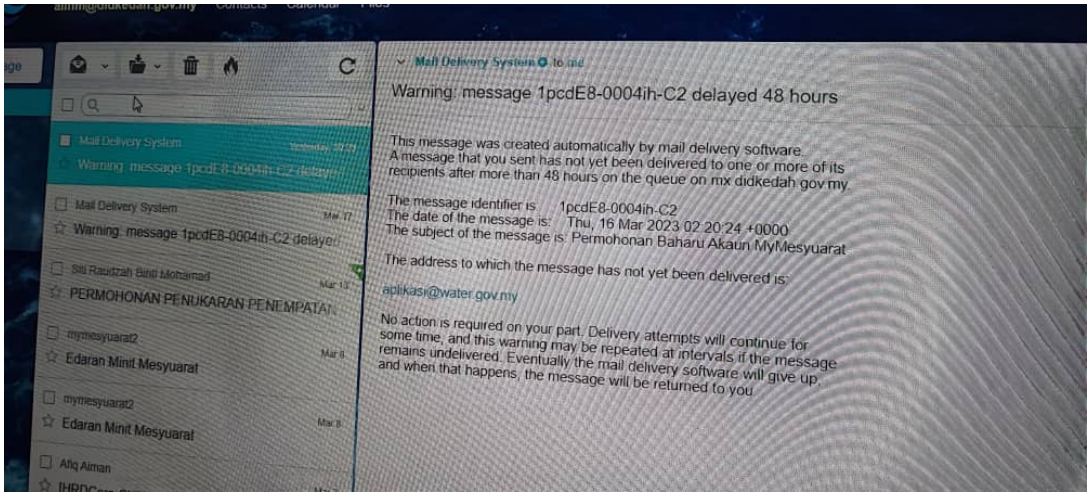
nadi versa technologies sdn. bhd.

Penyelenggaraan System Email di Jabatan Pengairan Negeri Kedah Bagi Tahun 2023

Report Period of 01/01/2023 - 31/10/2023

Date	Description
17/02/2023	Found email anomaly through DMARC warning. After checking, it was indeed an incident - email ID khairulazhar has been hacked, been accessed without proper authorization. The email/ID has been used to blast thousands of spams into the Internet. Changed the password of the email and log shows as follow: 2023-02-17 15:14:38 login authenticator failed for (localhost) [46.148.40.51] I=[172.16.1.2]:25: 535 Incorrect authentication data (set_id=inc@gov.my) 2023-02-17 15:14:41 login authenticator failed for (localhost) [46.148.40.176] I=[172.16.1.2]:25: 535 Incorrect authentication data (set_id=korolev@localhost) 2023-02-17 15:14:43 login authenticator failed for (localhost) [46.148.40.176] I=[172.16.1.2]:25: 535 Incorrect authentication data (set_id=triumph@localhost) 2023-02-17 15:14:45 login authenticator failed for (localhost) [46.148.40.51] I=[172.16.1.2]:25: 535 Incorrect authentication data (set_id=francom@gov.my) 2023-02-17 15:14:50 login authenticator failed for (localhost) [46.148.40.91] I=[172.16.1.2]:25: 535 Incorrect authentication data (set_id=mercado@localhost) 2023-02-17 15:14:52 login authenticator failed for (localhost) [46.148.40.139] I=[172.16.1.2]:25: 535 Incorrect authentication data (set_id=gl11@gov.my) 2023-02-17 15:14:54 login authenticator failed for (localhost) [46.148.40.139] I=[172.16.1.2]:25: 535 Incorrect authentication data (set_id=cp-ht-3@gov.my) A very quick check on ARIN shows the subnet 46.148.40.x is from the country Iran.
23/02/2023	Found spam attempt from 2 originating subnets - 212.193.29.43/24 2.229.91.59/24 Added them into etc/host/host_reject.list
19/03/2023	En. Alif reported that email cannot be sent out to external email servers. Went through investigation and found out that TM denied access to SMTP port (TCP 25). Immediately call 100 asking to rectify the issue pronto.

nadi versa technologies sdn. bhd.

Date	Description
	
19/03/2023	Found out that pro@didkedah.gov.my has been hacked and used to spam from the local email server. Advised En. Alif to reset the password and communicate with the overseer of the account, Ms Shatirah accordingly.
20/03/2023	Received a call from TM NOC (Network Operation Center) clarifying that the IP has been blocked from sending email using port TCP 25. The matter has been in investigation as to 'what exactly happened'. As of the call, Mr Syed from TM NOC has released the email IP from deny list as to resume email operation.
14/04/2023	Email ID muniroh@didkedah.gov.my has been hacked. Changed the password immediately and Informed personnel Aliff at 0713.
15/05/2023	Email ID habsah reported been spamming. Reset password and observe for RBL.
03/07/2023	Incident report - the email ID webmaster@didkedah.gov.my has been successfully attempted from these IP addresses: 45.129.14.31 141.98.10.151 Once successful it was being manipulated to spam from these IP addresses: 102.140.117.215 102.164.248.88 102.219.204.16 102.219.205.187 102.39.50.99 102.64.75.14 102.69.176.147 103.103.131.128 103.104.215.158 103.107.248.77 103.109.168.222 103.112.159.251 103.113.106.211

nadi versa technologies sdn. bhd.

Date	Description
	103.114.88.37
	103.115.128.14
	103.118.46.77
	103.118.47.254
	103.121.107.252
	103.12.161.145
	103.122.84.20
	103.122.84.62
	103.127.23.252
	103.132.3.54
	103.135.135.196
	103.139.223.158
	103.140.231.250
	103.140.31.136
	103.141.71.45
	103.142.192.54
	103.147.119.3
	103.147.64.52
	103.148.94.90
	103.151.74.86
	103.154.217.114
	103.157.162.66
	103.157.210.179
	103.159.155.234
	103.163.83.122
	103.165.108.202
	103.165.165.2
	103.166.197.42
	103.166.32.78
	103.168.234.38
	103.172.17.7
	103.174.18.20
	103.18.76.70
	103.194.184.18
	103.199.18.128
	103.200.35.178
	103.20.3.81
	103.212.181.99
	103.213.239.126
	103.215.164.10
	103.216.49.30
	103.216.51.154

nadi versa technologies sdn. bhd.

Date	Description
	103.229.46.53
	103.230.63.202
	103.231.172.106
	103.239.147.250
	103.244.7.218
	103.247.122.7
	103.253.154.184
	103.28.242.214
	103.28.243.141
	103.38.182.174
	103.38.182.194
	103.38.182.30
	103.38.4.190
	103.41.212.213
	103.47.238.240
	103.6.133.146
	103.63.190.112
	103.65.192.115
	103.65.195.45
	103.65.195.66
	103.69.70.194
	103.87.139.22
	103.90.177.102
	103.93.177.98
	104.131.212.234
	104.200.140.66
	104.220.13.119
	105.214.7.248
	105.96.10.201
	109.166.185.182
	109.196.12.221
	109.70.1.199
	109.98.208.42
	110.164.176.153
	110.172.191.82
	110.235.249.178
	110.44.122.90
	110.76.147.18
	110.77.138.235
	111.118.147.123
	111.118.148.221
	111.14.218.26

nadi versa technologies sdn. bhd.

Date	Description
	111.22.108.103
	111.221.6.102
	111.23.119.189
	111.39.206.23
	111.53.167.70
	111.68.31.134
	111.90.178.214
	112.115.191.43
	112.26.95.12
	112.46.141.230
	112.51.98.101
	113.125.166.57
	113.161.33.130
	113.161.92.79
	113.169.155.172
	113.175.199.75
	113.180.42.46
	113.193.240.214
	114.132.45.222
	114.132.56.16
	114.79.146.156
	115.127.65.18
	115.22.67.5
	115.238.94.18
	115.79.59.196
	115.84.76.125
	115.84.77.145
	115.84.91.138
	115.84.91.143
	115.84.91.153
	115.84.91.167
	115.84.91.174
	115.84.91.192
	115.84.91.250
	115.84.92.211
	115.84.92.68
	115.84.99.201
	115.84.99.94
	116.104.162.79
	116.104.35.96
	116.107.190.214
	116.107.238.115

Date	Description
	116.118.0.217
	116.118.3.29
	116.118.6.251
	116.212.180.171
	116.6.56.66
	117.186.11.218
	117.241.135.164
	117.241.135.175
	117.242.47.68
	117.247.231.163
	117.248.107.5
	118.179.216.113
	118.182.119.73
	1.182.192.80
	118.69.35.69
	118.71.66.50
	119.148.23.250
	119.159.234.127
	119.96.241.58
	120.232.182.13
	120.32.50.50
	120.57.37.156
	120.57.40.38
	120.57.46.205
	120.57.47.63
	120.77.2.252
	12.182.4.106
	122.14.250.16
	122.154.48.106
	122.165.181.165
	122.187.225.66
	122.187.229.104
	12.236.145.203
	123.24.70.57
	123.28.136.221
	124.167.20.103
	124.167.20.113
	124.167.20.115
	124.167.20.80
	124.167.21.95
	124.248.184.193
	124.248.184.254

nadi versa technologies sdn. bhd.

Date	Description
	124.88.248.142
	128.201.165.91
	128.201.167.77
	128.201.167.88
	131.0.88.142
	131.108.233.193
	134.0.204.182
	134.0.204.190
	134.0.204.194
	134.0.206.186
	134.122.253.125
	134.122.253.67
	134.122.255.106
	134.209.7.100
	134.236.151.43
	138.0.116.240
	138.117.43.50
	138.122.76.48
	138.185.35.161
	138.186.236.14
	138.59.142.229
	139.194.161.89
	139.194.241.2
	139.214.92.142
	139.5.159.33
	139.5.159.40
	140.238.50.215
	141.164.96.145
	14.161.24.24
	14.161.69.205
	14.161.74.253
	14.161.77.154
	14.161.78.105
	14.162.146.186
	14.167.98.6
	14.170.218.239
	14.177.143.173
	14.177.172.94
	14.177.207.249
	14.226.121.249
	14.226.222.33
	14.226.228.229

nadi versa technologies sdn. bhd.

Date	Description
	14.226.228.25
	14.226.229.111
	14.226.231.217
	14.226.249.75
	14.226.250.2
	14.241.238.176
	14.248.135.13
	143.137.87.161
	143.208.151.131
	147.75.124.228
	149.54.6.154
	154.159.244.35
	154.159.246.4
	154.72.72.202
	154.72.85.246
	156.59.51.112
	159.192.190.172
	159.192.74.14
	160.19.142.246
	161.8.178.101
	164.163.214.10
	165.154.70.168
	165.16.34.165
	168.167.55.106
	168.195.186.131
	170.106.179.191
	170.239.246.143
	170.239.247.220
	170.245.201.171
	170.254.252.20
	171.224.240.95
	171.226.239.238
	171.236.130.16
	171.236.137.236
	171.237.175.234
	171.237.91.17
	171.241.183.47
	171.242.90.15
	171.249.78.173
	171.249.78.176
	171.250.40.218
	175.100.89.247

nadi versa technologies sdn. bhd.

Date	Description
	176.106.121.203
	176.118.52.129
	176.236.112.90
	176.236.76.81
	177.101.2.233
	177.11.138.194
	177.125.21.1
	177.129.208.58
	177.135.97.82
	177.184.190.210
	177.203.153.25
	177.52.247.201
	177.93.160.58
	178.16.95.199
	178.216.26.132
	178.219.104.224
	179.108.89.106
	179.191.231.14
	179.235.204.123
	179.33.2.253
	179.40.16.141
	179.97.46.34
	180.166.198.138
	180.211.186.22
	181.176.174.95
	181.193.55.246
	181.204.237.234
	181.205.246.42
	181.233.91.150
	181.48.193.42
	181.49.129.22
	181.49.212.122
	182.253.34.137
	183.87.217.222
	183.87.63.126
	183.88.32.198
	185.101.130.33
	185.140.108.59
	185.149.196.91
	185.187.48.159
	185.221.253.91
	185.242.234.51

nadi versa technologies sdn. bhd.

Date	Description
	185.34.17.66
	185.36.81.95
	185.40.51.74
	185.53.229.176
	185.6.9.159
	185.6.9.170
	185.94.89.208
	185.94.89.227
	185.94.90.221
	186.103.148.138
	186.159.115.81
	186.159.3.225
	186.179.100.0
	186.179.105.210
	186.183.159.194
	186.195.160.70
	186.211.251.146
	186.224.29.74
	186.232.119.1
	186.232.48.196
	186.237.137.25
	186.56.31.12
	186.65.103.76
	186.96.126.191
	187.16.49.230
	187.60.33.218
	187.87.174.54
	187.95.136.46
	188.166.45.97
	189.85.17.18
	190.119.75.90
	190.241.187.130
	190.93.221.234
	191.102.120.255
	191.102.83.121
	191.102.83.122
	191.102.83.126
	191.243.147.6
	191.243.149.210
	191.37.68.153
	191.92.144.107
	191.97.10.193

nadi versa technologies sdn. bhd.

Date	Description
	192.141.200.226
	192.145.213.213
	192.147.231.106
	192.162.237.50
	192.186.135.58
	192.3.84.143
	193.105.62.180
	193.108.6.204
	194.147.164.10
	194.150.171.242
	194.31.38.94
	194.44.246.130
	195.135.228.201
	195.189.249.154
	195.82.103.103
	196.216.10.114
	196.216.49.46
	196.216.66.218
	196.3.99.170
	197.155.92.138
	197.234.38.54
	197.237.48.185
	197.243.232.221
	199.66.156.110
	200.11.105.6
	200.146.229.129
	200.192.248.38
	200.195.229.215
	200.25.254.175
	200.32.105.86
	200.35.183.94
	201.159.121.141
	201.174.82.2
	201.182.92.14
	201.20.118.139
	201.20.84.10
	201.20.88.31
	201.240.108.174
	201.240.108.178
	201.75.105.247
	201.76.164.237
	202.137.134.236

nadi versa technologies sdn. bhd.

Date	Description
	202.137.134.8
	202.137.154.11
	202.137.154.130
	202.137.154.137
	202.137.154.172
	202.137.154.249
	202.137.154.83
	202.137.155.209
	202.137.155.22
	202.137.155.97
	202.142.157.250
	202.158.96.98
	202.166.198.77
	202.178.115.90
	202.43.161.222
	202.61.164.240
	202.62.55.29
	202.62.55.91
	202.78.206.130
	202.84.74.16
	203.161.25.248
	203.176.135.155
	203.189.156.74
	203.192.246.110
	203.210.84.220
	203.217.146.10
	203.77.230.26
	203.77.254.10
	203.99.100.81
	206.214.40.242
	206.84.230.67
	210.56.7.38
	211.24.105.69
	212.225.238.244
	212.225.247.42
	213.25.46.9
	216.177.141.39
	2.176.107.80
	2.179.129.78
	218.2.101.210
	218.75.78.106
	218.82.112.44

nadi versa technologies sdn. bhd.

Date	Description
	218.89.222.81
	219.134.240.102
	219.142.106.107
	220.179.255.54
	221.13.140.170
	222.179.42.134
	222.252.116.95
	222.253.131.90
	222.254.162.238
	222.254.170.199
	222.254.171.253
	222.254.172.214
	222.254.213.22
	222.74.207.34
	222.75.12.66
	223.113.241.220
	223.113.73.226
	223.27.83.106
	24.164.58.61
	27.147.218.26
	27.66.116.72
	27.74.248.0
	31.134.96.139
	31.202.53.50
	31.210.225.135
	31.42.167.44
	36.66.203.185
	36.66.210.39
	36.67.143.221
	36.88.103.122
	36.88.12.10
	36.88.25.221
	36.88.29.26
	36.88.31.74
	36.88.42.209
	36.91.131.93
	36.95.129.199
	38.104.165.242
	38.130.38.34
	38.130.46.72
	38.177.176.72
	38.32.73.170

nadi versa technologies sdn. bhd.

Date	Description
	38.75.43.195
	41.33.160.174
	41.60.107.193
	41.60.123.12
	41.60.252.182
	43.139.28.157
	43.143.29.18
	43.153.70.188
	43.163.209.75
	43.225.213.50
	43.229.94.219
	43.230.192.222
	43.246.142.10
	45.176.243.96
	45.179.200.142
	45.180.244.196
	45.187.32.66
	45.191.106.73
	45.201.134.15
	45.224.216.146
	45.231.242.2
	45.231.88.54
	45.232.108.31
	45.232.18.156
	45.234.223.181
	45.5.152.126
	45.64.178.20
	45.85.186.240
	43.153.70.188
	43.163.209.75
	43.225.213.50
	43.229.94.219
	43.230.192.222
	43.246.142.10
	45.176.243.96
	45.179.200.142
	45.180.244.196
	45.187.32.66
	45.191.106.73
	45.201.134.15
	45.224.216.146
	45.231.242.2

nadi versa technologies sdn. bhd.

Date	Description
	45.231.88.54
	45.232.108.31
	45.232.18.156
	45.234.223.181
	45.5.152.126
	45.64.178.20
	45.85.186.240
	45.93.31.89
	46.219.78.147
	46.236.65.66
	46.29.224.18
	46.40.60.108
	46.55.211.225
	46.98.196.245
	5.154.22.242
	5.154.22.248
	5.206.236.130
	5.239.240.121
	5.28.35.196
	5.28.35.46
	5.61.203.35
	58.215.212.174
	58.250.36.51
	58.40.67.190
	59.152.102.195
	59.97.204.13
	59.97.204.213
	60.171.135.254
	60.172.193.61
	60.223.247.218
	61.184.176.231
	61.2.25.218
	61.247.179.126
	61.247.179.62
	62.220.116.74
	63.166.164.194
	64.124.191.100
	64.124.229.162
	66.44.168.69
	67.207.139.126
	68.183.89.219
	74.118.204.79

nadi versa technologies sdn. bhd.

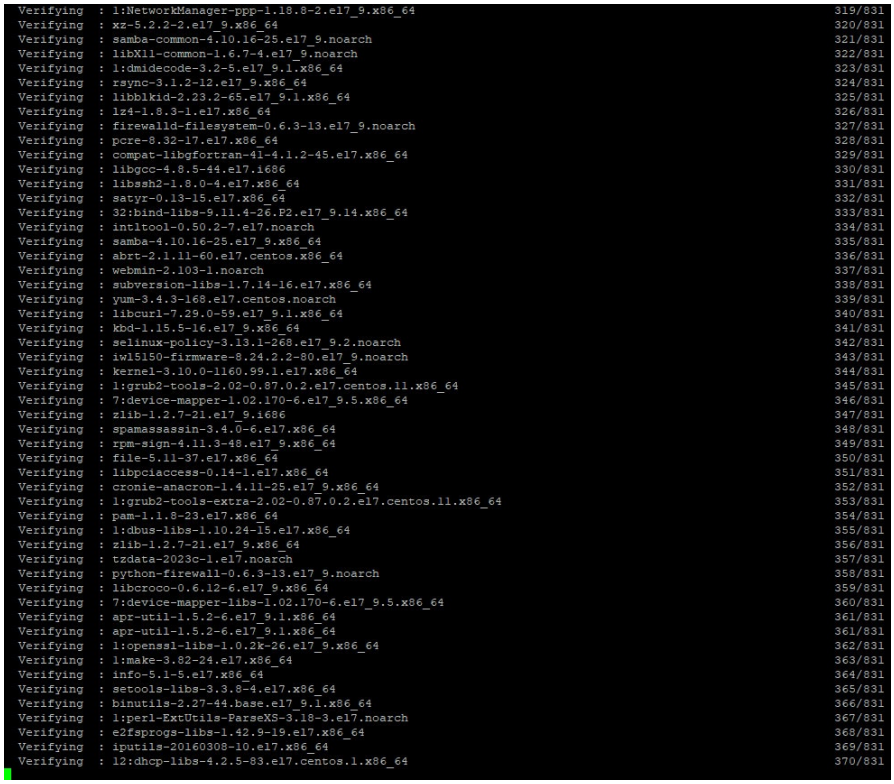
Date	Description
	77.48.136.127 77.52.39.226 78.26.253.251 80.63.107.90 82.117.199.206 82.129.17.246 82.194.17.61 82.200.235.134 8.40.252.12 85.114.97.18 85.121.204.112 85.121.204.165 85.122.180.235 85.62.5.150 87.107.144.115 89.44.32.158 91.225.203.225 91.226.112.138 91.232.241.194 91.241.39.159 93.118.121.184 93.175.248.98 93.175.249.123 93.175.249.236 93.175.250.64 94.20.136.109 95.142.87.35 95.170.201.34 Measure taken to clear all queues pertaining spam. IPs being added into blacklist by the /24.
13/07/2023	Updated kernel to kernel-devel-3.10.0-1160.99.1.el7.x86_64 and firmware linux-firmware-20200421-80.git78c0348.el7_9.noarch
20/07/2023	Whilst monitoring added the following subnet to the reject list: 80.94.95.184/24 141.98.10.150/24 77.90.185.18/24 95.124.251.22/24 192.72.6.177/24
20/07/2023	Spam detected from 124.217.226.112. Added into hosts_reject.list with /24 mask pronto.

nadi versa technologies sdn. bhd.

Date	Description
	Header as follows: Return-path: <eagle@blucorus.com> Envelope-to: najib@didkedah.gov.my Delivery-date: Mon, 02 Oct 2023 12:26:19 +0800 Received: from [124.217.226.112] (helo=server.blucorus.com) by mx.didkedah.gov.my with esmtps (TLSv1.2:AES256-GCM-SHA384:256) (Exim 4.85) (envelope-from <eagle@blucorus.com>) id 1qnAVd-0004tD-NB for najib@didkedah.gov.my; Mon, 02 Oct 2023 12:26:19 +0800 DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; d=blucorus.com; s=default; h=Content-Type:MIME-Version:Date:Subject:To:From: Message-ID:Reply-To:Sender:Cc:Content-Transfer-Encoding:Content-ID: Content-Description:Resent-Date:Resent-From:Resent-Sender:Resent-To:Resent-Cc :Resent-Message-ID:In-Reply-To:References:List-Id:List-Help:List-Unsubscribe: List-Subscribe:List-Post:List-Owner:List-Archive; bh=4kQdbzQNbUKn8H91seDTNUy5Zv4mC/Ih5i3om9ozUfk=; b=n1r1NKhM7FmxJVWyjbV6W0b3sB YaIHgzf+TOWnBPwEii0K0eJT0wL3OYwu0zm+OljDJrqMsGmD6FBP9bTjrZbipJUczvO8737OuS+5u FGoAmFUQWas4cjqfDw5k+LJotshgjIVGffhU9HysRhV6hS9GBRazZA1OJk0PT+Nr1hhaBRhKn7mb0 H8smUKMELmQla0vAwLyUw+Snr2Sx943IfoQ7j272ZoOnmLZZ2V8s/DKdy2c13uxZaANNse8hWV1bu VxDMDoQ1fh0h4iT6769H6JMKjBGoGP2Qu24hl/MQ3AsS/IwLQ5mm/XjrsaQzTgnRg9Q3R/xbk4ZDO RNrYGqaw==; Received: from [202.186.32.222] (port=10923 helo=124-217-226-112.cprapid.com) by server.blucorus.com with esmtpsa (TLS1.2) tls TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (Exim 4.96) (envelope-from <eagle@blucorus.com>) id 1qnAVY-009MYZ-2n for najib@didkedah.gov.my; Mon, 02 Oct 2023 12:26:16 +0800
26/07/2023	Updated BIND service to bind-9.11.4-26.P2.el7_9.14.x86_64. Disabled and re-enabled the services with new reverse configuration locally before deploying multi-user mode.
04/08/2023	Execute yum update to refresh 831 packages.

nadi versa technologies sdn. bhd.

Date	Description



16/08/2023 Spam detected from 177.83.203.241. Added into hosts_reject.list with /24 mask pronto.

Header as follows:

Return-path: <arctic@quoterange.shop>
Envelope-to: najib@didkedah.gov.my
Delivery-date: Wed, 27 Sep 2023 21:44:43 +0800
Received: from [77.83.203.241] (helo=quoterange.shop)
by mx.didkedah.gov.my with esmtp (Exim 4.85)
(envelope-from <arctic@quoterange.shop>)
id 1qlUqH-0007ex-Nb
for najib@didkedah.gov.my; Wed, 27 Sep 2023 21:44:43 +0800
Date: Wed, 27 Sep 2023 08:22:04 -0500
From: "GET-GX" <arctic@quoterange.shop>
MIME-Version: 1.0
Precedence: bulk
To: <najib@didkedah.gov.my>
Subject: This Smart Watch has Life saving Features !
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable