Establish Accounts: Email Accounts, Sub-technique T1585.002 - Enterprise

Archived: 2026-04-05 18:25:54 UTC

G0006 APT1

APT1 has created email accounts for later use in social engineering, phishing, and when registering domains.[1]

G1044 APT42

APT42 has created email accounts to use in spearphishing operations.[4]

G1052 Contagious Interview

Contagious Interview has created fake email accounts to correspond with social media accounts, fake LinkedIn personas, code repository accounts, and job announcements on development job board services.[5][6][7][8][9][10] Contagious Interview has also utilized fake email accounts with Threat Intelligence vendor services.[5]

G1012 CURIUM

CURIUM has created dedicated email accounts for use with tools such as IMAPLoader.[11]

G1011 EXOTIC LILY

EXOTIC LILY has created e-mail accounts to spoof targeted organizations.[12]

C0007 FunnyDream

For FunnyDream, the threat actors likely established an identified email account to register a variety of domains that were used during the campaign.[13]

G1001 HEXANE

HEXANE has established email accounts for use in domain registration including for ProtonMail addresses.[14]

G0119 Indrik Spider

Indrik Spider has created email accounts to communicate with their ransomware victims, to include providing payment and decryption details.[15]

G0094 Kimsuky

Kimsuky has created email accounts for phishing operations.[16][17][18]

G0032 Lazarus Group

Lazarus Group has created new email accounts for spearphishing operations.[19]

G0065 Leviathan

Leviathan has created new email accounts for targeting efforts.[20]

G0059 Magic Hound

Magic Hound has established email accounts using fake personas for spearphishing operations.[21][22]

G1051 Medusa Group

Medusa Group has created email accounts used in ransomware negotiations.[23]

G1036 Moonstone Sleet

Moonstone Sleet has created email accounts to interact with victims, including for phishing purposes.[24]

G0129 Mustang Panda

Mustang Panda has leveraged the legitimate email marketing service SMTP2Go for phishing campaigns.[25]
Mustang Panda has also created fake Google accounts to distribute malware via spear-phishing emails.[26]
Mustang Panda has also created accounts for spearphishing operations including the use of services such as Proton Mail.[27][28]

C0022 Operation Dream Job

During Operation Dream Job, Lazarus Group created fake email accounts to correspond with fake LinkedIn personas; Lazarus Group also established email accounts to match those of the victim as part of their BEC attempt.[29]

C0016 Operation Dust Storm

For Operation Dust Storm, the threat actors established email addresses to register domains for their operations.[30]

C0006 Operation Honeybee

During Operation Honeybee, attackers created email addresses to register for a free account for a control server used for the implants.[31]

C0014 Operation Wocao

For Operation Wocao, the threat actors registered email accounts to use during the campaign.[32]

C0059 Salesforce Data Exfiltration

During Salesforce Data Exfiltration, threat actors registered emails shinycorp@tuta[.]com and shinygroup@tuta[.]com to send victims extortion demands.[33]

G0034 Sandworm Team

Sandworm Team has created email accounts that mimic legitimate organizations for its spearphishing operations.[34]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors created Proton mail accounts for communication with organizations infected with ransomware.[35]

G0122 Silent Librarian

Silent Librarian has established e-mail accounts to receive e-mails forwarded from compromised accounts.[36]

G1033 Star Blizzard

Star Blizzard has registered impersonation email accounts to spoof experts in a particular field or individuals and organizations affiliated with the intended target.[37][38][39]

G0102 Wizard Spider

Wizard Spider has leveraged ProtonMail email addresses in ransom notes when delivering Ryuk ransomware.[40]
