Wayne Enterprises

Incident Report

Prepared by: Rapid7 Managed Detection and Response

Rapid7 Contact Information

Please direct any additional questions or concerns to your Customer Advisor via the Insight Platform: ‘https://insight.rapid7.com/login’.

If you require immediate assistance, please call the emergency hotline to speak with an MDR representative.

Region	24/7 Hotline Number
United States (US)	+1 844-777-7637
European Union (EU)	+44 800-088-5859
Singapore (SG)	+65 800-852-3321
Australia (AU)	+61-2-4734-7032

Table of Contents:

Executive Summary

On March 10th, 2023, Rapid7's Managed Detection and Response (MDR) was notified by Wayne Enterprises regarding two phishing incidents resulting from two compromised user accounts. Rapid7 initiated incident response services to identify the extent of the compromise within the Wayne Enterprises environment. Rapid7 determined that a total of five accounts were in scope for this investigation.

Rapid7 classified this incident with Medium severity.

Incident Synopsis

Rapid7 determined the Wayne Enterprises environment was initially compromised on 2023-01-19 at 16:25:26 UTC when a threat actor successfully authenticated to the Office 365 account 'user1', from the malicious IP address ***164[.]90.151[.]205***.

Rapid7 reviewed the available Ingress Authentication log data and determined the threat actor from the malicious IP address ***164[.]90.151[.]205*** also successfully authenticated to two additional user accounts on 2023-01-19; 'user2' at 16:32:57 UTC and 'user3' at 17:34:18 UTC.

Between a timeframe of 2023-01-19 to 2023-03-14, Rapid7 observed successful ingress authentication a total of 123 times for user accounts 'user1', 'user2' and 'user3' from the following malicious IP addresses: ***164[.]90.151[.]205***, ***163[.]5.160[.]114,***, ***23[.]105.110[.]208***, ***185[.]205.94[.]191***, ***51[.]89.94[.]136***, ***163[.]5.160[.]197***, ***85[.]239.44[.]247***, ***85[.]239.44[.]9,***, ***204[.]101.102[.]99***. A supplemental spreadsheet listing authentication times by each malicious IP address, for each user account, will be included with this report.

Rapid7 reviewed the available Cloud Service Activity log data and determined between 2023-01-19 to 2023-03-14, the threat actor interacted with compromised accounts 'user3' from IP addresses ***163[.]5.160[.]114,***, ***185[.]205.94[.]191*** and ***163[.]5.160[.]197*** a total of 16 times; 'user1' from the IP addresses ***23[.]105.110[.]208***, ***185[.]205.94[.]191***, ***85[.]239.44[.]9,***, ***85[.]239.44[.]247, 204[.]101.102[.]99, 163[.]5.160[.]197*** and ***51[.]89.94[.]136*** a total of 213 times; 'user2' from the IP addresses ***163[.]5.160[.]114,***, ***23[.]105.110[.]208***, ***51[.]89.94[.]136, 163[.]5.160[.]197, 85[.]239.44[.]247*** and ***204[.]101.102[.]99*** a total of 45 times. On 2023-03-05, 2023-03-06, 2023-03-10 and 2023-03-13, Rapid7 observed the threat actor creating multiple new Office 365 inbox rules for accounts 'user1' and 'user2' originating from the IP addresses ***204[.]101.102[.]99***, ***85[.]239.44[.]9,*** and ***51[.]89.94[.]136***. The purpose of these inbox rules were to delete all incoming messages.

The threat actor sent phishing emails from two of the compromised Office 365 accounts, 'user2' on 2023-03-10 and 'user1' on 2023-03-13. Both phishing events involved sending to recipients within the Wayne Enterprises organization. This is a common tactic used by threat actors for the purposes of potentially pivoting into an account containing sensitive information or belonging to a member of staff in a position of influence within the organization. Rapid7 identified evidence of accounts ‘user4@wayne_enterprise” and ‘user5@wayne_enterprise’ interacting with an embedded malicious link contained within the phishing email. Based on available evidence and confirmation from Wayne Enterprises, further malicious activity involving these phishing emails had been halted by Mimecast.

On 2023-03-13, the threat actor registered a remote device to the Office 365 account for ‘user1’ for the purpose of maintaining persistent access to this account.

Rapid7 did not identify evidence of data exfiltration within the Wayne Enterprises environment.

Recommended Actions

Remediation Actions

- **Lock the Affected Accounts**
  - Lock the affected accounts until their credentials are rotated.
  - InsightConnect could be used to perform these actions, which can be accessed through the 'Take Action' button in the *Investigations* section.
- **Change Passwords for Affected Accounts**
  - Change the affected account passwords as soon as possible to prevent a threat actor from leveraging the credentials to access services.
  - Instruct users to not just change one character of a password, such as changing ***Example1!*** to ***Example2!*** and to follow the NIST guidelines for the 'memorized secret' password policy: 'https://pages.nist.gov/800-63-3/sp800-63-3.html'.
  - A threat actor who has captured past credentials could be more successful in guessing credentials changed by only one character.
  - InsightConnect could be used to perform these actions, which can be accessed through the 'Take Action' button in the *Investigations* section.
- **Identify and Remove Malicious Email from All Inboxes**
  - Determine if other users received the malicious email and remove it from all inboxes.
- **End All Active Sessions for the Impacted User Account(s)**
  - End all active sessions for the impacted user account(s). This action will force a logout of all authenticated sessions associated with the compromised user account(s), including impersonated sessions.
- **Remove Malicious Office 365 Inbox Rules**
  - Remove malicious inbox rules created by the threat actor.

Corrective Actions

- **Review Email Rules**
  - Review Inbox rules for the identified user accounts. A threat actor could create Inbox rules to forward emails to external, threat actor-controlled email accounts.
  - More information on how to collect all inbox rules for review is available in the corresponding Microsoft documentation: 'https://learn.microsoft.com/en-us/powershell/module/exchange/get-inboxrule?view=exchange-ps'.

- **User Awareness Training**
    - Implement phishing-based training for users identified as opening unknown attachments or clicking unknown links. Train users on how to forward suspicious links or emails to information security for analysis.
    - Rapid7 recommends providing user awareness training at regular intervals to all users in the environment.
- **Implement a Conditional Access Policy**
    - Rapid7 recommends implementing conditional access policies to limit unauthorized access to the environment. Instructions on how to implement these policies can be found within the corresponding Microsoft documentation: ‘https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-location’.

Incident Details

This section describes the malicious activity that Rapid7 discovered while investigating the compromise.

Initial Access

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spear phishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

T1078.004 - Valid Accounts: Cloud Accounts

Rapid7 determined the Wayne Enterprises environment was initially compromised on 2023-01-19 at 16:25:26 UTC when a threat actor successfully authenticated to the Office 365 account ‘user1’ from the IP address ***164[.]90.151[.]205***.

```
{
     "timestamp": "2023-01-19T16:25:26.000Z",
     "user": "user1",
     "account": "user1",
     "result": "SUCCESS",
     "source_ip": "164[.]90.151[.]205",
     "service": "o365",
     "geoip_country_code": "US",
     "geoip_country_name": "United States",
     "geoip_organization": "Digital Ocean",
     "geoip_region": "CA"
     "user_agent": Mozilla/5.0 (iPhone; CPU iPhone OS 16_1_2 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.1 Mobile/15E148 Safari/604.1"
}
```

Figure #1: First Successful Ingress Authentication from the threat actor to account user1

Immediately following this activity, Rapid7 identified successful authentication from the IP address ***164[.]90.151[.]205*** to the Office 365 accounts for ‘user2’ at 16:32:57 UTC and ‘user3’ at 17:34:18 UTC.

```
{
    "timestamp": "2023-01-19T16:32:57.000Z",
    "user": "user2",
    "account": "user2",
    "result": "SUCCESS",
    "source_ip": "164[.]90.151[.]205",
    "service": "o365",
    "geoip_country_code": "US",
    "geoip_country_name": "United States",
    "geoip_organization": "Digital Ocean",
    "geoip_region": "CA",
    "user_agent": "Mozilla/5.0 (iPhone; CPU iPhone OS 16_1 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/109.0.5414.83 Mobile/15E148 Safari/604.1",
}
```

Figure #2: First Successful Ingress Authentication from the threat actor to account user2

```
{
    timestamp": "2023-01-19T17:34:18.000Z",
    "user": "user3",
    "account": "user3",
    "result": "SUCCESS",
    "source_ip": "164[.]90.151[.]205",
    "service": "o365",
    "geoip_city": "Santa Clara",
    "geoip_country_code": "US",
    "geoip_country_name": "United States",
    "geoip_organization": "Digital Ocean",
    "geoip_region": "CA",
    "user_agent": "Mozilla/5.0 (iPhone; CPU iPhone OS 16_1_2 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.1 Mobile/15E148 Safari/604.1",
}
```

Figure #3: First Successful Ingress Authentication from the threat actor to account user3

Rapid7 reviewed the available Ingress Authentication log evidence and identified a total of 123 successful authentication events from the threat actor to user accounts 'user1', 'user2' and 'user3' from the following nine suspicious IP addresses: ***164[.]90.151[.]205***, ***163[.]5.160[.]114,***, ***23[.]105.110[.]208***, ***185[.]205.94[.]191***, ***51[.]89.94[.]136***, ***163[.]5.160[.]197***, ***85[.]239.44[.]247***, ***85[.]239.44[.]9,***, ***204[.]101.102[.]99***. The authentication activity occurred between a timeframe of 2023-01-19 and 2023-03-14.

A supplemental spreadsheet listing successful ingress authentication events associated with these compromises will be included with this report.

Rapid7 did not identify attempted ingress authentication activity associated with the aforementioned nine suspicious IP addresses to any other user account in the Wayne Enterprises environment.

Further information regarding the usage of cloud accounts as a vector for initial access is available within MITRE's ATT&CK Framework documentation under ID T1078.004:

'https://attack.mitre.org/techniques/T1078/004/'.

Defense Evasion

Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross-listed here when those techniques include the added benefit of subverting defenses.

T1564.008 - Hide Artifacts: Email Hiding Rules

Rapid7 reviewed available Cloud Service Activity log evidence and identified four events involving the creation of new inbox rules for user accounts 'user1' and 'user2'. On 2023-03-05 at 22:37:01 UTC and originating from IP address ***85[.]239.44[.]9,***, the threat actor created a new inbox rule named 'dyts' under user account 'user1'. The purpose of this rule was to delete Office 365 messages for this user account.

```
{
    "timestamp": "2023-03-05T22:37:01.000Z",
    "source_user": "user1",
    "service": "o365",
    "action": "New-InboxRule",
    "source_account": "user1",
    "source_json": {
        "ClientIP": "85[.]239.44[.]9,:12827",
        "Name": "Name",
        "Value": "dyts"
        },
        {
        "Name": "DeleteMessage",
        "Value": "True"
        },
        {
        "Name": "MarkAsRead",
        "Value": "True"
         },
         {
}
```

Figure #4: Cloud Service Activity Log evidence referencing the creation of the new inbox rule

Immediately following this event at 22:37:25 UTC, Rapid7 observed this threat actor perform a remove inbox rule action while still under user account “user1’. Based on available evidence, Rapid7 could not confirm if the newly created inbox rule was also the rule removed by the threat actor.

```
{
    "timestamp": "2023-03-05T22:37:25.000Z",
    "source_user": "user1",
    "service": "o365",
    "action": "Remove-InboxRule",
    "source_account": "user1",
    "source_json": {
        "ClientIP": "85[.]239.44[.]9,:30914",
        "Operation": "Remove-InboxRule",
        "ResultStatus": "True",
}
```

Figure #5: Cloud Service Activity Log evidence referencing the removal of an inbox rule

On 2023-03-06 at 16:28:01 UTC and originating from IP address ***85[.]239.44[.]9,***, the threat actor created a new inbox rule named ‘ghjkkaff’ under user account ‘user1’. The purpose of this rule was to delete Office 365 messages for this user account.

```
{
    "timestamp": "2023-03-06T16:28:01.000Z",
    "source_user": "user1",
    "service": "o365",
    "action": "New-InboxRule",
    "source_account": "user1",
    "source_json": {
        "ClientIP": "85[.]239.44[.]9,:42074",
        "Name": "Name",
        "Value": "ghjkkaff"
        },
        {
        "Name": "DeleteMessage",
        "Value": "True"
        },
        {
        "Name": "MarkAsRead",
        "Value": "True"
         },
         {
}
```

Figure #6: Cloud Service Activity Log evidence referencing the creation of a second new inbox rule

On 2023-03-10 at 13:45:12 UTC and originating from IP address ***204[.]101.102[.]99***, the threat actor created a new inbox rule named 'vbfgd' under user account 'user2'. The purpose of this rule was to delete Office 365 messages for this user account.

```
{
    "timestamp": "2023-03-10T13:45:12.000Z",
    "source_user": "user2",
    "service": "o365",
    "action": "New-InboxRule",
    "source_account": "user1",
    "source_json": {
        "ClientIP": "204[.]101.102[.]99:54186",
        "Name": "Name",
        "Value": "vbfgd"
        },
        {
        "Name": "DeleteMessage",
        "Value": "True"
        },
        {
        "Name": "MarkAsRead",
        "Value": "True"
         },
         {
}
```

Figure #6: Cloud Service Activity Log evidence referencing the creation of a third new inbox rule

On 2023-03-13 at 15:24:13 UTC and originating from IP address ***51[.]89.94[.]136***, the threat actor created a new inbox rule named 'qw' under user account 'user1'. The purpose of this rule was to delete Office 365 messages for this user account.

```
{
    "timestamp": "2023-03-13T15:24:13.000Z",
    "source_user": "user1",
    "service": "o365",
    "action": "New-InboxRule",
    "source_account": "user1",
    "source_json": {
        "ClientIP": "51[.]89.94[.]136:16568",
        "Name": "Name",
        "Value": "qw"
        },
        {
        "Name": "DeleteMessage",
        "Value": "True"
        },
        {
        "Name": "MarkAsRead",
        "Value": "True"
         },
         {
}
```

Figure #6: Cloud Service Activity Log evidence referencing the creation of a fourth new inbox rule

A supplemental spreadsheet listing all suspicious Office 365 activity associated with user accounts ‘user3’, ‘user2’ and ‘user1’ during the timeframe of this compromise will be included with this report.

Further information regarding the usage of inbox rules to evade detection is available within MITRE’s ATT&CK Framework documentation under ID T1564.008: ‘https://attack.mitre.org/techniques/T1564/008/’.

Collection

Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives. Frequently, the next goal after collecting data is to steal (exfiltrate) the data. Common target sources include various drive types, browsers, audio, video, and email. Common collection methods include capturing screenshots and keyboard input.

T1213.002 - Data from Information Repositories: Sharepoint

A review of available Cloud Service Activity evidence indicates the threat actor accessed user accounts of ‘user1’ from IP addresses ***185[.]205.94[.]191***, ***85[.]239.44[.]9,***, ***163[.]5.160[.]197***, ***85[.]239.44[.]247*** and ***51[.]89.94[.]136;*** ‘user2’ from IP addresses ***51[.]89.94[.]136*** and ***163[.]5.160[.]197;*** ‘user3’ from IP addresses ***185[.]205.94[.]191*** and ***163[.]5.160[.]197*** and interacted with multiple Wayne Enterprises files hosted at the domain ***wayne_enterprise.sharepoint[.]com***.

Between a timeframe of 2023-01-19 to 2023-03-14, Rapid7 observed the threat actor performing 33 ***FilePreviewed*** actions on seven unique files.

Times Accessed	File Name	SharePoint URL
17	document1	hxxps://wayne_enterprise.sharepoint[.]com/sites/document1
5	document2	hxxps://wayne_enterprise.sharepoint[.]com/sites/document2
5	document3	hxxps://wayne_enterprise.sharepoint[.]com/sites/document3
2	document4	hxxps://wayne_enterprise-my.sharepoint[.]com/personal/document4

2	document5	hxxps://wayne_enterprise.sharepoint[.]com/sites/document5
1	document6	hxxps://wayne_enterprise-my.sharepoint[.]com/personal/document6
1	document7	hxxps://wayne_enterprise-my.sharepoint[.]com/personal/document7

Table #1: Files and the number of times viewed by the threat actor

Rapid7 recommends conducting a review of these seven files to determine if sensitive information may have been compromised.

Further information regarding the collection of data from repositories such as SharePoint is available within MITRE's ATT&CK Framework documentation under ID T1213.002:

'https://attack.mitre.org/techniques/T1213/002/'

Impact

Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.

T1565 - Data Manipulation

A review of available Office 365 log evidence during the timeframe of 2023-01-19 to 2023-03-14 indicate the threat actor performed 128 ***Update*** actions, 89 ***SoftDelete*** actions, 15 ***MoveToDeletedItems*** actions and 4 ***Create*** actions within the user accounts 'user1', 'user2' and 'user3'.

A supplemental spreadsheet listing all Cloud Service Activity actions performed by the threat actor during the timeframe of this compromise will be included with this report.

Further information regarding the impact of data manipulation is available within MITRE's ATT&CK Framework documentation under ID T1565:

'https://attack.mitre.org/techniques/T1565/'

Lateral Movement

Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain. Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

T1534 - Internal Spearphishing

On 2023-03-10 at 19:18:00 UTC, the threat actor utilized the Office 365 account 'user2' to send a phishing email containing the subject line 'subject1' to multiple recipients. These recipients include email addresses external to the organization, as well as internal. A sample email from this event was provided to Rapid7 for forensic review. However, based on available evidence, Rapid7 was not able to acquire the URL to the credential harvesting website or identify potential user accounts that may have interacted with the embedded link.

On 2023-03-13 at 19:26:00 UTC, the threat actor utilized the Office 365 account 'user1' to send a phishing email containing the subject line `Wayne Enterprises shared a RFP document with you' to multiple recipients. These recipients include email addresses internal to the organization. A sample email from this event was provided to Rapid7 for forensic review. Rapid7 identified an embedded link contained within this email sample that will direct the user to ***link1***. This webpage contains a secondary link that will direct the user to a credential harvesting page located at ***link2.*** A review of available log evidence indicates the user accounts 'user4@wayne_enterprise' and 'user5@wayne_enterprise' had interacted with the malicious link contained within this phishing email. However, based on available evidence as well as confirmation from Wayne Enterprises, further malicious activity had been halted by Mimecast. The purpose of sending additional phishing emails within the organization is a common tactic used by threat actors to allow for pivoting into additional accounts that may potentially contain sensitive information or belonging to a member of staff in a position of influence.

Further information regarding the usage of internal spearphishing as a vector for lateral movement is available within MITRE's ATT&CK Framework documentation under ID T1534: 'https://attack.mitre.org/techniques/T1534/'.

Persistence

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

T1098.005 - Device Registration

A review of available Cloud Service Activity evidence indicates the threat actor enrolled a remote device on 2023-03-13 at 19:18:39 UTC to the user account ‘user1’. The purpose of device enrollment is to allow the threat actor to maintain a persistent presence within the organizational Office 365 environment.

Further information regarding the usage of device registration as a method of maintaining persistence is available within MITRE’s ATT&CK Framework documentation under ID T1098.005:

https://attack.mitre.org/techniques/T1098/005/

Appendix A: Alert Summary

Time to Respond

Event Time	2023-03-10 22:10:54 UTC
Acknowledge Time	2023-03-11 00:06:14 UTC

Alert time and time to begin investigation

Associated Alerts

Alert Name	IDR Investigation URL
Suspicious Authentication - Digital Ocean	https://us2.idr.insight.rapid7.com
Suspicious Authentication - Digital Ocean	https://us2.idr.insight.rapid7.com
Suspicious Authentication - Digital Ocean	https://us2.idr.insight.rapid7.com

Investigation IDs from IDR

Appendix B: Incident Severity, Category, Type

Rapid7 classified this incident with Low severity.

Rapid7 determines the severity of an incident based on a number of factors, including:

- **Intent**: Whether the threat appears to be targeted or opportunistic/automated, and the likely objectives of the attack
- **Scope**: The number and criticality of systems and users impacted
- **Ongoing Activity**: Whether the incident appears to have been fully contained/no longer active, or whether the attacker remains active within the environment
- **Impact**: The criticality of in-scope assets or users, evidence of data exfiltration, etc.

Incident Severity	Incident Definition	Example Incident(s)
Low	A non-targeted, low-impact threat involving a small number of systems or users which is already contained by existing security controls.	A non-targeted phishing attack with evidence that the recipient(s) provided credentials.
Medium	A non-targeted, low-impact threat impacting a small number of systems or users, but requiring additional actions from you to fully contain and eradicate the threat.	Malware delivered via a non-targeted phishing attack that is only partially blocked on an endpoint.
High	A high risk or high impact threat, often impacting a large number of systems or users and ongoing attacker activity.	Unauthorized interactive network access with evidence of reconnaissance, privilege escalation, lateral movement, data exfiltration, or other signs of a late-stage compromise being observed.

Severity levels and Incident Types

Compromise Category	Compromise Type
Reconnaissance	Phishing
Intrusion	Account Compromise

Incident Category and Type

Appendix C: Affected Accounts

Account	Notes
user1@wayne_enterprise	Office 365 account compromised and subsequently leveraged to send phishing emails from. Additionally, the threat actor registered a remote device to this account.
user2@wayne_enterprise	Office 365 account compromised and subsequently leveraged to send phishing emails from.
user3@wayne_enterprise	Office 365 account compromised
user4@wayne_enterprise	Office 365 account identified as having interacted with the malicious link contained within the phishing email sent from the user1 account.
user5@wayne_enterprise	Office 365 account identified as having interacted with the malicious link contained within the phishing email sent from the user1 account.

Affected Accounts

Appendix D: Indicators of Compromise

Network

Network Based Indicator	Notes
link1	Malicious link embedded within the phishing email sent from the user1 account
link2	URL to the credential harvesting website

Network Based Indicators of Compromise