CASE STUDY

Finding and Stopping Russian Hackers

YEAR	INDUSTRY	EMPLOYEES
2021	Finance	25–50

Challenge

Merely days into a new client relationship where iuvo replaced an underperforming MSP, we were informed by our contact that she and the rest of the company were getting locked out of work accounts. The issue began two years ago but was dismissed by the former MSP. However, our contact noticed that lately, the lockouts were occurring at a higher frequency. Gaps in the client's legacy IT set up (uncovered during this investigation) added to the complexity of the issue.

Solution

Our seasoned professionals immediately started looking into logs to help identify the root cause. However, the prior MSP's inexperience created a situation that made the logs virtually unusable at the onset of our investigation. The client had Microsoft Active Directory setup for user authentication. The logs on the Active Directory Domain Controllers were set to use default options which did not allow for enough information to be captured and stored. Due to this, we were unable to view historical information for past instances of the issue. We enabled customized logging settings which increased the number of logs being saved and expanded the breadth of data we had access to for investigative purposes. With greater visibility we identified a significant security breach.

Our consultants saw that a computer in their network was attempting log ins with randomly generated usernames, often using common first names as the username. At the time, the client was, in fact, using first names as usernames. Once the machine matched a valid account name, it would try passwords until the account would lockout. Fortunately, the lockout threshold was set at three attempts, which prevented successful password matches. This was happening nearly daily.

iuvo further investigated the issue and determined that the best course of action was to shift from the domain controllers to the individual computer that was attempting these unsuccessful logins. As a test, we shut off the computer making these login attempts and monitored the domain controller logs. As soon as the computer was shut off, all attacks on the system stopped.

Through the course of the investigation, other significant legacy security issues were also uncovered. The computer in question was a Microsoft Windows terminal server that was directly connected to the Internet due to the client's firewall allowing all traffic to the system. While reviewing the history of the device, it also became clear that the computer and several others had never been patched. Additionally, two earlier terminal servers had been compromised in a similar fashion, powered off, and replaced with the current system. At this point our consultants decided it was best to bring in a specialized forensics security team to start assessing how widespread the hacking and additional issues went.

iuvo provided system images of the compromised servers to the forensic analysts and after a thorough investigation the results pointed to three servers being breached by a group of Russian hackers from St. Petersburg, though realistically their set up had so many gaps it would have been possible for hackers to penetrate additional systems. Once the full scope of the problem was determined, iuvo took immediate ownership of mitigating the issues, coordinating with the forensics team, and began implementing significant security measures for the client, including regular testing for vulnerabilities, patching and audits.

Leveraging a low-cost MSP resulted in several severe security breaches for this client. iuvo was able to rapidly identify the root cause of a problem the client had simply deemed a pain point. After the scope of the issue was clear, iuvo pivoted and reprioritized our work during the crisis and were able to do so due to our consultants having extended experience and broad IT knowledge.

CASE STUDY

Finding and Stopping Russian Hackers

Results

Discovered

UNKNOWN VULNERABILITIES

Reduced

POTENTIAL LIABILITIES

Secured Systems

& OFFER SECURITY SOLUTIONS

Increased

PRODUCTIVITY

Outcome

Due to iuvo investigating an offhand remark, an active security breach was stopped before serious damage was done. In addition, the other security issues found and fixed ensured the client's information was securely protected. The monetary and time savings associated with preventing a security incident is immeasurable. Finally, once the lockouts ceased, the client's employees no longer struggled with decreased productivity. They were able to seamlessly perform their duties during the workday with no time lost.