Advanced Persistent Threat

Welcome back. In this video, I'm going to introduce the concept of advanced persistent threat, or APT. This is very likely a buzzword that you might have heard within cybersecurity, and for very good reason. It's something which concerns many organisations.

In this video, we'll break it down into four components--

what is it, why is it so concerning, how does it happen, and what can we do about it. To start off with what it is, APT stands for advanced persistent threat. This is effectively well-funded, large, long-term attacks or campaigns against a particular organisation.

This could be an organisation within a government, or it could be a large conglomerate or other business. The advanced side of it doesn't necessarily relate specifically to the techniques used. Indeed, many of the entry points into the system or network are often through the end user. They exploit social engineering leaks often to gain access to the system.

Whilst there's not necessarily one agreed to definition of an advanced persistent threat, many of the definitions cover these common points. They are long term. So it's not a case of attacking the system once, gaining access, and gaining the data or whatever the attacker intends to do, and then leaving. They intend on maintaining access to that system.

And so campaigns can last for several years. As mentioned before, they're all well funded and they're often considered to be state actors. That is, for example, the American or Russian government or the Chinese government, or any government indeed could be funding cyber attacks such as these. They are very well organised, and they often involve a lot of research. So there's a significant investment in terms of time and resource in order to attack a system.

So why is this so concerning for organisations and governments? Well, the reality is that with this kind of attack, it's very, very stealthy. That is, they cover their tracks. Where attacks such as ransomware make it very clear to the end user that the system has been penetrated and

attacked, with an APT, they are trying to disguise that as much as possible. Effectively, any traffic going into the network is made to look like legitimate traffic.

So much so, that any of the tools or techniques which we might use traditionally to identify attacks--

such as firewalls or intrusion detection prevention systems or security information and event management systems--

find it incredibly difficult to identify such an attack. The long term nature of such attacks combined with this stealthiness means that it could be months before an organisation even identifies that such an attack has taken place. This means that damage is very likely to already have occurred. So how does this happen, what are the stages within an APT attack or campaign? Well, first of all, we have to do reconnaissance.

This stage involves finding as much as possible about the system itself, how it functions, the employees, any particular points of entry. The kind of activities here might be exploring publicly available websites, trying to identify members of staff who may be vulnerable for social engineering, or a variety of other information gathering processes. The next stage is initial compromise.

This is effectively the point where the attackers are trying to gain a foothold within the system. This could be, for example, through a phishing email, where a user is sent a dodgy email, they click the link, and as a result, they provide information to the attacker which could allow entry to the network. Other options might be types of malware or perhaps even exploiting network deficiencies or poor password management by end users.

At this stage, they'll also want to try and set up some form of outbound communication. The idea is that they're trying to gain access to data or other assets within the system, and they want to be able to send that back to themselves. The next step is to maintain access. At this point, they might set up software which allows them to bypass any of the security mechanisms which the system might have in place.

Effectively, since this is a long-term campaign, they want to ensure that they continue to have access to that system. The next step is lateral movement. It's at this point that they're trying to expand their foothold within the system. So they might try to compromise another host, get onto a related network, or other such activities.

They could also be trying to locate data for extraction--

which leads us into the next step, data exfiltration. It's at this point they may wish to start sending data back to their own devices. This is done through the outbound traffic set-up

which we completed in an earlier stage. And the final stage is to cover their tracks.

They want to ensure that if someone is looking over, for example, log data, that they are unable to identify that such an attack has taken place. So what can we do to try to mitigate the potential successful APT campaign. One of the things that we can do is to shift mentality. Traditional security often focuses on what can be referred to as perimeter security.

That is, it's very focused on incoming traffic to the network from external sources. So for example, using firewalls, we might block particular IP addresses, and so forth. However, with this kind of attack, we are also starting to look at internal traffic which is going out of the network. So it's that little bit of a shift in focus from stopping everything from coming in to also looking at data which may be coming out of the network.

This isn't to say that you stop using things like firewalls, looking at inbound traffic, but instead to just making sure that you're more encompassing of looking at that internal network as well as its perimeter. It's also important to maintain our usual mitigation techniques--

so ensuring that we use the principle of least privilege, where only people who require access to particular functionality are given that sort of access, having appropriate patch management, so ensuring that any vulnerabilities within the software or operating systems that you use are appropriately patched. Another option is to start looking at behaviour.

Often we use the mechanism of considering activities as good or bad. So in firewalls, for example, looking at inbound traffic that could look legitimate but by the time it gets into the network, it starts to perform bad behaviour. We'd want to make sure that we monitor this kind of activity and highlight it where possible. And as a final option, you also want to look at the end user.

Primarily social engineering is used as an entry point for attackers in advanced persistent threat. As a result, it's often helpful to look at supporting end users in behaving in a secure fashion. So things such as security awareness training can also help. Of course, as with all security, there is no hard and fast foolproof way of securing against such an attack.

All we can do is build up different layers of security. That's it for this video, where we've looked at advanced persistent threats. I hope this has given you some food for thought, and I'll see you next time.

UK TOP 20 RESEARCH-INTENSIVE UNIVERSITY

UK UNIVERSITY OF THE YEAR WINNER

UK ENTREPRENEURIAL UNIVERSITY OF THE YEAR WINNER

The place of useful learning

The University of Strathclyde is a charitable body, registered in Scotland, number SC015263