Ingress Tool Transfer

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as ftp. Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. Lateral Tool Transfer).

On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, certutil, and PowerShell commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`.[1]

Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Adversaries have also abused file application features, such as the Windows `search-ms` protocol handler, to deliver malicious files to victims through remote file searches invoked by User Execution (typically after interacting with Phishing lures).[2]

Files can also be transferred using various Web Services as well as native or otherwise present tools on the victim system.[3] In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.[4]

ID: T1105

Sub-techniques: No sub-techniques

ⓘ Tactic: Command and Control

ⓘ Platforms: Linux, Network, Windows, macOS

Contributors: Alain Homewood; Jeremy Hedges; Joe Wise; John Page (aka hyp3rlinx), ApparitionSec; Mark Wee; Selena Larson, @selenalarson; Shailesh Tiwary (Indian Army); The DFIR Report

Version: 2.4

Created: 31 May 2017

Last Modified: 11 April 2024

Version Permalink

Procedure Examples

ID	Name	Description
C0028	2015 Ukraine Electric Power Attack	During the 2015 Ukraine Electric Power Attack, Sandworm Team pushed additional malicious tools onto an infected system to steal user credentials, move laterally, and destroy data. [5]
S0469	ABK	ABK has the ability to download files from C2.[6]
S1028	Action RAT	Action RAT has the ability to download additional payloads onto an infected machine.[7]
S0331	Agent Tesla	Agent Tesla can download additional files for execution on the victim's machine.[8][9]
S0092	Agent.btz	Agent.btz attempts to download an encrypted binary from a specified domain.[10]
G0130	Ajax Security Team	Ajax Security Team has used Wrapper/Gholee, custom-developed malware, which downloaded additional malware to the infected system.[11]
S1025	Amadey	Amadey can download and execute files to further infect a host machine with additional malware. [12]