerability they also missed.

So in that case, this becomes a zero-day vulnerability. Zero-day vulnerabilities are then divided into two. One is that if I deliver an exploit of that vulnerability to your machine, You may have to double-click or something. Users may have to take an action before it can be launched. And the other division is what we call zero-click vulnerability.

That is, users do not have to necessarily do anything. As soon as the exploit comes in, it will execute. So these zero-day, zero-click vulnerabilities are the way the NSO, the Pegasus system works. They don't rely on the user to be fooled. Now these are the most virulent types of attacks because the user has no clue, right? So you may be very careful about phishing, not clicking on unknown links, not clicking on unknown files and so on, but zero-day, zero-click, all bets are off. So that's what Pegasus used, for example, initially in 2019, they found a zero-day, zero-click bug in the video call feature of WhatsApp.

And the latest one that was very famous in 2021, was FaceTime in the iOS exploit. Now there is a marketplace for these vulnerabilities. So there are websites where you can go and get even up to $1 million for giving a vulnerability report that nobody knows about yet. It's a zero-day vulnerability, and if it is zero-click, you get up to a billion dollars, right? So there is also a black market for that on the dark web. So there is a book by a New York Times cybersecurity journalist called, This is **How the World Will End.**

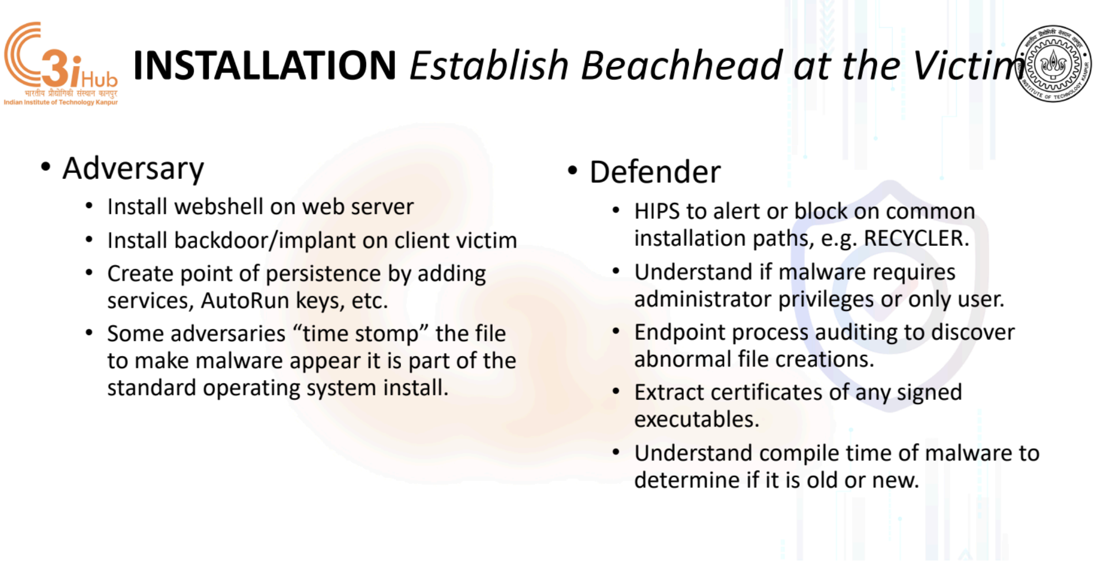
She predicts that if we do not control this zero-day marketplace, black marketplace, then countries will basically destroy each other's nuclear facilities and other things and eventually it will go out of control, right? So once a nuclear thing starts, Others will retaliate and that's a little bit of a pessimistic book, but it's a very good book if you want to know more about this dark market of zero-day vulnerabilities. So if it is not a zero-day vulnerability, then you expect the, somehow you have to lure the victim to actually click on the links or it may be a vulnerability that can be a remote code execution vulnerability or something through which you can actually make things start running on the system. So in this case, after delivery, we are now in the exploitation stage. This is stage four. So how do I stop exploitation? So let's assume that reconnaissance was done and somebody was targeted and the targeted person actually was fooled into clicking on something and then the actual weaponization and delivery happened.

Now I have to figure out how to stop the exploitation, right? So to stop the exploitation, of course, if it is not a zero click vulnerability, then user awareness goes a long way, right? So knowing what to do and what not to do is a very important one. And that's why we often do these phishing drills and other things to make sure that the users are used to being cautious. We also can do like most of these payloads will only do something if there is a vulnerability in some system, like it may be an application, it could be the operating system, it could be the network stack, it could be the web server, and all that. So secure coding, et cetera, are important to make sure that vulnerabilities are avoided as much as possible. We have to do regular vulnerability scan and patching so that we can patch these vulnerabilities.

There is also endpoint hardening. That is, you know, so when we go to MITRE DEFEND discussions, we'll see what hardening is all about. But when we basically take a system and make a lot of configuration changes, make sure all the operating systems and applications are up to date, We make sure that all the unnecessary ports are closed. We make sure that there are regular users and not administrative users, only there is a very responsible way of using the administrator's account. These are called hardening.

It's about making the system hardened against any kind of attacks. Doesn't mean that you will avoid all attacks, but many attacks can be avoided by hardening your system. So, hardening is another important thing to do. And then continuously monitor the endpoints, that is having a visibility into what's running on the system, whether new processes are being spawned, whether some file system is being changed, whether, suspicious IP is being contacted by the machine, all this information can be found by putting an agent on the device and have that agent report to the Security Operations Center what is happening at the endpoint. So all these things have to be done in order to avoid exploitation. So remember that the claim of Lockheed Martin is that I am telling you that these are the seven steps that all attackers have to take. If you can stop it in the first stage, good.

If you cannot stop it in stage one, try to stop in stage two. If not, then try to stop in stage three, that is at the delivery phase. If you cannot stop in the delivery phase, try to stop in the exploitation phase. So this is the way they think, that I have to cut the chain at some point to reduce the possibility of full-fledged damage, right? So that's the idea.



INSTALLATION *Establish Beachhead at the Victim*

- Adversary
  - Install webshell on web server
  - Install backdoor/implant on client victim
  - Create point of persistence by adding services, AutoRun keys, etc.
  - Some adversaries "time stomp" the file to make malware appear it is part of the standard operating system install.
- Defender
  - HIPS to alert or block on common installation paths, e.g. RECYCLER.
  - Understand if malware requires administrator privileges or only user.
  - Endpoint process auditing to discover abnormal file creations.
  - Extract certificates of any signed executables.
  - Understand compile time of malware to determine if it is old or new.

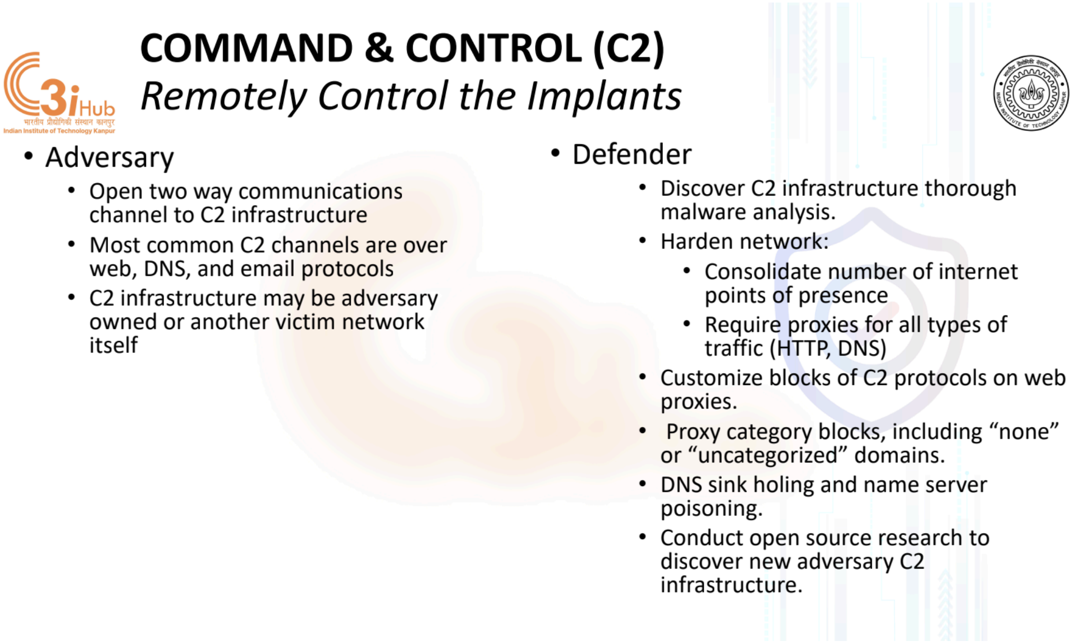
So the next one is installation. So the problem is that if you just have a payload that executes once, and then the user logs out or the user shuts down the machine and everything goes away, then that's not good for you as an attacker. So the attacker tries to do what is called persistence. So they are calling the installation here. So they remain persistent in the machine. So they can actually write their binaries into the startup folder in Windows so that next time Windows starts, the process will start or they will try to inject themselves into an important service. So the code will execute when that service turns on. So they can also put a web shell. So they can actually go to your web application and write down the address of the web shell and they can actually get a shell into your machine and then start doing their manual exploitation.

So there are various kinds of things they can do to create persistence. So the persistence or being installed into the system is one of their important objectives, right? To stay persistent, remain in the system so that they can provide a backdoor. They might be opening a port and the attacker from the far will use that as a service to connect to your system, right? So they can do various things or you can get a web shell and that web shell would actually allow you to have a shell access And if the person is running the web application as root, which many people by mistake do, then you will get a root shell, which means you will have full administrative control on that machine. So here, the defender has to actually continue to do what they're calling HIPS, a host intrusion prevention system. Nowadays, people call it endpoint detection or endpoint protection system. And then you have to understand if the malware requires administrative privileges or only the user, depending on what the malware wants to do.

But in most cases, they try to gain administrative privilege, and that is what is called a privilege escalation. So we have to keep auditing and monitoring the endpoints. If there are signed executables, we have to figure out the certificates.

And you have to understand when the malware was created and so on. Now, this certificate thing. So nowadays, no operating system wants to execute a binary which has not been certified with a digital certificate. That is, you take the hash of the binary and do encryption using the private key of the company, like for Microsoft, right? So no Microsoft binary comes without a certificate.

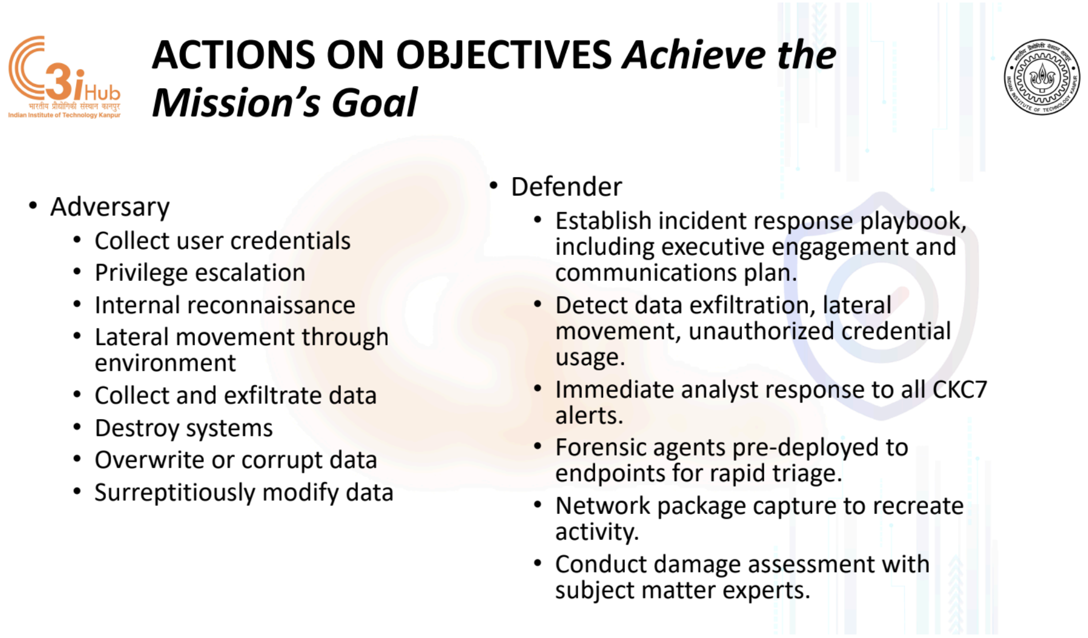
And the Microsoft operating system automatically knows the, I mean, it already knows the public key of Microsoft, signing public key, so it will check whether the binary has been signed and that gives them confidence that this is actually a patch from Microsoft and I can execute it safely. But things are not that simple anymore because the certificates get stolen, right? So in the case of Stuxnet, certificates of legitimate vendors were used. So therefore, this process doesn't necessarily always work if the certificate is stolen. Okay, so it's time, so we'll come to this installation stage tomorrow, and then two more stages.



COMMAND & CONTROL (C2)

Remotely Control the Implants

- Adversary
  - Open two way communications channel to C2 infrastructure
  - Most common C2 channels are over web, DNS, and email protocols
  - C2 infrastructure may be adversary owned or another victim network itself
- Defender
  - Discover C2 infrastructure thorough malware analysis.
  - Harden network:
    - Consolidate number of internet points of presence
    - Require proxies for all types of traffic (HTTP, DNS)
  - Customize blocks of C2 protocols on web proxies.
  - Proxy category blocks, including “none” or “uncategorized” domains.
  - DNS sink holing and name server poisoning.
  - Conduct open source research to discover new adversary C2 infrastructure.



ACTIONS ON OBJECTIVES *Achieve the Mission's Goal*

- Adversary
  - Collect user credentials
  - Privilege escalation
  - Internal reconnaissance
  - Lateral movement through environment
  - Collect and exfiltrate data
  - Destroy systems
  - Overwrite or corrupt data
  - Surreptitiously modify data

- Defender
  - Establish incident response playbook, including executive engagement and communications plan.
  - Detect data exfiltration, lateral movement, unauthorized credential usage.
  - Immediate analyst response to all CKC7 alerts.
  - Forensic agents pre-deployed to endpoints for rapid triage.
  - Network package capture to recreate activity.
  - Conduct damage assessment with subject matter experts.

We'll command and control, and the actions on objectives, that is the main impact. And then we'll, hopefully by tomorrow, finish Lockheed Martin, this CKC, Cyber Kill Chain.