Valid Accounts, Technique T1078 - Enterprise

Archived: 2026-04-05 16:48:28 UTC

C0028 2015 Ukraine Electric Power Attack

During the 2015 Ukraine Electric Power Attack, Sandworm Team used valid accounts on the corporate network to escalate privileges, move laterally, and establish persistence within the corporate network. [4]

C0057 3CX Supply Chain Attack

During 3CX Supply Chain Attack, AppleJeus has gained access to the 3CX corporate environment through legitimate VPN credentials.[5]

G1024 Akira

Akira uses valid account information to remotely access victim networks, such as VPN credentials.[6][7][8]

G0026 APT18

APT18 actors leverage legitimate credentials to log into external remote services.[9]

G0007 APT28

APT28 has used legitimate credentials to gain initial access, maintain access, and exfiltrate data from a victim network. The group has specifically used credentials stolen through a spearphishing email to login to the DCCC network. The group has also leveraged default manufacturer's passwords to gain initial access to corporate networks via IoT devices such as a VOIP phone, printer, and video decoder.[10][11][12][13]

G0016 APT29

APT29 has used a compromised account to access an organization's VPN infrastructure.[14]

G0064 APT33

APT33 has used valid accounts for initial access and privilege escalation.[15][16]

G0087 APT39

APT39 has used stolen credentials to compromise Outlook Web Access (OWA).[17]

G0096 APT41

APT41 used compromised credentials to log on to other systems.[18][19]

G0001 Axiom

Axiom has used previously compromised administrative accounts to escalate privileges.[20]

G1043 BlackByte

BlackByte has gained access to victim environments through legitimate VPN credentials.[21]

C0032 C0032

During the C0032 campaign, TEMP.Veles used compromised VPN accounts.[22]

G0008 Carbanak

Carbanak actors used legitimate credentials of banking employees to perform operations that sent them millions of dollars.[23]

G0114 Chimera

Chimera has used a valid account to maintain persistence via scheduled task.[24]

G1021 Cinnamon Tempest

Cinnamon Tempest has used compromised user accounts to deploy payloads and create system services.[25]

G0035 Dragonfly

Dragonfly has compromised user credentials and used valid accounts for operations.[26][27][28]

S0567 Dtrack

Dtrack used hard-coded credentials to gain access to a network share.[29]

S0038 Duqu

Adversaries can instruct Duqu to spread laterally by copying itself to shares it has enumerated and for which it has obtained legitimate credentials (via keylogging or other means). The remote host is then infected by using the compromised credentials to schedule a task on remote machines that executes the malware.[30]

G0051 FIN10

FIN10 has used stolen credentials to connect remotely to victim networks using VPNs protected with only a single factor.[31]

G0085 FIN4

FIN4 has used legitimate credentials to hijack email communications.[32][33]

G0053 FIN5

FIN5 has used legitimate VPN, RDP, Citrix, or VNC credentials to maintain access to a victim environment.[34][35][36]

G0037 FIN6

To move laterally on a victim network, FIN6 has used credentials stolen from various systems on which it gathered usernames and password hashes.[37][38][39]

G0046 FIN7

FIN7 has harvested valid administrative credentials for lateral movement.[40]

G0061 FIN8

FIN8 has used valid accounts for persistence and lateral movement.[41]

G0117 Fox Kitten

Fox Kitten has used valid credentials with various services during lateral movement.[42]

G0093 GALLIUM

GALLIUM leveraged valid accounts to maintain access to a victim network.[43]

C0038 HomeLand Justice

During HomeLand Justice, threat actors used a compromised Exchange account to search mailboxes and create new Exchange accounts.[44]

G1032 INC Ransom

INC Ransom has used compromised valid accounts for access to victim environments.[45][46][47][48]

G0119 Indrik Spider

Indrik Spider has used valid accounts for initial access and lateral movement.[49] Indrik Spider has also maintained access to the victim environment through the VPN infrastructure.[49]

S0604 Industroyer

Industroyer can use supplied user credentials to execute processes and stop services.[50]

G0004 Ke3chang

Ke3chang has used credential dumpers or stealers to obtain legitimate credentials, which they used to gain access to victim accounts.[51]

S0599 Kinsing

Kinsing has used valid SSH credentials to access remote hosts.[52]

G1004 LAPSUS$

LAPSUS$ has used compromised credentials and/or session tokens to gain access into a victim's VPN, VDI, RDP, and IAMs.[53][54]

G0032 Lazarus Group

Lazarus Group has used administrator credentials to gain access to restricted network segments.[55]

G0065 Leviathan

Leviathan has obtained valid accounts to gain initial access.[56][57][58]

C0049 Leviathan Australian Intrusions

Leviathan used captured, valid account information to log into victim web applications and appliances during Leviathan Australian Intrusions.[58]

S0362 Linux Rabbit

Linux Rabbit acquires valid SSH accounts through brute force. [59]

G1051 Medusa Group

Medusa Group has utilized compromised legitimate local and domain accounts within the victim environment to facilitate remote access and lateral movement sometimes in combination with PsExec.[60]

G0045 menuPass

menuPass has used valid accounts including shared between Managed Service Providers and clients to move between the two environments.[61][62][63][64]

C0002 Night Dragon

During Night Dragon, threat actors used compromised VPN accounts to gain access to victim systems.[65]

G0049 OilRig

OilRig has used compromised credentials to access other systems on a victim network.[66][67][19][68]

C0048 Operation MidnightEclipse

During Operation MidnightEclipse, threat actors extracted sensitive credentials while moving laterally through compromised networks.[69]

C0014 Operation Wocao

During Operation Wocao, threat actors used valid VPN credentials to gain initial access.[70]

G0011 PittyTiger

PittyTiger attempts to obtain legitimate credentials during operations.[71]

G1040 Play

Play has used valid VPN accounts to achieve initial access.[72]

G1005 POLONIUM

POLONIUM has used valid compromised credentials to gain access to victim environments.[73]

C0056 RedPenguin

During RedPenguin, UNC3886 used legitimate credentials to gain priviliged access to Juniper routers.[74][75]

G0034 Sandworm Team

Sandworm Team have used previously acquired legitimate credentials prior to attacks.[76]

G1015 Scattered Spider

Scattered Spider has used compromised credentials for initial access.[77][78]

G1041 Sea Turtle

Sea Turtle used compromised credentials to maintain long-term access to victim environments.[79]

S0053 SeaDuke

Some SeaDuke samples have a module to extract email from Microsoft Exchange servers using compromised credentials.[80]

G0091 Silence

Silence has used compromised credentials to log on to other systems and escalate privileges.[81]

G0122 Silent Librarian

Silent Librarian has used compromised credentials to obtain unauthorized access to online accounts.[82]

C0024 SolarWinds Compromise

During the SolarWinds Compromise, APT29 used different compromised credentials for remote access and to move laterally.[83][84][85]

G1033 Star Blizzard

Star Blizzard has used stolen credentials to sign into victim email accounts.[86][87]

G0039 Suckfly

Suckfly used legitimate account credentials that they dumped to navigate the internal victim network as though they were the legitimate account owner.[88]

G0027 Threat Group-3390

Threat Group-3390 actors obtain legitimate credentials using a variety of methods and use them to further lateral movement on victim networks.[89]

G1048 UNC3886

UNC3886 has used tools to hijack valid SSH accounts.[90]

G1017 Volt Typhoon

Volt Typhoon relies primarily on valid credentials for persistence.[91]

G0102 Wizard Spider

Wizard Spider has used valid credentials for privileged accounts with the goal of accessing domain controllers.[92] [93]

Source: https://attack.mitre.org/techniques/T1078