DarkComet RAT: Technical Analysis of Attack Chain

any.run/cybersecurity-blog/darkcomet-rat-technical-analysis/

Mostafa ElSheimy

October 23, 2024

DarkComet RAT: <br>Technical Analysis of Attack Chain

DarkComet RAT:
Technical Analysis of Attack Chain

Editor's note: The current article is authored by Mostafa ElSheimy, a malware reverse engineer and threat intelligence analyst. You can find Mostafa on X and LinkedIn.

In this malware analysis report, we take an in-depth look at how the Remote Access Trojan (RAT) DarkComet has been used by attackers to remotely control systems, steal sensitive data, and execute various malicious activities.

Overview

DarkComet is a Remote Access Trojan (RAT) initially developed by Jean-Pierre Lesueur in 2008. This malware runs silently in the background, collecting sensitive information about the system, users, and network activity.

It attempts to steal stored credentials, usernames, passwords, and other personal data, transmitting this information to a destination specified by the attacker.

Backdoor.DarkComet allows attackers to install further malicious software on the infected machine or enlist it in a botnet for sending spam or other malicious activities.

Symptoms of an infection may not be noticeable to the user, as it can disable antivirus programs and other Windows security features.

Distribution methods include:

- Bundling with free software.
- Disguising as harmless programs in emails.
- Exploiting software vulnerabilities on websites.

DarkComet became widely used due to its user-friendly graphical interface, which contributed to its popularity.

Technical Details

Let's run a sandbox analysis session using ANY.RUN to discover the technical details of this malware.

View analysis session

Changing file attributes

DarkComet uses a command-line operation to alter file attributes, making its components more difficult to detect.

The command line of DarkComet displayed in ANY.RUN’s sandbox

It uses **attrib** to display or change file attributes

1. **+s (System Attribute)**: Marks the file as a system file, making it appear as a critical part of the operating system.
2. **+h (Hidden Attribute)**: Hides the file from regular view in Windows Explorer, making it invisible to most users.

Dropped executable file inside the summary of IOCs

It drops an executable at C:\Users\admin\Documents\MSDCSC\msdcsc.exe and executes it, making it harder to detect.

Contacting Malicious Domains

The malware establishes communication with a specified malicious domain, enabling remote control and data exfiltration.

Malicious domain displayed inside the sandbox

Modifying Process Privileges

The malware interacts with the Windows APIs **LookupPrivilegeValueA** and **AdjustTokenPrivileges** to modify the privileges associated with the current process's access token (not the process itself).

This is done by obtaining a handle to the process's access token, which allows the malware to modify its security context.

Modification of process privileges

If a2 is 0, the privilege is removed (Attributes = 0).

If a2 is 1, the privilege is enabled (Attributes = 2).

Gathering System Information

Retrieving Hardware Profile

Use of GetCurrentHwProfileA API

DarkComet uses the **GetCurrentHwProfileA** API to collect detailed information about the infected system’s hardware:

Hardware Profile ID (HWID): A Globally Unique Identifier (GUID) that identifies the current hardware profile, allowing the malware to uniquely recognize the system.

Dock State: Extracted through the **dwDockInfo** field, this information reveals whether the system is docked (e.g., connected to a docking station) or undocked. This helps the malware adapt its behavior based on the system’s hardware configuration.

Demonstration of GUID and Dock State

Retrieving Date, Time, and Location

The malware also gets the date and time of the victim device.

Retrieval of date and time

It also checks the computer’s location settings by querying the registry key associated with the current user’s Security Identifier (SID):

\REGISTRY\USER{SID}\Control Panel\International\Geo\Nation

Data Processing and Manipulation

DarkComet uses a function called **sub_4735E8** multiple times with different strings as parameters.

Use of sub_4735E8 function

This function carries out resource management and processes various pieces of data, including:

- **C2 Domain Information**: The Command and Control server the malware communicates with.
- **SID (Security Identifier)**: Identifies the user profile associated with the malware's activity.
- **Mutex Values**: Used to ensure that only one instance of the malware runs on the infected system at a time.

This function helps obfuscate key information, preventing it from appearing directly in the strings section of the malware.

Data processing and data manipulation with v28

With this function, the malware loops through **DARKCOMET DATA** to retrieve specific attributes based on the provided parameter strings.

DARKCOMET DATA

Here is the loop that the malware uses to iterate through DARKCOMET DATA:

Demonstration of the loop used by DarkComet

Within sub_4735E8, DarkComet iterates through its internal data set, known as **DARKCOMET DATA**, to match specific parameters and extract corresponding attributes. This process involves looping through data entries to retrieve the needed values based on the provided strings.

Extracted DARKCOMET DATA:

```
#BEGIN DARKCOMET DATA --

MUTEX={DC_MUTEX-D1SPNDG}

SID={Sazan}

FWB={0}

NETDATA={8.tcp.eu.ngrok.io:27791}

GENCODE={fKTZRKdv0Nij}

INSTALL={1}

COMBOPATH={7}

EDTPATH={MSDCSC\\msdcsc.exe}

KEYNAME={MicroUpdate}

EDTDATE={16/04/2007}

PERSINST={0}

MELT={0}

CHANGEDATE={0}

DIRATTRIB={6}

FILEATTRIB={6}

FAKEMSG={1}

EF={1}

MSGCORE={{42696C67697361796172FD6EFD7A20332073616E6979652069E7696E64652079656E6964656E206261FE6C6174FD6C6163616B74FD722E2E2E}

MSGICON={48}

SH1={1}

CHIDEF={1}

CHIDED={1}

PERS={1}

OFFLINEK={1}

#EOF DARKCOMET DATA --
```

From this data, the malware extracts and processes key attributes, including:

- **C2 domain**: Specifies where the malware sends stolen data.
- **EDTDATE**: The date associated with the malware’s installation (e.g., 16/04/2007), indicating that it does not alter the date of the dropped executable.

The processed C2 domain & EDTDATE

Mutex: Ensures that only one copy of DarkComet runs on the system.

The processed Mutex

Campaign name: Used for identifying specific attacks or operations.

Processed campaign name

It also processes the attributes of the malware that define how it behaves and interacts with the system:

- **EDTPath**: Path of the executable (MSDCSC\msdcsc.exe)

The path of the new executable

Registry Key (KEYNAME): MicroUpdate, used to maintain persistence in the system’s registry.

reg_key (KEYNAME): MicroUpdate

From the DARKCOMET DATA, we can also notice that the malware does not change the original creation date of the dropped executable. The CHANGEDATE attribute is set to 0, indicating that the date remains unchanged, which can help the malware blend in with other files and avoid raising suspicion during forensic analysis.

Dropped Executable File

DarkComet drops a file named **msdcsc.exe** in the C:\Users\admin\Documents\MSDCSC\ directory and executes it from there.

The dropped executable file

This dropped file is identical to the original malware executable.

Comparison of the original and executable files

This means it can start itself from another location. By doing so, the malware can better evade detection, as running from a new path makes it more challenging for security tools to track its activity.

Persistence Mechanisms

To maintain persistence on the infected system, DarkComet:

Adds Run key: It creates a registry entry at SOFTWARE\Microsoft\Windows\CurrentVersion\Run\MicroUpdate with the path of the executable.

Modifies the WinLogon registry key: It alters \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\UserInit for persistance.

Registry entry creation

DLL Loading and Function Resolution

DarkComet retrieves handles to the modules (DLLs) such as kernel32.dll and user32.dll for further manipulation and execution of its malicious functions.

Module handle retrieval for DLL

RAT Functionalities

DarkComet has various capabilities that allow it to manipulate the infected system and gather information. These include functions for simulating user input, capturing data, and interacting with the system’s display and clipboard.

Simulating Mouse and Keyboard Actions

DarkComet uses the **mouse_event** function to simulate mouse motion and button clicks.

implementation of mouse_event

This helps the attacker to interact with the system as if a user is controlling the mouse.

DarkComet synthesizing the mouse motion and button clicks

This malware also uses Keyboard Event Simulation, particularly, the **keybd_event function** to allow the malware to manipulate the user's environment, input data, or perform actions without the user's knowledge.

Implementation of the keybd_event function

Capturing Keyboard Inputs

The malware calls **GetKeyboardType(0)** to determine the type of the primary keyboard. If it returns 7, it indicates that the keyboard is a “language” keyboard, which is often a Unicode keyboard.

DarkComet retrieving information about the current keyboard

The next function captures keystrokes from the user, allowing the malware to record input without detection.

Keyboard input capture

The function used by DarkComet processes each character input (ch), which could represent a keyboard key or a specific command. It applies a series of conditional checks and actions based on the character’s value.

This malware utilizes the **VkKeyScanA(ch)** function to convert the character into a virtual key code. This conversion allows the malware to accurately interpret and simulate keyboard actions, making it easier to log keystrokes or execute commands.

Conversion of characters into keystrokes

System and Display Information

The malware uses **EnumDisplayDevicesA** function to retrieve information about display devices connected to the system.

Retrieving Display information connected to the system

DarkComet attempts to access data from the clipboard, focusing on format 0xE, which is used for enhanced metafiles (EMF) – a vector graphics format. By doing so, the RAT can exfiltrate or manipulate clipboard data, such as copied images or text.

Retrieving data from the clipboard

C2 Commands and Remote Control

DarkComet receives instructions from its Command and Control (C2) server, allowing it to perform various remote tasks. These commands enable the attacker to control the malware's behavior and may include actions like:

- **Data exfiltration**: Extracting files or information from the infected system.
- **System manipulation**: Modifying system settings or terminating processes.
- **Additional payload delivery**: Deploying additional malicious software into the infected system.

See **Appendix I** for the extracted commands that the C2 server sends to the malware.

These commands help control the malware's behavior remotely and may provide insight into the attacker's objectives and tactics.

Conclusion

DarkComet is a highly capable Remote Access Trojan (RAT) that continues to be a threat due to its stealthy behavior and extensive feature set. It allows attackers to manipulate infected systems remotely, steal sensitive information, and install additional malware.

This analysis has demonstrated DarkComet's ability to evade detection by modifying file attributes, manipulating registry keys for persistence, and escalating privileges. It gathers system information, including hardware profiles and location settings, and communicates with a command-and-control (C2) server to execute a variety of commands, from capturing keystrokes to controlling display devices.

The malware's functionality, including its ability to modify system settings, simulate user input, and manage services, makes it a versatile tool for attackers. Its ease of use, coupled with a rich set of RAT functionalities, has contributed to its widespread deployment, especially in targeted cyberattacks.

Appendix I

IOCs

Hashes

md5: 1b540a732f2d75c895e034c56813676a

sha1: 0dd8c542fd46dd5b55eefcf35382ee8903533703

sha256: 90d3dbe2c8ae46b970a865f597d091688e7c04c7886a1ec287e4b7a0f5e2fcf1

C2

8[.]tcp[.]eu[.]ngrok[.]io[:]27791

Registry keys

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\UserInit = "C:\\Windows\\system32\\userinit.exe,C:\\Users\\Admin\\Documents\\MSDCSC\\msdcsc.exe"

\REGISTRY\USER\USER SID\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\MicroUpdate = "C:\\Users\\Admin\\Documents\\MSDCSC\\msdcsc.exe"

Dropped executable file

C:\Users\admin\Documents\MSDCSC\msdcsc.exe

TTPs

TACTIC	TECHNIQUE	MITRE ATT&CK ID
Persistence	Boot or Logon Autostart Execution	T1547
	Adds Run key to start application	T1547.001
	Winlogon Helper DLL	T1547.004
Privilege Escalation	Boot or Logon Autostart Execution	T1547
	Adds Run key to start application	T1547.001

TACTIC	TECHNIQUE	MITRE ATT&CK ID
	Winlogon Helper DLL	T1547.004
Defense Evasion	Modify Registry	T1112
	Hide Artifacts	T1564
	Hidden Files and Directories	T1564.001
Discovery	Query Registry	T1012
	System Information Discovery	T1082
	System Location Discovery	T1614
	System Language Discovery	T1614.001
Command and Control	Web Service	T1102

Commands

```
GetSIN
RefreshSIN
RunPrompt
GetDrives
GetSrchDrives
GetFileAttrib
KillProcess
GetAppList
GetServList
StartServices
StopServices
RemoveServices
InstallService
GetStartUpList
ActiveOnlineKeylogger
ActiveOfflineKeylogger
GetOfflineLogs
Shutdown
RestartComp
LogOffComp
PowerOff
GetFullInfo
GetSystemInfo
OpenWebPage
PrintText
GetTorrent
GetPrivilege
TraceRoute
#BOT#VisitUrl
#BOT#OpenUrl
#BOT#Ping
#BOT#RunPrompt
#BOT#CloseServer
#BOT#SvrUninstall
#BOT#URLUpdate
DOWNLOADFILE
UPLOADFILE
ACTIVEREMOTESHELL
DESKTOPCAPTURE
WEBCAMLIVE
```

```
WIFI

CHAT

FTPFILEUPLOAD
```

Mostafa ElSheimy

Mostafa ElSheimy

Malware Analyst | + posts

Mostafa ElSheimy is a malware reverse engineer and threat intelligence analyst, specializing in analyzing TTPs (Tactics, Techniques, and Procedures) and crafting YARA rules to detect and counter cyber threats. Mostafa's work focuses on dissecting malware to uncover hidden dangers and protect organizations from emerging threats.

Find him on X and LinkedIn.

mostafa-elsheimy

Mostafa ElSheimy

Malware Analyst

Mostafa ElSheimy is a malware reverse engineer and threat intelligence analyst, specializing in analyzing TTPs (Tactics, Techniques, and Procedures) and crafting YARA rules to detect and counter cyber threats. Mostafa's work focuses on dissecting malware to uncover hidden dangers and protect organizations from emerging threats.

Find him on X and LinkedIn.

View all posts Twitter

What do you think about this post?

4 answers

- Awful
- Average
- Great

No votes so far! Be the first to rate this post.

0 comments