DARKCOMET - Threat Encyclopedia | Trend Micro (US)

Archived: 2026-04-05 21:25:52 UTC

DARKCOMET (also known as FYNLOS) is a Remote Administration Tool (RAT) that is used in many targeted attacks. It has the ability to take pictures via webcam, listen in on conversations via a microphone attached to a PC, and gain full control of the infected machine.

This RAT is also known for its keylogging and file transfer functionality. As such, any remote attacker can load any files onto the infected machine or even steal documents.

DARKCOMET steals the following information:

- Admin rights
- Computer/User name
- Language/Country
- Operating System information
- RAM used
- Web Cam information

This backdoor modifies certain registry entries to disable Security Center functions. Doing this allows this malware to execute its routines without being detected. It disables Task Manager, Registry Editor, and Folder Options. It modifies registry entries to disable the Windows Firewall settings. This action allows this malware to perform its routines without being deteted by the Windows Firewall.

Installation

This backdoor drops the following copies of itself into the affected system:

- %User Temp%\WinDefender.Exe
- %Application Data%\VIA\vc.exe
- %User Temp%\lsasrv.exe
- %System%\Windupdt\winupdate.exe
- %Application Data%\HostProcess\{malware name}.exe

(Note: *%User Temp%* is the current user's Temp folder, which is usually C:\Documents and Settings\{user name}\Local Settings\Temp on Windows 2000, XP, and Server 2003, or C:\Users\{user name}\AppData\Local\Temp on Windows Vista and 7.. *%Application Data%* is the current user's Application Data folder, which is usually C:\Documents and Settings\{user name}\Application Data on Windows 2000, XP, and Server 2003, or C:\Users\{user name}\AppData\Roaming on Windows Vista and 7.. *%System%* is the Windows system folder, which is usually C:\Windows\System32.)

It creates the following folders:

- %Application Data%\dclogs

- %Application Data%\VIA
- %System%\Windupdt
- %Application Data%\HostProcess

(Note: *%Application Data%* is the current user's Application Data folder, which is usually C:\Documents and Settings\{user name}\Application Data on Windows 2000, XP, and Server 2003, or C:\Users\{user name}\AppData\Roaming on Windows Vista and 7.. *%System%* is the Windows system folder, which is usually C:\Windows\System32.)

Autostart Technique

This backdoor adds the following registry entries to enable its automatic execution at every system startup:

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
WinDefender = "%User Temp%\WinDefender.Exe"

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
VIAChipset = "%Application Data%\VIA\vc.exe"

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
Microsoft® Windows® Operating System = "%User Profile%\Templates\msadrh10.exe"

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
winupdater = "%System%\Windupdt\winupdate.exe"

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
HostProcess = "%Application Data%\HostProcess\{malware name}.exe"

It modifies the following registry entries to ensure it automatic execution at every system startup:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows NT\CurrentVersion\Winlogon
Userinit = "%System%\userinit.exe,%Application Data%\VIA\vc.exe"

(Note: The default value data of the said registry entry is *%System%\userinit.exe,*.)

Other System Modifications

This backdoor adds the following registry entries as part of its installation routine:

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Policies\

System
EnableLUA = "0"

It adds the following registry keys as part of its installation routine:

HKEY_CURRENT_USER\Software\DC3_FEXEC

It modifies the following registry entries to disable Security Center functions:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Security Center
AntiVirusDisableNotify = "1"

(Note: The default value data of the said registry entry is *0*.)

It creates the following registry entry(ies) to disable Task Manager, Registry Tools and Folder Options:

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Policies\
System
DisableTaskMgr = "1"

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Policies\
System
DisableRegistryTools = "1"

It modifies the following registry entries to disable the Windows Firewall settings:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile
EnableFirewall = "0"

(Note: The default value data of the said registry entry is *"1"*.)

Dropping Routine

This backdoor drops the following files:

- %Application Data%\dclogs\{date executed}-{number}.dc
- %User Temp%\NovoUpdate.exe
- %User Profile%\Templates\msadrh10.exe
- %User Temp%\vbc.exe

(Note: *%Application Data%* is the current user's Application Data folder, which is usually C:\Documents and Settings\{user name}\Application Data on Windows 2000, XP, and Server 2003, or C:\Users\{user name}\AppData\Roaming on Windows Vista and 7.. *%User Temp%* is the current user's Temp folder, which is

usually C:\Documents and Settings\{user name}\Local Settings\Temp on Windows 2000, XP, and Server 2003, or C:\Users\{user name}\AppData\Local\Temp on Windows Vista and 7.. *%User Profile%* is the current user's profile folder, which is usually C:\Documents and Settings\{user name} on Windows 2000, XP, and Server 2003, or C:\Users\{user name} on Windows Vista and 7.)

Other Details

This backdoor connects to the following possibly malicious URL:

- {BLOCKED}ount3.no-ip.org
- {BLOCKED}604.no-ip.org
- {BLOCKED}x-update.zapto.org
- http://{BLOCKED}e.habbo-dev.com/files
- {BLOCKED}554.no-ip.biz
- {BLOCKED}ster1.no-ip.org
- {BLOCKED}2.{BLOCKEDmedia.net
