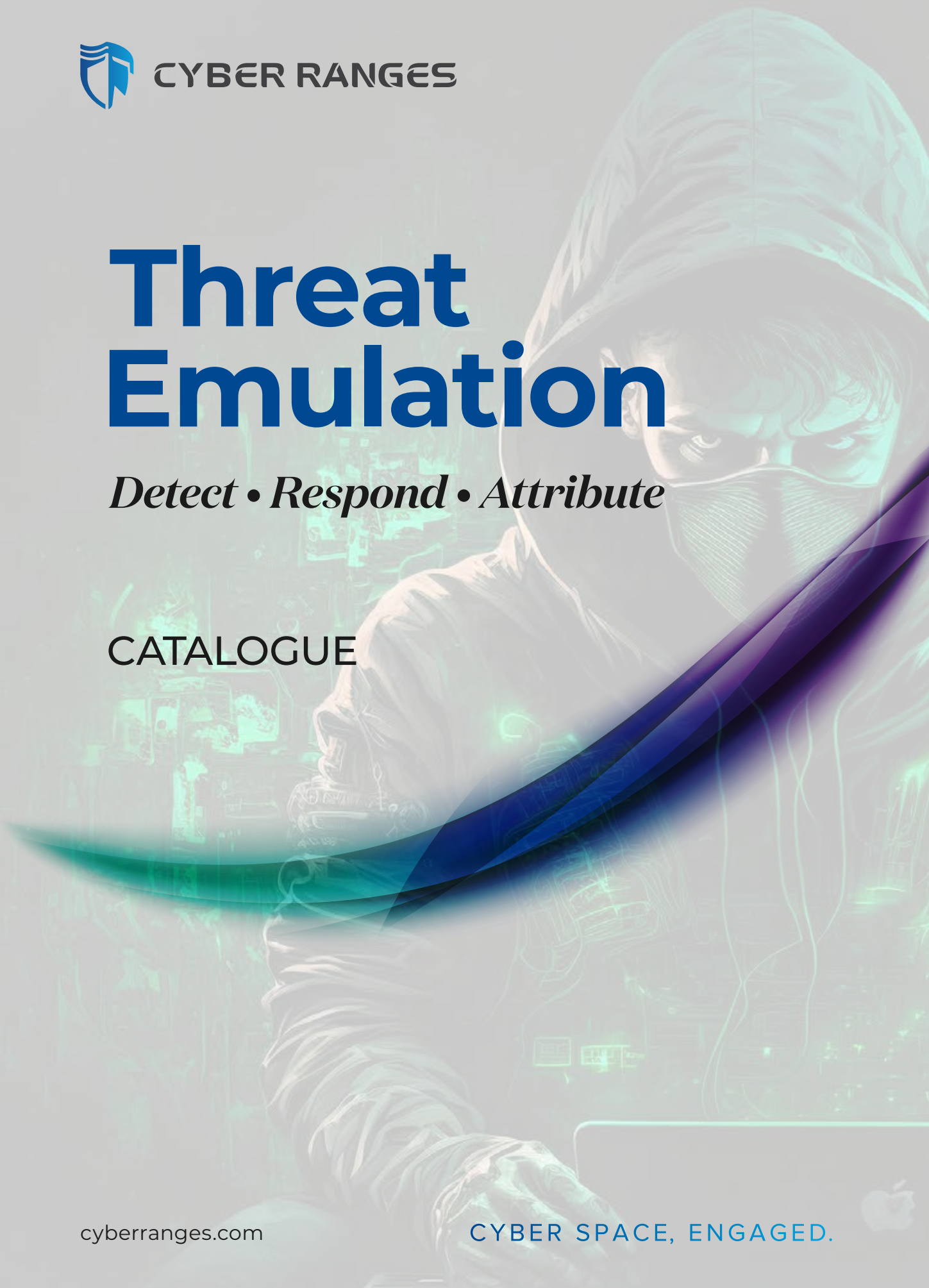
CYBER RANGES

Threat Emulation

Detect • Respond • Attribute

CATALOGUE



cyberranges.com

CYBER SPACE, ENGAGED.

Contents

1 Supply Chain Attack

THREAT ACTOR: **Indrik Spider**

THREAT TYPE: **Ransomware**

ATTACKER TOOLS: **WastedLocker, Cobalt Strike**

THREAT RATING: **High**

THREAT IMPACT:
- **Money Theft**
- **Data Exfiltration**
- **Service Availability**

DIFFICULTY: **Intermediate**

Scenario Description

In a sophisticated attack, an attacker adeptly employs spear phishing to compromise a software development team member within a targeted organization. This initial breach enables the attacker to infect both the team member's system and several deployed code servers. Subsequently, the attacker establishes a command-and-control connection, facilitating lateral movement through the network. This progression culminates in the compromise of the core banking application, allowing the attacker to successfully conduct fraudulent transactions. Following the fund transfer, the attacker deploys ransomware across the network and sends extortion emails to multiple accounts, demanding payment to prevent the exposure of exfiltrated data.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Develop Capabilities - T1587
- Phishing mail – T1566
- User Execution – T1204
- Supply Chain Compromise - T1195
- Command and Scripting Interpreter: Windows Command Shell - T1059.003
- System Network Connections Discovery - T1049
- Steal Application Access Token - T1528
- Create Account: Domain Account - T1136.002
- Valid Accounts: Domain Accounts - T1078.002
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder - T1547.001
- Input Capture: Keylogging - T1056.001
- Application Window Discovery - T1010
- Exfiltration Over C2 Channel - T1041
- Use Alternate Authentication Material: Application Access Token - T1550.001
- Data Encrypted for Impact – T1486

2 Hunting Threats

THREAT ACTOR: **APT33**

THREAT TYPE: **Espionage**

ATTACKER TOOLS: **Cobalt Strike, Mimikatz**

THREAT RATING: **High**

THREAT IMPACT:
- **Data Exfiltration**

DIFFICULTY: **Intermediate**

Scenario Description

A start-up named BigTapTech has been breached. A recent update of the firewall configuration by the network administrator has left some of the internal systems exposed to the public Internet.

Threat actors successfully gained access to one of the exposed assets and from there they were able to quickly compromise other systems, elevate privileges and finally compromise the entire Active Directory domain of the company.

In this scenario, you play the role of a SOC analyst, monitoring the network of the organization as the attack from the threat actor unfolds under your own eyes. Your objective is to detect and respond to the security attack.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Active Scanning - T1595
- Brute Force – T1110
- Command and Scripting Interpreter: Windows Command Shell - T1059.003
- System Network Connections Discovery - T1049
- Exploitation for Privilege Escalation – T1068
- Scheduled Task/Job: Scheduled Task - T1053.005
- OS Credential Dumping – T1003
- Remote Services: SMB/Windows Admin Shares - T1021.002
- Steal or Forge Kerberos Tickets: Golden Ticket - T1558.001
- Exfiltration Over C2 Channel – T1041

3 BGP Hijack Attack

THREAT ACTOR: **Aoqin Dragon**

THREAT TYPE: **Espionage**

ATTACKER TOOLS: **Mongall**

THREAT RATING: **High**

THREAT IMPACT:
- **Data Exfiltration**
- **Service Availability**

DIFFICULTY: **Intermediate**

Scenario Description

The scenario is based around a user who is phished and inadvertently introduces vulnerabilities into a telecommunication organization. The user is phished from their personal Gmail and following the instructions in the mail claiming to be from the local tax revenue authority ends up downloading and installing malware on their machine, which becomes the entry point for the threat actor.

Once inside the network, the attackers are able to move laterally and eventually compromise the edge router and route traffic to their malicious router, effectively denying network communications between router A and router B through a BGP hijack attack.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Develop Capabilities - T1587
- Phishing mail - T1566
- User Execution - T1204
- Command and Scripting Interpreter: Windows Command Shell - T1059.003
- System Network Connections Discovery - T1049
- Remote System Discovery - T1018
- Valid Accounts: Domain Accounts - T1078.002
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder - T1547.001
- Remote Services - T1021
- Exfiltration Over C2 Channel – T1041
- Adversary-in-the-Middle - T1638

4 The Hunt - EMOTET

THREAT ACTOR: **Wizard Spider**

THREAT TYPE: **Ransomware**

ATTACKER TOOLS: **Emotet, Cobalt Strike**

THREAT RATING: **High**

THREAT IMPACT:
- **Data Exfiltration**

DIFFICULTY: **Intermediate**

Scenario Description

An organization undergoes a spear-phishing attack involving malicious office documents known to be associated with the Emotet malware strain.

As a security analyst at the organization, you are tasked to investigate and analyze the attack.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Develop Capabilities - T1587
- Phishing: Spearphishing Attachment - T1566.001
- User Execution - T1204
- Windows Management Instrumentation - T1047
- Defense Evasion – TA0005
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder - T1547.001
- Email Collection: Local Email Collection - T1114.001
- Account Discovery: Email Account - T1087.003
- Compromise infrastructure - T1584

5 Active Directory Compromise

THREAT ACTOR:	THREAT TYPE:	ATTACKER TOOLS:	THREAT RATING:	THREAT IMPACT:	DIFFICULTY:
APT33	**Espionage**	**Cobalt Strike**	**High**	• **Data Exfiltration**	**Intermediate**

Scenario Description

An attacker has managed to gain network-level access into the internal network and is performing different attacks against your Active Directory environment.

As a security analyst with access to real-time logs, can you detect what the attacker is doing against your Windows workstations and servers?

As an analyst for the Hogwarts domain you are tasked with performing log analysis in order to detect various attacks against your Active Directory environment.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Active Scanning - T1595
- Brute Force - T1110
- Valid Accounts: Domain Accounts - T1078.002
- Compromise infrastructure - T1584
- System Service Discovery – T1007
- OS Credential Dumping – T1003
- System Services: Service Execution - T1569.002
- Steal or Forge Kerberos Tickets - T1558
- Obtain Capabilities: Malware - T1588.001
- Exploitation for Privilege Escalation – T1068
- Exfiltration Over C2 Channel – T1041

6 APT40

THREAT ACTOR:	THREAT TYPE:	ATTACKER TOOLS:	THREAT RATING:	THREAT IMPACT:	DIFFICULTY:
APT40	**Espionage**	**Cobalt Strike**	**High**	• **Data Exfiltration**	**Intermediate**

Scenario Description

This scenario mimics the tactics used by APT40 during their operations. The campaign leveraged spear-phishing emails that contained links to lookalike domains, created to mimic or resemble the domains of legitimate companies.

In some cases, the threat actors leveraged hijacked credentials, to gain access to legitimate mail servers and then launch spear-phishing campaigns from within the victim entity or at other targeted entities once the threat actors gained a foothold in the victim environment.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Develop Capabilities - T1587
- Phishing - T1566
- User Execution - T1204
- Software Deployment Tools – T1072
- Remote System Discovery - T1018
- Remote Services: SMB/Windows Admin Shares - T1021.002
- Server Software Component: Web Shell - T1505.003
- Gather Victim Host Information - T1592
- Account Manipulation - T1098
- OS Credential Dumping – T1003
- Use Alternate Authentication Material: Pass the Hash - T1550.002
- Exfiltration Over C2 Channel – T1041

7 XCall Center Under Attack

THREAT ACTOR: **Wizard Spider**

THREAT TYPE: **Ransomware**

ATTACKER TOOLS: **Cobalt Strike**

THREAT RATING: **High**

THREAT IMPACT: • **Data Exfiltration**

DIFFICULTY: **Intermediate**

Scenario Description

XCallCenter has been caught off guard by constant attacks on its infrastructure and its stakeholders are increasingly worried that they have been targeted by unknown assailants.

The IT department has taken appropriate steps to ensure visibility throughout the network, but lack they lack the knowledge to understand and respond to security incidents.

Your team of experts has been called in to manage the monitoring and incident response of the organization until a suitable replacement can be found.

You are tasked with identifying and tracing the attacker's action on the network.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Active Scanning - T1595
- Exploit Public-Facing Application – T1190
- Remote Services: SSH - T1021.004
- Server Software Component: Web Shell - T1505.003
- Gather Victim Host Information - T1592
- Brute Force - T1110
- Remote Services: SMB/Windows Admin Shares - T1021.002
- Lateral Tool Transfer - T1570
- Exfiltration Over C2 Channel – T1041

8 GISEC – The Hunt

THREAT ACTOR: **MuddyWater**

THREAT TYPE: **Espionage**

ATTACKER TOOLS: **Koadic**

THREAT RATING: **High**

THREAT IMPACT: • **Data Exfiltration**

DIFFICULTY: **Intermediate**

Scenario Description

XCallCenter has been caught off guard by constant attacks on its infrastructure and its stakeholders are increasingly worried that they have been targeted by unknown assailants.

The IT department has taken appropriate steps to ensure visibility throughout the network, but lack the knowledge to understand and respond to security incidents.

Your team of experts has been called in to manage the monitoring and incident response of the organization until a suitable replacement can be found.

MITRE ATT&CK® TTPs:

- Exploit Public-Facing Application – T1190
- Brute Force - T1110
- Valid Accounts: Domain Accounts - T1078.002
- Compromise infrastructure - T1584
- Active Scanning - T1595
- Phishing email - T1566
- Account Manipulation - T1098
- Exploitation for Privilege Escalation – T1068
- Remote Services: SSH - T1021.004

9 Silverthorn Power Plant Attack

THREAT ACTOR: **Lazarus Group**

THREAT TYPE: **Ransomware**

ATTACKER TOOLS: **Dtrack**

THREAT RATING: **High**

THREAT IMPACT:
- **Data Exfiltration**
- **Service Availability**

DIFFICULTY: **Intermediate**

Scenario Description

An attacker successfully sends a phishing mail with link to a backdoored putty setup to a user.

The user downloads and runs the backdoored putty file and the attacker manages to gain code execution on the server and establish C2 comms.

The attacker can run various commands and enumerate various information on the workstation. The attacker was able to get the IP address, perform keylogging (capturing user credentials), list shares in the network, list running processes, list contents of the shares, exfiltrate contents in the shares, and retrieve browser history.

MITRE ATT&CK® TTPs:

- Develop Capabilities: Malware - T1587.001
- Phishing: Spearphishing Attachment - T1566.001
- User Execution: Malicious File - T1204.002
- Gather Victim Host Information - T1592
- Gather Victim Network Information - T1590
- Account Discovery: Domain Account - T1087.002
- Exfiltration Over C2 Channel - T1041
- Data Destruction - T1485
- Data Encrypted for Impact - T1486
- Abuse Elevation Control Mechanism: Bypass User Account Control - T1548.002
- Access Token Manipulation - T1134
- Command and Scripting Interpreter: Windows Command Shell - T1059.003
- Inhibit System Recovery - T1490

10 Winter Vivern

THREAT ACTOR: **Winter Vivern**

THREAT TYPE: **Espionage**

ATTACKER TOOLS: **Exfil Mail Server**

THREAT RATING: **High**

THREAT IMPACT:
- **Data Exfiltration**

DIFFICULTY: **Easy**

Scenario Description

An attacker launches a targeted phishing campaign leveraging a cross-site scripting vulnerability in the Roundcubel client.

The IT Officer of the targeted organization triggers the payload to execute and the mails from their account are exfiltrated to the attackers server.

From the exfiltrated data the attacker is able to retrieve credential material allowing them to access one of the targeted organizations external facing server.

MITRE ATT&CK® TTPs:

- Develop Capabilities: Exploits - T1587.004
- Spearphishing with a link - T1566.002
- User Execution: Malicious Link - T1204.001
- Account Discovery - T1087
- Exfiltration Over C2 Channel - T1041
- Remote Services: SSH - T1021.004
- Abuse Elevation Control Mechanism - T1548

11 Network Compromise to Ransomware Attack

THREAT ACTOR:	THREAT TYPE:	ATTACKER TOOLS:	THREAT RATING:	THREAT IMPACT:	DIFFICULTY:
MuddyWater	**Ransomware**	**Koadic, Mimikatz**	**High**	• **Data Exfiltration**	**Difficult**

Scenario Description

The scenario is based around the network compromise of an organization from a vulnerable website/webserver allowing the attacker to infiltrate the organization and move laterally and disrupt the backup procedure of the organization and rolling out of ransomware across the various endpoints on the network.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Exploit Public-Facing Application – T1190
- Command and Scripting Interpreter - T1059
- Defense Evasion - TA0005
- Gather Victim Host Information - T1592
- Process Discovery - T1057
- OS Credential Dumping – T1003
- File And Directory Discovery - T1083
- Remote System Discovery - T1018
- Account Discovery: Domain Account - T1087.002
- Permission Groups Discovery: Domain Groups - T1069.002
- Valid Accounts: Domain Accounts - T1078.002
- Windows Management Instrumentation - T1047
- Exfiltration Over C2 Channel – T1041
- Archive Collected Data - T1560
- Data Destruction - T1485

12 Contact Us

THREAT ACTOR:	THREAT TYPE:	ATTACKER TOOLS:	THREAT RATING:	THREAT IMPACT:	DIFFICULTY:
MuddyWater	**Espionage**	**Koadic, Mimikatz**	**High**	• **Data Exfiltration**	**Intermediate**

Scenario Description

An attacker exploits a web server vulnerability that exposes a configuration file, obtaining credentials to breach a company's internal server. With access secured, the attacker deploys agents onto employee desktops, communicating sensitive data to a Command-and-Control (C2C) server.

After post-exploitation activities, the resulting damage includes webpage defacement and the publication of company files containing compromising information. The attacker then demands a ransom from the company to prevent further leaks of such documents to the public.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Active Scanning - T1595
- Exploit Public-Facing Application – T1190
- Command and Scripting Interpreter - T1059
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder - T1547.001
- System Shutdown/Reboot - T1529
- Gather Victim Host Information - T1592
- Input Capture: Keylogging - T1056.001
- System Information Discovery - T1082
- Input Capture: Keylogging - T1056.001
- Valid Accounts: Domain Accounts - T1078.002
- Application Window Discovery - T1010
- Remote System Discovery - T1018
- Remote Services: SMB/Windows Admin Shares - T1021.002
- Exfiltration Over C2 Channel – T1041
- Archive Collected Data - T1560

13 Insurance Company Under Attack

THREAT ACTOR: **MuddyWater**

THREAT TYPE: **Espionage**

ATTACKER TOOLS: **Metasploit, Mimikatz**

THREAT RATING: **High**

THREAT IMPACT: • **Data Exfiltration**

DIFFICULTY: **Easy**

Scenario Description

The scenario simulates a network compromise to an insurance firm through an unpatched WordPress server allowing the attacker to infiltrate the organization and escalate privileges to Domain Administrator.

Your objective as a security analyst at the organization is to analyze and detect the attack.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Active Scanning - T1595
- Exploit Public-Facing Application – T1190
- Command and Scripting Interpreter - T1059
- Gather Victim Host Information - T1592
- Account Discovery: Domain Account - T1087.002
- Process Discovery - T1057
- Password Policy Discovery - T1201
- Remote System Discovery - T1018
- Permission Groups Discovery: Domain Groups - T1069.002
- Valid Accounts: Domain Accounts - T1078.002
- OS Credential Dumping – T1003
- Brute Force: Password Cracking - T1110.002
- Account Manipulation - T1098
- Steal or Forge Kerberos Tickets - T1558
- Compromise infrastructure – T1584
- Windows Management Instrumentation - T1047

14 Ransomware Rampage

THREAT ACTOR: **LockBit**

THREAT TYPE: **Ransomware**

ATTACKER TOOLS: **Custom Ransomware**

THREAT RATING: **High**

THREAT IMPACT: • **Data Exfiltration** • **Service Availability**

DIFFICULTY: **Intermediate**

Scenario Description

An attacker exploits an SMB server within the corporate DMZ, leading to the establishment of command-and-control communication. Operating system credentials are extracted from the compromised server, providing valid usernames and corresponding hashes. This information enables the attacker to execute a credential-stuffing attack on the corporate LAN, permitting login to a single workstation through a standard user account. Once within the LAN, the attacker leverages an unquoted service path vulnerability to elevate privileges to NT\Authority. Further exploitation involves additional operating system hash extraction. With the obtained credentials, the attacker initiates a ransomware deployment on the LAN workstations.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Active Scanning - T1595
- Brute Force - T1110
- Gather Victim Identity Information - T1589
- Command and Scripting Interpreter - T1059
- OS Credential Dumping – T1003
- System Owner User Discovery - T1033
- Remote System Discovery - T1018
- Account Discovery: Domain Account - T1087.002
- Permission Groups Discovery - T1069
- Valid Accounts: Local Accounts - T1078
- Valid Accounts: Domain Accounts - T1078.002
- Exploitation for Privilege Escalation – T1068
- Compromise infrastructure - T1586
- Archive Collected Data - T1560
- Data Encrypted for Impact - T1486

15 Wizard Spider

THREAT ACTOR: **Wizard Spider**

THREAT TYPE: **Ransomware**

ATTACKER TOOLS: **Ryuk, Emotet**

THREAT RATING: **High**

THREAT IMPACT:
- **Data Exfiltration**
- **Service Availability**

DIFFICULTY: **Intermediate**

Scenario Description

During a successful phishing campaing, a threat actor establishes C2 comms after a staff member of a targetted organization opens an Emotet maldoc. Once the attacker obtained communication on the workstation they managed to discover other assets on the network and successfully exploit vulnerabilities enumerated allowing for them to move laterally within the network. The attacker is able to exfiltrate sensitive medical records of patients as well as destroy backups before rolling out of their ransomware and threatening to expose the information collected.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Develop Capabilities - T1587
- Phishing: Spearphishing Attachment - T1566.001
- User Execution - T1204
- Defense Evasion - TA0005
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder - T1547.001
- Process Discovery - T1057
- Gather Victim Host Information - T1592
- Compromise Client Software Binary - T1554
- Password Policy Discovery - T1201
- Permission Groups Discovery: Domain Groups - T1069.002
- Account Discovery: Domain Account - T1087.002
- Remote System Discovery - T1018
- Valid Accounts: Local Accounts - T1078
- Windows Management Instrumentation - T1047
- Steal or Forge Kerberos Tickets - T1558
- OS Credential Dumping – T1003
- Compromise infrastructure – T1584
- Exfiltration Over C2 Channel – T1041
- Data Encrypted for Impact- T1486

16 Atom Silo

THREAT ACTOR: **Atom Silo**

THREAT TYPE: **Ransomware**

ATTACKER TOOLS: **Atom Silo Ransomware**

THREAT RATING: **High**

THREAT IMPACT:
- **Data Exfiltration**

DIFFICULTY: **Intermediate**

Scenario Description

After a network configuration change, an application endpoint is exposed to the internet. Attackers successfully exploits a vulnerability on the exposed endpoint and gain code execution. They are able to bring additional malware on to the target and establish C2 communication.

The attackers then proceed to perform post-exploitation procedures to gain privileges and move laterally accross various infrastructures on the organization's internal networks.

Once they have achieved the escalation objective, they proceed to deploy ransomware across the workstations of the network.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Active Scanning - T1595
- Exploitation of Remote Services - T1210
- Valid Accounts: Domain Accounts - T1078.002
- Deploy Container - T1610
- Command and Scripting Interpreter - T1059
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder - T1547.001
- Exfiltration Over C2 Channel – T1041
- Impair Defenses: Disable or Modify Tools - T1562.001

17 Attacker In the Middle

THREAT ACTOR:
Lazarus Group

THREAT TYPE:
Ransomware

ATTACKER TOOLS:
Proxy Mail Server Wannacry

THREAT RATING:
High

THREAT IMPACT:
- **Data Exfiltration**
- **Service Availability**

DIFFICULTY:
Hard

Scenario Description

An attacker successfully phishes an IT officer at the targeted organization and is able to get access to a Windows file share server as this user.

On this beachhead server, they can use legitimate software to execute their payload as well as set persistence using a link file. They can then gain access to the load balancer on the network from where they move further laterally into the network.

Additionally, from the compromised email account, the attacker is able to perform spear phishing attacks against privileged users. After that, the attacker is able to disrupt operations by bringing down the load balancer but before that, they exfiltrate data, disable privileged accounts, roll out ransomware and partially delete files.

They then demand for a ransom after rolling out ransomware to the rest of the network.

MITRE ATT&CK® TTPs:

- Spearphishing with a link - T1566.002
- Proxy - T1090
- User Execution: Malicious Link - T1204.001
- Browser Session Hijacking - T1185
- Account Discovery - T1087
- Remote Access Software - T1219
- Boot or Logon Autostart Execution - T1547
- Hijack Execution Flow: DLL Side-Loading - T1574.002
- Active Scanning - T1595
- External Proxy - T1090.002
- Bidirectional Communication - T1102.002
- Ingress Tool Transfer - T1105
- Spearphishing with a link - T1566.002
- Input Capture: Keylogging - T1056.001
- Exploitation of Remote Services - T1210
- Server Software Component: Webshell - T1505.003
- Account Discovery: Domain Account - T1087.002
- OS Credential Dumping - T1003
- Exfiltration Over C2 Channel - T1041
- Network Denial of Service - T1498
- Disk Wipe - T1561
- Data Encrypted for Impact - T1487
- Account Access Removal - T1531

18 Someone Got Phished

THREAT ACTOR:
Wizard Spider

THREAT TYPE:
Ransomware

ATTACKER TOOLS:
Emotet

THREAT RATING:
High

THREAT IMPACT:
- **Money Theft**
- **Data Exfiltration**

DIFFICULTY:
Easy

Scenario Description

As a dedicated security analyst at an organization, you are tasked with investigating a sophisticated and ongoing security incident. A highly skilled threat group has initiated a malicious campaign specifically targeting financial institutions, with your organization squarely in their sights. This group employs advanced spear-phishing tactics, meticulously crafting emails to impersonate trusted sources, deceiving bank employees into divulging sensitive credentials.

Your mission as the organization's vigilant defender is critical. Armed with comprehensive access to corporate system logs and advanced forensic tools, you are responsible for unravelling this intricate campaign. You must identify the breach's origin, understand the attacker's techniques, and neutralize their access to prevent further exploitation. It is a race against time to safeguard customer data and protect the organization's assets from this hidden adversary.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Develop Capabilities - T1587
- Phishing mail – T1566
- User Execution – T1204
- Command and Scripting Interpreter: Windows Command Shell - T1059.003
- System Network Connections Discovery - T1049

19 Alloy Taurus

THREAT ACTOR:
Alloy Taurus

THREAT TYPE:
Ransomware

ATTACKER TOOLS:
Cobalt Strike, Mimikatz

THREAT RATING:
High

THREAT IMPACT:
- **Money Theft**
- **Data Exfiltration**

DIFFICULTY:
Hard

Scenario Description

In a covert breach, an unsuspecting bank employee downloaded an application, unknowingly opening the door to a sophisticated cyber attack. This concealed software, leveraging a well known vulnerability, established stealthy Command and Control (C2) communications on boot-up. The attacker, having compromised the initial system, began mapping out the lay of the land and establish potential attack paths. Leveraging covert techniques, the attacker maneuvered through critical network nodes, reaching a gateway to financial systems. Funds were subtly redirected.

As the organization's vigilant system analyst, armed with comprehensive access to corporate system logs, you are entrusted with the critical mission of Incident Response. Your task is to unravel the intricate web of deception enabling the adversary's infiltration.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Develop Capabilities - T1587
- Hijack Execution Flow: DLL Side-Loading, Sub-technique T1574.002
- Defense Evasion – TA0005
- Gather Victim Network Information - T1590
- Account Discovery: Domain Account - T1087.002
- Network Share Discovery - T1135
- Command and Scripting Interpreter: Windows Command Shell - T1059.003
- System Network Connections Discovery - T1049
- Exploitation for Privilege Escalation – T1068
- Steal or Forge Kerberos Tickets: Kerberoasting - T1558.003
- OS Credential Dumping – T1003
- Exfiltration Over C2 Channel – T1041
- Archive Collected Data - T1560
- Data Destruction - T1485
- Data Encrypted for Impact - T148

20 Phantom Update

THREAT ACTOR:
BlackCat/ALPHV

THREAT TYPE:
Ransomware

ATTACKER TOOLS:
BlackCat

THREAT RATING:
High

THREAT IMPACT:
- **Data Exfiltration**
- **Service Availability**

DIFFICULTY:
Intermediate

Scenario Description

In a calculated breach, an attacker gains access to an enterprise's internal network through a compromised update package. Moving stealthily, they discovered sensitive information, which they used to launch an internal phishing campaign targeting key personnel. With elevated access, the attacker disrupted critical services, exfiltrated backups, and deployed ransomware across the network. The attack was further escalated by a denial-of-service assault on external servers, followed by demands for ransom under the threat of data exposure and further disruption. The organization is now in a race against time to contain the damage and restore its systems.

MITRE ATT&CK® TTPs:

- Acquire Infrastructure: Server - T1583.004
- Develop Capabilities - T1587
- Supply Chain Compromise: Compromise Software Supply Chain - T1195.002
- Gather Victim Network Information - T1590
- Account Discovery: Domain Account - T1087.002
- Network Share Discovery - T1135
- Remote Services: SMB/Windows Admin Shares - T1021.002
- Unsecured Credentials: Credentials In Files - T1552.001
- Remote Services: SSH - T1021.004
- Internal Spearphishing - T1534
- User Execution: Malicious File - T1204.002
- Exfiltration Over C2 Channel - T1041
- Data Destruction - T1485
- Data Encrypted for Impact - T1486
- Abuse Elevation Control Mechanism: Bypass User Account Control - T1548.002
- Access Token Manipulation - T1134
- Command and Scripting Interpreter: Windows Command Shell - T1059.003
- File and Directory Permissions Modification: Windows File and Directory Permissions Modification - T1222.001
- Network Denial of Service - T1498
- Inhibit System Recovery -T1490

CYBER RANGES

About Us

CYBER RANGES is the ISO27001 certified next-generation military-grade full-content-lifecycle simulation platform for the validation of threat-informed defense capability and cyber resilience. Built on powerful cloud technology, CYBER RANGES is available as subscription-based, as managed service, as On-Premise and Portable rugged deployment options.

CYBER RANGES applies high automation, high orchestration and high scalability to the delivery of even complex large-audience deep-dive management tabletop and technical exercises based on high-fidelity IT/OT infrastructure replicas. CYBER RANGES fully supports MITRE (PRE-)ATT&CK across its entire cyber range architecture. Through its proprietary Injector Engine CYBER RANGES automatically emulates user traffic and the latest intel-based attacks, APTs and specific tactics and exploits from the MITRE ATT&CK Matrix™.

CYBER RANGES actively participates as a key member organization in the European Cyber Security Organization (ECSO) WG5 on Cyber Ranges, Education and Training and Technical Exercises, advancing best practice in the domain of cybersecurity capability and resilience. CYBER RANGES also spearheads the "Top 10 Abilities" initiative, which helps CISOs to focus on pertinent, observable, measurable abilities for the development and assessment of job-specific capabilities in the workplace.

CYBER RANGES is also an active Partner of the Global Cyber Alliance – GCA (New York, Brussels, London) in its worldwide mission to sustain a trustworthy Internet by reducing cyber risk. CYBER RANGES is a founding member of the Canada-based Cyber Security Global Alliance (CSGA). CYBER RANGES is an ecosystem partner of the Quantico Cyber Hub in Virginia, where it runs the Quantico Cyber Range.

bsi. ISO/IEC 27001 Information Security Management
IS 616580

contact@cyberranges.com

Call us toll-free (North America)
1-800-959-0163

cyberranges.com

CYBER SPACE, ENGAGED.