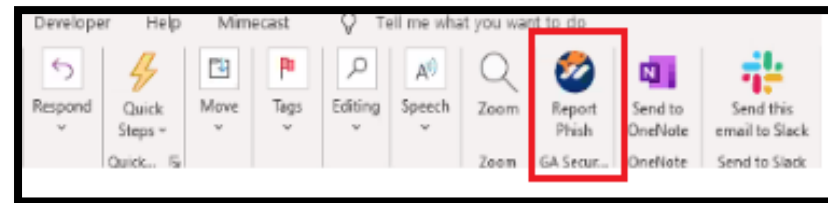


The background of the slide features a hand reaching out from the bottom left towards a glowing, wireframe globe. The globe is composed of a network of white dots connected by thin lines, representing a global network or data flow. The background is a blurred cityscape at night with blue and white light effects.

Runbook for Phishing Alert

Make Digital Real | Execute Smart

How to report Phishing Mail: When the user presumes that the received mail is Phishing. He/She can report to the security team by Clicking on report phish button on Outlook.







- Once the user clicked on Phishing button in the outlook the email will be reported to the security team by creating a ticket Automatically in ServiceNow with the headers.
- The moment the new ticket popped up in ServiceNow Then the security team will assign the ticket and start investigation on the reported Suspicious phishing mail.

- When a user reported as Phishing automatically ticket creates in ServiceNow
- SN_IT_SOC Team has to assign for investigation with recommendations towards closure

<




≡

Incident
INC0016859



Follow

Update




Manage Attachments (3):  image001.jpg [rename] [download]  message.eml [rename] [download]  ~WRD000.jpg [rename] [download]

Number

INC0016859



* Caller

John McKegney




* Affected user

John McKegney




* Category

Security Incidents (CSI)




* Subcategory

Initial Access




Item

-- None --




* Type

Issue




* Short description

Suspected Phishing




* Description

From: no-reply@dropbox.com
Subject: Nathan Hoffman sent you "Frankford Candy, Payment.pdf"




* Contact type

Alert




State

Resolved




* Impact

2 - Medium



* Urgency

1 - High





Priority


2 - High



* Assignment group

SN_IT_SOC



* Assigned to





Analysis:

- Check the headers in mxtoolbox(<https://mxtoolbox.com/EmailHeaders.aspx>).
- Check for reply-to if its different its good indicator of spoofed mail.
- Check for SPF, DKIM markers for any failures. If it fails then sender is not authorized to send mail on behalf of the domain and can be considered spam.
- Check for originating ip address against various threat intelligence like: Virus total, IBM xforce and cisco talos.
- Check for any suspicious links/attachments. Check risk score of these against various threat intelligence tools.
- Run the attachments in any.run or hybrid analysis to find more indicators or where these links are leading to.
- When attachment is opened in sandbox check for DNS requests being made, if they are malicious then its good indicator to flag mail as malicious and perform further purge activities.

Once it is found to be Phishing mail the below steps will be followed:

- Identify the sender of the Phishing mail and check with the details of sender in Mimecast, to confirm that how many users might have been receive the same phishing mail and validate the Mimecast headers and analysis.

The screenshot shows the Mimecast Message Tracking interface. The background is a dark grey panel with the title 'Message Tracking' and a subtitle 'Search the message status queues to troubleshoot recent m...'. There are two tabs: 'Search by Data' (selected) and 'Search by ID'. Below the tabs are three input fields: 'From' with the value 'no-reply@dropbox.com', 'To' with the placeholder 'Email address or domain', and 'Date Range' with the value 'Past 48 hours'. A 'Show more' link is below these fields. A 'Search' button is at the bottom right. A white modal dialog titled 'Search Reason' is open in the foreground. It contains the text 'For audit purposes, enter the reason you're searching the message status queues.' and a text input field with the value 'INC0016859'. At the bottom of the modal are 'Cancel' and 'Submit and search' buttons.

Dashboard x Message Tracki... x

Message Center > Message Tracking

Message Tracking

Search the message status queues to troubleshoot recent m...

Search by Data Search by ID

From no-reply@dropbox.com

To Email address or domain

Date Range Past 48 hours

Show more v

Search

Search Reason

For audit purposes, enter the reason you're searching the message status queues.

INC0016859

Cancel Submit and search

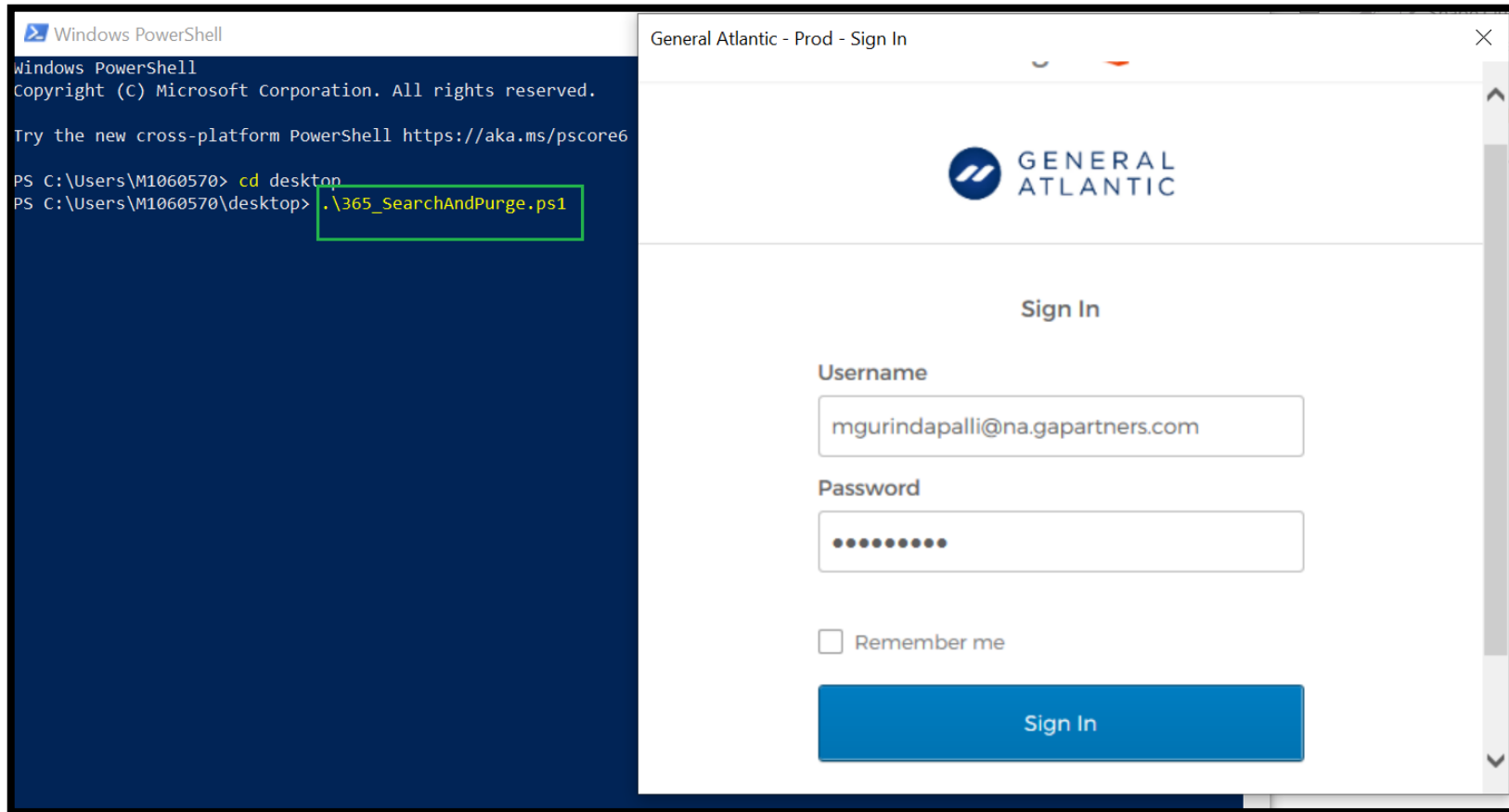
After identifying the list of users received the Phishing mail , check for the status of the mail and validate the header analysis on Mimecast.

The screenshot shows the Mimecast Message Tracking interface. The top navigation bar includes the Mimecast logo, an 'Administration' dropdown, a search bar for 'Mimecaster Central', and user information for 'mgurindapalli@generalatlan... GA Help Desk Administrator'. The main header shows 'Message Center > Message Tracking' and a timestamp 'Last refreshed today at 3:56 A'. The 'Message Tracking' section has a subtitle 'Search the message status queues to troubleshoot recent message delivery.' and two search tabs: 'Search by Data' (selected) and 'Search by ID'. Below these are search filters: 'From' (no-reply@dropbox.com), 'To' (Email address or domain), 'Date Range' (Past 48 hours), 'Subject' (empty), and 'Sender IP Address' (e.g. 000.000.000.000). A 'Search' button is on the right. Below the filters is an 'Export Results' button and a pagination indicator '1-5 of 5'. The main content area shows a table of search results with columns: Status, From (Header), To, Subject, Date/Time, IP Address, Info, and a settings gear icon. The table contains two rows: one with status 'Bounced' and another with status 'Archived'. Both rows show the same email details: from no-reply@dropbox.com, to dgeorge@generalatlan..., subject 'You're almost out of space!', date/time '07 Oct 2020 - 11:39:50' and '07 Oct 2020 - 11:39:00', IP address '104.47.74.10' and '54.240.60.158', and info 'Hard Bounce' and 'Indexed and archived'. The 'Status' column is highlighted with a red box.

Status	From (Header)	To	Subject	Date/Time	IP Address	Info	
Bounced	no-reply@dropbox.com	dgeorge@generalatlan...	You're almost out of space!	07 Oct 2020 - 11:39:50	104.47.74.10	Hard Bounce	...
Archived	no-reply@dropbox.com	dgeorge@generalatlan...	You're almost out of space!	07 Oct 2020 - 11:39:00	54.240.60.158	Indexed and archived	...

Once it is found to be Phishing mail the below steps will be followed:

- initiate the purging operation by running the [power shell Script](#)



- After validating GA credentials take the sender email id and mention that mail-id when it is prompted by the power shell Script
- If we want to purge the email only for the reported user enter the subject as it is received in the mail and email that arrived today[Y/N:] hit on Y
- If we want to purge the mail from all the recipients of Phishing email from the same sender then need to mention only sender mail-id.

```

Windows PowerShell
Enter in content search name [InfoSec_2020-10-07T23:20:48]:
Enter Sender or leave blank to search all senders: no-reply@dropbox.com
Enter subject or leave blank to search all subjects: Nathan Hoffman sent you "Frankford Candy, Payment.pdf "
Search only email that arrived today? [Y/n]: Y

Query used: From:"no-reply@dropbox.com" AND Subject:Nathan Hoffman sent you ` "Frankford Candy, Payment.pdf` " AND Received:10/7/2020

InProgress
InProgress
InProgress

Number of mailboxes that have search hits: 1
jmckegney@generalatlantic.com

Purge these emails? [y/N]: Y

Confirm
Are you sure you want to perform this action?
This operation will make message items meeting the criteria of the compliance search "InfoSec_2020-10-07T23:20:48"
completely inaccessible to users. There is no automatic method to undo the removal of these message items.
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"): Y

InProgress
InProgress
InProgress
InProgress

Purge Completed

```


- If the recipient doesn't want to receive any further mails from the sender, we can block the sender in Mimecast and hit on save and Exit.
- Administration -> Gateway -> Managed Senders

The screenshot displays the Mimecast Administration interface. At the top, the 'mimecast' logo is on the left, followed by a settings icon and the 'Administration' dropdown menu. A search bar labeled 'Search Mimecaster Central' is on the right. Below the header, a breadcrumb trail shows 'Dashboard', 'Message Tracki...', and 'Managed Send...'. The main content area is titled 'Gateway > Managed Senders'. At the top of this section are 'Go Back' and 'Save and Exit' buttons. Below them is a 'Managed Senders Selection' form. The form contains four fields: 'Sender Address / Domain' with the value 'no-reply@dropbox.com', 'To Address' with the value 'jmckegney@generalatlantic.com', 'Action' with a dropdown menu set to 'BLOCK', and 'Trust Sender' with an unchecked checkbox. Each input field has a help icon (question mark) to its right. The 'Save and Exit' button and the 'BLOCK' dropdown are highlighted with red rectangular boxes.

mimecast Administration Search Mimecaster Central

Dashboard Message Tracki... Managed Send...

Gateway > Managed Senders

Go Back Save and Exit

Managed Senders Selection

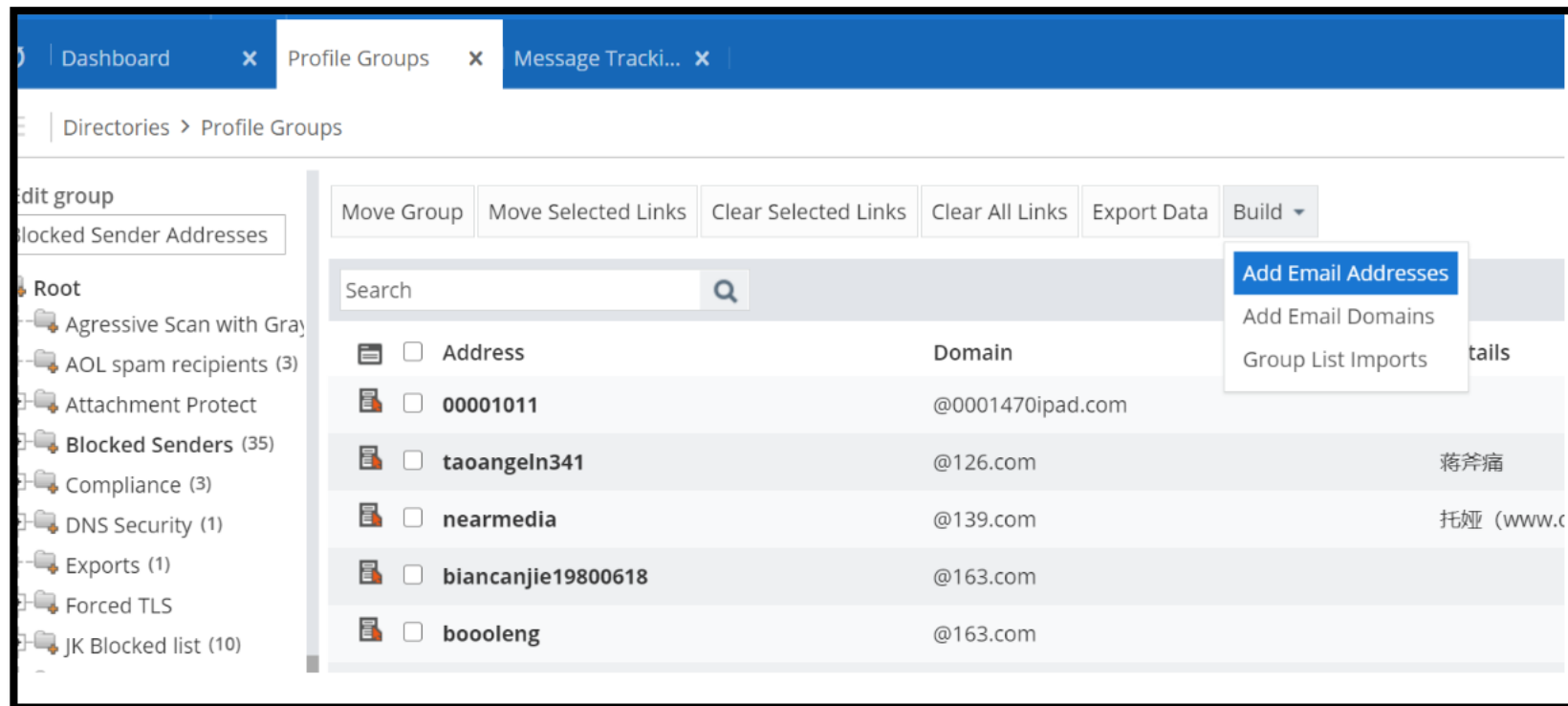
Sender Address / Domain no-reply@dropbox.com ?

To Address jmckegney@generalatlantic.com ?

Action BLOCK ?

Trust Sender ☐ ?

- To block the sender permanently after confirming its phishing attempt block the sender by going to:
Directories -> Profile Groups -> Blocked Senders -> Build ->Add Email address
- No user will receive any kind of mails from blocked sender
- If we want to block the Domain (We are not blocking any domains exert caution and do so only there are repeated phishing attempts from particular domain)
- Directories -> Profile Groups -> Blocked Senders -> Build ->Add Email Domains
- No user will receive any kind of mails from blocked domain



The screenshot shows a web application interface with a blue header bar containing navigation tabs: "Dashboard", "Profile Groups", and "Message Tracki...". Below the header, a breadcrumb trail reads "Directories > Profile Groups". The main content area has a "Group Additions" section with a text input field. Above the input field is a "Go Back" button and a highlighted "Save and Exit" button. The input field contains the email address "no-reply@dropbox.com" and is accompanied by the instruction "Type or paste in Email Addresses (in full) - one line per email address". Below the input field is an "Add a Note" button. At the bottom of the form, there is a text input field containing the note "INC0016859".


- Add the sender mail-id and add a note and hit on save and Exit
- The sender mail-id will be blocked permanently for all users


- For the ticket closure mention the comments and recommendations in work notes and resolve it.


<


≡

Incident
INC0016859









Follow

▼

Update

Notes

Related Records

Resolution Information

* Resolution code

Resolved – Permanent Fix Applie ▼

Resolved by

Resolved

2020-10-07 17:00:28

* Resolution notes

This is a Phishing Mail! Attacker has sent a file through the Dropbox transfer towards John McKegney. Dropbox team suggests forwarding such mails to abuse@dropbox.com for them to investigate and close it from their end. SOC Team have purged the email from the mail box of John McKegney.

Update

