Incident Response Program Results in Speedy Security Breach Identification

SIXGEN CASE STUDY

Summary at a Glance

CLIENT
- Private Client
- Enrolled in IRR Plus
- Located in the US

ISSUE
- "Security Consultant" claimed to have discovered private member PII compromised

SOLUTION
- Diagnosis and remediation within 4 hours of contact

Introduction

SixGen was contacted to provide in-depth Incident Response support to a private social club. Club leadership received a suspicious call from a "security consultant" claiming to have discovered private member personal identification information was publicly compromised.

Challenges

The alleged consultant showed up unannounced at the private club in person asking to speak to the club's leadership. This heightened anxiety within leadership, but agreed to meet the consultant face-to-face in two days. This left them less than 24 hours to determine if the allegations of breach were true, and if so, to determine the extent of the exposure.

Process

SixGen was contacted to remediate the issue and within 2 hours of initial contact, an external vulnerability assessment was conducted to substantiate the report claiming the membership database was compromised allowing public access to sensitive data. SixGen investigated the Dark web, breached databases, social media, and other sources to determine that a redirected API token allowed access to vulnerability in subdomain login. This would allow an adversary to compromise user enumeration through the clubs Microsoft O365 portal. SixGen shared the findings with remediation recommendations for unauthorized access and infiltration details with the client IR team.

Solution

After conducting triage with the client and performing an initial investigation, SixGen utilized a combination of prior experience, tradecraft and tools to validate, determine the root cause, and level of exposure of this compromise. Because the client was enrolled in the IRR Plus program, the entire process took less than four hours to diagnose and provide remediation recommendations to the client. During this time, SixGen provided regular updates to the client IR and IT team and guided them through the suggested remediation, and other security abnormalities determined during our investigation.

Key Takeaways

- Reduced response time due to IRR program enrollment and proactive measures taken in advance of the attack
- Accelerated use of past performance, tradecraft, and security tools to diagnose problem
- Implementation for problem remediation and other vulnerabilities quickly identified