A CASE STUDY

SYNOPSYS®

# Red Teaming a Law Firm

# Overview

Law firms 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 information obtained by our Red Team in this assessment would have represented a severe breach, including the loss of client information, the ability to attack clients leveraging the firm's email and cause overall harm to the organization's brand and reputation if similarly conducted by a real-world adversary.

Our Red Team was able to construct multiple composite attacks that allowed us to compromise sensitive client data and the internal corporate network (outlined in section 4) including escalating privileges to that of domain administrator. Each of these composite attacks were developed using a variety of testing techniques and vulnerabilities across multiple components in the same manner that sophisticated real-world adversaries do.

# 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.** Once these were identified, we were able to assess them from an unauthenticated perspective, identifying low-hanging fruit vulnerabilities as well as collecting information that we could later cross-reference to identify relationships between components such as shared authentication services, routing paths, or authorization frameworks.
- **Collecting information on employees that may facilitate targeted or dragnet social engineering attacks** later in the assessment. The base-level information collected included name, phone number, job title, and email address. (Note: For red team assessments in general, various combinations of this base-level information and additional employee-specific information are used depending on the composite attacks being developed).
- Utilizing open-source intelligence gathering to identify information about the organization. Information gathered included employee social media profiles, photos of the target's corporate offices posted by employees to social media, general background information, and current trends and events impacting the organization. This information was used to advise later composite attacks.

# 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<br><br>Attack clients directly using firm resources | • Internet-facing services lack multi-factor authentication<br><br>• 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<br><br>• 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. |

Leveraging employee susceptibility to social engineering attacks, technical vulnerabilities, and testing techniques all within a single composite attack allowed us to accomplish our adversarial objectives in ways that a real-world adversary would.

## Execution

Building on the reconnaissance efforts and the composite attack paths that were developed, our Red Team started to build and execute each attack, targeting our adversarial objectives. Here we discuss two of the composite attacks that were executed within this Red Team.

## Employee Email Services Attack

The first composite attack launched by our Red Team targeted email services for specific employees. The idea behind the attack was that email access would allow us to view sensitive client communications as well as potentially launch attacks directly against clients leveraging the trust of our victim's email address. We started with open-source intelligence gathering techniques to identify employee roles, case profiles, and email addresses for targeting purposes in our spear phishing attacks. We then assessed the externally-exposed MobileIron MDM service used by employees to access corporate email on their mobile devices.

The first composite attack launched by our Red Team targeted email services for specific employees.

As part of larger spear phishing efforts launched throughout this red team assessment, we obtained the credentials for several high-ranking employees in the organization. Based on the configuration of the MDM service, we were able to register new mobile devices (i.e., iPhones and iPads) to access specific employee Outlook services, including email, contacts, and calendar using just the employee's username and password. Once we were able to register our devices with the MDM service, our Red Team could send emails as the victim user and completely impersonate our target, responding to actual email threads, reading sensitive information stored in the service, or sending new correspondence to contacts.

## Multi-Factor Authentication Attack

Our Red Team launched a composite attack with the goal of accessing the target's sensitive client data and virtualized desktop environment. This attack combined elements of open-source intelligence gathering, active network reconnaissance, social engineering and took advantage of services missing multi-factor authentication as well as those that used it on public-facing services. The attack involved harvesting user credentials and token values via an email-based phishing campaign, and using these credentials to access a range of services that handled sensitive client data.

Initially, our Red Team used port-scanning tools to identify services used by the target's employees that are available on the Internet. The precursor to the scan was to identify the target's IP ranges. Attackers commonly use techniques such as DNS enumeration, lookups in regional Internet registries such as ARIN and traceroute to identify the network infrastructure employed by the target. The next step was to perform a deep port scan on the identified IP ranges, enumerating live hosts and services. Our Red Team heavily utilized the nmap port-scanning tool in this phase and identified Internet-facing live hosts and services used by the target firm. We then visited all the HTTP/HTTPS services identified by the scan, noting that some services did not require multi-factor authentication and others that did.

The Red Team then crafted a cover story requiring that employees complete an online IT security awareness training program. We sent an email to target addresses collected via open-source intelligence gathering, directing users to log into a falsified IT security awareness training program. This ruse resulted in multiple users disclosing their LDAP credentials to our Red Team. After sending the phishing emails, We also followed up with select employees via telephone. This pushed employees into executing the phishing workflow by telling them that their awareness program had not yet been completed and that their accounts would soon be suspended and followed up with disciplinary action.

Having full access to the network, our Red Team was able to identify locations containing sensitive client information.

Armed with credentials and one-time token values, we attempted to authenticate to the services not requiring multi-factor authentication. The harvested credentials were valid for a secure file-sharing system that appeared to handle sensitive data. The secure file-sharing system used by the target was also accessible using the harvested credentials without multi-factor authentication. This system appeared to be used to share sensitive data with clients, and also provided access to the target's internal file shares containing current and historical client data.

We also leveraged the employee credentials and one-time token values from our phishing attack by passing the values immediately through to services using multi-factor authentication. Using this vector, we were able to authenticate and access the remote desktop virtualization environment on the internal network.

With access to the internal network, we quickly discovered that their Windows environment was fully patched, meaning public exploits would not work and would likely be a quick path to getting caught. Nevertheless, we were able to explore the environment, discover multiple vulnerabilities and chain them together into a composite attack that escalated our privileges to those of domain administrator. With this level of access, compromising the entire organization was trivial and we established footholds in their environment.

Having full access to the network, our Red Team was able to indentify locations containing sensitive client information. This information included lawsuits and merger information for very large companies throughout the country. A malicious attacker could have very easily exfiltrated the information and distributed it on the Internet.

# Employee Email Services Attack

Based on our analysis of the target organization, our Red Team identified 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 first 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 firm 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 configuration and patch management processes. Based on some of the issues identified 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 firm. These guidelines were to outline the risks for the firm 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 plan in the event of a disclosure.
- Finally, our Red Team provided guidance on how to mitigate the post-exploitation techniques leveraged in the engagement. These included the immediate hardening of critical infrastructure, long-term plans to redesign the client's network and on-going activities for monitoring to help ensure that if they were to get compromised, there would be a higher chance that footholds would be identified and terminated long before access could be persisted.

# Summary Discussion and Results

Overall, we found that the target's security posture, organizational footprint, and security awareness level of the target's employees introduced real-world, exploitable weaknesses. The confluence of insufficient employee security awareness, lack of multi-factor authentication for services containing sensitive data and the target's informational and network presence allowed our Red Team to achieve all of the adversarial objectives outlined at the start of the red team assessment; these included compromising sensitive client data, gaining persistent internal network access, and the ability to read and send email as employees.

The level of access and information obtained would have represented a severe breach, financial damages, and harm to the organization's brand and reputation if similarly conducted by a real-world adversary. Each of the risks outlined within this case study are real and immediately exploitable by a similarly skilled adversary, given that we operated from the perspective of a remote, technically skilled, and coordinated black-box adversary.

# 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