COMP2216 - Cyber Security Cyber-Attack Analysis: Report

33381836

S. Zagrosi (sz10g21@soton.ac.uk)

Produced for

Electronics & Computer Science
University of Southampton
United Kingdom

Contents

1 Task 1 – Kill Chain-based Analysis

1.1 Kill-Chain 1 - Infiltration via CRM System Vulnerability

Reconnaissance Phase 1

Open-source intelligence gathering identified GovVault and SecProv. Leaked databases pinpointed key personnel and system vulnerabilities. GovVault had an RCE vulnerability; SecProv was compromised via a vulnerable RDP service. Detailed network mapping and vulnerability scans were likely employed, using tools like Shodan for network device identification and vulnerability scanners for weak spots discovery. It's inferred that attackers also gathered details on the CRM system's hosting infrastructure within SecProv's network, leveraging information from social media and internal forums frequented by employees.

Weaponisation Phase 1

Custom malware was designed, incorporating malicious packets for GovVault's buffer overflow exploit and a backdoor for SecProv's SecMon. Malware likely used encryption to avoid detection, and polymorphic techniques to evade signature-based antivirus solutions. Test environments may have been established to refine the malware against configurations mimicking the targets, ensuring high success rates upon deployment. The inclusion of a downloader script, a component of the malware, was prepared for initial foothold establishment, tailored to exploit the RCE vulnerability with high precision.

Delivery Phase 1

Spear-phishing emails targeted selected GovVault employees, while SecProv received a compromised update through social engineering or phishing. Delivery methods were chosen for their likelihood to bypass traditional security measures, possibly including email spoofing and exploiting trusted third-party communications. The dual delivery strategy maximised chances of successful infiltration, leveraging human error and system trust. The downloader script was transmitted via the internet, exploiting the CRM's RCE vulnerability, with the attack timed to coincide with periods of low monitoring to reduce detection risk.

Exploitation Phase 1

GovVault's system was compromised, allowing root-level access. Simultaneously, the backdoor in SecProv's network facilitated unauthorized access. This phase likely involved exploiting unpatched software and leveraging zero-day vulnerabilities, indicating advanced preparation and targeting. Automated tools could have been used to exploit these vulnerabilities quickly once access was gained. The RCE vulnerability's exploitation enabled remote execution of the downloader script, bypassing standard security measures through sophisticated evasion techniques.

Installation Phase 1

Malware installed on both networks ensured persistent access. Techniques for maintaining persistence included creating scheduled tasks, modifying registry keys, and exploiting system or application auto-update features. This phase's success relied on stealth, with malware mimicking legitimate processes and using rootkits to hide from system administrators and security tools. The downloader script, upon execution, downloaded further malicious components, ensuring persistence by modifying OS registry for automatic execution on boot, a tactic designed to maintain long-term access without detection.

Command and Control Phase 1

A secure C&C infrastructure was established, possibly using TOR for anonymity and encrypted messaging for command transmission. The C&C allowed real-time control over compromised systems, data exfiltration, and malware deployment. Techniques to maintain C&C could include domain generation algorithms (DGA) to prevent blocking and mimic legitimate network traffic. Presumably, C&C communication may have also been established through HTTP or anonymous Tor connections, employing multi-layered encryption to obscure malicious traffic further to ensure uninterrupted C&C operations.

1.2 Kill-Chain 2 - Breach of Developer's Workstation via RDP

Reconnaissance Phase 2

Detailed examination of SecProv's network identified a developer workstation with misconfigured RDP service. Research likely involved passive scanning techniques to avoid detection, using tools like Nmap for port scanning and identifying services running on open ports. Social engineering may have been employed to gather information on internal network practices and security policies. Additionally, attackers may have leveraged engagement in developer forums or scrutinised social media profiles to ascertain SecMon development team's structure and pinpoint individuals with weak security practices.

Weaponisation Phase 2

Attackers prepared a set of tools for brute-force attack, selecting software known for effectiveness in password cracking, such as Hydra or John the Ripper. These tools were tailored to exploit RDP's vulnerabilities, using custom dictionaries based on known password trends and data breaches. A malicious update for the SecMon application was crafted, incorporating a stealthy backdoor for later stages of the attack, helped with understanding of SecMon's security protocols to bypass code review mechanisms seamlessly.

Delivery Phase 2

The brute-force attack was planned carefully, with password combinations tested against the RDP service under guise of legitimate traffic, presumably facilitated by IP spoofing and botnets. The attackers' approach ensured low profile to evade detection systems. Following the breach, attackers exploited the compromised developer's credentials to upload the maliciously modified SecMon build, exploiting comprehensive repository access without immediate detection.

Exploitation Phase 2

The successful compromise of the developer's workstation through the brute-force attack granted unrestricted access within SecProv's network, showing an understanding of internal security architectures and vulnerability exploitation methods. The attack's execution showed strategic exploitation of identified weaknesses in SecProv's RDP configuration and the subsequent manipulation of developer privileges.

Installation Phase 2

Establishing persistence, attackers discretely manipulated system configs and deployed more backdoors, allowing uninterrupted access. The use of existing administrative tools for these purposes remained under the radar, requiring both technical know-how and stealth. Attackers' decision to preserve the developer's original credentials and disable RDP service notifications was calculated to maintain silent presence within the network.

Command and Control Phase 2

With the developer's workstation under control, attackers strengthened their position by setting up a C&C framework, possibly utilising encrypted channels and cloud services to obscure malicious traffic. C&C network architecture was designed for resilience, employing fast-flux techniques and possibly using Tor for anonymity. This setup allowed both silent extraction of sensitive data and for attackers to create further intrusions, showing advanced operational capability towards the digital environment of SecProv.

1.3 Kill-Chain 3 - Malicious Update to SecMon & Govault Breach

Reconnaissance Phase 3

Detailed analysis of SecMon's development lifecycle revealed vulnerabilities in the software update process. Attackers possibly conducted this phase over an extended period, employing social engineering and/or phishing campaigns to gather insider information, possibly infiltrating developer forums or communications channels to gain insight into SecMon's architecture and development practices. Attackers may have monitored employee activity on professional networks (e.g. LinkedIn, Facebook) to identify targets for social engineering attacks, making assumptions about internal update procedures and identifying key personnel involved in the update chain.

Weaponisation Phase 3

The malicious update was designed to pass code review processes, suggesting deep understanding of SecMon's codebase and development practices. The update included sophisticated evasion techniques, including code obfuscation and stolen digital certificate signing, appearing legitimate to bypass security checks during the update process. Attackers prepared secondary payloads intended for specific targets within the network, fitting gathered intelligence during reconnaissance, including downloader scripts for initial compromise whilst leveraging existing vulnerabilities within the network infrastructure.

Delivery Phase 3

Utilising compromised credentials, attackers submitted the malicious update to SecProv's code repository. This likely involved timing the submission during periods of high activity or using spoofed IP addresses to appear as legitimate developer activity, thereby avoiding immediate detection, ensuring the update's approval and distribution. To ensure the update's approval, phishing emails may have been sent to SecProv employees, encouraging expedition of the update under guise of addressing critical security vulnerabilities, employing tactics to mimic internal communications believably.

Exploitation Phase 3

Post-installation, the backdoor enabled unauthorised access to GovVault, exploiting trust relationships between SecProv and GovVault. This exploitation bypassed perimeter defences, taking advantage of implicit trust in the software update process and highlighting the attackers' ability to manipulate supply chain relationships in a targeted way. This was coordinated to happen during system maintenance windows, reducing likelihood of detection by system monitoring tools and ensuring a smooth transition to gain access without alerting IT security.

Installation Phase 3

Ensuring persistence within GovVault's network, attackers blend with regular network traffic and operations. This may have involved modification of legitimate network management tools or creation of ghost accounts with minimal privileges, allowing long-term access and control for espionage and/or data theft. Attackers established covert communication channels with the compromised system, using encrypted DNS queries to exfiltrate data without attracting undue attention, ensuring the data exfiltration process was slow and stealthy to data loss prevention (DLP) systems system detection.

Command and Control Phase 3

Attackers established C&C infrastructure for GovVault, possibly leveraging cloud services and/or other high-reputation domains to obfuscate command traffic. Methods like multi-layered encryption and steganography in seemingly normal files ensured persistent/undetected control. This could have involved machine learning algorithms to adapt communication patterns to network security responses, for higher level of adaptability in maintaining network presence. The C&C infrastructure was adjusted to route traffic through proxies and VPN services, complicating efforts to trace the attack, possibly employing HTTP connections and/or Tor for anonymisation.

1.4 Kill-Chain 4 - Cloud Infrastructure Compromise

Reconnaissance Phase 4

Attackers focus on cloud services used by GovVault and SecProv for data backup and/or additional computing resources. With passive scanning and social engineering, vulnerabilities in cloud service configurations are identified. The use of compromised employee credentials to access cloud management consoles is considered a potential entry point. Assumptions include attackers' prior knowledge of cloud environments, targeted reconnaissance on cloud infrastructure specifics, using both public and private data sources to map cloud architecture.

Weaponisation Phase 4

Exploits developed target identified cloud service vulnerabilities, including stolen API tokens or exploiting mis-configured storage buckets. Custom phishing campaigns are prepared, targeting employees with cloud administrative access to steal credentials. Tools likely included cloud-specific exploitation frameworks and/or scripts designed to automate credential theft process, showing technical understanding of cloud security mechanisms. Preparation of downloader scripts tailored for cloud environments ensured smooth deployment of secondary payloads.

Delivery Phase 4

Spear-phishing attacks target cloud administrators, whilst exploits against exposed cloud services are deployed. The delivery leverages sophisticated social engineering, designed to bypass two-factor authentication mechanisms, with exploit scripts programmed to manipulate cloud APIs for unauthorised access. Usage of compromised legitimate accounts for delivery may have further obfuscated attackers' actions, blending with normal user activities to avoid detection. These activities are well-timed to coincide with periods of low monitoring, exploiting security coverage gaps.

Exploitation Phase 4

Exploitation grants access to cloud environments, allowing attackers to manipulate cloud resources, escalate privileges, and possibly access vast amounts of sensitive data stored in cloud infrastructures. Mis-configured cloud storage and weakly protected API endpoints are exploited for lateral movement within the cloud. Attackers may have used automated scanning tools to identify exploitable vulnerabilities in real-time, increasing exploitation efficiency. Strategic exploitation of vulnerabilities enabled the discreet installation of backdoors without detection.

Installation Phase 4

Persistent access mechanisms are established within cloud infrastructure, including deployment of malicious cloud functions and creation of hidden admin accounts. This ensured continuous access to cloud resources/data, allowing stealthy monitoring and data exfiltration. The creation of new, unauthorised cloud resources for persistence shows attackers' skill, and strategic use of cloud services against the victims. Attackers' activities are carefully hidden within legitimate cloud operations to avoid suspicion.

Command and Control Phase 4

New C&C infrastructure is set up within compromised cloud environment, utilising cloud-native services to mask malicious traffic. This includes using cloud storage services for data exfiltration and utilising serverless platforms to host C&C servers, making detection and attribution more difficult. The use of encrypted channels and serverless architectures for C&C communication aids in both evading traditional network-based detection mechanisms and demonstrates advanced understanding of cloud-based operational security (OpSec) practices. Attackers may have employed HTTP(S) connections or Tor for communications to ensure anonymity and complicate traceability.

Actions on Objective Phase

Attackers executed primary objectives using access gained from GovVault and SecProv. Data exfiltration was conducted with encryption to minimise network footprint, avoiding DLP system detection. Documents exfiltrated to external server, possibly using FTP over SSL/TLS for obfuscation with encrypted DNS queries. Data likely staged within compromised network using fileless storage methods, avoiding physical traceability. Strategic leak of information timed for maximum impact, distributed through anonymous file-sharing platforms, social media to ensure widespread dissemination for difficult containment. Given 4-month duration, process likely paced deliberately for slow, methodic exfiltration without alarming internal security measures, ensuring unauthorised access remained undetected.

2 Task 2 – Attacker Analysis

2.1 Cybercriminal

Motivations

Cybercriminals' drive for financial gain may extend to exploiting chaos for indirect benefits. Information could be used for blackmail, sold to interested parties, leveraged for future cyber attacks. The attack's broader impact hints at a sophisticated understanding of information's value beyond immediate financial gain, suggesting long-term strategy for exploiting stolen data, diverging from traditional cybercriminal motives, showing possible evolution or diversification in cybercriminal objectives towards strategic disruption.

Attack Strategy

APT tactics typically associated with state actors, this operation's scale and precision deviate from conventional cybercriminal playbook focused on quick financial returns. Absence of ransom demands or immediate financial exploitation underlines strategic patience, resource allocation, usually not characteristic of normal cybercriminal attacks; however, indirect financial gain may be present. Complexity of attacks, including supply chain manipulation, stealthy persistence, could align with sophisticated cybercriminals expanding their methodologies.

Technical Skills

Demonstrating ability to exploit complex vulnerabilities, program custom malware, maintain long-term stealth, attack's technical profile suggests group with resources and skills of advanced cybercriminal organisations. The OpSec, counter-forensic measures point to professional, well-organised groups with greater cyber-offensive capabilities, able to plan and execute a multifaceted attack strategy including elements traditionally associated with nation-state actors.

2.2 Nation State

Motivations

The operation's sophistication, target choice, point to objectives closer to national security interests, geopolitical maneuvering, (e.g. undermining foreign government's credibility, destabilising sociopolitical landscapes). Strategic nature of document leaks could serve dual purposes; disruption within target nation and providing leverage in diplomatic channels. Further emphasised by attack's ultimate goal of inciting public outcry and potentially instigation of political or social upheaval.

Attack Strategy

With comprehensive, multi-layered cyber engagement strategy, attack's execution shows tell-tale nation-state operational planning, including deep reconnaissance, supply chain vulnerability exploitation, leveraging cyber-espionage for strategic gains. This level of coordination and goal orientation generally exceeds non-state actors' capabilities and/or resources, indicating highly organised, resource-rich actor, with strategic objectives.

Technical Skills

Attack required in-depth knowledge of cybersecurity defences, advanced exploitation techniques, custom tool development, underscoring capabilities associated with; national cyber units, and/or state-sponsored APT groups. The strategic silence post-attack, lack of attribution efforts, suggest high level of sophistication in OpSec, aligning with nation-state attributes. Use of APT and influence campaigns indicate technical and operational sophistication consistent with nation-state capabilities, objectives.

2.3 Hacktivist

Motivations

Driven by ideology, attack's focus on public exposure of sensitive documents align with hacktivist aims to push social, political change. This suggests desire to catalyse public scrutiny, governmental accountability, leveraging cyber tactics for activism. The attack's outcome, inciting public outcry, potentially destabilising trust in government institutions, mirrors typical hacktivist goals.

Attack Strategy

The complexity, stealth of attack diverge from general hacktivist operations, which generally are more overt, aimed at immediate public impact. This may indicate a change in hacktivist methodologies towards more sophisticated, less detectable operations, possibly reflecting evolution in hacktivist capabilities and/or collaborations with more technically adept entities. Data breach's execution, combining malware use with a strategic release of sensitive information, suggests high-level understanding of the targeted impact.

Technical Skills

The technical depth required for this operation diverges from general hacktivist activity, possibly alluding external support, or subgroup within hacktivism with more advanced skills. The ability to maintain operational secrecy, execute multi-phased attack strategy, shows skill not common with grassroots hacktivist campaigns. Sophistication of this supply chain attack suggests greater technical capability and/or possible collaboration with more skilled entities.

Total Words: 2421, Headers: 43

No sections exceed the 100 word limit