

SISA



SISA TOP
5

2023-2024

**Forensic
Driven
Learnings**

Table of Contents

Foreword	03
Preface	07
Introduction	08
Distinct Use Cases	10
• Insider-assisted Ransomware Attack at a Manufacturing Enterprise	11
• MDR Detects MFA Brute Forcing Attack On A Payment Aggregator	12
• Ransomware Embedded in Application Code	13
• API-based Attack	14
Investigative Trends	15
• Trends Observed in Ingress	15
• Trends in Lateral Movement	16
• Trends in Action on Objective	17
SISA Top 5 Controls to Keep You Secure	18
• Faster Vulnerability Mitigation	19
• Endpoint Protection	19
• Intelligent Detection and Response	20
• MFA Everywhere	21
• Attack Surface Reduction	21
Concluding the 4th Edition of Top 5	22

Foreword

The rapid advancements in technology have resulted in borderless and connected societies. At the same time, it has enabled cyber criminals to devise new threats and more readily exploit vulnerabilities in the blink of an eye. As such, CISOs and their teams must remain vigilant in not only keeping pace with cyberattacks but also by learning from recent data breaches to develop their strategy and future budgets to address areas of greatest risk.

SISA's flagship annual report - *SISA Top 5 Forensic-driven Learnings 2023-24* is an essential and insightful read to prepare cybersecurity professionals to build the proper Identification, Protection, Detection, Response and Recovery controls to prevent a future data breach. This report is a culmination of investigations into several cybersecurity incidents to analyse the evidence and identify the root causes. From these trends, you can see where and how to shift your risk management posture. What I particularly like is not only the insight from specific use cases, but the recommendations for which type of controls would be most relevant to prevent future incidents from taking place.

Forensic analysis is critical to decoding emerging threats and devising effective security levers to combat them. For protection of data to evolve, we must first understand and agree how risk persists today. Our ability to fairly evaluate and consistently apply the lessons learned from data compromises is the only way we can improve expectations.

To do so, requires commitment from industry stakeholders to share their knowledge. I have been fortunate in my career to work with many organizations that have been willing to share their learnings so that the entire industry can be better prepared. I congratulate the SISA team for this report that provides a practitioner-led approach on forensics investigations, for enterprises to stay cybersecure.



Troy Leach

Chief Strategy Officer for Cloud Security Alliance and Former PCI Security Standards Council CTO and Chief Standards Architect

As the Chief Strategy Officer of Cloud Security Alliance, Troy is responsible for the corporate strategy and ongoing mission to provide new and relevant cloud security awareness, education, research, programs, and membership participation. He specifically focuses on external engagements and corporate initiatives surrounding the financial services and payment industries, cryptocurrency and related government activities and serves as a featured CSA speaker at various industry events.

Troy sits on advisory boards as an expert in information security and financial payments and advises universities on future cybersecurity curriculum. He speaks with regulators all over the world looking to address emerging risks and has testified in various United States Congressional Hearings as a payment's security expert. He also is recognized within the World Economic Forum as an expert in blockchain and cybersecurity. Previously, Troy helped establish and lead the PCI Security Standards Council, as their CTO and Chief Standards Architect. He also served on the Board of Directors for the standards body, ANSI X9.

Foreword

As technology continues to evolve and permeate every aspect of our lives, the importance of cybersecurity cannot be overstated. Every day, we hear about new threats and vulnerabilities, and the stakes are higher than ever before. Sharpening the defences and improving preparedness is key for organizations to stay ahead of the bad actors.

SISA's flagship publication on cybersecurity – '*SISA Top 5 Forensic-driven Learnings 2023-24*' report is an invaluable resource for anyone looking to stay informed and prepared. It provides a comprehensive overview of the evolving threat landscape, and a detailed analysis of attackers' Techniques, Tactics, and Procedures (TTPs) across the cyber kill chain. One of the notable trends highlighted in the report is the evolution of the RaaS model with a deeper understanding of shifting tactics and distinct use cases.

The report will be a valuable read for cybersecurity leaders and practitioners, especially as it is based on real world experience from SISA in carrying out their forensic investigations, compliance audits and incident response cases. I highly recommend all CISOs study and adopt the best practices highlighted in this report to help build resilience to ransomware and breaches and improve the overall security posture of their enterprise.



Brian O'Higgins

**Cybersecurity Technology Evangelist –
Canada**

Brian is an angel investor and Board Member with more than 30 years of experience as a leader in security technology development – known best for his role pioneering PKI (Public Key Infrastructure). His approach to security is both visionary and pragmatic. Brian is a founding author and contributor to the Cloud Security Alliance. His current list of affiliations includes advisory board positions with Defence R&D, Canada, The Ontario Centers of Excellence and the Canadian Association of Defence and Security Industries.

The power of technology has pushed human boundaries and enabled us to achieve feats that were once considered impossible. As crime exists as part of the human condition, criminals have gravitated to cyberspace. As the threat landscape evolves, I truly believe that managing this risk requires all industry stakeholders to adopt a shared approach to information dissemination. It requires organizations to have up-to-date information and actionable intelligence to help them proactively defend against cyber threats.

I congratulate the SISA team for the launch of their fourth edition of their flagship report - *SISA Top 5 Forensic-driven Learnings 2023-24*. This report outlines attackers' techniques, tactics, and procedures by focusing on unique cases that showcase uncommon or innovative intrusion methods. All of this derived from the hundreds of real-world cases in which SISA has been involved.

The rise in Ransomware-as-a-Service observed by SISA is certainly concerning. This threatens to increase attacks in number and provide sophistication to more attackers. The SISA Top 5 acts as a reminder of critical importance of maintaining vigilant controls.

Foreword

In my advisory role, I have the privilege of working with many organizations that are at the forefront of technology-led innovation. I commend SISA for their continued dedication and commitment to sharing their forensics-driven learnings for enterprises to stay cybersecure.



**Peter Tapling,
APRP**

Managing Director, PTap Advisory, LLC

Peter Tapling is an advisor, board member and investor at the intersection of payments, risk, and emerging technologies. He serves as an advisor to several security and fintech companies, and on the Board Advisory Group for the U.S. Faster Payments Council, the Board of Regents for The Payments Institute and as a technology advisor to the Board of Directors for ePayResources. Peter is an Accredited Payments Risk Professional and a member of the Association for Financial Professionals.

The past year has been a challenging one for organizations around the world as they have had to contend with an ever-evolving threat landscape alongside the macro-economic challenges. Cybersecurity has become more important than ever, and organizations of all sizes and industries must be vigilant in protecting their assets and data. One way to achieve this is by applying learnings from industry-wide breaches and continuous improvement in security controls.

In this context, SISA's Top 5 Forensic-driven Learnings Report 2023-2024 is a valuable resource for organizations as they navigate the complex and ever-changing world of cyber threats. The report contains critical insights into a wide range of cybersecurity topics, including the latest threats and trends, uncommon and novel attack tactics of adversaries, and best practices for improving cybersecurity posture. It also provides practical guidance on how organizations can build a robust, secure, and resilient digital ecosystem. As a leading forensics investigator with an unwavering focus to secure the payments space, this thought leadership report is a testament to SISA's deep expertise and commitment to staying at the forefront of the industry.

Foreword

This blend of learnings from observed attack patterns combined with practitioner-led insights to improve resilience, is a must-read for any organization looking to enhance its cybersecurity posture. I encourage all industry participants to read this report and consider implementing the recommendations and best practices it provides.



**Lt General (Dr)
Rajesh Pant**

**National Cyber Security Coordinator
Prime Minister's Office, Government of
India**

General Rajesh Pant is an internationally recognised Cyber Security expert, who is presently tenanted the prestigious appointment of National Cyber Security Coordinator in the National Security Council Secretariat of India at the Prime Minister's Office. In this capacity, he is responsible for coordinating all cybersecurity activities across multiple sectors to ensure a secure and resilient cyber space within the nation. He holds a Ph.D. the field of Information Security metrics.

Prior to this appointment, he was the head of the Army's Cyber Training establishment for three years. He served in the Army Signals Corps for 41 years wherein he was awarded three times by the President of India for distinguished service of the highest order. Consequent to his retirement, he was Chairman of a listed Electronics Company, peer review member of NAAC, and Governing Council member of IETE (India).

There are many wise sayings about learning from others' mistakes since we can't possibly experience all of them ourselves. The SISA Top 5 Forensic Driven Learnings 2023-24 report documents many of these "mistakes" from past data breach investigations as observed by SISA in its role as a PCI Forensic Investigator (PFI). Many "mistakes" are the result of poor cybersecurity practices, and business leaders need to drive changes to embed security as a continuous process. This is one of the four goals listed by PCI SSC as we worked with industry stakeholders to publish PCI DSS v4.0 in March 2022. Cybersecurity practitioners should pay heed to the five recommendations listed out in the report, including the actionable best practices to secure their payment environment, and maintain the trust of their customers and stakeholders.



**Yew Kuann
Cheng**

**Regional VP for Asia Pacific
PCI Security Standards Council (PCI SSC)**

Yew Kuann Cheng is the Regional Vice President of PCI Security Standards Council (PCI SSC), and he leads the industry engagement activities in Asia Pacific. Through the various stakeholders of the Council, he hopes to continue increasing the awareness of PCI SSC's mission to enhance the security of payment account data through the development of security standards and supporting services. Yew Kuann has more than 20 years of experience in risk management, of which, 15 years was at Visa's Risk Management team.

Preface

The past few years have been overwhelming for all of us. The complexity of the cyber threat landscape has continued to evolve in 2022, becoming more challenging for organizations to defend against. The threat environment has been characterized by a whole slew of cyberattacks from Advanced Persistent Threats, multi-vector attacks, complex privacy-related attacks including advanced evasion and encryption techniques. Complex multiple attack vectors, such as social engineering and malware to compromise organizations have risen in frequency and complexity. Attackers have also increased their focus on stealing sensitive data, leading to more complex privacy-related attacks. They are also increasingly using encryption to hide their tracks and evade detection, making it more difficult for organizations to detect and respond to cyberattacks. New evasion techniques, such as fileless attacks and obfuscation, are on the rise, making it more challenging for security solutions to detect and prevent attacks.

Amidst this tough landscape, 2023 will be characterized by the additional challenge of economic uncertainty, inflation and financial stress. SISA's latest edition of the Top 5 Forensics Driven Learnings report comes at an appropriate time, as organizations try to prioritize improving business resilience and their security posture while navigating an uncertain climate.

With that in mind, let's revisit the genesis to the SISA Top 5: "Over the years, SISA has conducted numerous investigations, and our clients have been keen to learn from these experiences to enhance their security posture. These clients sought a list of controls with the highest likelihood of preventing a breach instead of implementing a complete set of controls, as they were already PCI DSS or ISO 27001 certified. SISA discovered that some breaches could be prevented while others could only be detected. Consequently, in 2020, SISA began compiling annual investigations, identifying controls that could prevent or detect breaches, and collaborated with payment brands to incorporate their findings. From this data, SISA devised a list of controls with the highest probability of preventing or detecting a breach, known as the SISA Top 5.

This annual initiative is based on the investigations and incident responses conducted by SISA every year".

In its 4th edition, the *SISA Top 5 Forensic-driven Learnings 2023-24* report presents a detailed analysis of cybersecurity breaches, focusing on unique cases that showcase uncommon or innovative intrusion methods. These incidents offer valuable insights into the constantly evolving threat landscape. The study examines trends across various stages of the cyber attack lifecycle, such as ingress, lateral movement, and action on objectives.

This comprehensive approach enables a deeper understanding of attackers' Techniques, Tactics, and Procedures (TTPs), empowering organizations to effectively prepare for and defend against such threats. Moreover, the report highlights the importance of implementing robust security controls through the SISA Top 5 to prevent or detect breaches at each stage.

To realize our vision of creating a digitally secure society, this report with insights from forensic investigations and incident responses is what I believe we all need to stay secure and prevail against the bad. Overall, this report serves as a call to action for organizations to prioritize cyber security and invest in the necessary controls to proactively defend against cyber threats. I hope you enjoy the report and find the information useful.

Happy reading and stay safe!



Dharshan Shanthamurthy

Founder & CEO, SISA

Introduction

Digital transformation and hybrid work environments continued to expose new vulnerabilities and more surfaces to cyber attacks, in 2022. Cyber adversaries were increasingly persistent, persuasive, and targeted. New research continues to reveal a familiar theme – diverse threats, threats bypassing traditional security solutions, increasing sophistication etc. While adversaries continued to evolve and the threat landscape gets increasingly treacherous, we at SISA too have been dedicated to combating cyber threats by helping clients investigate and contain breaches and supporting them in recovering from attacks.

Our casework revealed several significant trends in 2022

- 

Service providers were involved in more investigations than merchants due to the potential for a larger volume of card data in a single breach.
- 

Ransomware recovery cases increased fourfold compared to card data breach investigations, with 73% of these cases involving data exfiltration.
- 

All organizations examined for card breaches belonged to the Payment Industry and had implemented basic security hygiene practices. The average time to identify a breach spanned between 6 to 12 months while containing the breach took approximately three weeks.
- 

Industries involved in incident response and ransomware recovery cases (excluding Internal Forensic Investigations) included Payments (23%), Manufacturing (52%), IT/ITES/BPO (11%), and Telecommunications (12%).
- 

Breached organizations in the payment industry generally maintained a strong security posture but still required 6-12 months to detect a breach, typically after notification from a third party or payment brand.

A prominent new trend this year was the evolution of the Ransomware as a Service (RaaS) model. This model consists of multiple roles, such as Initial Access Brokers (IAB), Affiliates, Data Operators, and Ransomware Operators, each playing a crucial part in the ransomware attack chain.

IAB tactics have notably changed in RaaS operations, shifting from backdoor malware or web shells to using harvested credentials and Multi-Factor Authentication (MFA) for persistence. This method is harder to detect and provides better access to an organization's critical infrastructure. Consequently, the dark web market value for credentials with MFA persistence is more than three times higher than web shell malware or backdoors.

IABs have utilized various tactics to acquire credentials, such as phishing, deploying stealer malware, and purchasing credentials from the dark web. We also observed a 4.2X increase in the identification of stealer malware or its traces on compromised user devices.

MFA circumvention techniques included brute force attacks, social engineering, and insider collusion. MFA persistence was primarily achieved through brute force or social engineering, with only 1% of cases involving insider cooperation. Our red team successfully accessed networks using purchased credentials in 23% of cases.

In ransomware attacks, 11% of organizations opted to pay the ransom, while 89% did not. Recovery times varied based on the number of systems affected, with smaller organizations (less than 100 systems) taking 3-4 weeks and larger organizations (more than 100 systems) taking 4-7 weeks.

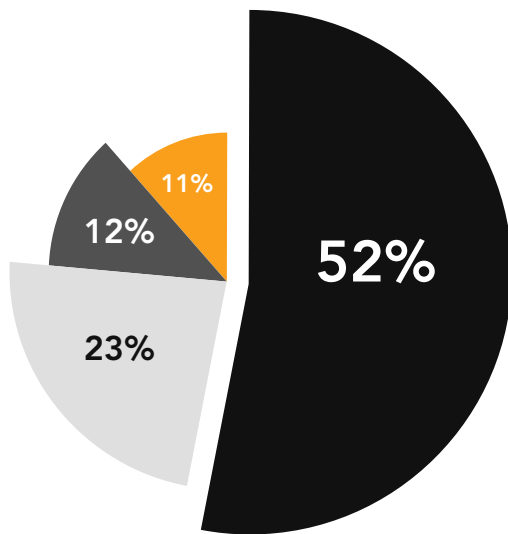


Report Coverage

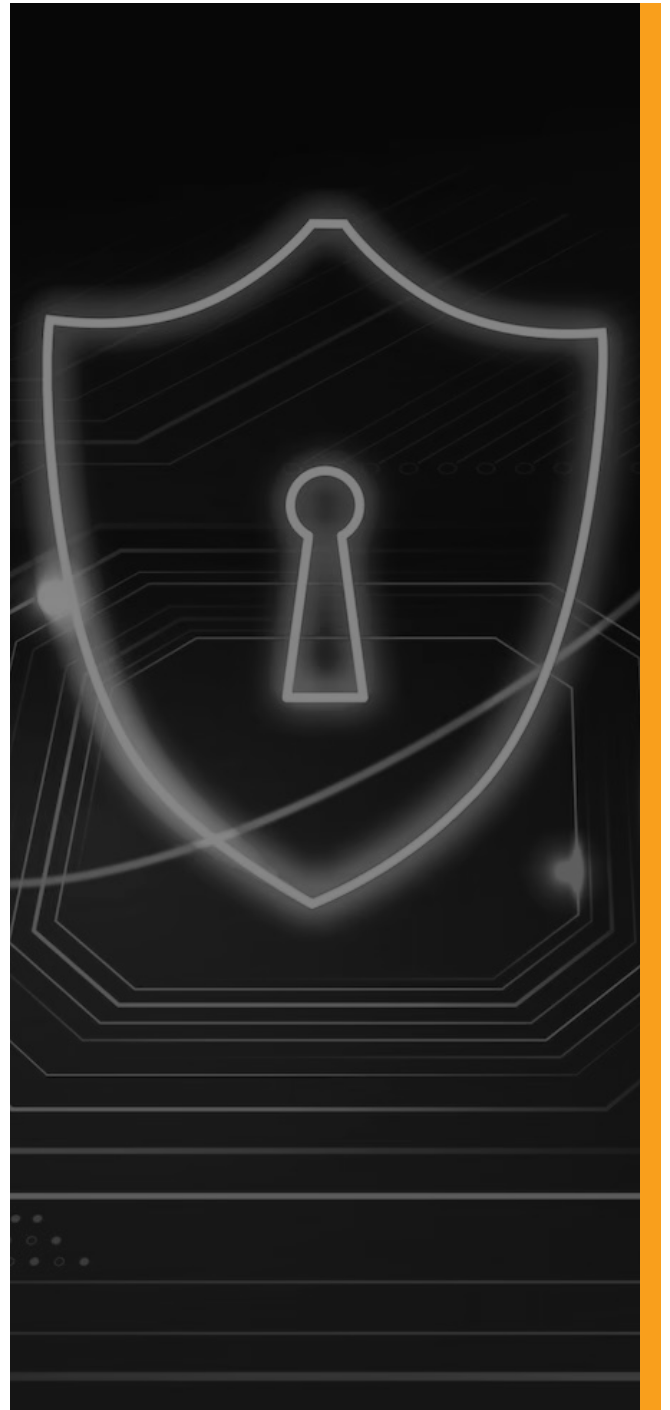
Throughout the year, we conducted 158 investigations and incident response activities, distributed as follows:



The industries we served for incident response and ransomware recovery activities were diverse. led by **Manufacturing (52%)**, **Payments (23%)**, **Telecommunications (12%)**, and **IT/ITES/BPO (11%)**.



It is essential to note that the security posture of manufacturing clients was frequently lacking, with some exhibiting almost no security hygiene.



Distinct Use Cases

As part of every forensic investigation we carry out, we collate the various methods through which the intruders have gained access to the system, performed lateral movements, and met their Action on Objective. Based on these details, we have shortlisted the common methods used by intruders under the following sections.

The next section includes a set of distinct use cases that go beyond the typical incidents and common ingress and egress methods. These unique scenarios feature unconventional ingress methods, where most controls might not prevent such incidents. The primary approach to handling these cases is early detection and containment.

MITRE created the **MITRE ATT&CK** framework to document attackers' tactics and techniques used in a breach. To simplify the attacker/intruder tactics, we have condensed the entire MITRE ATT&CK framework tactics into three categories. They are the Ingress Point, Lateral Movement, and Action on Objective.

- The **Ingress Point** deals with how the intruder can compromise the network and gain a foothold into the environment. The Ingress Point covers the first four tactics outlined in the MITRE ATT&CK framework.
- The **Lateral Movement** covers various tactics such as Privilege Escalation, Defence Evasion, Credential Access, Discovery, Collection, Command, and Control - the tactics mentioned in the MITRE ATT&CK framework.
- The **Action on Objective** covers the exfiltration and impact tactics defined in the MITRE ATT&CK.



Insider-assisted Ransomware Attack at a Manufacturing Enterprise

Scenario

A manufacturing client fell victim to a ransomware attack when an intruder bribed an administrator with cryptocurrency to manipulate the user's MFA authentication mechanism. During the user's 10-day absence, the administrator replaced the user's phone number with that of the intruder. The intruder then reset the user's O365 password, receiving the OTP on the new number. Following this, the intruder reset the user's domain and VPN credentials. Finally, the intruder accessed the network domain and deployed ransomware via the domain GPO.

Ingress

The intruder initially accessed the network by exploiting the user's MFA mechanism, allowing them to reset the user's O365 password.

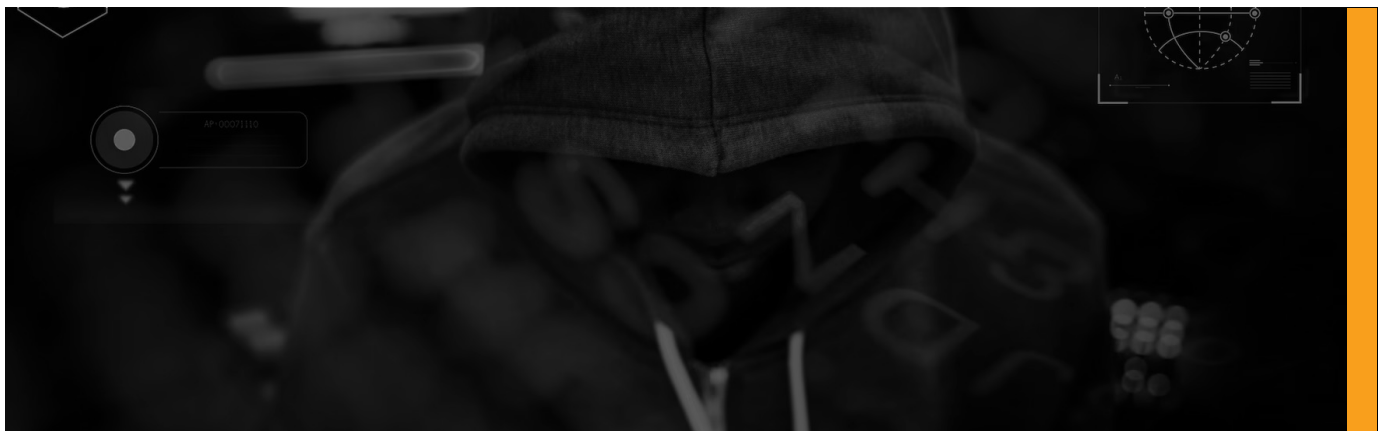
Lateral Movement

After compromising the user's account, the intruder reset the domain and VPN credentials to gain further access to sensitive data and systems within the network.

Action on Objective

The intruder's goal was to deploy ransomware using the domain GPO. They successfully achieved this by gaining access to the domain and utilizing the compromised credentials.

MITRE Tactic & Technique					
Ingress		Lateral Movement		Action on Objective	
Tactic	Technique	Tactic	Technique	Tactic	Technique
External Remote Services	Compromised MFA Mechanisms	Persistence	Valid Accounts	Impact	vData Encryption for Impact
		Lateral Movement	Remote Services		
		Execution	PowerShell		



MDR Detects MFA Brute Forcing Attack on a Payment Aggregator



Scenario

The MDR team discovered an unauthorized addition of a user to the domain administrator group, of a payment aggregator. Unable to provide a change request form, the client prompted an incident response. The analysis identified administrator "User A" as responsible, although they denied involvement. Investigating "User A's" system revealed credential stealer malware and disabled antivirus software. "User A" recalled receiving multiple MFA push notifications and accidentally approving one during a meeting.

The intruder, using credentials obtained via the malware, logged into the VPN and sent multiple MFA requests to "User A's" mobile application. Despite declining several requests, "User A" inadvertently granted access during a meeting. With "User A's" administrative privileges and stolen credentials, the intruder accessed the domain and other systems, adding their mobile details to the VPN MFA authentication application for persistence.

Detection occurred as the intruder attempted lateral movement and added a new user to the domain administrator group.



Ingress

The compromise of "User A's" system via credential stealer malware allowed the intruder to access the network using stolen VPN credentials.



Lateral Movement

The attacker, having gained network access, moved laterally to other systems, creating persistence by adding their mobile details to the VPN MFA authentication application.



Action on Objective

The intruder aimed to access the company network and systems by adding a new user to the domain administrator group. The MDR team detected lateral movement and the attempted new user addition, exposing the attacker's activities.

MITRE Tactic & Technique			
Ingress		Lateral Movement	
Tactic	Technique	Tactic	Technique
Initial Access	Valid Accounts	Lateral Movement	Valid Accounts
Credential Access	Two-factor Authentication Interception (by confusing the user into accepting the MFA prompt)	Defense Evasion	Persistence
Defense Evasion	Disabling Security Tools		

Ransomware Embedded in Application Code



Scenario

An e-commerce merchant with mobile and web applications fell victim to a ransomware attack. The company restored their systems from backups, but they were encrypted again within two days. The ransomware code was embedded within the application source code and stored in a cloud-based repository. The developers worked in a hybrid environment.



Ingress

The intruder accessed the code repository platform using stolen credentials from stealer malware deployed on the developers' systems. 5% of the analyzed systems had stealer malware. The client had not implemented MFA authentication for the source code repository application.



Lateral Movement

None observed in this scenario.



Action on Objective

The intruder injected ransomware script into the code repository. During deployment, the malicious script was executed in production, encrypting the systems. The systems were recovered by redeploying the application from the code repository, but the ransomware and scheduled task scripts remained in the code, causing repeated encryption. The ransomware script was deployed as a DLL during code deployment, and another script created a scheduled task to execute the DLL file.



Recovery

The environment was down for 1.5 months during the second attack, taking three weeks to identify the root cause and another month to review and remove malicious code components manually.



Recommendations

To implement MFA authentication for the code repository platform and review log retention periods to improve the client's security posture.



MITRE Tactic & Technique			
Ingress		Action on Objective	
Tactic	Technique	Tactic	Technique
Initial Access	Valid Accounts: The intruder used stolen credentials to access the code repository platform.	Data Encrypted for Impact: Intruder encrypted systems with ransomware to cause disruption.	Software Deployment Tools: Malicious DLL file was deployed during the code deployment process.
	Email Collection: Stealer malware collected email credentials, potentially used to access the code repository platform.		Scheduled Task/Job: The intruder used a scheduled task to execute the DLL file, encrypting the systems.

API-based Attack



Scenario

A service provider offering real-time point calculation and redemption services to banks experienced issues with the settlement, as points were being calculated or redeemed in unusual ways. Investigation revealed that the service provider used the same credential pattern for all banks' authentication and shared these with the banks, including the bank name as the username and "Bankname@123*" as the password. The API used for point calculation was publicly available, allowing the intruder to send requests by modifying parameters and authenticating with the credential pattern. The intruder sent malicious requests to update points for specific card sets, and since reward points were calculated in real-time, these points were used for subsequent transactions. This scenario highlights the importance of securing API authentication credentials and restricting access to publicly available APIs to prevent unauthorized access and attacks.



Ingress

The intruder accessed the publicly available service provider API and manipulated the point calculation parameters. The service provider used a predictable pattern for bank authentication credentials, with the bank name as the username and "Bankname@123*" as the password.



Lateral Movement

No lateral movement or evidence of malicious activity was found in either the bank or service provider networks.

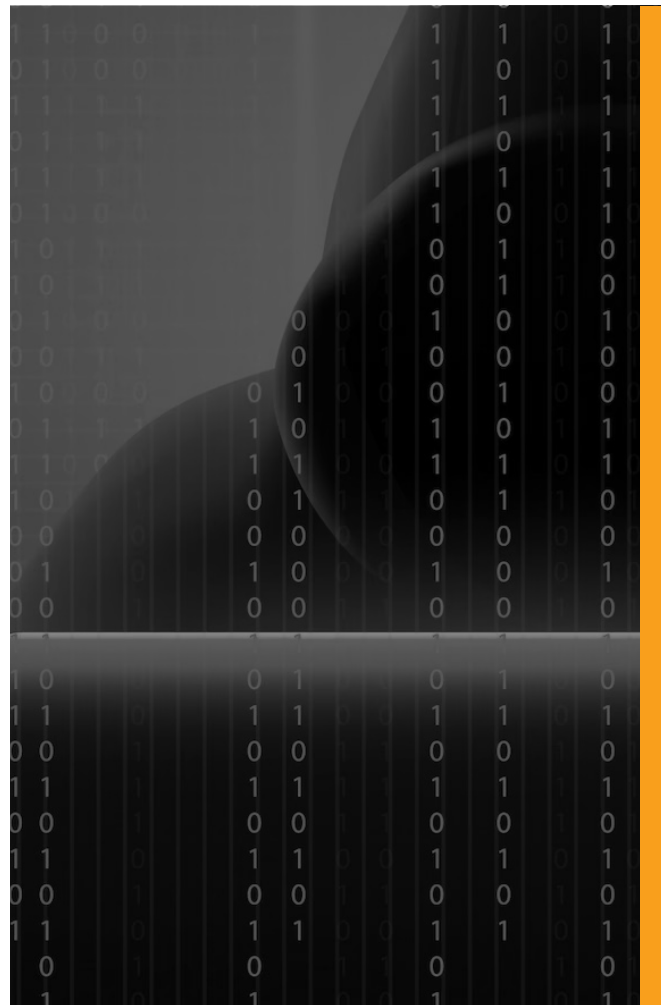


Action on Objective

The intruder sent malicious requests to update points for specific card sets. As reward points were calculated in real-time, these points were used for subsequent transactions.

Recommendations

Secure API authentication credentials, limit access to publicly available APIs and implement robust authentication methods to prevent unauthorized access and attacks.



Investigative Trends



Trends Observed in Ingress

During our investigations, we observed the following ingress trends:

Ingress Trends 2022



Remote Access (48%): Intruders utilized stolen credentials to access networks via remote services like VPN, application login, RDP, and SSH.

- **Phishing (32%):** Fraudulent emails or messages designed to trick users into revealing sensitive information remain a prevalent attack method.

- **Unpatched User System Vulnerabilities (10%):** In 10% of remote access cases, the malware was delivered through phishing emails containing malicious Microsoft Office documents with macro-based payloads, exploiting vulnerabilities in the Microsoft Office suite.

- **Social Engineering (17%):** Intruders used social engineering tactics to trick users into revealing MFA OTPs in 17% of remote access cases. Additionally, 24% of these cases involved MFA brute force, with intruders sending multiple MFA prompts to gain access.



Exploited System/Network Component Vulnerabilities (14%): In 14% of cases, intruders exploited vulnerabilities in internet-exposed systems to gain initial access.



Web Application Vulnerability (23%): In 23% of cases, web application layer vulnerabilities were exploited for initial access, with 'Malicious File Upload' being a common vulnerability.



Business Logic Vulnerability (7%): In 7% of cases, intruders exploited business logic vulnerabilities in mobile applications or API calls to conduct fraudulent transactions without gaining network access.

- **Weak or Default Passwords (55%):** In 55% of business logic vulnerability cases, intruders used guessable passwords to authenticate API requests and exploit vulnerabilities.



Supply Chain Attacks (1%): We investigated 1% of cases involving supply chain attacks, where the target's network was used to gain access to a client network.



Insider Threats (2%): In 2% of cases, insider threats initiated ingress, including sharing credentials with intruders upon leaving the organization or updating another user's phone number in the MFA device.



IoT Devices: In one case, we believe an IoT device was used for initial access, as retracing the intruder's steps led us to a network segment hosting IoT devices.



Cloud Misconfiguration (2%): In 2% of cases, data exfiltration resulted from cloud misconfigurations in S3 buckets.

In 23% of cases, web application layer vulnerabilities were exploited for initial access, with 'Malicious File Upload' being a common vulnerability.



Trends in Lateral Movement

We observed the following methods intruders used to create persistence within the network:

- 

Backdoors: Installing backdoors on compromised systems, providing persistent access. Web shells, deployed upon exploiting web application layer vulnerabilities, were the most common backdoors observed.
- 

Registry Keys: Creating registry keys that execute malicious code every time the system starts up, mainly observed in user systems.
- 

Service Installation: Installing services on target systems that execute malicious code on startup, mainly observed in user systems.
- 

Scheduled Tasks: Creating scheduled tasks that execute malicious code at specific times or intervals, mainly observed in compromised servers and for creating backdoors.
- 

Malicious DLLs: Replacing legitimate DLLs with malicious ones, executing code every time the system starts up, mainly observed in user systems.
- 

Malicious Scripts: Utilizing scripts, such as PowerShell or batch files, to create persistence and move laterally within the environment, mainly observed in compromised servers.


Intruders used the following methods for lateral movement within the network:


Windows Services that include PowerShell, PsExec, and WMIC to move laterally and connect to other systems within the network.

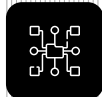
Remote Control Mechanisms that include TeamViewer, AnyDesk, and ScreenConnect. In some cases, these applications were already in use by the organization.


The commonly observed tools used by intruders to navigate client environments include:

- 

BloodHound: An open-source tool for identifying and exploiting Active Directory vulnerabilities.
- 

Cobalt Strike: Mainly observed for establishing command-and-control (C2) communication.
- 

Mimikatz: A tool for extracting credentials from system memory. Various custom versions of Mimikatz have been observed.
- 

PowerShell Empire: A framework built on PowerShell for executing post-exploitation tasks on compromised systems.
- 

File System Scanning Scripts: In 15% of cases, we identified scripts scanning the network for card numbers, PII data, and keywords like 'pass,' 'password,' and 'credentials.' In 23% of cases, we found files containing admin usernames and passwords stored in clear text or password-protected Excel files.



Trends in Action on Objective

Our investigation and incident response activities have revealed the most observed Actions on Objectives:

Action on Objectives Trends 2022



Ransomware Attack: In **73%** of the cases we supported, clients faced ransomware attacks where their entire environment was locked out or some of their systems were encrypted.

Data Breach



Card Data Breach: **14%** of cases involved PCI Forensic Investigations, in which payment brands identified the client's environment as a 'Common Purchase Point' and requested a PFI to investigate



PII Data Exfiltration: In **5%** of cases, the clients' or their customers' data were found on the dark web, prompting them to request a forensic investigation.



Fraudulent Transactions: **7%** of cases involved internal forensic investigations in which clients experienced fraudulent transactions on their platforms and sought to determine the cause.



Unauthorized Access to Sensitive Data: In **1%** of cases, intruders accessed sensitive applications containing confidential data, triggering incident response and internal forensic investigations.



SISA Top 5 Controls to Keep You Secure

The SISA Top 5 is a result of our extensive experience in investigating and responding to cyber incidents. We have established critical controls by analyzing each case and identifying ways to prevent or detect incidents. Our investigations and incident responses follow the SISA 4D approach to forensics-driven cybersecurity: **Deciphering, Deconstructing, Developing, and Disseminating** essential information across our service offerings. The SISA Top 5 controls below aim to strengthen an organization's security posture:



Faster Vulnerability Mitigation: Address and patch known vulnerabilities in systems and applications to minimize attack vectors.



Endpoint Protection: Protect user systems and servers by implementing security measures such as Endpoint Detection and Response (EDR) and DNS security solutions.



Intelligent Detection and Response: Utilize advanced threat detection and incident response capabilities to detect breaches and lateral movements early, enabling containment.



MFA Everywhere: Enforce Multi-Factor Authentication (MFA) across all systems and applications to improve access controls and prevent unauthorized access.



Attack Surface Reduction: Minimize exposed attack surfaces by reducing entry points and implementing robust security measures for all exposed points.



Faster Vulnerability Mitigation

Effective patch management is the most critical preventive measure organizations can implement against cyber threats.

Even the once-considered-safe Mac operating system has experienced exploitation of critical vulnerabilities. Though Microsoft's Windows operating system had the highest number of vulnerabilities identified last year, there has been a significant increase in vulnerabilities detected for various devices and applications.

In the dark web, exploits for vulnerabilities with a CVSS score of 7 become available within hours of a patch's release.

Some vulnerabilities are even actively exploited before vendors release patches.

Patch management can create conflicts between an organization's information security and IT teams. Ensuring all systems are patched with the latest security updates as the organization grows becomes more challenging. To address this challenge, we recommend the following patch management approach:

Patch Management Best Practices



Implement an automated, cloud-based patch management solution for all user systems.



Divide all other system components, including servers and network devices, into two categories.



For category one components, deploy patches with a CVSS score of 6.5 or above within a week.



For patches with a CVSS score below 6.5, organizations can follow best practices and deploy them every quarter for category one and two components.

Endpoint Protection

Most clients we investigated had deployed antivirus solutions; however, intruders are increasingly using custom-based malware that can easily evade traditional antivirus software. To extend their presence within an organization, attackers must bypass these defenses. We recommend deploying Endpoint Detection and Response (EDR) solutions rather than relying solely on antivirus software.

The primary difference between EDR and antivirus solutions lies in their capabilities to identify and respond to threats. EDR solutions detect malware, Trojans, backdoors, and web shells and identify malicious files that may have evaded antivirus detection by monitoring executed processes or commands through PowerShell, PsExec, WMIC processes, etc. If a team suspects malicious activity within a system through EDR, they can review suspicious files or processes and take appropriate action.

Many malware samples we reverse-engineered used the DNS protocol for exfiltrating data or establishing Command and Control (C2C) communication.

Implementing a DNS security solution to route traffic, particularly for remote systems, can prevent C2C communication, identify systems with malicious DNS traffic, and proactively contain threats to protect remote devices.

Recent trends indicate that remote systems have been actively exploited with credential-stealing malware. Intruders then use the stolen credentials to access the production network. Securing endpoint devices with EDR solutions and DNS security can significantly strengthen defenses against these threats and minimize the risk of unauthorized network access.

Intelligent Detection and Response

In 95% of analyzed cases, robust detection and response processes could have led to earlier identification and containment of breaches during the lateral movement stage.

Of the clients we worked with for investigation or incident response, 91% had a SIEM and some form of a monitoring team, with 40% having a mature monitoring process and team. However, there were areas for improvement in their capability to identify breaches:

Coverage: Only 6% of clients covered their entire environment for log collection and monitoring. While most clients covered their production environment, they often ignored non-critical environments like user segments and UAT. Intruders target these non-critical environments for initial access before moving to the production network.

Log Enrichment: Basic enrichment, such as mapping external IP addresses to geolocation and ASN, can help identify anomalies in user login processes. Long-tail analysis of geolocation and username aggregated for remote access (e.g., VPN) can reveal compromised user credentials and intrusion attempts.

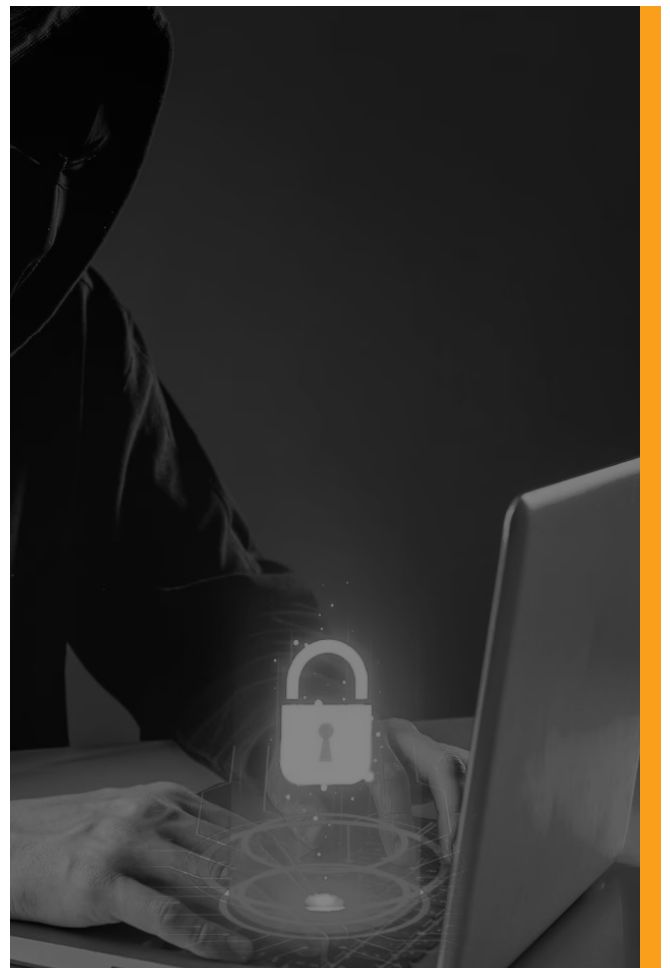
Use Cases for Log Types: 58% of clients captured logs but had not configured use cases for detecting unknown or malicious activity. A default set of use cases for each log type can help alert organizations to malicious activities within their network.

Threat Intelligence: Integrating threat intelligence, which consists of Indicators of Compromise (IOCs), can help organizations determine whether malicious communications or files are present within their network. Open-source and commercial threat intelligence sources can be integrated into existing SIEM solutions.

A critical process missing in 97% of clients was an incident playbook.

Most organizations needed a clearer plan for responding to alerts generated by the monitoring team. In many cases, clients focused on containing incidents in isolation and failed to identify the incident's root cause. Consequently, they missed the bigger picture, allowing breaches to continue.

Deception technology can help detect intruders or ransomware scanning the network. Instead of deploying commercial deception technology, organizations can implement cost-effective deception measures by creating fake card numbers and fake PII data and enabling folder-level auditing of specific files. Generating an alert if the file is accessed can indicate network compromise, allowing the organizations to respond proactively.



MFA Everywhere

Multi-Factor Authentication (MFA) is a crucial control for preventing data breaches and impeding lateral movement by intruders. By requiring users to provide two or more authentication factors to access a system or application, MFA adds an extra layer of security. Even if an attacker compromises a user's password, they cannot gain access without the second factor, such as a code generated by a mobile device or biometric data.

OTP (One-Time Password) based MFA solutions offer greater security than those that prompt users to accept authentication.

OTP-based MFA requires users to input a unique password generated by a token or mobile application, valid only for a short period (typically 30 seconds). This prevents reuse and ensures attackers cannot access the system or application without the OTP. In contrast, MFA solutions relying on user-approved authentication are more vulnerable to social engineering attacks, where attackers may deceive users into approving fake authentication requests.

Implementing MFA for all access points, including remote access, VPN, email, SaaS applications, code repository applications, and any other system or application requiring authentication, is vital. Remote access, which allows users to connect to the corporate network from outside the organization's perimeter, is particularly vulnerable. By implementing MFA for remote access, organizations can significantly mitigate the risk of unauthorized access from external threats.

Organizations increasingly use SaaS applications, code repository applications, and other cloud-based services to manage critical data and applications, so implementing MFA for these services is essential. MFA protects sensitive information and ensures only authorized users can access these resources.

Attack Surface Reduction

An attack surface includes any entry point an attacker can exploit to gain unauthorized access to an organization's systems or data. Attack surfaces extend beyond firewalls to encompass all applications with web interfaces. Organizations' attack surfaces have expanded to include mobile and web applications, cloud infrastructure, Internet of Things (IoT) devices, remote workforces' systems, and a growing list of APIs.

There has been a 37% increase in intruders exploiting unknown web interfaces and API calls that information security teams were unaware and for which they had not deployed controls.

As a starting point, organizations can use open-source API discovery tools to identify various API calls within their network. With domain names, organizations can employ applications like Shodan.IO to detect exposed interfaces.

After documenting the complete inventory, organizations should consider implementing necessary controls to secure each exposed attack surface area. One crucial control is routing all web-based traffic through a web application firewall, which can protect against web application-based attacks.

Another essential control is conducting a comprehensive web application layer penetration test, covering all API calls, to identify both web application vulnerabilities and application business logic vulnerabilities. This thorough assessment helps organizations fortify their attack surfaces and protect their systems and data from unauthorized access.

Concluding the 4th Edition of Top 5

In conclusion, SISA's investigation into the attackers' Techniques, Tactics, and Procedures (TTPs) has revealed the severity of the impact that such incidents can have on organizations including their customers and stakeholders. Threats and breaches are a present reality that must be tackled with urgency and diligence.

The Top 5 controls are the foundation to establishing a robust cyber security posture, that can help organizations remain vigilant and continuously adapt to stay ahead of potential attackers.

Our effort to disseminate forensics based learnings is critical to fostering a culture of cyber security awareness. It aims to arm everyone from top-level executives to front-line employees with an understanding of the risks and propels them to take an active role in protecting the organization.

Cybersecurity is not a cost, it's an investment in the future. Invest in the right strategy and controls to create a secure digital society.



About SISA

SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective cybersecurity solutions. Our problem-first, human-centric approach helps businesses strengthen their cybersecurity posture. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

SISA is one of the leading global forensic investigators for the payments industry.

Compliance	Security Testing	Cyber Resilience	Data Governance	Cyber Academy
<p>Payment Data Security</p> <ul style="list-style-type: none"> • PCI DSS • PCI PIN • PCI 3DS • PCI P2PE • PCI S3 • PCI S-SLC • PCI CP (Card Production) • Facilitated PCI SAQ • Quarterly Health Check-ups • Central Bank Compliance • SWIFT <p>Strategy and Risk</p> <ul style="list-style-type: none"> • CCPA • GDPR • HIPAA • ISO • NIST • SOC 1 • SOC 2 • Cloud Security 	<p>Application Security</p> <ul style="list-style-type: none"> • Application Penetration Testing • CREST/CERT-in Approved Security Testing • API Security Testing • Secure Code Review <p>Network Security</p> <ul style="list-style-type: none"> • Vulnerability Assessment • Penetration Testing • Configuration Review • Red Teaming Exercise • Firewall Rule Review • PCI ASV Scan • Phishing Simulation <p>Hardware and IoT Security Testing</p> <ul style="list-style-type: none"> • Firmware Security Testing • Hardware/Embedded Security Testing • IoT Network Security Testing • IoT/Embedded Application and Management Layer Security Testing 	<p>Managed Detection and Response Solution – SISA ProACT</p> <ul style="list-style-type: none"> • Monitoring • Attack Simulation • Use-case Factory • Advanced Threat Hunting <p>Digital Forensics and Incident Response</p> <ul style="list-style-type: none"> • Incident Response / Compromise Assessment Services • Forensic Readiness Audit • Forensic and Incident Response Retainer Service • Payment Forensics Investigation • Internal Forensics Investigation • Ransomware Simulation 	<p>Data Discovery and Classification - SISA Radar</p> <ul style="list-style-type: none"> • Card Data Discovery • PII (Privacy) Discovery • Data Classification • Data Masking/Encryption <p>Data Security as a Service</p>	<p>Payment Data Security Implementation</p> <ul style="list-style-type: none"> • CPISI • CPISI Advanced • CPISI-D (Developers) <p>Security Incident Detection and Response Programs</p> <ul style="list-style-type: none"> • CIDR <p>Cybersecurity Awareness</p> <p>Forensic Learning Sessions for Senior Management</p>

USA | Canada | UK | Bahrain | Saudi Arabia | UAE | Qatar | India | Singapore | Malaysia | Australia

To learn more about SISA's offerings visit us at www.sisainfosec.com or Contact your SISA sales representative at contact@sisainfosec.com