WIKIPEDIA

DarkComet

DarkComet is a remote access trojan (RAT) developed by Jean-Pierre Lesueur (known as DarkCoderSc[2]), an independent programmer and computer security coder from France. Although the RAT was developed back in 2008, it began to proliferate at the start of 2012. The program was discontinued, partially due to its use in the Syrian civil war to monitor activists but also due to its author's fear of being arrested for unnamed reasons. [1] As of August 2018, the program's development "has ceased indefinitely", and downloads are no longer offered on its official website. [3]

DarkComet

Developer(s)	Jean-Pierre Lesueur (DarkCoderSc)
Last release	5.3.1
Operating system	Microsoft Windows
Type	Remote Administration Tool
License	freeware
Website	https://www.darkcomet-rat.com/ [1]

DarkComet allows a user to control the system with a Graphical User Interface (GUI). It has many features which allows a user to use it as administrative remote help tool; however, DarkComet has many features which can be used maliciously. DarkComet is commonly used to spy on the victims by taking screen captures, key-logging, or password stealing.

Contents

History of DarkComet

Syria

In 2014 DarkComet was linked to the Syrian conflict. People in Syria began using secure connections to bypass the government's censorship and the surveillance of the internet. This caused the Syrian Government to resort to using RATs to spy on its civilians. Many believe that this is what caused the arrests of many activists within Syria.[1]

The RAT was distributed via a "booby-trapped Skype chat message" which consisted of a message with a Facebook icon which was actually an executable file that was designed to install DarkComet.[4] Once infected, the victim's machine would try to send the message to other people with the same booby-trapped Skype chat message.

Once DarkComet was linked to the Syrian regime, Lesueur stopped developing the tool stating that, “I never imagined it would be used by a government for spying,” he said. “If I had known that, I would never have created such a tool.”[1]

Target Gamers, Military and Governments

In 2012 Arbos Network company found evidence of DarkComet being used to target military and gamers by unknown hackers from Africa. At the time, they mainly targeted the United States.[5]

Je Suis Charlie

In the wake of the January 7, 2015, attack on the *Charlie Hebdo* magazine in Paris, hackers used the "#JeSuisCharlie" slogan to trick people into downloading DarkComet. DarkComet was disguised as a picture of a newborn baby whose wristband read "Je suis Charlie." Once the picture was downloaded, the users became compromised.[6] Hackers took advantage of the disaster to compromise as many systems as possible. DarkComet was spotted within 24 hours of the attack.

Architecture and Features

Architecture

DarkComet, like many other RATs, uses a reverse-socket architecture. The uninfected computer with a GUI enabling control of infected ones is the client, while the infected systems (without a GUI) are servers.[7]

When DarkComet executes, the server connects to the client and allows the client to control and monitor the server. At this point the client can use any of the features which the GUI contains. A socket is opened on the server and waits to receive packets from the controller, and executes the commands when received.

Features

The following list of features is not exhaustive but are the critical ones that make DarkComet a dangerous tool. Many of these features can be used to completely take over a system and allows the client full access when granted via UAC.

- Spy Functions
  - Webcam Capture
  - Sound Capture
  - Remote Desktop
  - Keylogger
- Network Functions
  - Active Ports
  - Network Shares
  - Server Socks5
  - LAN Computers
  - Net Gateway
  - IP Scanner
  - Url Download
  - Browse Page
  - Redirect IP/Port
  - WiFi Access Points
- Computer Power
  - Poweroff
  - Shutdown
  - Restart
  - Logoff
- Server Actions

    - Lock Computer
    - Restart Server
    - Close Server
    - Uninstall Server
    - Upload and Execute
    - Remote Edit Service
- Update Server
    - From URL
    - From File

DarkComet also has some "Fun Features".

- Fun Features
    - Fun Manager
    - Piano
    - Message Box
    - Microsoft Reader
    - Remote Chat

Detection

DarkComet is a widely known piece of malware, If you install an antivirus, or a darkcomet remover, you can un-infect your computer quickly. Its target machines are typically anything from Windows XP, all the way up to Windows 10.

Common anti-virus tags for a dark comet application are as follow:

- Trojan[Backdoor]/Win32.DarkKomet.xyk

- BDS/DarkKomet.GS

- Backdoor.Win32.DarkKomet!O

- RAT.DarkComet

When a computer is infected, it tries to create a connection via socket to the controllers computer. Once the connection has been established the infected computer listens for commands from the controller, if the controller sends out a command, the infected computer receives it, and executes whatever function is sent.

References

1. McMillan, Robert. "How the Boy Next Door Accidentally Built a Syrian Spy Tool" (https://www.wired.com/2012/07/dark-comet-syrian-spy-tool/). *Wired*.
2. "DarkCoderSc | SOLDIERX.COM" (https://www.soldierx.com/hdb/DarkCoderSc). *SoldierX*. Retrieved 13 October 2017.
3. "Project definitively closed since 2012" (https://www.darkcomet-rat.com). "DarkComet-RAT development has ceased indefinitely in July 2012. Since the [sic], we do not offer downloads, copies or support."
4. "Spy code creator kills project after Syrian abuse" (https://www.bbc.com/news/technology-18783064). BBC. 10 July 2012.
5. Wilson, Curt. "Exterminating the RAT Part I: Dissecting Dark Comet Campaigns" (https://asert.arbornetworks.com/exterminating-the-rat-part-i-dissecting-dark-comet-campaigns/). Arbor.
6. Vinton, Kate. "How Hackers Are Using #JeSuisCharlie To Spread Malware" (https://www.forbes.com/sites/katevinton/2015/01/15/darkcomet-malware-cyber-attacks-follow-charlie-hebdo-shooting/). Forbes.
7. Denbow, Shawn; Hertz, Jesse. "pest control: taming the rats" (http://matasano.com/research/PEST-CONTROL.pdf) (PDF). *Matasano*.

External links

- Official Website (now defunct) (https://www.darkcomet-rat.com/)

Retrieved from "https://en.wikipedia.org/w/index.php?title=DarkComet&oldid=854375584"

This page was last edited on 10 August 2018, at 21:41 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.