Case study: Insider threat at global media company

Case study: Insider threat at global media company

The client's challenge	WithSecure's client, a global media company, was an incident response retainer client who had previously worked with WithSecure to navigate a previous Ransomware attempt. The client contacted WithSecure's incident response team when they noticed the firewall rules on their major domain sectors had been changed to be ineffective. This attack was particularly novel as it did not appear as though linked to any visible malicious activity, and was only identified as the client's CISO was due to report on changes made to improve the resilience of the network following a previous incident. The CISO was concerned with these changes and asked WithSecure to look for any signs of attack or exploitation. An insider threat is one of the most challenging cyber security threats for an organisation to mitigate. Traditional security models are designed around the concept of a perimeter, where the majority of security controls are designed to prevent external threats from breaking into the internal network, and detecting unauthenticated malicious activity once inside. This case was one of the most challenging forensics investigations that WithSecure has dealt with, and resulted in crucial developments to Countercept, WithSecure's MDR service, to improve the detection and mitigation of insider threats.
WithSecure's approach	Initially, the activity identified by WithSecure appeared to be accidental. At the client's request WithSecure investigated the source and identified the account which had been the change. It belonged to a member of the IT team that WithSecure had worked with on the previous incident – an individual known to be competent and unlikely to have made the change by mistake. The member of staff strongly denied making the change, arousing further suspicion, and so WithSecure was prompted to investigate further. Upon further examination, it transpired that the changes had been made at 1am (user time). At this point, it was hypothesised than the user account had been compromised or fraudulently used by a member of the third-party sysadmin team – either with direct intent to cause harm, or to cover up previous errors and avoid having their account tied to the mistake. Further small-scale security downgrades were identified, performed by both the first account and other third-party sysadmin accounts at unusual times of day. All of the changes identified would have required deep knowledge of the client's internal management software, and could only be accessed through an admin panel with admin credentials. The investigation was slow moving, with regular security downgrades being covertly monitored by WithSecure over time. WithSecure built a profile to track the origin, which appeared to be a different admin account, which routed through seven different accounts via different instances of third party software. The IP address of the malicious party was initially triangulated to a user in India – however shortly before an intervention was to be staged investigators realised that the IP was being spoofed. This was highly unusual, as IP is assigned by the internal VPN and spoofing requires control of the VPN server, an area of the network heavily locked down and difficult to change by an external attacker. Tracking the IP through the VPN server, investigators were first led to Malaysia, and then back to an IP in the UK. They discovered that the UK IP was one a sysadmin had previously connected from before he had been fired. The UK user had personally known the spoofed users in India and Malaysia and disliked them, having openly criticised their work before he had been fired. The UK user had set up and configured many of the management systems being used to implement the security changes, including the VPN server, and his changes had been carefully timed to embarrass the CISO who had terminated his employment.
Client benefits	To stop this user from causing any more damage, WithSecure performed a full reconfiguration of the VPN server so that they could no longer spoof their IP, along with domain wide password resets. The client was not concerned about legal action against the user – their priority was to stop his access to their estate and ensure that the security controls were no longer being tampered with. Despite this, investigators believed that the UK user still had contacts in the client organisation and logged in initially with valid credentials, before then using a contact for the admin

	account or accessing it through one of the management tools he was familiar with. As a result of this investigation, User Behavioural Analytics has been developed and added to the Countercept service, enhancing the agent’s ability to detect legitimate users behaving abnormally or maliciously.