

WELCOME TO



BGD e-GOV CIRT

CYBER THREAT INFORMATION SHARING PORTAL

Login

Email

Password

Login



বাংলাদেশ কম্পিউটার কাউন্সিল

# CYBER THREAT REPORT

EXPLOITATION OF MICROSOFT EXCHANGE SERVER  
VULNERABILITIES: CONTEXT BANGLADESH

Cyber threat research unit

BGD E-GOV CIRT | BANGLADESH COMPUTER COUNCIL



## Cyber Threat Report

### Exploitation of Microsoft Exchange Server Vulnerabilities: Context Bangladesh

TLP: White

Distribution: Public

Type of Threat: Microsoft Exchange Server Vulnerability Exploitation

Date: 1<sup>st</sup> April, 2021

#### Executive Summary:

In order to observe the current threat landscape, by following the latest exploitation of Microsoft Exchange Server Vulnerabilities, Cyber Threat Research Unit of BGD e-GOV CIRT recently found some IP Addresses associated to different Bangladeshi Organizations, some of these are already exploited and also some others are vulnerable to these threats.

This report includes both tactics, techniques and procedures (TTPs) and the indicators of compromise (IOCs) associated with this malicious activity. To secure against this threat, BGD e-GOV CIRT recommends organizations examine their systems for the TTPs and use the IOCs to detect any malicious activity.

If an organization discovers exploitation activity, they should assume network identity compromise and follow incident response procedures. If an organization finds no activity, they should apply available patches immediately and implement the mitigations in this Alert.

**Sources of Report:** Threat Intel Research

**Research Conducted By:** Cyber Threat Research Unit, BGD e-GOV CIRT

#### Threat Info:

- HAFNIUM targeting Exchange Servers with 0-day exploits
- CISA.gov - AA21-062A Mitigate Microsoft Exchange Server Vulnerabilities
- March 2021 Exchange Server Security Updates for older Cumulative Updates of Exchange Server
- OSINT - DearCry ransomware (abusing Exchange Server)

**Threat level:** High

#### Associated Vulnerabilities:

- [CVE-2021-26855](#) is a server-side request forgery (SSRF) vulnerability in Exchange which allowed the attacker to send arbitrary HTTP requests and authenticate as the Exchange server.
- [CVE-2021-26857](#) is an insecure deserialization vulnerability in the Unified Messaging service. Insecure deserialization is where untrusted user-controllable data is deserialized by a program. Exploiting this vulnerability gave HAFNIUM the ability to run code as SYSTEM on the Exchange server. This requires administrator permission or another vulnerability to exploit.
- [CVE-2021-26858](#) is a post-authentication arbitrary file write vulnerability in Exchange. If HAFNIUM could authenticate with the Exchange server then they could use this vulnerability to write a file to any path on the server. They could authenticate by exploiting the [CVE-2021-26855](#) SSRF vulnerability or by compromising a legitimate admin's credentials.
- [CVE-2021-27065](#) is a post-authentication arbitrary file write vulnerability in Exchange. If HAFNIUM could authenticate with the Exchange server then they could use this vulnerability to write a file to any path on the server. They could authenticate by exploiting the [CVE-2021-26855](#) SSRF vulnerability or by compromising a legitimate admin's credentials.

**Threat Actors:** HAFNIUM and some other threat actors.

**Attack Surface:** Windows Operating Systems specifically Microsoft Exchange Server.



BGD e-GOV CIRT



## Threat Index:

With coordination of threat intelligence sources, peer organization's feed and OSINT assessments BGD e-GOV CIRT identifies some attributes, IOCs and other associated information regarding exploitation of recent Microsoft Exchange Server Exploitations indicating exposures of Bangladeshi organizations.

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Add Event Report

Populate from...

Enrich Event

Merge attributes from...

Propose Attribute

Propose Attachment

Publish Sightings

Publish event to ZMQ

Download as...

List Events

Add Event

### HAFNIUM targeting Exchange Servers with 0-day exploits

|                       |                                                        |
|-----------------------|--------------------------------------------------------|
| Event ID              | 1513                                                   |
| UUID                  | 16ee036b-17f5-4f17-b3c3-9fe89176274a                   |
| Creator org           | CUDES0                                                 |
| Owner org             | BGD e-GOV CIRT                                         |
| Creator user          | admin@misp.cirt.gov.bd                                 |
| Tags                  | ttp:white                                              |
| Date                  | 2021-02-15                                             |
| Threat Level          | High                                                   |
| Analysis              | Ongoing                                                |
| Distribution          | All communities                                        |
| Info                  | HAFNIUM targeting Exchange Servers with 0-day exploits |
| Published             | Yes (2021-03-14 09:44:32)                              |
| #Attributes           | 66 (0 Objects)                                         |
| First recorded change | 2021-03-07 19:21:37                                    |
| Last change           | 2021-03-11 23:08:52                                    |
| Modification map      |                                                        |
| Sightings             | 0 (0) - restricted to own organisation only            |

Pivots

Galaxy

Event graph

Event timeline

Correlation graph

ATT&CK matrix

Event reports

Attributes

Discussion

## Related Events & Attributes:

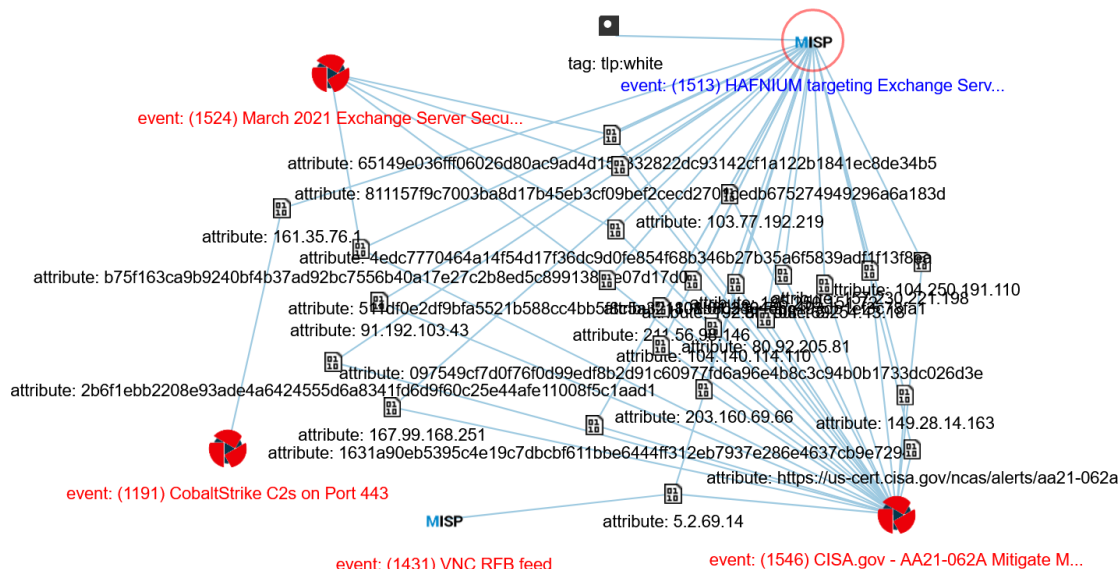


Fig: Correlated Events to Microsoft Exchange Server Exploitation

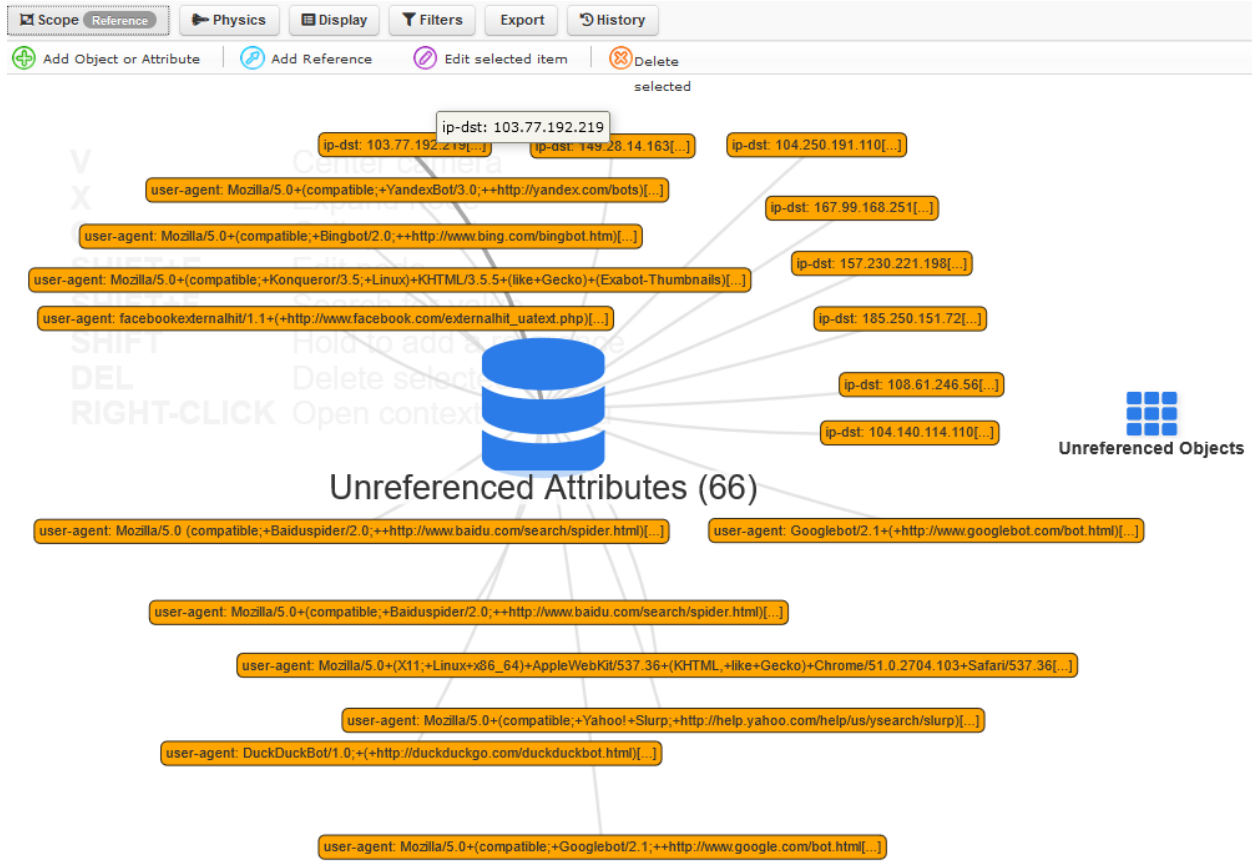


Fig-2: Community Distribution of Alert

## Compromised Bangladeshi Organizations

### Compromised with Web Shell Injection

| Country | Seen At                    | Ip             | Tls Cert Cn           | Has Web Shells | Live Web Shells Paths         |
|---------|----------------------------|----------------|-----------------------|----------------|-------------------------------|
| BD      | 2021-03-10T23:49:21.645078 | 123.200.24.82  | mail.mamiyaopb.com    | TRUE           | /aspnet_client/OutlookEN.aspx |
| BD      | 2021-03-10T23:28:46.229889 | 202.164.212.9  | mail.adury.com        | TRUE           | /aspnet_client/discover.aspx  |
| BD      | 2021-03-10T23:28:46.229889 | 202.164.212.9  | mail.adury.com        | TRUE           | /aspnet_client/0QWYSE.aspx    |
| BD      | 2021-03-10T23:43:12.471442 | 202.164.212.10 | mail.thermaxgroup.com | TRUE           | /aspnet_client/discover.aspx  |



|    |                            |                |                             |      |                               |
|----|----------------------------|----------------|-----------------------------|------|-------------------------------|
| BD | 2021-03-10T23:43:12.471442 | 202.164.212.10 | mail.thermaxgroup.com       | TRUE | /aspnet_client/0QWYSEXe.aspx  |
| BD | 2021-03-10T23:25:18.308188 | 43.240.103.204 | mail.techrepublicbd.com     | TRUE | /aspnet_client/discover.aspx  |
| BD | 2021-03-10T23:25:18.308188 | 43.240.103.204 | mail.techrepublicbd.com     | TRUE | /aspnet_client/load.aspx      |
| BD | 2021-03-10T23:10:30.451414 | 103.248.13.147 | MAILSVRSRL                  | TRUE | /aspnet_client/discover.aspx  |
| BD | 2021-03-11T00:02:35.637670 | 116.193.220.13 | ex01.selbn.com              | TRUE | /aspnet_client/OutlookEN.aspx |
| BD | 2021-03-11T00:34:44.647888 | 103.17.180.87  | rangs.com.bd                | TRUE | /aspnet_client/discover.aspx  |
| BD | 2021-03-11T00:34:44.647888 | 103.17.180.87  | rangs.com.bd                | TRUE | /aspnet_client/0QWYSEXe.aspx  |
| BD | 2021-03-11T00:34:28.657919 | 116.193.219.70 | mail.texeuropbangladesh.com | TRUE | /aspnet_client/discover.aspx  |
| BD | 2021-03-11T00:05:42.978436 | 27.147.142.150 | mail.technodrugsLtd.com     | TRUE | /aspnet_client/discover.aspx  |
| BD | 2021-03-11T00:30:13.694953 | 103.250.69.202 | *.enafood.com               | TRUE | /aspnet_client/discover.aspx  |
| BD | 2021-03-11T00:34:28.657919 | 116.193.219.70 | mail.texeuropbangladesh.com | TRUE | /aspnet_client/0QWYSEXe.aspx  |
| BD | 2021-03-11T00:05:42.978436 | 27.147.142.150 | mail.technodrugsLtd.com     | TRUE | /aspnet_client/0QWYSEXe.aspx  |
| BD | 2021-03-11T00:30:13.694953 | 103.250.69.202 | *.enafood.com               | TRUE | /aspnet_client/0QWYSEXe.aspx  |
| BD | 2021-03-11T00:05:42.978436 | 27.147.142.150 | mail.technodrugsLtd.com     | TRUE | /aspnet_client/OutlookEN.aspx |



|    |                            |                 |                          |      |                              |
|----|----------------------------|-----------------|--------------------------|------|------------------------------|
| BD | 2021-03-11T00:48:24.686780 | 116.193.216.234 | emailtiger.data-path.net | TRUE | /aspnet_client/discover.aspx |
| BD | 2021-03-11T00:48:24.686780 | 116.193.216.234 | emailtiger.data-path.net | TRUE | /aspnet_client/0QWYSEXe.aspx |

## Vulnerable Assets

Below mentioned IP addresses/ assets are found vulnerable and are in risk to these vulnerabilities:

| Country | Seen At                    | Has Web Shells | Ip             | Longname                           | Tls Cert Cn         | vulnerable |
|---------|----------------------------|----------------|----------------|------------------------------------|---------------------|------------|
| BD      | 2021-03-10T23:35:21.462648 | FALSE          | 116.68.194.90  | Agni Systems Ltd.                  | MKMAIL01            | TRUE       |
| BD      | 2021-03-10T23:43:46.283846 | FALSE          | 119.148.9.2    | Agni Systems Ltd.                  | mail.radiant.com.bd | TRUE       |
| BD      | 2021-03-11T00:22:43.681016 | FALSE          | 116.68.205.230 | Agni Systems Ltd.                  | mail.aci-bd.com     | TRUE       |
| BD      | 2021-03-11T00:51:21.403414 | FALSE          | 119.148.54.151 | Agni Systems Ltd.                  | *.buft.edu.bd       | TRUE       |
| BD      | 2021-03-10T22:56:34.406092 | FALSE          | 103.9.185.11   | Bangla Trac Communications Limited | mail2.btraccl.com   | TRUE       |
| BD      | 2021-03-11T00:06:53.737211 | FALSE          | 103.46.149.65  | Bangladesh Army                    | *.army.mil.bd       | TRUE       |
| BD      | 2021-03-11T00:06:53.737211 | FALSE          | 103.46.149.65  | Bangladesh Army                    | *.army.mil.bd       | TRUE       |
| BD      | 2021-03-10T22:56:40.729785 | FALSE          | 114.130.42.60  | Bangladesh Bank                    | *.bb.org.bd         | TRUE       |
| BD      | 2021-03-10T23:36:01.342123 | FALSE          | 202.164.210.69 | Bangladesh Bank                    | mail.nrgroup-bd.com | TRUE       |
| BD      | 2021-03-11T00:47:28.994687 | FALSE          | 202.164.210.68 | Bangladesh Bank                    | mail.nrgroup-bd.com | TRUE       |
| BD      | 2021-03-10T23:12:56.870879 | FALSE          | 202.164.210.67 | Bangladesh Bank                    | mail.nrgroup-bd.com | TRUE       |
| BD      | 2021-03-11T00:06:53.737211 | FALSE          | 103.46.149.65  | bangladesh.gov.bd                  | *.army.mil.bd       | TRUE       |
| BD      | 2021-03-11T00:06:53.737211 | FALSE          | 103.46.149.65  | bangladesh.gov.bd                  | *.army.mil.bd       | TRUE       |
| BD      | 2021-03-10T23:43:58.768452 | FALSE          | 103.98.64.6    | btrc.gov.bd                        | mail.btrc.gov.bd    | TRUE       |
| BD      | 2021-03-11T00:16:58.849050 | FALSE          | 103.98.64.7    | btrc.gov.bd                        | mail.btrc.gov.bd    | TRUE       |



|    |                            |       |                 |                                  |                              |      |
|----|----------------------------|-------|-----------------|----------------------------------|------------------------------|------|
| BD | 2021-03-10T23:35:59.658954 | FALSE | 203.202.242.106 | Evercare Group Management Group  | mail.apollodhaka.com         | TRUE |
| BD | 2021-03-10T23:35:59.658954 | FALSE | 203.202.242.106 | Evercare Group Management Group  | mail.apollodhaka.com         | TRUE |
| BD | 2021-03-10T23:35:59.658954 | FALSE | 203.202.242.106 | Evercare Hospital Dhaka          | mail.apollodhaka.com         | TRUE |
| BD | 2021-03-10T23:35:59.658954 | FALSE | 203.202.242.106 | Evercare Hospital Dhaka          | mail.apollodhaka.com         | TRUE |
| BD | 2021-03-10T23:19:12.291542 | FALSE | 202.4.98.146    | Gas Transmission Company Limited | mail.gtcl.org.bd             | TRUE |
| BD | 2021-03-10T23:13:06.526193 | FALSE | 103.249.56.9    | LankaBangla Finance Ltd.         | *.lankabangla.com            | TRUE |
| BD | 2021-03-10T23:39:08.281834 | FALSE | 118.179.130.250 | Standard Bank Limited            | sblexch03.standardbankbd.com | TRUE |
| BD | 2021-03-10T23:39:08.281834 | FALSE | 118.179.130.250 | Standard Bank Limited            | sblexch03.standardbankbd.com | TRUE |
| BD | 2021-03-11T00:28:28.890888 | FALSE | 118.179.131.243 | Standard Bank Limited            | sblexch03.standardbankbd.com | TRUE |
| BD | 2021-03-11T00:28:28.890888 | FALSE | 118.179.131.243 | Standard Bank Limited            | sblexch03.standardbankbd.com | TRUE |
| BD | 2021-03-11T00:30:28.117421 | FALSE | 118.179.131.51  | Standard Bank Limited            | sblexch03.standardbankbd.com | TRUE |
| BD | 2021-03-11T00:30:28.117421 | FALSE | 118.179.131.51  | Standard Bank Limited            | sblexch03.standardbankbd.com | TRUE |
| BD | 2021-03-11T00:28:28.890888 | FALSE | 118.179.131.243 | sunshine-zone.com                | sblexch03.standardbankbd.com | TRUE |
| BD | 2021-03-11T00:28:28.890888 | FALSE | 118.179.131.243 | sunshine-zone.com                | sblexch03.standardbankbd.com | TRUE |
| BD | 2021-03-11T00:01:56.899096 | FALSE | 202.4.124.12    | sunshine-zone.com                | *.rupashigroup.com           | TRUE |
| BD | 2021-03-10T23:39:08.281834 | FALSE | 118.179.130.250 | sunshine-zone.com                | sblexch03.standardbankbd.com | TRUE |
| BD | 2021-03-10T23:39:08.281834 | FALSE | 118.179.130.250 | sunshine-zone.com                | sblexch03.standardbankbd.com | TRUE |
| BD | 2021-03-11T00:30:28.117421 | FALSE | 118.179.131.51  | sunshine-zone.com                | sblexch03.standardbankbd.com | TRUE |
| BD | 2021-03-11T00:30:28.117421 | FALSE | 118.179.131.51  | sunshine-zone.com                | sblexch03.standardbankbd.com | TRUE |
| BD | 2021-03-10T23:38:39.756589 | FALSE | 203.76.108.151  | Trust Bank                       | *.tblbd.com                  | TRUE |



|    |                            |       |                 |  |                            |      |
|----|----------------------------|-------|-----------------|--|----------------------------|------|
| BD | 2021-03-10T22:57:16.452223 | FALSE | 180.92.225.85   |  | mail.farr.com.bd           | TRUE |
| BD | 2021-03-10T23:58:48.288971 | FALSE | 27.147.133.109  |  | mail.paragon.com.bd        | TRUE |
| BD | 2021-03-10T23:23:23.953000 | FALSE | 202.5.56.71     |  | Mailserver                 | TRUE |
| BD | 2021-03-10T23:14:19.691655 | FALSE | 43.240.103.169  |  | mail.asrotex.com           | TRUE |
| BD | 2021-03-10T23:40:07.044153 | FALSE | 118.67.215.167  |  | email.novoair-bd.com       | TRUE |
| BD | 2021-03-10T23:35:04.241810 | FALSE | 118.67.222.147  |  | EXSRV01                    | TRUE |
| BD | 2021-03-10T23:21:54.386104 | FALSE | 182.160.123.43  |  | mail.nextslbd.com          | TRUE |
| BD | 2021-03-10T23:24:45.364745 | FALSE | 202.126.127.67  |  | *.akij.net                 | TRUE |
| BD | 2021-03-10T23:12:18.924314 | FALSE | 111.221.0.220   |  | mail.sisalapparel.com.bd   | TRUE |
| BD | 2021-03-10T23:06:15.639399 | FALSE | 43.240.102.44   |  | mail.bitopibd.com          | TRUE |
| BD | 2021-03-10T23:46:02.365942 | FALSE | 103.157.74.6    |  | mail.modhumotibankltd.com  | TRUE |
| BD | 2021-03-10T23:32:27.796927 | FALSE | 43.240.102.54   |  | *.mfghbd.net               | TRUE |
| BD | 2021-03-10T23:04:36.838722 | FALSE | 103.112.147.201 |  | *.rhd.gov.bd               | TRUE |
| BD | 2021-03-10T23:10:30.802501 | FALSE | 103.250.69.233  |  | Mailserver                 | TRUE |
| BD | 2021-03-10T23:06:48.648987 | FALSE | 123.200.12.12   |  | mail.mplmagnum.com         | TRUE |
| BD | 2021-03-10T23:02:15.140312 | FALSE | 202.40.181.86   |  | *.rangsgroup.com           | TRUE |
| BD | 2021-03-10T23:07:05.559772 | FALSE | 182.160.122.43  |  | mail.newzealanddairybd.com | TRUE |
| BD | 2021-03-10T23:27:18.537957 | FALSE | 175.29.186.153  |  | www.nbrtax.gov.bd          | TRUE |
| BD | 2021-03-10T23:45:01.101107 | FALSE | 180.210.132.41  |  | *.meghnabank.com.bd        | TRUE |
| BD | 2021-03-10T23:20:51.382148 | FALSE | 103.206.184.21  |  | prgmail.prangroup.com      | TRUE |



|    |                            |       |                 |  |                           |      |
|----|----------------------------|-------|-----------------|--|---------------------------|------|
| BD | 2021-03-10T22:59:58.990015 | FALSE | 103.17.69.62    |  | mail.bankasia-bd.com      | TRUE |
| BD | 2021-03-10T23:53:02.363844 | FALSE | 27.147.133.110  |  | mail.paragon.com.bd       | TRUE |
| BD | 2021-03-10T23:30:24.047015 | FALSE | 116.193.221.46  |  | mail.sfdw.org             | TRUE |
| BD | 2021-03-10T23:29:41.263802 | FALSE | 43.240.103.167  |  | mail.asrotex.com          | TRUE |
| BD | 2021-03-10T23:02:34.660137 | FALSE | 103.36.102.235  |  | mail.runnerbd.com         | TRUE |
| BD | 2021-03-10T23:59:01.402550 | FALSE | 103.36.102.227  |  | mail.runnerbd.com         | TRUE |
| BD | 2021-03-10T23:44:17.372923 | FALSE | 163.47.84.187   |  | *.pacificjeans.com        | TRUE |
| BD | 2021-03-10T23:13:08.510420 | FALSE | 116.212.106.145 |  | *.basicbanklimited.com    | TRUE |
| BD | 2021-03-10T23:03:08.282336 | FALSE | 118.67.215.240  |  | email.novoair-bd.com      | TRUE |
| BD | 2021-03-10T23:51:58.448241 | FALSE | 116.212.106.146 |  | *.basicbanklimited.com    | TRUE |
| BD | 2021-03-10T23:02:18.323239 | FALSE | 103.155.96.99   |  | *.akijresources.com       | TRUE |
| BD | 2021-03-10T23:46:57.888851 | FALSE | 103.114.171.31  |  | *.ssgbd.com               | TRUE |
| BD | 2021-03-10T23:27:19.666631 | FALSE | 182.160.117.173 |  | *.citygroupbd.com         | TRUE |
| BD | 2021-03-10T23:27:51.367135 | FALSE | 103.36.103.68   |  | *.metro.net.bd            | TRUE |
| BD | 2021-03-10T23:02:59.127076 | FALSE | 103.157.74.5    |  | mail.modhumotibankltd.com | TRUE |
| BD | 2021-03-10T23:15:54.214795 | FALSE | 103.206.184.17  |  | prgmail.prangroup.com     | TRUE |
| BD | 2021-03-10T23:22:20.304779 | FALSE | 103.206.185.3   |  | mail.rflgroupbd.com       | TRUE |
| BD | 2021-03-10T23:45:46.321177 | FALSE | 45.251.57.131   |  | mail.amanknittings.com    | TRUE |
| BD | 2021-03-10T23:53:26.101119 | FALSE | 118.67.218.230  |  | *.mfcbd.net               | TRUE |
| BD | 2021-03-10T23:13:55.368037 | FALSE | 119.40.88.26    |  | mail.bcbl.com.bd          | TRUE |



|    |                            |       |                 |  |                               |      |
|----|----------------------------|-------|-----------------|--|-------------------------------|------|
| BD | 2021-03-10T23:05:21.566015 | FALSE | 203.202.241.123 |  | *.bg.com.bd                   | TRUE |
| BD | 2021-03-10T23:48:22.884143 | FALSE | 120.50.25.53    |  | *.bg.com.bd                   | TRUE |
| BD | 2021-03-10T23:58:01.307567 | FALSE | 103.254.85.161  |  | *.bdbl.com.bd                 | TRUE |
| BD | 2021-03-10T23:08:05.706842 | FALSE | 103.15.246.57   |  | mail.summitcommunications.net | TRUE |
| BD | 2021-03-11T00:00:16.188835 | FALSE | 220.247.167.82  |  | *.pbi.gov.bd                  | TRUE |
| BD | 2021-03-11T00:18:21.521923 | FALSE | 202.5.36.70     |  | mail.bd.soorty.com            | TRUE |
| BD | 2021-03-11T00:10:01.820816 | FALSE | 103.36.100.194  |  | mail.rosesweater.com          | TRUE |
| BD | 2021-03-11T00:17:26.379999 | FALSE | 182.163.96.242  |  | mail.edra-bd.energy           | TRUE |
| BD | 2021-03-11T00:00:48.090010 | FALSE | 124.109.104.29  |  | mail.mtbexchangebd.com        | TRUE |
| BD | 2021-03-11T00:20:17.949378 | FALSE | 202.40.176.66   |  | *.rancon.com.bd               | TRUE |
| BD | 2021-03-11T00:16:58.867156 | FALSE | 103.105.74.15   |  | *.standard-group.com          | TRUE |
| BD | 2021-03-11T00:58:43.362208 | FALSE | 116.193.217.90  |  | mail.circle-bd.com            | TRUE |
| BD | 2021-03-11T00:32:55.160562 | FALSE | 202.59.140.116  |  | webmail.vmail360.com          | TRUE |
| BD | 2021-03-11T00:01:32.798884 | FALSE | 103.254.85.162  |  | *.bdbl.com.bd                 | TRUE |
| BD | 2021-03-11T00:13:45.908224 | FALSE | 203.202.240.83  |  | mail.bengalglass.com          | TRUE |
| BD | 2021-03-11T00:32:50.422909 | FALSE | 221.120.103.74  |  | mail2.btraceng.com            | TRUE |
| BD | 2021-03-11T00:34:31.182087 | FALSE | 43.240.102.43   |  | mail.bitopibd.com             | TRUE |
| BD | 2021-03-11T00:23:08.879310 | FALSE | 202.59.140.104  |  | *.squaregroup.com             | TRUE |
| BD | 2021-03-11T00:14:24.466573 | FALSE | 116.193.221.102 |  | mail.sfdw.org                 | TRUE |
| BD | 2021-03-11T00:07:27.752557 | FALSE | 43.240.100.135  |  | *.metro.net.bd                | TRUE |



|    |                            |       |                 |  |                             |      |
|----|----------------------------|-------|-----------------|--|-----------------------------|------|
| BD | 2021-03-11T00:11:07.250553 | FALSE | 210.4.76.220    |  | mail.jamunabank.com.bd      | TRUE |
| BD | 2021-03-11T00:07:40.627588 | FALSE | 182.160.123.42  |  | mail.nextslbd.com           | TRUE |
| BD | 2021-03-11T00:35:36.386271 | FALSE | 202.5.62.65     |  | EX-01                       | TRUE |
| BD | 2021-03-11T00:23:41.925716 | FALSE | 103.36.100.195  |  | mail.rosesweater.com        | TRUE |
| BD | 2021-03-11T00:39:29.239376 | FALSE | 45.64.134.201   |  | webmail.viyellatexgroup.com | TRUE |
| BD | 2021-03-11T00:22:43.126788 | FALSE | 182.163.114.98  |  | mail.edra-bd.energy         | TRUE |
| BD | 2021-03-11T00:39:54.109507 | FALSE | 27.147.133.174  |  | mail.creativepapermills.com | TRUE |
| BD | 2021-03-11T00:45:13.622148 | FALSE | 116.193.217.126 |  | mail.octopibd.com           | TRUE |
| BD | 2021-03-11T00:41:57.386337 | FALSE | 118.67.215.230  |  | email.novotel-bd.com        | TRUE |
| BD | 2021-03-11T00:29:23.833967 | FALSE | 118.67.215.154  |  | email.novotel-bd.com        | TRUE |
| BD | 2021-03-11T00:47:59.675944 | FALSE | 103.114.170.31  |  | *.sugbd.com                 | TRUE |
| BD | 2021-03-11T00:15:39.556373 | FALSE | 116.193.217.92  |  | webmail.goldenbd.net        | TRUE |
| BD | 2021-03-10T23:19:29.169052 | FALSE | 103.155.96.35   |  | *.akijholding.com           | TRUE |
| BD | 2021-03-10T23:25:24.234033 | FALSE | 202.164.212.90  |  | *.pakizaknit.com            | TRUE |
| BD | 2021-03-10T23:34:29.950226 | FALSE | 180.210.132.42  |  | *.meghnabank.com.bd         | TRUE |
| BD | 2021-03-10T23:37:17.759319 | FALSE | 119.40.88.25    |  | mail.bcbl.com.bd            | TRUE |
| BD | 2021-03-10T23:42:59.017110 | FALSE | 210.4.76.215    |  | mail.jamunabank.com.bd      | TRUE |
| BD | 2021-03-10T23:16:18.931404 | FALSE | 45.251.57.132   |  | mail.amanknittings.com      | TRUE |
| BD | 2021-03-10T23:15:14.874789 | FALSE | 202.164.208.25  |  | ramail.rahimafrooz.com      | TRUE |
| BD | 2021-03-10T23:09:39.541009 | FALSE | 103.248.13.138  |  | spectrum-bd.com             | TRUE |



|    |                            |       |                 |  |                        |      |
|----|----------------------------|-------|-----------------|--|------------------------|------|
| BD | 2021-03-10T23:34:46.846670 | FALSE | 203.76.126.214  |  | mail.bd.soorty.com     | TRUE |
| BD | 2021-03-11T00:59:01.756776 | FALSE | 115.127.82.116  |  | mail.anwargroup.net    | TRUE |
| BD | 2021-03-11T00:03:38.134775 | FALSE | 103.106.238.197 |  | mail.reyesltd.com      | TRUE |
| BD | 2021-03-11T00:46:18.536061 | FALSE | 103.155.96.131  |  | *.akijventure.com      | TRUE |
| BD | 2021-03-11T00:46:12.629124 | FALSE | 202.164.208.27  |  | ramail.rahimafooz.com  | TRUE |
| BD | 2021-03-11T00:40:17.231253 | FALSE | 203.76.102.130  |  | webmail.caritasbd.org  | TRUE |
| BD | 2021-03-10T23:51:42.845154 | FALSE | 27.147.152.86   |  | *.dhakabank.com.bd     | TRUE |
| BD | 2021-03-11T00:38:47.206244 | FALSE | 175.29.186.154  |  | www.nbrtax.gov.bd      | TRUE |
| BD | 2021-03-11T00:41:45.179718 | FALSE | 103.218.164.11  |  | mail.cg-bd.com         | TRUE |
| BD | 2021-03-10T23:54:49.088933 | FALSE | 182.160.124.44  |  | mail.auko-texgroup.com | TRUE |
| BD | 2021-03-10T23:41:22.456493 | FALSE | 202.84.36.19    |  | *.bpl.net              | TRUE |
| BD | 2021-03-10T23:38:43.579180 | FALSE | 202.164.208.22  |  | ramail.rahimafooz.com  | TRUE |

## Focused Threat Actor

The focused threat actor behind the malware is known as '**HAFNIUM**'. This is also observed that, *there are activities of several hacker groups that exploit vulnerabilities in Microsoft Exchange.*

HAFNIUM, a group assessed to be state-sponsored and operating out of China, based on observed victimology, tactics and procedures. HAFNIUM primarily targets entities in the United States across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs. This group has overlaps in tactics and technique with other Chinese hacker groups. If we establish an exact match with another known group, we will supplement it with this profile.

## Targeted Countries

 Chile  United States  Germany  Canada  France

 Uzbekistan  Bangladesh  Belgium  Hong Kong  Italy  Kazakhstan

 South Korea  Turkey  United Arab Emirates  Slovenia  Pakistan  Mongolia

 Israel  Guyana  Brazil  Russian Federation  South Africa  Mauritius

## Targeted Industries/ Sectors

- Banking & Finance
- government-local
- healthcare
- Law and Law Enforcement Agencies
- Defense
- Heavy industries and engineering
- Aerospace
- Science-and-education: universities and colleges
- Energy & Power
- Non-profit

## Recent ACTIVITIES

- **15<sup>th</sup> March' 2021:** Chile's bank regulator was compromised through ProxyLogon vulnerabilities  
Chile's **Comisión para el Mercado Financiero (CMF)** has disclosed that their Microsoft Exchange server was compromised through the recently disclosed ProxyLogon vulnerabilities (Microsoft Exchange). The CMF operates under the Ministry of Finance and is the regulator and inspector for banks and financial institutions in Chile.
- **5<sup>th</sup> March' 2021 – 10<sup>th</sup> march' 2021:** New information about stages of HAFNIUM group attack.
- **1<sup>st</sup> march' 2021 – 13<sup>th</sup> March' 2021:** New indicators of attack with the vulnerabilities in Microsoft Exchange Server products.  
A researcher identifies web-shells associated with exploitation of the vulnerabilities in Microsoft Exchange Server products. After successful exploiting a Microsoft Exchange Server vulnerability for initial accesses, a malicious cyber actor can upload a web-shell to enable remote administration of the affected system.
- **1<sup>st</sup> January' 2021 – 2<sup>nd</sup> March' 2021:** HAFNIUM targeting Exchange Servers with 0-day exploits

## Infection Chain

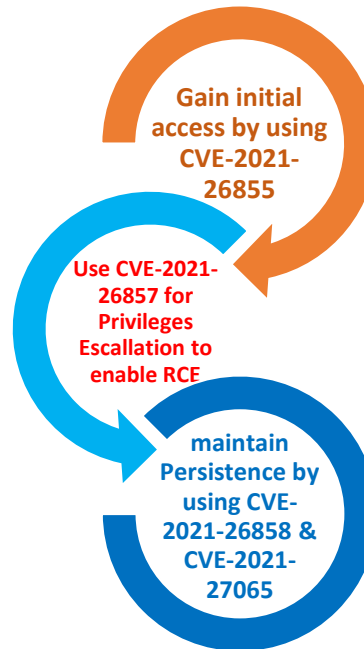


Fig: Infection Chain

| Initial Access<br>9 techniques                                                                                                                                                                                                                       | Execution<br>10 techniques                                                                                                                                                                                                                                                                  | Persistence<br>18 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Privilege Escalation<br>12 techniques                                                                                                                                                                                                                                                                                                                                                                                                          | Defense Evasion<br>37 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Credential Access<br>15 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                              | Discovery<br>25 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Lateral Movement<br>9 techniques                                                                                                                                                                                                                                                           | Collection<br>17 techniques                                                                                                                                                                                                                                                                                                                                                                                                             | Command and Control<br>16 techniques                                                                                                                                                                                                                                                                                                                                                                                    | Exfiltration<br>9 techniques                                                                                                                                                                                                                                                                                                                                                           | Impact<br>13 techniques                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Drive-by Compromise<br>Exploit Public-Facing Application<br>External Remote Services<br>Hardware Additions<br>Phishing (0/3)<br>Replication Through Removable Media<br>Supply Chain Compromise (0/3)<br>Trusted Relationship<br>Valid Accounts (0/4) | Command and Scripting Interpreter<br>Exploitation for Client Execution<br>Inter-Process Communication (0/2)<br>Native API<br>Scheduled Task/Job (0/6)<br>Shared Modules<br>Software Deployment Tools<br>System Services (0/2)<br>User Execution (0/2)<br>Windows Management Instrumentation | Account Manipulation (0/4)<br>BITS Jobs<br>Boot or Logon Autostart Execution (0/12)<br>Boot or Logon Initialization Scripts (0/5)<br>Browser Extensions<br>Compromise Client Software Binary<br>Create Account<br>Create or Modify System Process (0/4)<br>Event Triggered Execution (0/15)<br>External Remote Services<br>Hijack Execution Flow (0/11)<br>Hijack Execution Flow (0/11)<br>Implant Container Image<br>Office Application Startup (0/6)<br>Pre-OS Boot (0/5)<br>Scheduled Task/Job (0/6)<br>Server Software Component (0/3)<br>Traffic Signaling (0/1)<br>Valid Accounts (0/4) | Abuse Elevation Control Mechanism (0/4)<br>Access Token Manipulation (0/5)<br>Boot or Logon Autostart Execution (0/12)<br>Boot or Logon Initialization Scripts (0/5)<br>Create or Modify System Process (0/4)<br>Domain Policy Modification (0/2)<br>Event Triggered Execution (0/15)<br>Exploitation for Privilege Escalation<br>Hijack Execution Flow (0/11)<br>Process Injection (0/11)<br>Scheduled Task/Job (0/6)<br>Valid Accounts (0/4) | Abuse Elevation Control Mechanism (0/4)<br>Access Token Manipulation (0/5)<br>BITS Jobs<br>Deobfuscate/Decode Files or Information<br>Direct Volume Access<br>Domain Policy Modification (0/2)<br>Execution Guardrails (0/1)<br>Exploitation for Defense Evasion<br>File and Directory Permissions Modification (0/2)<br>Hide Artifacts (0/7)<br>Hijack Execution Flow (0/11)<br>Indicator Removal on Host (0/6)<br>Indirect Command Execution<br>Masquerading (0/6)<br>Modify Authentication Process (0/4)<br>Modify Cloud Compute Infrastructure (0/4)<br>Modify Registry (0/2)<br>Modify System Image (0/2)<br>Network Boundary Bridging (0/1)<br>Obfuscated Files or Information (0/2)<br>Pre-OS Boot (0/5)<br>Process Injection (0/11)<br>Rogue Domain Controller | Brute Force (0/4)<br>Credentials from Password Stores (0/3)<br>Exploitation for Credential Access<br>Forced Authentication<br>Forge Web Credentials (0/2)<br>Input Capture (0/4)<br>Man-in-the-Middle (0/2)<br>Modify Authentication Process (0/4)<br>Network Sniffing<br>OS Credential Dumping<br>Steal Application Access Token<br>Steal or Forge Kerberos Tickets (0/4)<br>Steal Web Session Cookie<br>Two-Factor Authentication Interception<br>Unsecured Credentials (0/6) | Account Discovery<br>Application Window Discovery<br>Browser Bookmark Discovery<br>Cloud Infrastructure Discovery<br>Cloud Service Dashboard<br>Cloud Service Discovery<br>Domain Trust Discovery<br>File and Directory Discovery<br>Network Service Scanning<br>Network Share Discovery<br>Network Sniffing<br>Password Policy Discovery<br>Peripheral Device Discovery<br>Permission Groups Discovery (0/3)<br>Process Discovery<br>Query Registry<br>Remote System Discovery<br>Software Discovery (0/1)<br>System Information Discovery<br>System Network Configuration Discovery<br>System Network Connections Discovery<br>System Owner/User Discovery<br>System Service Discovery | Exploitation of Remote Services<br>Internal Spearphishing<br>Lateral Tool Transfer<br>Remote Service Session Hijacking (0/2)<br>Remote Services<br>Replication Through Removable Media<br>Software Deployment Tools<br>Taint Shared Content<br>Use Alternate Authentication Material (0/4) | Archive Collected Data (0/3)<br>Audio Capture<br>Automated Collection<br>Clipboard Data<br>Data from Cloud Storage Object<br>Data from Configuration Repository (0/2)<br>Data from Information Repositories (0/2)<br>Data from Local System<br>Data from Network Shared Drive<br>Data Staged (0/2)<br>Email Collection (0/3)<br>Input Capture (0/4)<br>Man in the Browser<br>Man-in-the-Middle (0/2)<br>Screen Capture<br>Video Capture | Application Layer Protocol<br>Communication Through Removable Media<br>Data Encoding (0/2)<br>Data Obfuscation (0/3)<br>Dynamic Resolution (0/3)<br>Encrypted Channel (0/2)<br>Fallback Channels<br>Ingress Tool Transfer<br>Multi-Stage Channels<br>Non-Application Layer Protocol<br>Non-Standard Port<br>Protocol Tunneling<br>Proxy (0/4)<br>Remote Access Software<br>Traffic Signaling (0/1)<br>Web Service (0/3) | Automated Exfiltration (0/1)<br>Data Transfer Size Limits<br>Data Encrypted for Impact<br>Data Manipulation (0/3)<br>Defacement (0/2)<br>Disk Wipe (0/2)<br>Endpoint Denial of Service (0/4)<br>Exfiltration Over Other Network Medium (0/1)<br>Exfiltration Over Physical Medium (0/1)<br>Exfiltration Over Web Service (0/2)<br>Scheduled Transfer<br>Transfer Data to Cloud Account | Account Access Removal<br>Data Destruction<br>Data Encrypted for Impact<br>Data Manipulation (0/3)<br>Defacement (0/2)<br>Disk Wipe (0/2)<br>Endpoint Denial of Service (0/4)<br>Firmware Corruption<br>Inhibit System Recovery<br>Network Denial of Service (0/2)<br>Resource Hijacking<br>Service Stop<br>System Shutdown/Reboot |

Fig: Followed MITRE ATT&CK Techniques



## Indicator of Compromises (IOCs)

## FILE NAMES, TYPES &amp; HASHES

| DETAIL DESCRIPTION of THE MALWARES                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Suspicious File                                                                | IOC and Other Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Category:</b> Backdoor<br><b>Name:</b> zXkZu6bn.aspx                        | <b>File name:</b> zXkZu6bn.aspx<br><b>File Size:</b> 2287 bytes<br><b>File Types:</b> HTML document, ASCII text, with CRLF line terminators<br><b>File Hashes:</b> <ul style="list-style-type: none"> <li>MD5: 3e9201b5021dccc29ada4b74e79f2790</li> <li>SHA1: 32f7b3cddf1e8670cc2725107313fc7c6a90ad94</li> <li>SHA256:<br/>71ff78f43c60a61566dac1a923557670e5e832c4adfe5efb91cac7d8386b70e0</li> <li>SHA512:<br/>8a1cf70640ef649ba06db5d1d65f436e5f8d339bd0622a30b026c6c3af9092e1c44be5c2a943d8adb1a122df678ddf258aa05d922ee856e94bd383300fd89453</li> </ul> |
| <b>Category:</b> Backdoor<br><b>Name:</b> shell.aspx                           | <b>File Name:</b> shell.aspx<br><b>File Size:</b> 2292 bytes<br><b>File Type:</b> ASCII text, with CRLF line terminators<br><b>File Hashes:</b> <ul style="list-style-type: none"> <li>MD5: 81a94d49a40cbb980b33c9365e9c102f</li> <li>SHA1: eaae8f25c1062b7d61a6e1a0a2e3d0e3bb9cc7d0</li> <li>SHA256:<br/>ee883200fb1c58d22e6c642808d651103ae09c1cea270ab0dc4ed7761cb87368</li> <li>SHA512:<br/>687561052e3d6218da275c1cd36cd835956acce0fb5c146250cf795547e35b4297745dcd2b7c2abc4051db06de9f73465c34036ec7d9c675b102e6d7b7fe10a7</li> </ul>                    |
| <b>Category:</b> backdoor, webshell<br><b>Name:</b> RedirSuiteServerProxy.aspx | <b>File Name:</b> RedirSuiteServerProxy.aspx<br><b>File Size:</b> 2349 bytes<br><b>File Type:</b> HTML document, ASCII text, with CRLF line terminators<br><b>File Hashes:</b> <ul style="list-style-type: none"> <li><b>MD5:</b> ab3963337cf24dc2ade6406f11901e1f</li> <li><b>SHA1:</b> 9a29c483b38a7ae645c6c43a0b543f9def8818cc</li> </ul>                                                                                                                                                                                                                   |



|                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                          | <ul style="list-style-type: none"> <li>• <b>SHA256:</b><br/>c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5</li> <li>• <b>SHA512:</b><br/>e37cd29532106a7f5ae4c248429190541d1b8403ec7df40616a8c6a0d0d4f98ac8a520277f18df3654f00eed4faa05d787adff5f498f5684117775cc49e22baf</li> </ul>                                                                                                                                                                                                                                                                                                        |
| <b>Category:</b> backdoor,<br>Webshell<br><br><b>Name:</b> discover.aspx | <b>File Name:</b> discover.aspx<br><br><b>File Size:</b> 2230 bytes<br><br><b>File Type:</b> HTML document, ASCII text, with CRLF line terminators<br><br><b>File Hashes:</b> <ul style="list-style-type: none"> <li>• <b>MD5:</b> ca7df873422d59c358397d3cb44ae6aa</li> <li>• <b>SHA1:</b> f95be23d52cbaa24bde99cf33a9be55bca688972</li> <li>• <b>SHA256:</b><br/>1e0803ffc283dd04279bf3351b92614325e643564ed5b4004985eb0486bf44ee</li> <li>• <b>SHA512:</b><br/>9e696ad26291e391cb29aff1845f78f0024f4808b10aa17cf7192f6f144378ea43b5533e3e0669cc19b07d88e00f4be39a95fa5500559573177b59585b7dad30</li> </ul> |
| <b>Category:</b> Backdoor<br><br><b>Name:</b> discover.aspx              | <b>File Name:</b> discover.aspx<br><br><b>File Size:</b> 2204 bytes<br><br><b>File Type:</b> HTML document, ASCII text, with CRLF line terminators<br><br><b>File Hashes:</b> <ul style="list-style-type: none"> <li>• <b>MD5:</b> 751a5e2e6c97f55c86cb7d4e5afb0928</li> <li>• <b>SHA1:</b> b2ce5a315c8dfdbe89b5bfa834491a71452b0c76</li> <li>• <b>SHA256:</b><br/>c0caa9be0c1d825a8af029cc07207f2e2887fce4637a3d8498692d37a52b4014</li> <li>• <b>SHA512:</b><br/>3ecb7044d4534db78952ab9c3c773323df6b938c246f533265b9945750043475f51fcf68904b9be98193c4fabeadc4060878172fd8caa312e3f8a6d16ff97837</li> </ul> |
| <b>Category:</b> Backdoor<br><br><b>Name:</b> Fc1b3WDP.aspx              | <b>File Name:</b> Fc1b3WDP.aspx<br><br><b>File Size:</b> 2230 bytes<br><br><b>File Type:</b> ASCII text, with CRLF line terminators<br><br><b>File Hashes:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                |



|                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                          | <ul style="list-style-type: none"> <li>• <b>MD5:</b> 6221e5f594a1eb04279d7e217801e90d</li> <li>• <b>SHA1:</b> 34a34682efe6e9bd7102db6ab52e7bdcfb573a5d</li> <li>• <b>SHA256:</b><br/>be17c38d0231ad593662f3b2c664b203e5de9446e858b7374864430e15fbf22d</li> <li>• <b>SHA512:</b><br/>6afdc18162219606c26742cc569320e5b2bf348ee8387502b8b746e69eb677a505f422c0d278b2386debdccf3f971270a14f8b5d522a50128978d1f9670c</li> </ul>                                                                                                                                                                                   |
| <b>Category:</b> Backdoor<br><br><b>Name:</b> F48zhi6U.aspx              | <b>File Name:</b> F48zhi6U.aspx<br><br><b>File Size:</b> 2211 bytes<br><br><b>File Type:</b> HTML document, ASCII text, with CRLF line terminators<br><br><b>File Hashes:</b> <ul style="list-style-type: none"> <li>• <b>MD5:</b> 08a939f320ffbdb82db2d57520677725</li> <li>• <b>SHA1:</b> c3011f31d556a0b1422e78c0906406283bdfa12f</li> <li>• <b>SHA256:</b><br/>d9c75da893975415663c4f334d2ad292e6001116d829863ab572c311e7edea77</li> <li>• <b>SHA512:</b><br/>506236cd328d840b741cd2e80ca58b7d2815e6d1a7dfd036e19b18526b57197bf93884907909524156d8e291e78f0da8f4c56ce19ec854dc58997ac9d5c8c9f3</li> </ul> |
| <b>Category:</b> Backdoor,<br>Webshell<br><br><b>Name:</b> UwSPMsFi.aspx | <b>File Name:</b> UwSPMsFi.aspx<br><br><b>File Size:</b> 2186 bytes<br><br><b>File Type:</b> HTML document, ASCII text, with CRLF line terminators<br><br><b>File Hashes:</b> <ul style="list-style-type: none"> <li>• <b>MD5:</b> 78564702783ba738aa6a920f3b15a202</li> <li>• <b>SHA1:</b> a75fa74ae35ce20c9cfc273c219ef58f1c4714a6</li> <li>• <b>SHA256:</b><br/>d637b9a4477778a2e32a22027a86d783e1511e999993aad7dca9b7b1b62250b8</li> <li>• <b>SHA512:</b><br/>63afff12ac7cf65ba31aad61bab534040fc3ff8b782336fcdbe171bf43f733734770c5f11bfbf9f4b5a1beaf279e8ad8d6509ff6e07b7afba098a8e6ba52a6c</li> </ul>  |
| <b>Category:</b> Backdoor<br><br><b>Name:</b> 2XJHwN19.aspx              | <b>File Name:</b> 2XJHwN19.aspx<br><br><b>File Size:</b> 2177 bytes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |



|                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                      | <p><b>File Type:</b> ASCII text, with CRLF line terminators</p> <p><b>File Hashes:</b></p> <ul style="list-style-type: none"> <li>• <b>MD5:</b> 4580f7f2f2d7ac1af26693132c2e756d</li> <li>• <b>SHA1:</b> 1fead8d37f73b87ab75d0096d49b797afe7d0445</li> <li>• <b>SHA256:</b><br/>31a750f8dbdd5bd608cfec4218ccb5a3842821f7d03d0cff9128ad00a691f4bd</li> <li>• <b>SHA512:</b><br/>fceddb90d8a9445a726eefa6df7fe928006d6a29279138e1b7906534d3b188d08eda62a939617a7944889d8e2e160417600947f48d5704cb537e64b2523ba1a4</li> </ul>                                                                                             |
| <p><b>Category:</b> Backdoor</p> <p><b>Name:</b> E3MsTjP8.aspx</p>   | <p><b>File Name:</b> E3MsTjP8.aspx</p> <p><b>File Size:</b> 2353 bytes</p> <p><b>File Type:</b> HTML document, ASCII text, with CRLF line terminators</p> <p><b>File Hashes:</b></p> <ul style="list-style-type: none"> <li>• <b>MD5:</b> ed0ec81113331d241f15e2ca73de1176</li> <li>• <b>SHA1:</b> 0b68b4efe6cbe1e2db940486f089be7eefae6ceb</li> <li>• <b>SHA256:</b><br/>bda1b5b349bfc15b20c3c9cbfabd7ae8473cee8d000045f78ca379a629d97a61</li> <li>• <b>SHA512:</b><br/>e307f966fb1bdea44adfa5939da76f40e7082cac9014d18d21ba6d4f1a60aff022885cddf0670662595dc4078d68658a925f7f59e55827ae7ba2b7037e60e600</li> </ul>   |
| <p><b>Category:</b> Backdoor</p> <p><b>Name:</b> web.config.aspx</p> | <p><b>File Name:</b> web.config.aspx</p> <p><b>File Size:</b> 2241 bytes</p> <p><b>File Type:</b> HTML document, ASCII text, with CRLF line terminators</p> <p><b>File Hashes:</b></p> <ul style="list-style-type: none"> <li>• <b>MD5:</b> 742b340f8739e73d9347d68e7ffc1590</li> <li>• <b>SHA1:</b> fc5e612238d4217b10ba2c6701f487d1346f8338</li> <li>• <b>SHA256:</b><br/>5ac7dec465b3a532d401afe83f40d336ffc599643501a40d95aa886c436bfc0f</li> <li>• <b>SHA512:</b><br/>9893f5c6e204b8188bf2e6670d590abdd0f7bba403d4b641f87ee59d037ee0c692d591f3eba10bd6c1142003a246964036465b1f813eaa1d5fc8aaf75628994c</li> </ul> |



|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Category:</b> Backdoor<br><b>Name:</b> uHSPTWMG.aspx | <b>File Name:</b> uHSPTWMG.aspx<br><b>File Size:</b> 2226 bytes<br><b>File Type:</b> ASCII text, with CRLF line terminators<br><b>File Hashes:</b> <ul style="list-style-type: none"> <li><b>MD5:</b> f04aa369ceee2d1388f9453d0d9758df</li> <li><b>SHA1:</b> 888d1a0e10222a80c8076728d16eb10072b1473b</li> <li><b>SHA256:</b><br/>c7e1b386b472a26a36632f4ccc25e37458546b9c864b7ef0ec5ebece5e8cc704</li> <li><b>SHA512:</b><br/>4dd200a585fe93f2f8f102fd0359c4290d4b516ce5ec6a8b304ded61bf3a332d5c81272cada303109a366c42fa38956387e33b7309fcfb3ef6dbf7a27cf0a10e</li> </ul>               |
| <b>Category:</b> Backdoor<br><b>Name:</b> supp0rt.aspx  | <b>File Name:</b> supp0rt.aspx<br><b>File Size:</b> 2328 bytes<br><b>File Type:</b> HTML document, ASCII text, with CRLF line terminators<br><b>File Hashes:</b> <ul style="list-style-type: none"> <li><b>MD5:</b> b5aff5be558e41243225a3e2480fc8dc</li> <li><b>SHA1:</b> 4bc72b82af2f455eb69e582793593db8fb03c7da</li> <li><b>SHA256:</b><br/>5e09ea8b70a386f0812a8cafb94e2d2365849ce67fda42377389f18e56d860d0</li> <li><b>SHA512:</b><br/>68f92197cc11748e88aa18012bdfa910e30bc2bd605ad6fe5291f3f87b5cd00f65d201b41945d9dea392f526eb5736ef5fff2d7628b7859665d01743d4eadb58</li> </ul> |

#### Suspicious IP Addresses

| event_date | IP DESTINATION (C2C) | ISP                               | Location | Function       | Actor   | MISP_event_member_org | MISP_event_source_org |
|------------|----------------------|-----------------------------------|----------|----------------|---------|-----------------------|-----------------------|
| 2/15/2021  | 103.77.192[.]219     | Multibyte Info Technology Limited | HK       | Exploit Source | HAFNIUM | BGD e-GOV CIRT        | CUDESO                |
| 2/15/2021  | 104.140.114[.]110    | Eonix                             | US       | Exploit Source | HAFNIUM | BGD e-GOV CIRT        | CUDESO                |
| 2/15/2021  | 104.248.49[.]97      | DigitalOcean                      | US       | Exploit Source | N/A     | BGD e-GOV CIRT        | CUDESO                |



BGD e-GOV CIRT



|           |                   |                       |    |                          |         |                |        |
|-----------|-------------------|-----------------------|----|--------------------------|---------|----------------|--------|
| 2/15/2021 | 104.250.191[.]110 | PERFORMIVE            | US | Exploit Source           | HAFNIUM | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 108.61.246[.]56   | Choopa                | JP | Exploit Source           | HAFNIUM | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 112.66.255[.]71   | Chinanet              | CN | Exploit Source           | N/A     | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 139.59.56[.]239   | DigitalOcean          | IN | Exploit Source           | N/A     | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 149.28.14[.]163   | Choopa                | US | Exploit Source           | HAFNIUM | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 157.230.221[.]198 | DigitalOcean          | US | Exploit Source           | HAFNIUM | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 161.35.1[.]207    | DigitalOcean          | US | Exploit Source           | N/A     | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 161.35.1[.]225    | DigitalOcean          | US | Exploit Source           | N/A     | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 161.35.45[.]41    | DigitalOcean          | GB | Exploit Source, Scanning | N/A     | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 161.35.51[.]41    | DigitalOcean          | US | Exploit Source           | N/A     | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 161.35.76[.]1     | DigitalOcean          | DE | Exploit Source           | N/A     | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 165.232.154[.]116 | DigitalOcean          | US | Exploit Scanning         | UNC2639 | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 167.99.168[.]251  | DigitalOcean          | US | Exploit Source           | HAFNIUM | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 167.99.239[.]29   | DigitalOcean          | US | Exploit Source           | N/A     | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 182.18.152[.]105  | CtrlS Datacenters Ltd | IN | Unknown                  | UNC2639 | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 185.250.151[.]72  | Innovation IT         | US | Exploit Source           | HAFNIUM | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 188.166.162[.]201 | DigitalOcean          | DE | Exploit Source           | N/A     | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 192.81.208[.]169  | DigitalOcean          | US | Exploit Source           | HAFNIUM | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 194.87.69[.]35    | LLC Baxet             | RU | Webshell C2              | N/A     | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 203.160.69[.]66   | China Unicom          | HK | Exploit Source           | HAFNIUM | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 211.56.98[.]146   | Korea Telecom         | KR | Exploit Source           | HAFNIUM | BGD e-GOV CIRT | CUDESO |



|           |                 |                          |    |                |         |                |        |
|-----------|-----------------|--------------------------|----|----------------|---------|----------------|--------|
| 2/15/2021 | 45.77.252[.]175 | Choopa                   | SG | Exploit Source | N/A     | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 5.2.69[.]14     | The Infrastructure Group | NL | Exploit Source | N/A     | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 5.254.43[.]18   | Voxility                 | US | Exploit Source | HAFNIUM | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 77.61.36[.]169  | KPN                      | NL | Exploit Source | N/A     | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 80.92.205[.]81  | Innovation IT            | US | Exploit Source | HAFNIUM | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 86.105.18[.]116 | WorldStream              | NL | Unknown        | UNC2643 | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 89.34.111[.]11  | 23Media                  | DE | Unknown        | UNC2643 | BGD e-GOV CIRT | CUDESO |
| 2/15/2021 | 91.192.103[.]43 | Datasource               | CH | Exploit Source | N/A     | BGD e-GOV CIRT | CUDESO |

## Required Action Measures

According to All the organizations are requested to take action measures as following:

- Run newly developed tools —Microsoft's [Test-ProxyLogon.ps1 script](#) and Safety Scanner [MSERT](#)—to investigate whether their Microsoft Exchange Servers have been compromised
- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).
- Report or inform **BGD e-GOV CIRT** regarding any incident/ issues to work in collaborated fashion through <https://www.cirt.gov.bd/incident-reporting/>

## References

- <https://cyber.dhs.gov/ed/21-02/#supplemental-direction>
- <https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download>
- <https://github.com/microsoft/CSS-Exchange/tree/main/Security>
- <https://www.fireeye.com/blog/threat-research/2021/03/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities.html>
- <https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/>