

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

This message contains content and links to content which are the property of FireEye, Inc. and are protected by all applicable laws. This cyber threat intelligence and this message are solely intended for the use of the individual and organization to which it is addressed and is subject to the subscription Terms and Conditions to which your institution is a party. Onward distribution in part or in whole of any FireEye proprietary materials or intellectual property is restricted per the terms of agreement. By accessing and using this and related content and links, you agree to be bound by the subscription .

For more information please visit: <https://intelligence.fireeye.com/reports/16-00018592>

© 2020, FireEye, Inc. All rights reserved.