Microsoft Security

Multi-stage incident involving Execution & Lateral movement on multiple endpoints reported by multiple sources

PDF file generated on Jul 27, 2024 10:30 PM Timestamps are generated in UTC-6

🟥🟥🟥 High | ● Active | Mimik Emails - AlpineSkiHouse

Critical asset | Defender Experts | LATEST | MidnightBlizzard | Missing Alerts | AlpineSkiHouse | MDE-Management

Contents

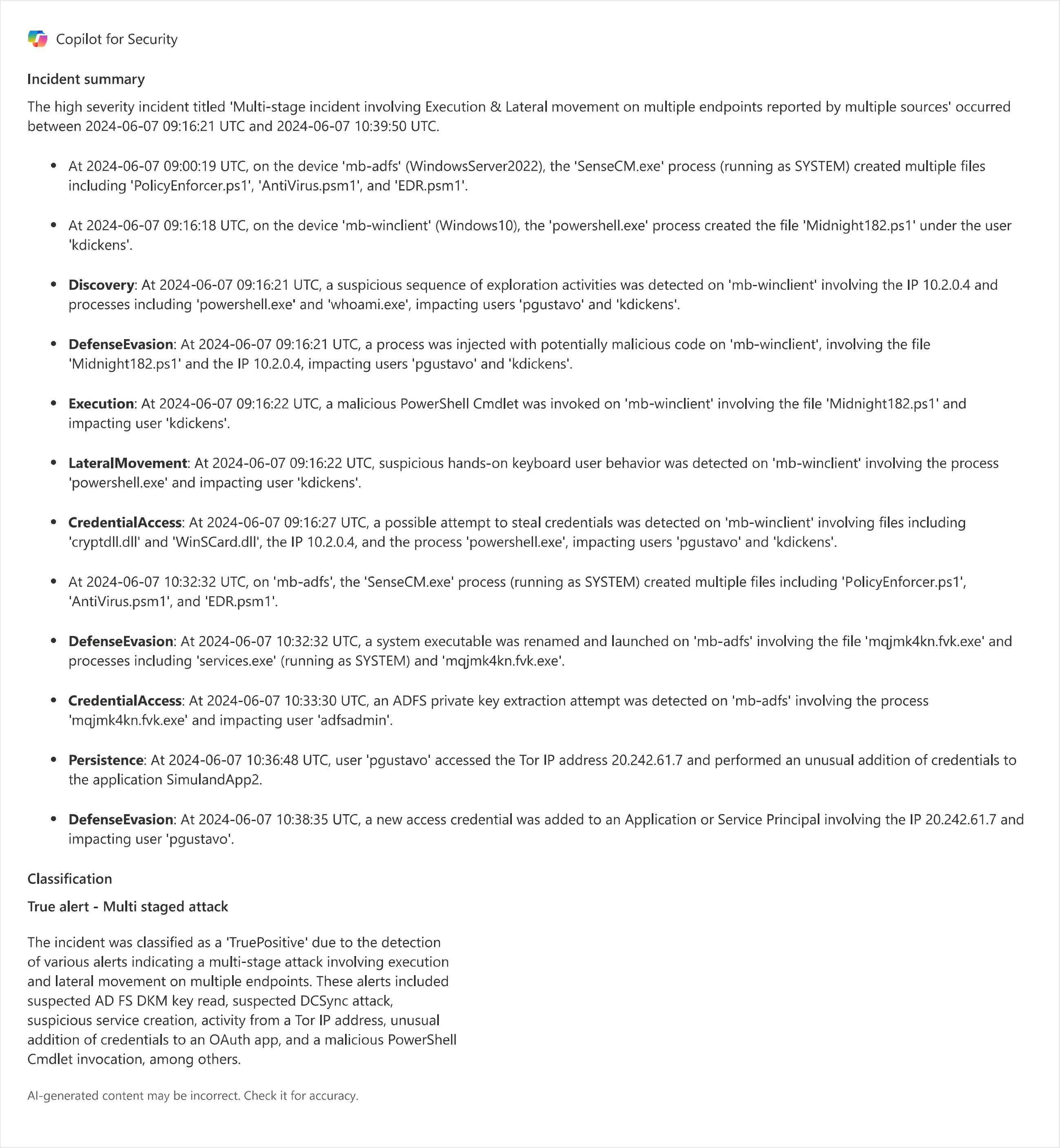
Overview

Incident details

Severity	High
Status	Active
Assigned to	Mimik Emails - AlpineSkiHouse
Incident ID	3150
Classification	True alert - Multi staged attack
Categories	Execution, Persistence, Defense evasion, Credential access, Discovery, Lateral movement
Time created	Jun 7, 2024 3:16 AM
First activity	Jun 7, 2024 3:16 AM
Last activity	Jun 7, 2024 4:39 AM
First log	Jun 7, 2024 3:19 AM
Last log	Jun 28, 2024 10:43 PM
Time closed	-

Analysts involved in the incident:

Mimik Emails - AlpineSkiHouse, Customer, ruizmauricio_microsoft.com#EXT#@seccxpdemo.onmicrosoft.com, <div>We observed a spear phishing campaign with weaponized document from Kristan Costello, impersonating as a co-worker. The emails from this user were blocked. However, user Karla Dickens was able to able to click the malicious email which initiated the lateral movement impacting high privileged user Pedro Gustavo and adfsadmin service account.</div><div>&nbsp;</div><div>We have issued managed response to remediate the impacted assets and take corrective actions to block malicious URL and weaponized document.</div>, Defender Experts, malbada@microsoft.com, adm_ajourn@seccxpdemo.onmicrosoft.com



Incident summary

The high severity incident titled 'Multi-stage incident involving Execution & Lateral movement on multiple endpoints reported by multiple sources' occurred between 2024-06-07 09:16:21 UTC and 2024-06-07 10:39:50 UTC.

- At 2024-06-07 09:00:19 UTC, on the device 'mb-adfs' (WindowsServer2022), the 'SenseCM.exe' process (running as SYSTEM) created multiple files including 'PolicyEnforcer.ps1', 'AntiVirus.psm1', and 'EDR.psm1'.
- At 2024-06-07 09:16:18 UTC, on the device 'mb-winclient' (Windows10), the 'powershell.exe' process created the file 'Midnight182.ps1' under the user 'kdickens'.
- **Discovery**: At 2024-06-07 09:16:21 UTC, a suspicious sequence of exploration activities was detected on 'mb-winclient' involving the IP 10.2.0.4 and processes including 'powershell.exe' and 'whoami.exe', impacting users 'pgustavo' and 'kdickens'.
- **DefenseEvasion**: At 2024-06-07 09:16:21 UTC, a process was injected with potentially malicious code on 'mb-winclient', involving the file 'Midnight182.ps1' and the IP 10.2.0.4, impacting users 'pgustavo' and 'kdickens'.
- **Execution**: At 2024-06-07 09:16:22 UTC, a malicious PowerShell Cmdlet was invoked on 'mb-winclient' involving the file 'Midnight182.ps1' and impacting user 'kdickens'.
- **LateralMovement**: At 2024-06-07 09:16:22 UTC, suspicious hands-on keyboard user behavior was detected on 'mb-winclient' involving the process 'powershell.exe' and impacting user 'kdickens'.
- **CredentialAccess**: At 2024-06-07 09:16:27 UTC, a possible attempt to steal credentials was detected on 'mb-winclient' involving files including 'cryptdll.dll' and 'WinSCard.dll', the IP 10.2.0.4, and the process 'powershell.exe', impacting users 'pgustavo' and 'kdickens'.
- At 2024-06-07 10:32:32 UTC, on 'mb-adfs', the 'SenseCM.exe' process (running as SYSTEM) created multiple files including 'PolicyEnforcer.ps1', 'AntiVirus.psm1', and 'EDR.psm1'.
- **DefenseEvasion**: At 2024-06-07 10:32:32 UTC, a system executable was renamed and launched on 'mb-adfs' involving the file 'mqjmk4kn.fvk.exe' and processes including 'services.exe' (running as SYSTEM) and 'mqjmk4kn.fvk.exe'.
- **CredentialAccess**: At 2024-06-07 10:33:30 UTC, an ADFS private key extraction attempt was detected on 'mb-adfs' involving the process 'mqjmk4kn.fvk.exe' and impacting user 'adfsadmin'.
- **Persistence**: At 2024-06-07 10:36:48 UTC, user 'pgustavo' accessed the Tor IP address 20.242.61.7 and performed an unusual addition of credentials to the application SimulandApp2.
- **DefenseEvasion**: At 2024-06-07 10:38:35 UTC, a new access credential was added to an Application or Service Principal involving the IP 20.242.61.7 and impacting user 'pgustavo'.

Classification

True alert - Multi staged attack

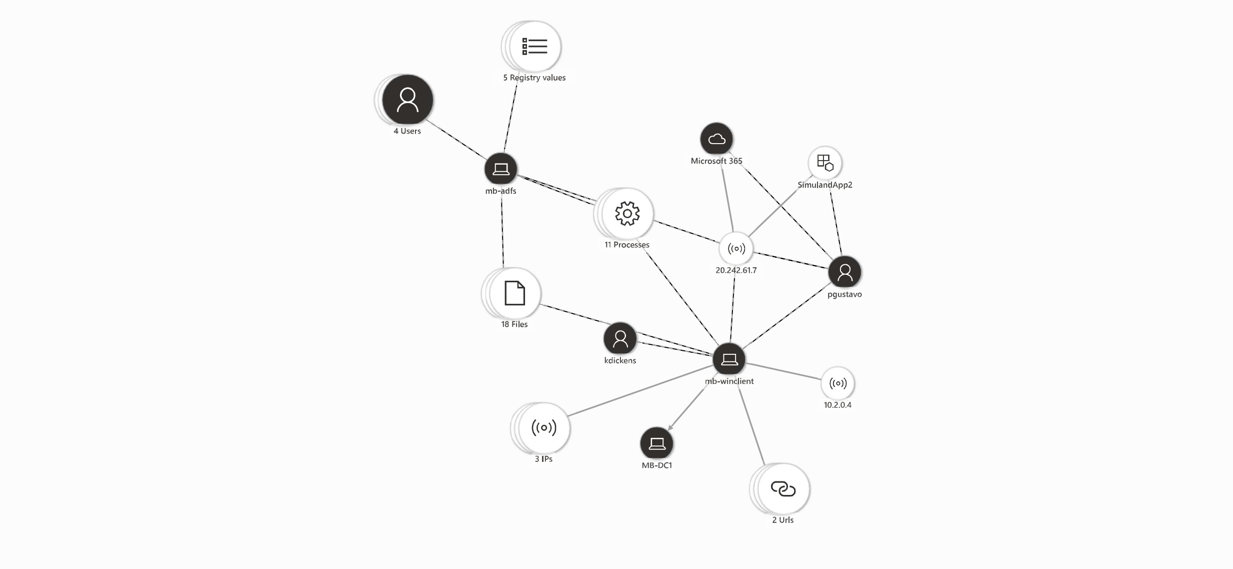
The incident was classified as a 'TruePositive' due to the detection of various alerts indicating a multi-stage attack involving execution and lateral movement on multiple endpoints. These alerts included suspected AD FS DKM key read, suspected DCSync attack, suspicious service creation, activity from a Tor IP address, unusual addition of credentials to an OAuth app, and a malicious PowerShell Cmdlet invocation, among others.

AI-generated content may be incorrect. Check it for accuracy.

Attack story

Attack story graph

MITRE categories	Number of alerts	Impacted assets	Evidence
6	**30**	**8**	**6**



┈┈┈┈┈┈ Association
A relationship between two entities based on affiliation of one entity to another

—— Communication
Transmission of data between entities

Threat categories

6 threat categories

Alerts and categories

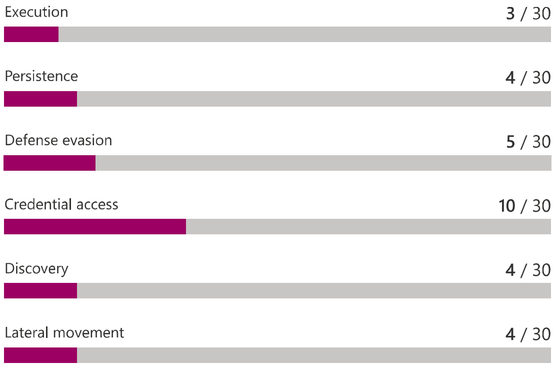
Active alerts	Tactics	Other categories
27/30	**6**	**0**

MITRE ATT&CK tactics

Execution, Persistence, Defense evasion, Credential access, Discovery, Lateral movement

Other categories

No categories found



Scope

Impacted assets

8 impacted assets

Devices	Users	Applications
3	4	1

Devices

Device name	Device ID	Risk level↑	Exposure level	OS Platform	Tags	First activity	Last activity	Related alerts

Users

User	Domain	Status	Priority↑	Email	Title	Department

Apps

App name	Application ID	Application client ID	Risk	Publisher	Related alerts

Evidence and response

Evidence

53 evidence

Processes	Files	Registry Values	URLs	IP Addresses	OAuth Applications
21	19	5	2	5	1

Top evidence

First seen↓	Entity	Entity type	Verdict	Remediation status	Impacted assets	Detection origin

Top evidence

First seen↓	Entity	Entity type	Verdict	Remediation status	Impacted assets	Detection origin

Top evidence

First seen↓	Entity	Entity type	Verdict	Remediation status	Impacted assets	Detection origin

Top evidence

First seen↓	Entity	Entity type	Verdict	Remediation status	Impacted assets	Detection origin

Top evidence

First seen↓	Entity	Entity type	Verdict	Remediation status	Impacted assets	Detection origin

Investigation actions

Copilot for Security

3 investigation actions

1. The Playbook-Get-DeviceHealthStatus was executed to assess the health status of the devices involved in the incident. The execution revealed that the machines mb-winclient.internal.niseko.alpineskihouse.co and mb-adfs.internal.niseko.alpineskihouse.co were misconfigured and required attention.
2. The Playbook-Get-IPReputation was executed to investigate the reputation of the IP address involved in the incident. The execution detected a malicious IP address, 20.242.61.7, which was accessed by user Pedro Gustavo.
3. The Playbook-Get-UserRiskDetails was executed to assess the risk level of the user involved in the incident. The execution showed that the user Pedro Gustavo, who is the CIO and part of the IT Support department, had a risk level of 'None' and a risk state of 'Dismissed'. The user's account was enabled during the time of the incident.

AI-generated content may be incorrect. Check it for accuracy.

Remediation actions

Copilot for Security

1 remediation actions

1. An action to enable a user was performed on an entity account. However, the account's AadUserId id, Sid, email, and display name were not specified.

AI-generated content may be incorrect. Check it for accuracy.

Follow-up actions

Copilot for Security

No follow-up actions yet

AI-generated content may be incorrect. Check it for accuracy.

Supporting data

27 Active alerts

Low	Medium	High
3	16	11

All alerts

Alert name	Severity	Status	Detection	Impacted assets	First activity	Last activity↓
Suspicious hands on keyboard user behavior	Medium	InProgress	WindowsDefenderAtp	mb-winclient, kdickens	Jun 7, 2024 3:16 AM	Jun 7, 2024 3:16 AM
Suspicious access to LSASS service	High	InProgress	WindowsDefenderAtp	mb-winclient, kdickens	Jun 7, 2024 3:16 AM	Jun 7, 2024 3:16 AM
A malicious PowerShell Cmdlet was invoked on th...	Medium	InProgress	WindowsDefenderAtp	mb-winclient, kdickens	Jun 7, 2024 3:16 AM	Jun 7, 2024 3:16 AM
Sensitive credential memory read	High	InProgress	WindowsDefenderAtp	mb-winclient, kdickens	Jun 7, 2024 3:18 AM	Jun 7, 2024 3:18 AM
Possible attempt to steal credentials	High	New	WindowsDefenderAtp	mb-winclient, kdickens	Jun 7, 2024 4:26 AM	Jun 7, 2024 4:28 AM
Suspicious access to LSASS service	High	New	WindowsDefenderAtp	mb-winclient, kdickens	Jun 7, 2024 4:28 AM	Jun 7, 2024 4:28 AM
A malicious PowerShell Cmdlet was invoked on th...	Medium	New	WindowsDefenderAtp	mb-winclient, kdickens	Jun 7, 2024 4:26 AM	Jun 7, 2024 4:28 AM
Sensitive credential memory read	High	New	WindowsDefenderAtp	mb-winclient, kdickens	Jun 7, 2024 4:28 AM	Jun 7, 2024 4:28 AM
Suspicious LDAP query	Medium	New	WindowsDefenderAtp	mb-winclient, pgustavo	Jun 7, 2024 4:30 AM	Jun 7, 2024 4:30 AM
A process was injected with potentially...	Medium	InProgress	WindowsDefenderAtp	mb-winclient, 2 Accounts	Jun 7, 2024 3:16 AM	Jun 7, 2024 4:32 AM
Suspicious System Hardware Discovery	Low	InProgress	WindowsDefenderAtp	mb-winclient, 2 Accounts	Jun 7, 2024 3:16 AM	Jun 7, 2024 4:32 AM
Suspected DCSync attack (replication of directory...	High	New	AzureATP	MB-WINCLIENT, pgustavo	Jun 7, 2024 4:32 AM	Jun 7, 2024 4:32 AM

All alerts

Alert name	Severity	Status	Detection	Impacted assets	First activity	Last activity↓
Suspicious sequence of exploration...	Low	InProgress	WindowsDefenderAtp	mb-winclient, 2 Accounts	Jun 7, 2024 3:16 AM	Jun 7, 2024 4:32 AM
Possible attempt to steal credentials	High	InProgress	WindowsDefenderAtp	mb-winclient, 2 Accounts	Jun 7, 2024 3:16 AM	Jun 7, 2024 4:32 AM
Suspicious Remote activity	Medium	New	CustomDetection	mb-winclient	Jun 7, 2024 4:32 AM	Jun 7, 2024 4:32 AM
Suspicious service creation	Medium	New	AzureATP	MB-ADFS, adfsadmin	Jun 7, 2024 4:32 AM	Jun 7, 2024 4:32 AM
Suspicious service registration	Medium	InProgress	WindowsDefenderAtp	mb-adfs	Jun 7, 2024 4:32 AM	Jun 7, 2024 4:32 AM
Suspicious Task Scheduler activity	Medium	InProgress	WindowsDefenderAtp	mb-adfs	Jun 7, 2024 4:32 AM	Jun 7, 2024 4:32 AM
System executable renamed and launched	Medium	Resolved	WindowsDefenderAtp	mb-adfs	Jun 7, 2024 4:32 AM	Jun 7, 2024 4:32 AM
Attempt to hide use of dual-purpose tool	Medium	Resolved	WindowsDefenderAtp	mb-adfs, adfsadmin	Jun 7, 2024 4:32 AM	Jun 7, 2024 4:32 AM
Suspicious sequence of exploration...	Low	InProgress	WindowsDefenderAtp	mb-adfs, adfsadmin	Jun 7, 2024 4:32 AM	Jun 7, 2024 4:32 AM
Suspicious remote activity	Medium	Resolved	WindowsDefenderAtp	mb-adfs, 2 Accounts	Jun 7, 2024 4:32 AM	Jun 7, 2024 4:32 AM
Suspected AD FS DKM key read	High	New	AzureATP	MB-DC1	Jun 7, 2024 4:33 AM	Jun 7, 2024 4:33 AM
ADFS private key extraction attempt	High	New	WindowsDefenderAtp	mb-adfs, adfsadmin	Jun 7, 2024 4:33 AM	Jun 7, 2024 4:33 AM

All alerts

Alert name	Severity	Status	Detection	Impacted assets	First activity	Last activity↓

Activity log

26 related activities

Playbook-Get-UserRiskDetails
User Account Risk Details

AccountDisplayName	MailAddress	RiskLevel	RiskState	IsAccountEnabled	AdditionalMailAddresses	Department
Pedro Gustavo	pgustavo@niseko.alpineskihouse.co	None	Dismissed	True		IT Support

Jun 24, 2024 11:12:07 AM

API-App:Mimik Emails - AlpineSkiHouse
Status changed from 'Awaiting Customer Action' to 'Active'.
Jun 20, 2024 4:35:16 PM

API-App:Mimik Emails - AlpineSkiHouse
Incident was assigned to Mimik Emails - AlpineSkiHouse.
Jun 20, 2024 4:35:16 PM

API-App:Defender Experts for XDR
Status changed from 'Active' to 'Awaiting Customer Action'.
Jun 19, 2024 8:00:53 PM

API-App:Defender Experts for XDR
Incident was assigned to Customer.
Jun 19, 2024 8:00:52 PM

User-malbada@microsoft.com
Changed determination to Multi staged attack.
Jun 17, 2024 4:05:14 PM

User-malbada@microsoft.com
Changed classification to 'True positive'.
Jun 17, 2024 4:05:14 PM

Playbook-Get-UserRiskDetails
User Account Risk Details

AccountDisplayName	MailAddress	RiskLevel	RiskState	IsAccountEnabled	AdditionalMailAddresses	Department
Pedro Gustavo	pgustavo@niseko.alpineskihouse.co	None	Dismissed	True		IT Support

Jun 17, 2024 4:00:46 PM

Playbook-Get-DeviceHealthStatus
Endpoint Health Status

***Warning** - There are misconfigured devices that needs attention*

DeviceId	DeviceName	OSPlatform	AntivirusEnabled	AntivirusRe
358af7aeed120ee740f05ba7988e36f5f8e7b66f	mb-adfs.internal.niseko.alpineskihouse.co	WindowsServer2022	GOOD	GOOD
31a048e5eea6ad6e6bc025bfa9e0e571c4c20f7e	mb-winclient.internal.niseko.alpineskihouse.co	Windows10	GOOD	GOOD

Jun 17, 2024 3:59:11 PM

Playbook-Get-IPReputation
IP Reputation

***Warning** - Malicious IP Address Detected (Virus Total Reputation < 0)*

City	Country	Harmless	IPAddresss	Malicious	Reputation	Suspicious	Undetected	isTorIP
san francisco	united states	1	185.199.108.133	0	-3	0	29	
boydton	united states	0	20.242.61.7	0	0	0	29	

Jun 17, 2024 3:59:00 PM

API-App:Mimik Emails - AlpineSkiHouse
Incident was assigned to Mimik Emails - AlpineSkiHouse.
Jun 12, 2024 4:33:21 PM

User-ruizmauricio_microsoft.com#EXT#@seccxpdemo.onmicrosoft.com
Incident was assigned to ruizmauricio_microsoft.com#EXT#@seccxpdemo.onmicrosoft.com.
Jun 12, 2024 6:07:46 AM

User-ruizmauricio_microsoft.com#EXT#@seccxpdemo.onmicrosoft.com
We observed a spear phishing campaign with weaponized document from Kristan Costello, impersonating as a co-worker. The emails from this user were blocked. However, user Karla Dickens was able to able to click the malicious email which initiated the lateral movement impacting high privileged user Pedro Gustavo and adfsadmin service account.

We have issued managed response to remediate the impacted assets and take corrective actions to block malicious URL and weaponized document.
Jun 12, 2024 6:07:39 AM

API-App:Mimik Emails - AlpineSkiHouse
Status changed from 'Awaiting Customer Action' to 'Active'.
Jun 11, 2024 4:32:56 PM

API-App:Mimik Emails - AlpineSkiHouse
Incident was assigned to Mimik Emails - AlpineSkiHouse.
Jun 11, 2024 4:32:56 PM

API-App:Defender Experts for XDR
Status changed from 'Active' to 'Awaiting Customer Action'.
Jun 11, 2024 11:30:04 AM

API-App:Defender Experts for XDR
Incident was assigned to Customer.
Jun 11, 2024 11:30:03 AM

API-App:Mimik Emails - AlpineSkiHouse
Incident was assigned to Mimik Emails - AlpineSkiHouse.
Jun 7, 2024 4:32:54 PM

adm_ajourn@seccxpdemo.onmicrosoft.com
linked
Jun 7, 2024 5:19:32 AM

User-adm_ajourn@seccxpdemo.onmicrosoft.com
adm_ajourn@seccxpdemo.onmicrosoft.com linked 11 alerts:
ADFS private key extraction attempt, Attempt to hide use of dual-purpose tool, Ongoing hands-on-keyboard attack via Impacket toolkit, Suspected AD FS DKM key read, Suspicious remote activity, Suspicious sequence of exploration activities, Suspicious service creation, Suspicious service registration, Suspicious Task Scheduler activity, System executable renamed and launched
Jun 7, 2024 5:19:31 AM

User-adm_ajourn@seccxpdemo.onmicrosoft.com
Status changed from 'Resolved' to 'Active'.
Jun 7, 2024 3:35:16 AM

User-adm_ajourn@seccxpdemo.onmicrosoft.com
Status changed from 'In Progress' to 'Resolved'.
Jun 7, 2024 3:34:55 AM

Playbook-Get-DeviceHealthStatus
Endpoint Health Status

***Warning** - There are misconfigured devices that needs attention*

DeviceId	DeviceName	OSPlatform	AntivirusEnabled	AntivirusReporting
31a048e5eea6ad6e6bc025bfa9e0e571c4c20f7e	mb-winclient.internal.niseko.alpineskihouse.co	Windows10	GOOD	GOOD

Jun 7, 2024 3:23:46 AM

API-App:Defender Experts for XDR
Status changed from 'Active' to 'In Progress'.
Jun 7, 2024 3:19:39 AM

API-App:Defender Experts for XDR
Incident was assigned to Defender Experts.
Jun 7, 2024 3:19:39 AM

Automation
Incident severity changed to High
Jun 7, 2024 3:19:30 AM