# Case study: Defending a global market research company from a live attack

WITH secure

## Case study: Defending a global market research company from a live attack

### The client’s challenge

WithSecure’s client were alerted to the possibility that a number of their hosts were communicating with “known bad” IP addresses, suggesting a breach. The WithSecure Incident Response team were engaged to contain and investigate the breach. Initial breach of the perimeter was traced to a vulnerable external-facing website, with attackers estimated to have been active for around 25 days.

WithSecure later identified that the attacker was in position to execute an attack which would have installed ransomware across the majority of critical business systems, taking the organization fully offline; only the rapid intervention of the Incident Response team prevented catastrophic damages being incurred.

### WithSecure’s approach

By analysing Windows event logs, the team was able to identify that the attacker had been able to exfiltrate the Active Directory database, giving offline access to high-privilege account credentials across the estate. It became immediately apparent that this breach was widespread, making it impossible to use traditional incident response forensics to triage hundreds of endpoints effectively.

WithSecure deployed its endpoint Agent to over 16,000 endpoints to support incident response. A number of Cobalt Strike beacons were detected connecting to malicious IP addresses, and attackers were found to have gained full domain access through a compromised SQL server, from which the attacker was directly executing PowerShell.

Due to the severity and extent of the compromise, the incident response team was joined with WithSecure Countercept support, providing 24/7 monitoring and additional protection while the critical investigation continued.

Forensic investigation of artefacts allowed WithSecure to identify that the attacker was using a default SSL certificate that had been previously attributed to FIN6 – an organized crime group associated with historical and concurrent attacks costing victims upwards of £50m. WithSecure also found hosts connecting to another C2 server, enabled by uploading a malicious executable into a legitimate Google process. Reverse engineering of this malware linked the implant, “Goopy”, to a known threat actor group APT32 – also known as Vietnam-based OceanLotus. This attacker was estimated to have gone undetected for at least 2 years.

WithSecure developed a containment plan while degrading attacker C2 channels, using the results of attributing the malicious activity to known APT groups to inform the priority and severity of response actions. Actions were performed covertly so as not to raise attacker suspicions – if response activity was noticed, the attacker might have been prompted to act unpredictably. When ready, WithSecure killed the Cobalt Strike beacons – closing the C2 channels and isolating the infected hosts.

### Client benefits

Once access had been denied to the attacker, WithSecure carried out a range of remediations, from removing the malicious implants and rebuilding infected hosts, to performing a full password reset for users and services across the estate, including a reset of the KRBTGT account. WithSecure then supported the client in implementing detection rulesets to detect the specific techniques used in the attack, to safeguard at any attempts at re-entry. This proved to be essential, as re-entry attempts were detected soon after by attackers using stolen credentials on the Citrix environment. The Citrix environment was taken offline to prevent access passwords were again reset.

The timely and decisive intervention by WithSecure prevented any long-lasting damage to the client. Following this engagement, the client has continued to use WithSecure’s Managed Detection and Response service, which could be seamlessly carried on by using the endpoint Agent. No further attempts by the threat actor(s) were detected.