dspanz. digital service providers australia new zealand

'Anatomy of a Cyber Attack' Webinar Q&A

1. ***What does a typical timeline of a cyber attack look like from the initial access to your involvement? Are we talking hours, days, weeks?***

   Guest Speaker - Jordan Hunt (ForensicIT): All of the above. The attack from the time the attackers get in there normally goes weeks to, if not, a month prior to when the client notices. The very large one we're finishing at the moment saw the attack activity on the 11th of May, but we traced the initial actions of the threat actor back to the 22nd of April. They'd been there well before. The initial attack activity, when you look at it in the context of being ransomed, starts to make sense to the organisation because even they brought up that, "Oh, we should have acted then." Yes, but you would have also then have to have been looking. So, it depends on the level of visibility you've got in the environment, but the notification to us and the actions you take relate back to that cost of a data breach.

   The faster you take action and kick them out has a direct correlation with the cost of the breach as it goes forward. You want them out of the environment as quickly as possible. Normally, we're talking from the day they get access to them taking actions within a month, but ransomware threat actors are skewing that quite significantly because they will come in very quickly, do their work, and then encrypt the environment because they want to get money and have an impact as quickly as possible.

2. ***Can you highlight the top three vulnerabilities that attackers are using to get into the environment and how we could protect ourselves?*** *For example, is something like MFA a good control?*

   Guest Speaker - Jordan Hunt (ForensicIT): At the moment, the main ones we've seen are insecure remote access processes and poor passwords. They all come in hand in hand with password management or hygiene. One of them was using a generic account that was used for tender submission for the organisation, because it was a group and a shared account, they decided they couldn't have MFA on it because multiple people needed access to it. I would have then said, "Don't make it have interactive login. Make it a shared mailbox," because you're reducing that risk. Unfortunately for them, the password was also the name of the company with a one at the end. The password policy and complexity is something that we still see as quite an issue. If you can brute force it, it's a problem. There's been quite a few recently, like a username called Temp with a rubbish password that is part of the VPN coming into the environment. The main things we see as far as the initial

entry point go are being able to access and brute force remote access methods and then poor password management.

The MFA side of things is interesting because we've been telling people for years to do it because it stops this type of attack. Then someone built Evilginx, a pen-testing tool used for phishing emails and things like that, but it will bypass MFA because it collects the authentication token. It's not that they've broken MFA, they're exploiting the process where it creates a token that is authorised to impersonate you. The process of you clicking on the phishing email establishes a link to Microsoft through their Evilginx server. You enter your password, it collects it. The MFA allow it collects the authorisation token on the way back. So, Microsoft's 90 days that token will last. Essentially, they have a way of impersonating you as an MFA authenticated user for the next 90 days without any issue. That has caused an issue recently. The concept of creating authorised tokens is the issue, not necessarily MFA. Having MFA is still a good idea, but it means you have more of an onus on education for users to not click on phishing links than you did prior. MFA was the saviour, whereas now it's not.

Host - Charles Gillman (DSPANZ): Notwithstanding that new technique, it sounds like they're not getting the basics right.

3. ***"Do you have experience of attacks occurring in OT environments? If so, what differences have you observed?"*** For those who don't know, OT is an operational technology.

   Guest Speaker - Jordan Hunt (ForensicIT): We do a lot of work with critical infrastructure and operational technology in the transport, gas, electricity, and water sectors. The main difference in the response approach is the consideration of the impacts on operations. This outweighs a lot of the containment strategies. You can't just disconnect the network because it may cause more of an event than the cyber incident was. We spend a lot more time doing preparation with them. I'm actually doing it tomorrow with a client because getting an understanding of the incident response process in the operational technology side of their plant has already been done. Now, we're working into the impacts that can potentially be seen from the IT network. We're looking at the fact that their ordering and delivery systems are in the IT environment. If you disrupt those, you have to stop production because you no longer know where to deliver the product and when. That overlap is the other thing we're considering a lot with the OT space.

   The other more technical differences are the need for more network forensics in OT environments because there's usually a lot more smaller, lower-spec equipment and PLCs and things like that. You're not going to be able to collect really detailed logs and forensic artefacts from them. Identifying choke points for network

communications and then figuring out what network telemetry info you can get to understand what malicious activity is occurring on the network would be the primary differences. The preparation in an OT network is very different from what we would normally do for a corporate environment.

4. ***"Have you seen any incidents where AI has been used by the threat actors to facilitate the attack?"*** And I'll add to that, ***"How did you know it was AI facilitation?"***

   Guest Speaker - Jordan Hunt (ForensicIT): Not really. Brute forcing passwords and things can be done through AI-driven tools. There are now pen-testing frameworks where you can test a network and find every vulnerability in it through AI. We haven't seen it showing up well from our perspective because we're looking at it from the evidence point of view. If it's not leaving logs behind that show us where it came from, it becomes less noticeable. The one strange one we've had recently was a developer testing code in ChatGPT and similar AI tools, but he was uploading code with keys in it and all sorts of stuff.

   So, you're getting this thing where it's now learning from your application and your secret keys and all the passwords and credentials. If you want to, you can now go to ChatGPT and say, "Show me the codes and AWS keys for this organisation," and it will come back and give it to you because it learned them. It's not really used for the attack, but it would be used as an initial entry point. How that plays out in the next few years will be interesting to watch.

   Host - Charles Gillman (DSPANZ): I think it's already playing out. I saw a report that since the launch of ChatGPT, global phishing volumes went up by 1200%. So, they're certainly being used to craft very realistic-looking emails.

5. ***"The study case was intentionally targeting the crypto company. Can you give an example of a non-target attack? Some less appealing company getting attacked."*** As lot of companies say, "Oh, we're not going to get hacked, we've got nothing interesting."

   Guest Speaker - Jordan Hunt (ForensicIT): We get that a lot. "Why did they target us?" They didn't. They found you because you had some insecure application or open remote access point. One we just finished was a small Australian company. They had IT people not following good hygiene. They had opened RDP directly to the internet, not even a firewall. Someone found that, came straight through, and encrypted the place. They're quite mean. They deleted the backups, reinitialised the NAS storage device, reset all the admin passwords, encrypted the data, then the virtual machine disks as a second layer of encryption, and deleted the passwords. Then they saw a remote desktop icon and used it to go to another organisation and encrypt them as well. That was all through insecure

administrative practices. It's not because they were targeted specifically. You could argue that Australia is a good target because we're relatively wealthy, rely heavily on IT infrastructure, and some organisations have a relaxed attitude toward security. The primary reason for those attacks is insecure administrative practices.

We've done jobs for very large financial software services, multinational chemical organisations, and down to a one-person optometrist in regional Victoria. The threat actors don't care. They asked that one-man optometrist for three and a half million in ransom. His business turnover was struggling to get 50k, so clearly, he's not going to pay 3 million in ransom. They don't know who they're attacking until they've already done it. Hopefully, that clarifies things.

5. Are there some tips that you can give us at the employee level to prevent some of these types of attacks? How can people look out for telltale signs of phishing, for example?

Guest Speaker - Jordan Hunt (ForensicIT): It's hard to say, "Don't click on any links," because there are reasons for you to do it. If we share reports with you at the end of an incident, we'll likely use Citrix ShareFile and say, "Click on this and put your email address in it." If you're expecting it from the person and know it's from their legitimate email address, that's fine. There are technical things you can put in around that, like Safe Links and Defender and other email security platforms. The social engineering side is harder because there's a lot in that that's quite nuanced. A reasonably young bloke at his first job as a developer, being approached by a company called Orby, another cryptocurrency firm. It's relevant to his organisation; he's got development skills. A government-backed hacking group has a lot of resources to impersonate and manipulate him well. In that scenario, education is key. Be sceptical of things if you see them offering you work and asking you to move to an uncontrolled environment, like from LinkedIn to Telegram. They don't want it on LinkedIn because that's traceable. Moving to WhatsApp or Telegram is a red flag. Understanding that a legitimate recruitment company wouldn't take you off to an encrypted messaging channel. Education around these signs is critical to prevent phishing and social engineering attacks. The amount of things now that will bypass security measures is amazing. We've had six jobs from one phishing email around November to December last year about Christmas bonuses with a QR code. Everyone's expecting a bonus due to the cost of living crisis and Christmas. Sixteen people clicked on it and chatted among themselves about it. There's a bit of organisational education needed to address this.

6. ***"If we're using online messaging and meeting platforms like WhatsApp and Zoom, is it a good practice to close all other applications such as Gmail and Internet banking? Does that reduce the risk or make no difference at all?"***

Guest Speaker - Jordan Hunt (ForensicIT): Not a huge amount from the threat actor's point of view. Not saving passwords in your browser is a good start. Use a protected password manager like 1Password or Bitwarden for additional security. There are many known information stealers that grab cached information from browsers. Keeping your device up to date and not using very old devices is also important. Privacy risks around having applications open come more from WhatsApp and Google recording everything on the device. It's more about privacy and invasion of privacy that you agree to in their terms and conditions. Apple's and Microsoft's new AI features also record a lot of activity. The use of apps on mobile phones is generally safer because it's harder to get malware on mobile devices.