Case Study

BINARY DEFENSE

Counterintelligence Team Uncovers Potential Attack on MSP and Takes Quick Action

Business

Managed Services Provider (company name kept anonymous in this case study)

Challenges

Many different client accounts that could be compromised

Could be a big payday for a cybercriminal to obtain MSP customer information

Cyberattacks could have huge financial consequences for a business—such as the business ceasing operations

Results

Binary Defense Counterintelligence noticed a threat actor attempting to sell backdoor access to an unnamed MSP

CI team was able to pose as a cybercriminal and obtain the MSP's name

CI team worked with proper authorities to pursue justice for the victim MSP

"It is satisfying to know that our work resulted in such a positive outcome for this MSP and all its customers. What could have been a costly and destructive event for the MSP was transformed into an opportunity to re-assess cybersecurity defenses, without any disruption to service."
-Randy Pargman, Senior Director of Threat Hunting & Counterintelligence

Counterintelligence Team proactively looks for threats
Binary Defense Intelligence Analysts are always on the lookout for potential threats to customers ... but if they happen to run across a threat to a non-customer of Binary Defense, they take action nonetheless. They would tell you it's "all in a day's work," because that's their job—they aim to stop cybercriminals from carrying out attacks on unsuspecting businesses.

The Counterintelligence (CI) team is unique in that they are proactively looking for threats, rather than reacting to an existing threat. This is a powerful method of learning about the latest types of attacks, and informing customers so they can be prepared.

Part of the work done by the CI team is to scour the Clearnet (the Internet as most people know it) and Darknet for criminal activity. The team, many of whom have prior military or government experience, is able to gain access to criminal forums and pose as cybercriminals themselves to discern what threats are being discussed. When a threat is identified, the CI team takes action to inform the parties involved and attempt to remediate or prevent the threat from being carried out.

Analyst found threat against Managed Services Provider and took action
One of the Intelligence Analysts spotted an anonymous post from a person who claimed to have obtained backdoor access to a Managed Services Provider (MSP) located in the United States. They further claimed that this access could be used to install software (such as ransomware) on all of the MSP's computers, as well as on the computers of the MSP's customers.

MSPs have customer bases of all sizes, so this threat carried extra weight. If a cybercriminal gained access to the MSP and its customers, they could successfully paralyze or completely shut down several companies.

Posing as a cybercriminal allows an Intelligence Analyst to gain the trust of others on the forum. The threat actor was offering to sell the MSP access to anyone on the forum for bitcoins. The "undercover" Binary Defense analyst was ultimately able to obtain the name of the MSP from the threat actor.

Once the Counterintelligence Team learned of this criminal activity, they involved law enforcement. Working collaboratively with law enforcement is something the CI team does on a regular basis. This ensures that operations are done in a manner which preserves evidence, and is geared to bring justice to the victim. The MSP was informed of the potential breach and was able to take immediate, corrective action to prevent illlegal access from a threat actor. Without the diligence and skill of the CI analyst, the results could have been devastating.