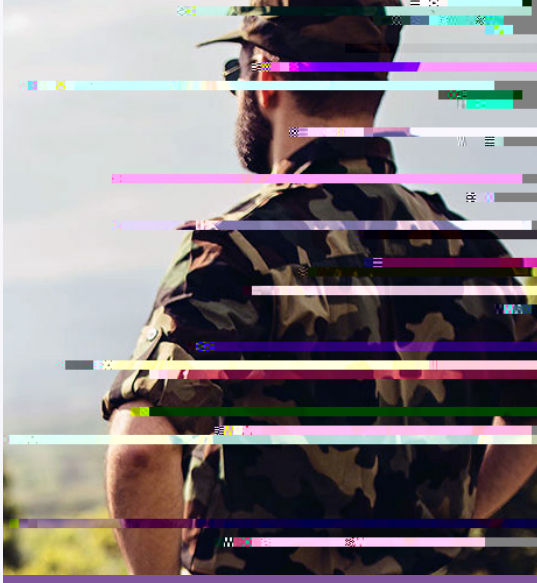
Red Teaming a Law Firm

Overview

Law frms face unique security challenges driven by the highly sensitive information entrusted to them by their clients, the advice their clients expect from them and the severe legal and reputational damage that could result from a breach.

A Synopsys red team assessment takes a big-picture, holistic view of the organization from the perspective of an adversary that is contextually relevant to the organization and the challenges they face. This assessment process is designed to help complex organizations handle a variety of sensitive assets to uncover non-traditional, equally complex attack paths that employ technical, physical, social or process-based attack vectors.



Severe legal and reputational damage could result from a breach.

This case study highlights the shortcomings of restricted-scope security assessments that do not provide visibility into overall organizational and asset-driven risk. The level of access and inform Ŏ ss-base T cs "

Adversarial Objectives and Strategy

This red team assessment started by defining the organization's core assets and a set of adversarial objectives. From this point, we designed the testing strategies to apply and the attack paths to follow. Our overall strategy for this assessment was to emulate a professional and technically sophisticated criminal organization with the following objectives:

- Gain access to sensitive client data including pending litigation, M&A, and other historical and current legal casework.
- Obtain access to the internal corporate network, facilitating longer-term, persistent attacks and data exfiltration.
- Obtain access to the firm's email system, enabling us to read and send emails from employee accounts to clients.

Getting Started

Once we identified the adversary we were emulating and defined our objectives and overall strategy, we were able to move into the actual assessment process. Reconnaissance and intelligence gathering were our immediate next steps as we began to quantify the remotely accessible attack surface of our target.

In all red team assessments, this initial phase is an ongoing activity and serves as the initial base upon which the Red Team builds scanning, attack path generation, and execution. Intelligence gathering also allows us to understand how adversaries perceive the target organization, how assets are secured, and how various technologies, processes and components fit together.

Reconnaissance efforts in this case focused on several key areas:

- **Identifying all web applications and live hosts/services within the target's IP address ranges.**

Attack Path Modeling

The following table illustrates a high-level and abstracted version of the composite attack matrix generated by the Red Team for this particular assessment. The matrix highlights several attack paths used to compromise sensitive client data and gain access to the internal corporate network. These composite attacks leveraged a variety of techniques at different stages in the assessment. For brevity, only three composite attacks are discussed in detail in section five.

Motivation	Relevant Technical Risks	Relevant Non-Technical Risks	Composite Attack Description
Compromise client data Attack clients directly using firm resources	• Internet-facing services lack multi-factor authentication • Unauthorized devices registered through MobileIron MDM service	• Employees susceptible to dragnet and spear phishing attacks	See section 5.1
Compromise customer data	• Internet-facing services lack multi-factor authentication	• Employees susceptible to email-based phishing attacks	See section 5.2
Compromise client data	• OpenSSL heartbleed on select servers • Anti-virus policy excludes Microsoft Office components, discovered via Heartbleed	• Employees susceptible to non-traditional phishing attacks	Use open-source intelligence to identify office receptionists that work with the job application process. Using this information, we developed payloads involving malicious office documents, that would not be detected by desktop anti-virus, based on company policy, and delivered them via mailed USB drives, traditional phishing, and the target's careers webpage.
Compromise client data	• N/A	• Employees posting sensitive data on social media services	After identifying a large set of employees, our Red Team started to associate names and contact information with social media services. We then mined publicly accessible profiles for anything related to our target goals or that would facilitate other attacks. Several instances of leaked client information were identified from cell phone camera pictures.
Compromise client data	• Lack of additional hardening to the internal network beyond applying patches	• Users susceptible to advanced phishing attacks that give the attacker access to the internal network	After gaining a foothold on the internal network, we were able to gain complete control over the network and exfiltrate sensitive information.

Employee Email Services Attack

Based on our analysis of the target organization, our Red Team identifed several mitigation strategies to address the risks associated with the adversarial objectives. These strategies were partially developed based on clusters of risks in our composite attack development process.

- Based on the success of various social engineering attacks across several composite attacks, implementing multi-factor authentication on all externally accessible employee services was a critical frst step. Implementing multi-factor authentication on these services effectively minimized the risk associated with an employee credential compromise.
- To further strengthen the security posture against social engineering attacks, we recommended a continuous security awareness program for employees of all levels. Promoting a culture of security awareness across the frm helps to drive down the likelihood of success from these kinds of attacks.
- The use of COTS software services across the external network infrastructure left security largely to confguration and patch management processes. Based on some of the issues identifed through this Red Team, we recommended regular vulnerability scanning and patch auditing to ensure that critical security updates were not missing from systems exposed to the Internet.
- We also recommended that a set of secure usage guidelines for social media services be published, promoted and enforced throughout the frm. These guidelines were to outline the risks for the frm due to unauthorized disclosure and what kinds of information is acceptable for employees to discuss in a public setting such as social media. As part of this step, we also worked to implement a response % li ȝ l m] ȳ ɔ T ced thor

THE SYNOPSYS DIFFERENCE

Synopsys offers the most comprehensive solution for integrating security and quality into your SDLC and supply chain. Whether you're well-versed in software security or just starting out, we provide the tools you need to ensure the integrity of the applications that power your business.

Our holistic approach to software security combines best-in-breed products, industry-leading experts, and a broad portfolio of managed and professional services that work together to improve the accuracy of findings, speed up the delivery of results, and provide solutions for addressing unique application security challenges. We don't stop when the test is over.

Our experts also provide remediation guidance, program design services, and training that empower you to build and maintain secure software.

For more information go to www.synopsys.com/software.

SYNOPSYS®

185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: software-integrity-sales@synopsys.com