External Remote Services, Technique T1133 - Enterprise

Archived: 2026-04-05 17:38:36 UTC

C0028 2015 Ukraine Electric Power Attack

During the 2015 Ukraine Electric Power Attack, Sandworm Team installed a modified Dropbear SSH client as the backdoor to target systems.[7]

G1024 Akira

Akira uses compromised VPN accounts for initial access to victim networks.[8]

G0026 APT18

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

G0007 APT28

APT28 has used Tor and a variety of commercial VPN services to route brute force authentication attempts.[10]

G0016 APT29

APT29 has used compromised identities to access networks via VPNs and Citrix.[11][12]

G0096 APT41

APT41 compromised an online billing/payment service using VPN access between a third-party service provider and the targeted payment service.[13]

C0046 ArcaneDoor

ArcaneDoor used WebVPN sessions commonly associated with Clientless SSLVPN services to communicate to compromised devices.[14]

C0027 C0027

During C0027, Scattered Spider used Citrix and VPNs to persist in compromised environments.[15]

C0032 C0032

During the C0032 campaign, TEMP.Veles used VPN access to persist in the victim environment.[16]

G0114 Chimera

Chimera has used legitimate credentials to login to an external VPN, Citrix, SSH, and other remote services.[17] [18]

C0004 CostaRicto

During CostaRicto, the threat actors set up remote tunneling using an SSH tool to maintain access to a compromised environment.[19]

S0600 Doki

Doki was executed through an open Docker daemon API port.[20]

G0035 Dragonfly

Dragonfly has used VPNs and Outlook Web Access (OWA) to maintain access to victim networks.[21][22]

G1003 Ember Bear

Ember Bear have used VPNs both for initial access to victim environments and for persistence within them following compromise.[23]

G1016 FIN13

FIN13 has gained access to compromised environments via remote access services such as the corporate virtual private network (VPN).[24]

G0053 FIN5

FIN5 has used legitimate VPN, Citrix, or VNC credentials to maintain access to a victim environment.[25][26][27]

G0093 GALLIUM

GALLIUM has used VPN services, including SoftEther VPN, to access and maintain persistence in victim environments.[28][29]

G0115 GOLD SOUTHFIELD

GOLD SOUTHFIELD has used publicly-accessible RDP and remote management and monitoring (RMM) servers to gain access to victim machines.[30]

S0601 Hildegard

Hildegard was executed through an unsecure kubelet that allowed anonymous access to the victim environment.[4]

G0004 Ke3chang

Ke3chang has gained access through VPNs including with compromised accounts and stolen VPN certificates.[31][32]

G0094 Kimsuky

Kimsuky has used RDP to establish persistence.[33]

S0599 Kinsing

Kinsing was executed in an Ubuntu container deployed via an open Docker daemon API.[34]

G1004 LAPSUS$

LAPSUS$ has gained access to internet-facing systems and applications, including virtual private network (VPN), remote desktop protocol (RDP), and virtual desktop infrastructure (VDI) including Citrix. [35][36]

G0065 Leviathan

Leviathan has used external remote services such as virtual private networks (VPN) to gain initial access.[37]

S0362 Linux Rabbit

Linux Rabbit attempts to gain access to the server via SSH.[38]

S1060 Mafalda

Mafalda can establish an SSH connection from a compromised host to a server.[39]

C0002 Night Dragon

During Night Dragon, threat actors used compromised VPN accounts to gain access to victim systems.[40]

G0049 OilRig

OilRig uses remote services such as VPN, Citrix, or OWA to persist in an environment.[41]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors enabled WinRM over HTTP/HTTPS as a backup persistence mechanism using the following command: `cscript //nologo "C:\Windows\System32\winrm.vbs" set winrm/config/service@{EnableCompatibilityHttpsListener="true"}` .[42]

C0014 Operation Wocao

During Operation Wocao, threat actors used stolen credentials to connect to the victim's network via VPN.[43]

G1040 Play

Play has used Remote Desktop Protocol (RDP) and Virtual Private Networks (VPN) for initial access.[44][45]

G0034 Sandworm Team

Sandworm Team has used Dropbear SSH with a hardcoded backdoor password to maintain persistence within the target network. Sandworm Team has also used VPN tunnels established in legitimate software company infrastructure to gain access to internal networks of that software company's users.[46][47][48][49]

G1015 Scattered Spider

Scattered Spider has leveraged legitimate remote management tools to maintain persistent access.[50]

G1041 Sea Turtle

Sea Turtle has used external-facing SSH to achieve initial access to the IT environments of victim organizations.[51]

C0024 SolarWinds Compromise

For the SolarWinds Compromise, APT29 used compromised identities to access networks via SSH, VPNs, and other remote access tools.[52][53]

G0139 TeamTNT

TeamTNT has used open-source tools such as Weave Scope to target exposed Docker API ports and gain initial access to victim environments.[54][55] TeamTNT has also targeted exposed kubelets for Kubernetes environments.[4]

G0027 Threat Group-3390

Threat Group-3390 actors look for and use VPN profiles during an operation to access the network using external VPN services.[56] Threat Group-3390 has also obtained OWA account credentials during intrusions that it subsequently used to attempt to regain access when evicted from a victim network.[57]

G1047 Velvet Ant

Velvet Ant has leveraged access to internet-facing remote services to compromise and retain access to victim environments.[58]

G1017 Volt Typhoon

Volt Typhoon has used VPNs to connect to victim environments and enable post-exploitation actions.[59]

G0102 Wizard Spider

Wizard Spider has accessed victim networks by using stolen credentials to access the corporate VPN infrastructure.[60]
