DarkComet Malware Overview

Operational (OP) | Fusion (FS)

Cyber Espionage (CE) | Cyber Crime (CC)

June 09, 2017 01:14:00 PM, 16-00018592, Version: 2

OPERATING SYSTEM

DESCRIPTION

The DarkComet malware is a publicly available remote access Trojan (RAT) capable of more than 60 different functions, including collecting system information, controlling all processes currently running on an infected system, viewing and modifying registries, creating a reverse shell, modifying or adding start-up processes and services, keylogging, stealing credentials, recording audio, scanning networks, locking, restarting and shutting down infected systems, updating malware with a new command and control (C&C) server or new functionality, and downloading, modifying, and uploading files.

ALIASES

Fynloski

FIREEYE DETECTION NAMES

Backdoor.DarkComet , Trojan.DarkComet , Backdoor.Fynloski , Trojan.Fynloski

RELATED ACTORS

Katar

ROLE

Backdoor

5950 Berkshire Lane, Suite 1600 Dallas, TX 75225