Lateral Tool Transfer, Technique T1570 - Enterprise

Archived: 2026-04-05 15:11:04 UTC

C0028 2015 Ukraine Electric Power Attack

During the 2015 Ukraine Electric Power Attack, Sandworm Team moved their tools laterally within the corporate network and between the ICS and corporate network. [3]

C0025 2016 Ukraine Electric Power Attack

During the 2016 Ukraine Electric Power Attack, Sandworm Team used `move` to transfer files to a network share. [4]

C0034 2022 Ukraine Electric Power Attack

During the 2022 Ukraine Electric Power Attack, Sandworm Team used a Group Policy Object (GPO) to copy CaddyWiper's executable `msserver.exe` from a staging server to a local hard drive before deployment.[5]

G1030 Agrius

Agrius downloaded some payloads for follow-on execution from legitimate filesharing services such as `ufile.io` and `easyupload.io` .[6]

G1007 Aoqin Dragon

Aoqin Dragon has spread malware in target networks by copying modules to folders masquerading as removable devices.[7]

G0050 APT32

APT32 has deployed tools after moving laterally using administrative accounts.[8]

G0096 APT41

APT41 uses remote shares to move and remotely execute payloads during lateral movemement.[9]

S0190 BITSAdmin

BITSAdmin can be used to create BITS Jobs to upload and/or download files from SMB file servers.[10]

G1043 BlackByte

BlackByte transfered tools such as Cobalt Strike and the AnyDesk remote access tool during operations using SMB shares.[11]

S1180 BlackByte Ransomware

BlackByte Ransomware spreads itself laterally by writing the JavaScript launcher file to mapped shared folders. [12]

S1068 BlackCat

BlackCat can replicate itself across connected servers via `psexec`.[13]

C0015 C0015

During C0015, the threat actors used WMI to load Cobalt Strike onto additional hosts within a compromised network.[14]

C0018 C0018

During C0018, the threat actors transferred the SoftPerfect Network Scanner and other tools to machines in the network using AnyDesk and PDQ Deploy.[15][16]

G0114 Chimera

Chimera has copied tools between compromised hosts using SMB.[17]

S0106 cmd

cmd can be used to copy files to/from a remotely connected internal system.[18]

S0062 DustySky

DustySky searches for network drives and removable media and duplicates itself onto them.[19]

G1003 Ember Bear

Ember Bear retrieves follow-on payloads direct from adversary-owned infrastructure for deployment on compromised hosts.[20]

S0367 Emotet

Emotet has copied itself to remote systems using the `service.exe` filename.[21]

S0404 esentutl

esentutl can be used to copy files to/from a remote share.[22]

S0361 Expand

Expand can be used to download or upload a file over a network share.[23]

G0051 FIN10

FIN10 has deployed Meterpreter stagers and SplinterRAT instances in the victim network after moving laterally. [24]

S0095 ftp

ftp may be abused by adversaries to transfer tools or files between systems within a compromised environment. [25][26]

G0093 GALLIUM

GALLIUM has used PsExec to move laterally between hosts in the target network.[27]

S1229 Havoc

Havoc has the ability to copy files from one location to another.[28]

S0698 HermeticWizard

HermeticWizard can copy files to other machines on a compromised network.[29]

C0038 HomeLand Justice

During HomeLand Justice, threat actors initiated a process named Mellona.exe to spread the ROADSWEEP file encryptor and a persistence script to a list of internal machines.[30]

S0357 Impacket

Impacket has used its `wmiexec` command, leveraging Windows Management Instrumentation, to remotely stage and execute payloads in victim networks.[31]

G1032 INC Ransom

INC Ransom has used a rapid succession of copy commands to install a file encryption executable across multiple endpoints within compromised infrastructure.[32][33]

S1139 INC Ransomware

INC Ransomware can push its encryption executable to multiple endpoints within compromised infrastructure.[32]

S1132 IPsec Helper

IPsec Helper can download additional payloads from command and control nodes and execute them.[34]

S0372 LockerGoga

LockerGoga has been observed moving around the victim network via SMB, indicating the actors behind this ransomware are manually copying files form computer to computer instead of self-propagating.[1]

S0532 Lucifer

Lucifer can use certutil for propagation on Windows hosts within intranets.[35]

G0059 Magic Hound

Magic Hound has copied tools within a compromised network using RDP.[36]

G1051 Medusa Group

Medusa Group has utilized legitimate software services such as PDQ Deploy to transfer malicious binaries and tools to other victimized hosts within the target environment.[37]

S0457 Netwalker

Operators deploying Netwalker have used psexec to copy the Netwalker payload across accessible systems.[38]

S0365 Olympic Destroyer

Olympic Destroyer attempts to copy itself to remote machines on the network.[39]

C0014 Operation Wocao

During Operation Wocao, threat actors used SMB to copy files to and from target systems.[40]

S1017 OutSteel

OutSteel can download the Saint Bot malware for follow-on execution.[41]

S0029 PsExec

PsExec can be used to download or upload a file over a network share.[42]

G0034 Sandworm Team

Sandworm Team has used `move` to transfer files to a network share and has copied payloads--such as Prestige ransomware--to an Active Directory Domain Controller and distributed via the Default Domain Group Policy Object.[4][43] Additionally, Sandworm Team has transferred an ISO file into the OT network to gain initial access.[5]

S0140 Shamoon

Shamoon attempts to copy itself to remote machines on the network.[44]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors used Impacket to remotely stage and execute payloads via WMI.[45]

G1046 Storm-1811

Storm-1811 has used the Impacket toolset to move and remotely execute payloads to other hosts in victim networks.[46]

S0603 Stuxnet

Stuxnet uses an RPC server that contains a file dropping routine and support for payload version updates for P2P communications within a victim network.[47]

G0010 Turla

Turla RPC backdoors can be used to transfer files to/from victim machines on the local network.[48][49]

G1048 UNC3886

UNC3886 has utilzed Python scripts to transfer files between ESXi hosts and guest VMs.[50]

G1047 Velvet Ant

Velvet Ant transferred files laterally within victim networks through the Impacket toolkit.[31]

S1218 VIRTUALPIE

VIRTUALPIE has file transfer capabilities.[51]

S1217 VIRTUALPITA

VIRTUALPITA is capable of file transfer and arbitrary command execution.[51]

G1017 Volt Typhoon

Volt Typhoon has copied web shells between servers in targeted environments.[52]

S0366 WannaCry

WannaCry attempts to copy itself to remote computers after gaining access via an SMB exploit.[53]

G0102 Wizard Spider

Wizard Spider has used stolen credentials to copy tools into the `%TEMP%` directory of domain controllers.[54]
