Analysis of DarkComet RAT

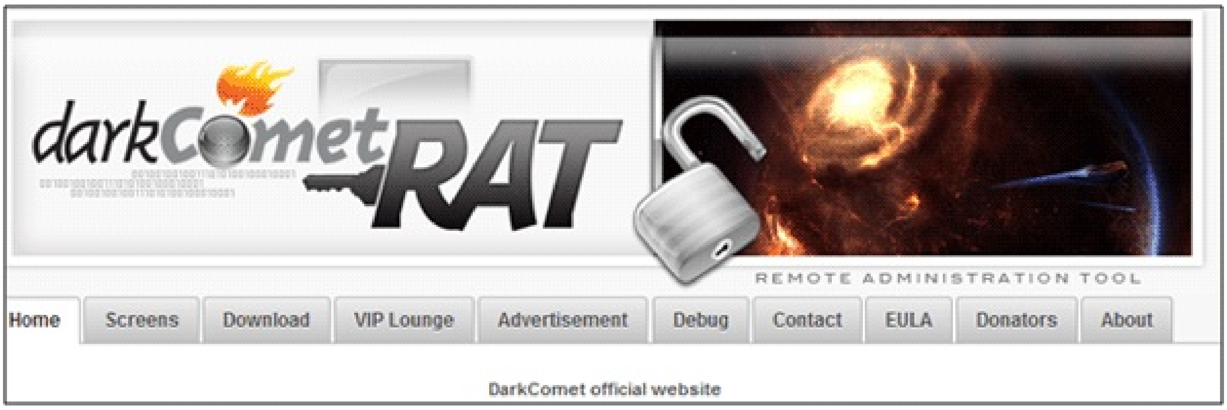
February 29, 2012 05:49:00 AM, 12-18880, Version: 1 Risk Rating: MEDIUM

Executive Summary

DarkComet is a do-it-yourself (DIY) Trojan that includes a robust set of features in its editor and builder. It has typical control features, like keylogging and modifying mouse or keyboard settings, but also has innovative features like playing a remote digital piano on an infected computer. It also supports encrypted command and control (C&C) communications and was used recently in a Breut Trojan attack linked to Syria (for information on this attack, see iSIGHT Partners. "Breut Trojan with C&C Out of Syria," Malware Report #12-18872. Feb. 28, 2012).

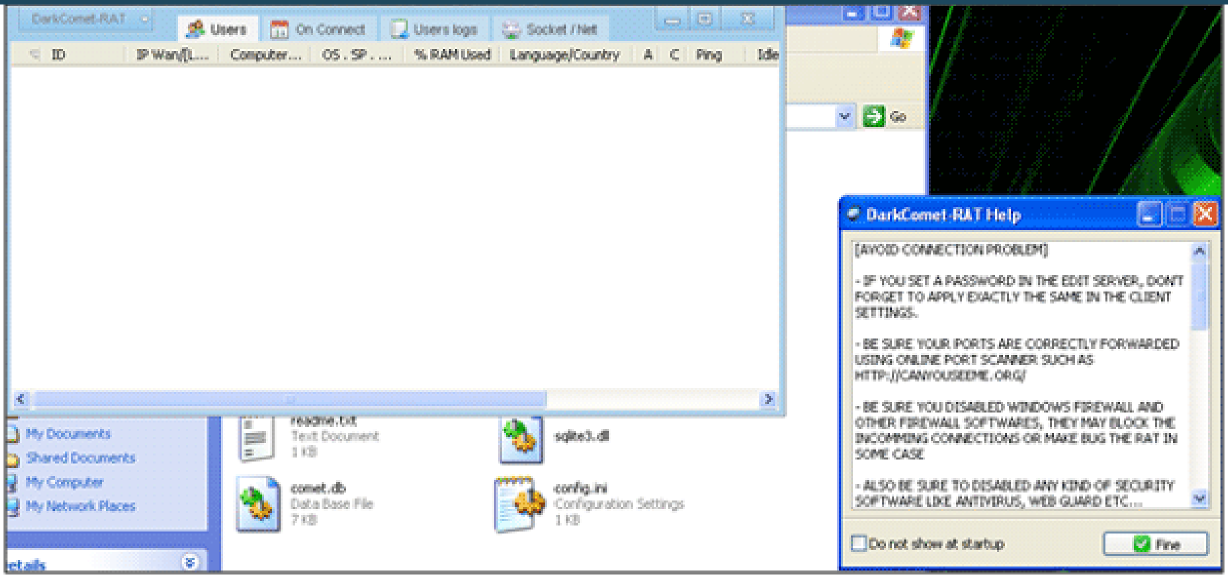
Analysis

DarkComet is a full featured Remote Administration Trojan or Remote Access Tool (RAT) that has been freely available to the public since 2008 via hxxp://darkcomet-rat.com:



DarkComet website banner

When run for the first time, common EULAs are expressed, followed by a standard RAT interface and a help window:



[AVOID CONNECTION PROBLEM]

- IF YOU SET A PASSWORD IN THE EDIT SERVER, DONT FORGET TO APPLY EXACTLY THE SAME IN THE CLIENT SETTINGS.

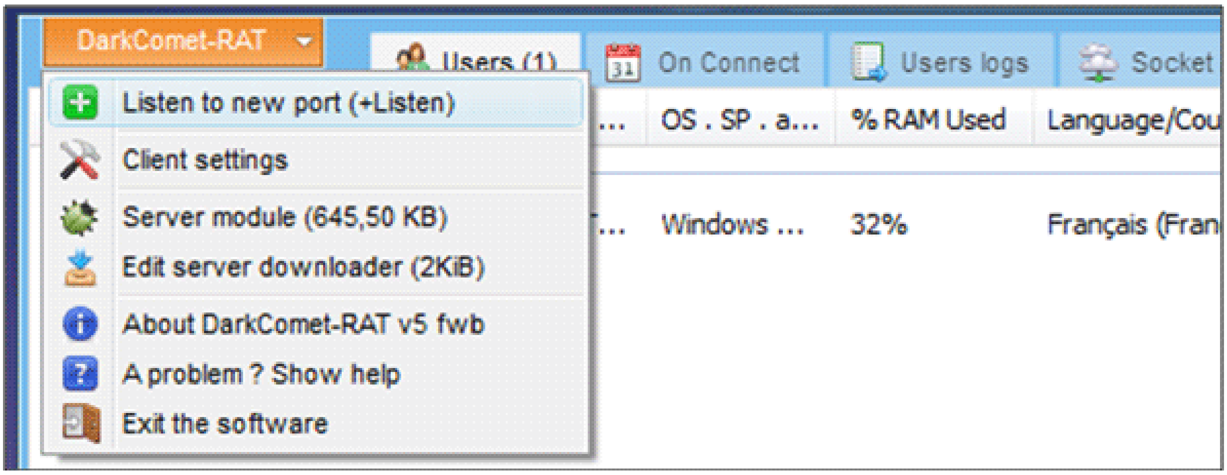
- BE SURE YOUR PORTS ARE CORRECTLY FORWARDED USING ONLINE PORT SCANNER SUCH AS HTTP://CANYOUSEEME.ORG/

- BE SURE YOU DISABLED WINDOWS FIREWALL AND OTHER FIREWALL SOFTWARES, THEY MAY BLOCK THE INCOMMING CONNECTIONS OR MAKE BUG THE RAT IN SOME CASE

- ALSO BE SURE TO DISABLED ANY KIND OF SECURITY SOFTWARE LIKE ANTIVIRUS, WEB GUARD ETC...

□ Do not show at startup

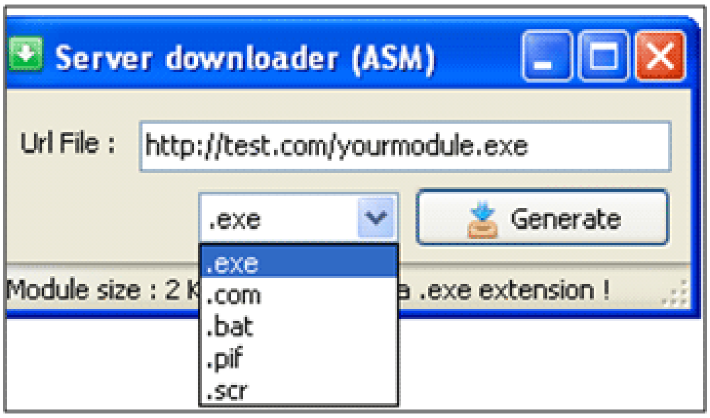
DarkComet GUI and help window



DarkComet GUI menu options

Downloader Editor

The program includes a downloader component that enables an actor to create a downloader, which is then pointed at a remote downloader URL. Downloaders are commonly used as a lightweight method to install a fully functional Trojan, such as DarkComet, by downloading and installing it from a remote location following initial compromise.



Server downloader (ASM)

Url File : http://test.com/yourmodule.exe

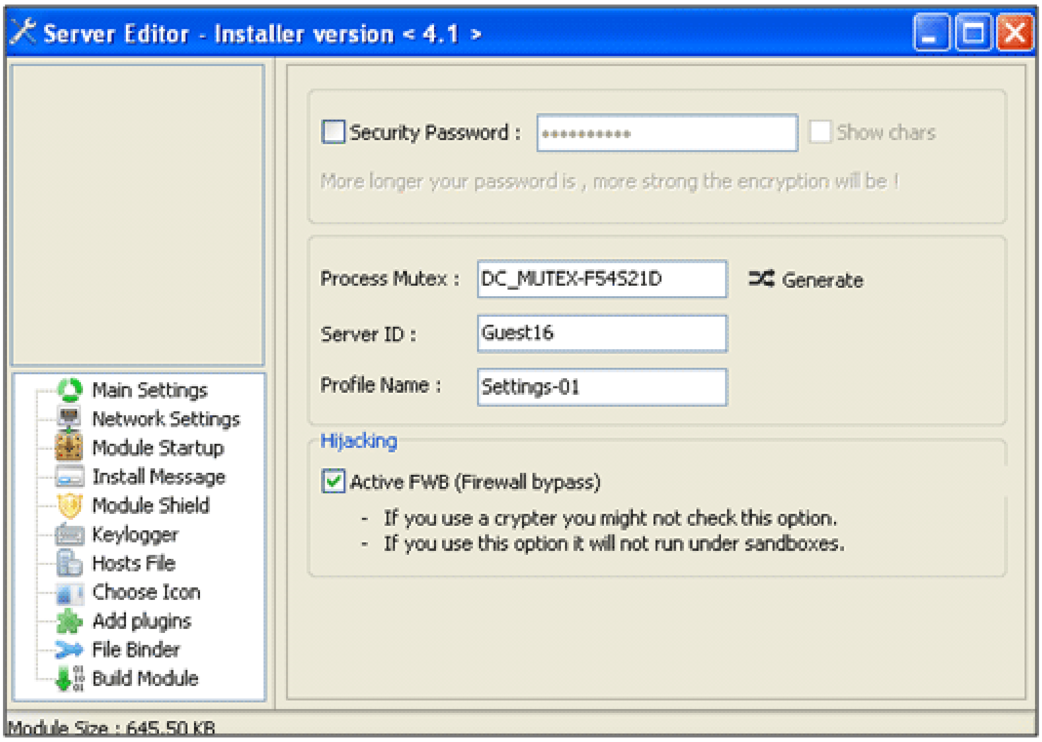
.exe

Module size : 2 K… a .exe extension !

Downloader configuration window

Server Editor

The server module enables an actor to configure and deploy a full featured DarkComet RAT.



Server Editor - Installer version < 4.1 >

□ Security Password : ••••••••••• □ Show chars

More longer your password is , more strong the encryption will be !

Process Mutex : DC_MUTEX-F54S21D

Server ID : Guest16

Profile Name : Settings-01

Hijacking

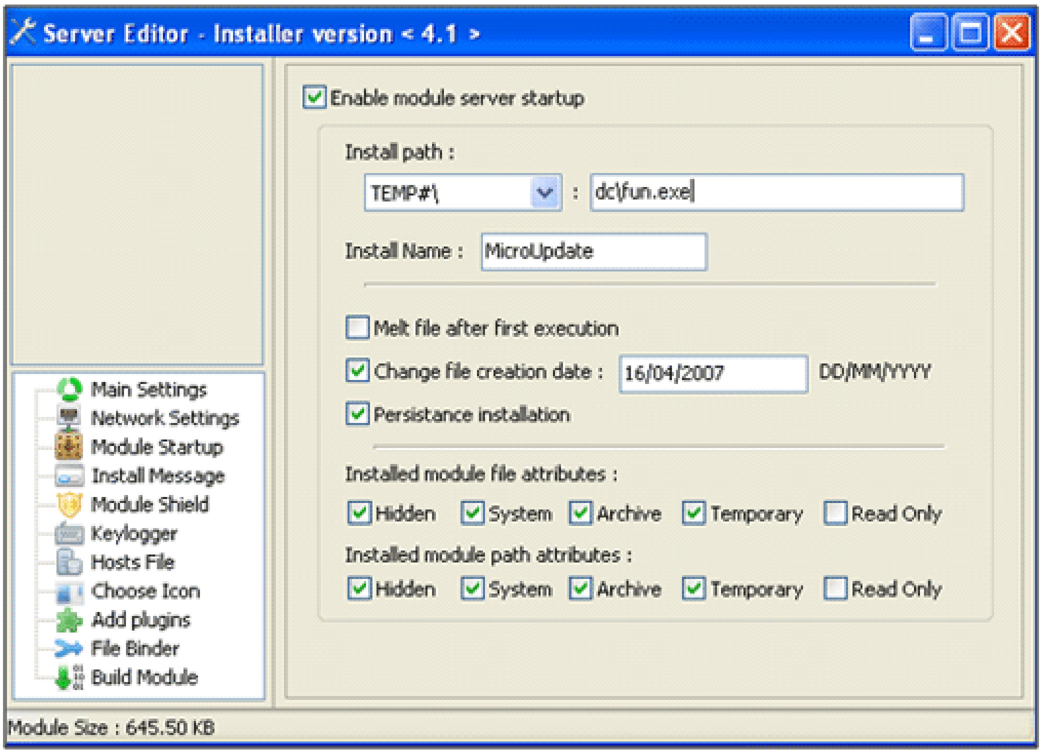
☑ Active FWB (Firewall bypass)

- If you use a crypter you might not check this option.
- If you use this option it will not run under sandboxes.

Module Size : 645.50 KB

Server setup showing default MUTEX and other values

A variety of persistence (i.e., startup) methods also exists for an actor to configure during server editing:



Server Editor - Installer version < 4.1 >

☑ Enable module server startup

Install path : TEMP#\ : dc\fun.exe

Install Name : MicroUpdate

☐ Melt file after first execution

☑ Change file creation date : 16/04/2007 DD/MM/YYYY

☑ Persistance installation

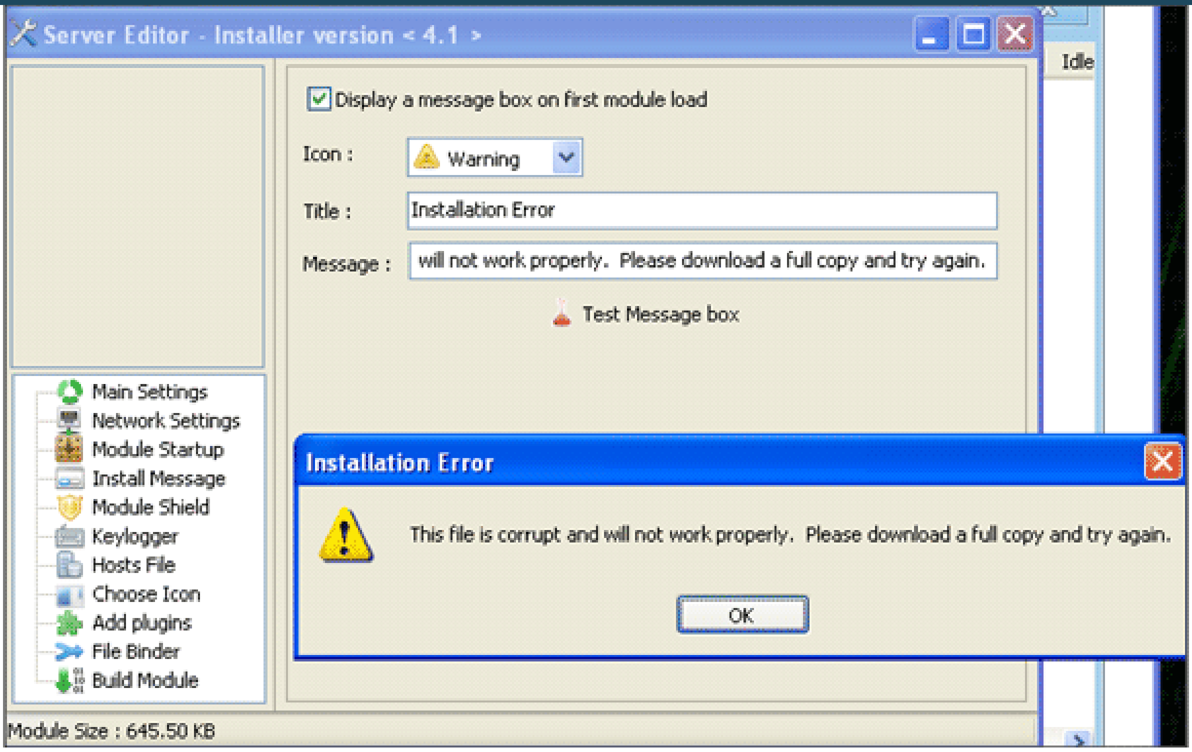
Installed module file attributes : ☑ Hidden ☑ System ☑ Archive ☑ Temporary ☐ Read Only

Installed module path attributes : ☑ Hidden ☑ System ☑ Archive ☑ Temporary ☐ Read Only

Module Size : 645.50 KB

Startup options for DarkComet

An actor may also configure a fake error, insulting message or whatever they choose to display, if at all, once the server is run:



☑ Display a message box on first module load

Icon : Warning

Title : Installation Error

Message : will not work properly. Please download a full copy and try again.

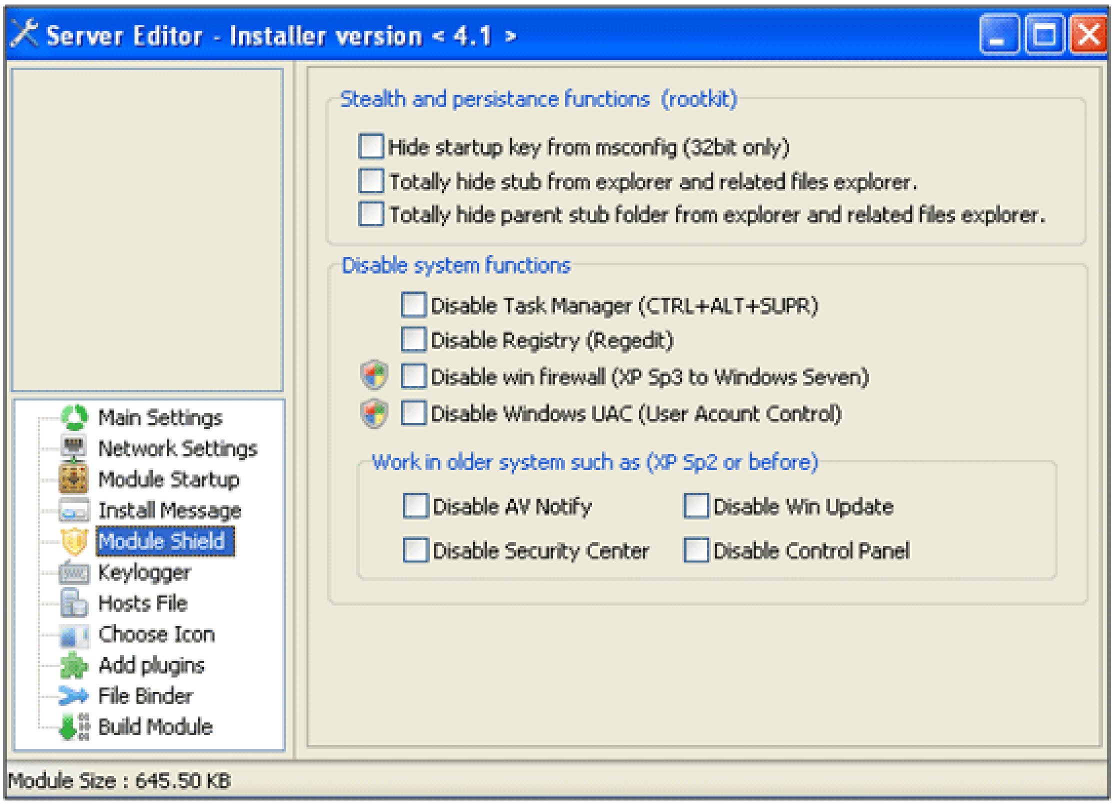
Installation Error

This file is corrupt and will not work properly. Please download a full copy and try again.

Module Size : 645.50 KB

A fake "Installation Error" window is configured for the server when run, tested here

A variety of stealth options also exist for configuration:



Stealth and persistance functions (rootkit)

□ Hide startup key from msconfig (32bit only)
□ Totally hide stub from explorer and related files explorer.
□ Totally hide parent stub folder from explorer and related files explorer.

Disable system functions

□ Disable Task Manager (CTRL+ALT+SUPR)
□ Disable Registry (Regedit)
□ Disable win firewall (XP Sp3 to Windows Seven)
□ Disable Windows UAC (User Acount Control)

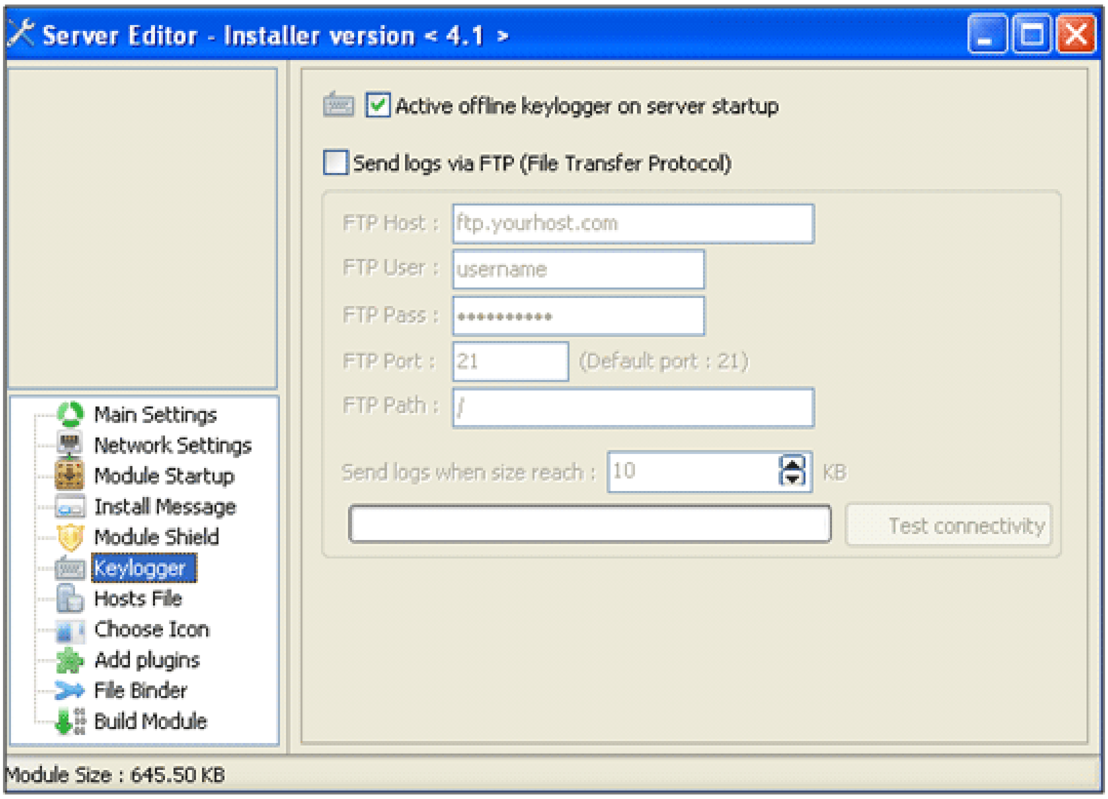
Work in older system such as (XP Sp2 or before)

□ Disable AV Notify
□ Disable Win Update
□ Disable Security Center
□ Disable Control Panel

Module Size : 645.50 KB

Stealth options for DarkComet

Keylogger and exfiltration options also exist:



Server Editor - Installer version < 4.1 >

☑ Active offline keylogger on server startup

□ Send logs via FTP (File Transfer Protocol)

FTP Host : ftp.yourhost.com
FTP User : username
FTP Pass : •••••••••••
FTP Port : 21 (Default port : 21)
FTP Path : /

Send logs when size reach : 10 KB

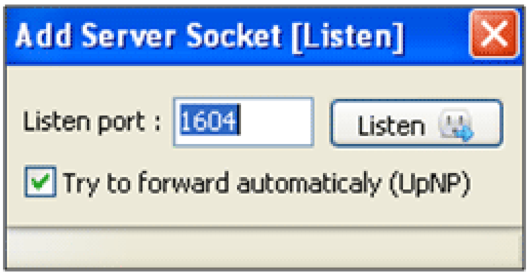
Module Size : 645.50 KB

Keylogger and FTP configuration options

The Windows HOSTS file on an infected computer can also be loaded and modified if desired. This includes during server creation and via client management post-infection. Custom icons may be used for the server, a standard feature of most RATs. DarkComet also supports the use of plugins, which are configured during server editing if desired, and/or rolled out to infected computers via an update later. Prior to distribution of a finished server, an actor may choose to use the "file binder" option of DarkComet to bundle it with another program. This is a common tactic used to masquerade a Trojan's functionality by silently installing it while a victim runs a file bound to the Trojan. UPX and MPRESS packers are also built into the DarkComet builder.

Client Manager

Client settings are used to work with clients (i.e., infected computers) to remotely control them and/or exfiltrate data of interest. The image below shows the client being configured to listen on a port for a server recently configured via the builder:



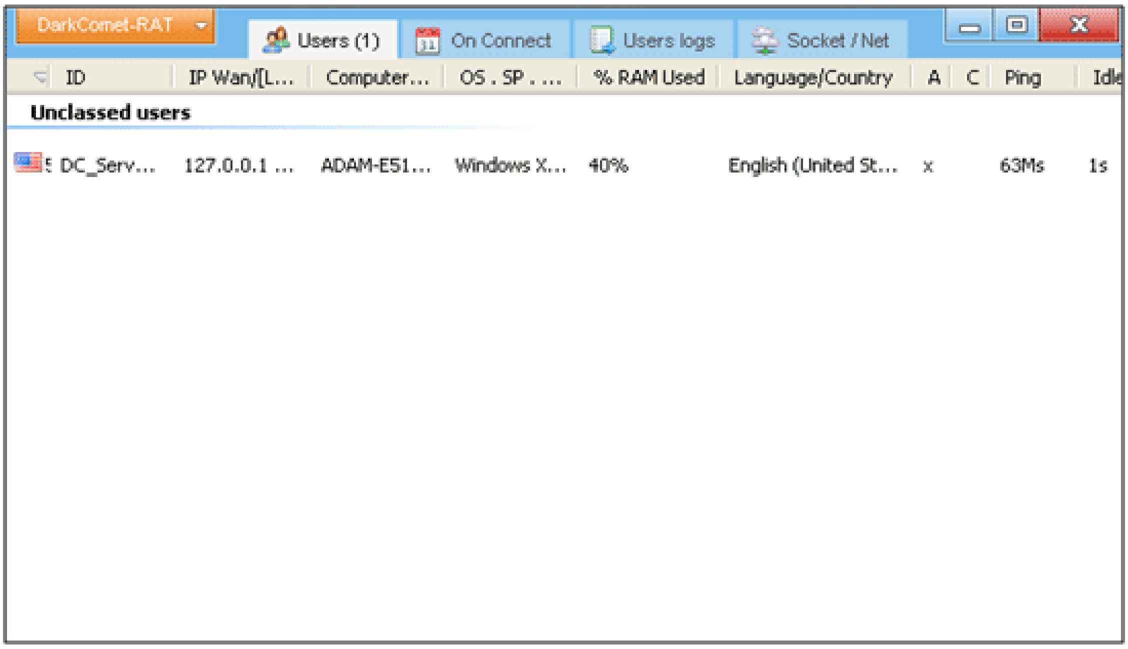
Add Server Socket [Listen]

Listen port : 1604

☑ Try to forward automaticaly (UpNP)

Client listener setup

Setup of the listener may trigger a Windows firewall warning, as it requires a port be opened to enable listening. This is a trivial step for an actor to undertake in order to then listen remotely to any remotely infected computers. Once connected, a status window update is performed:

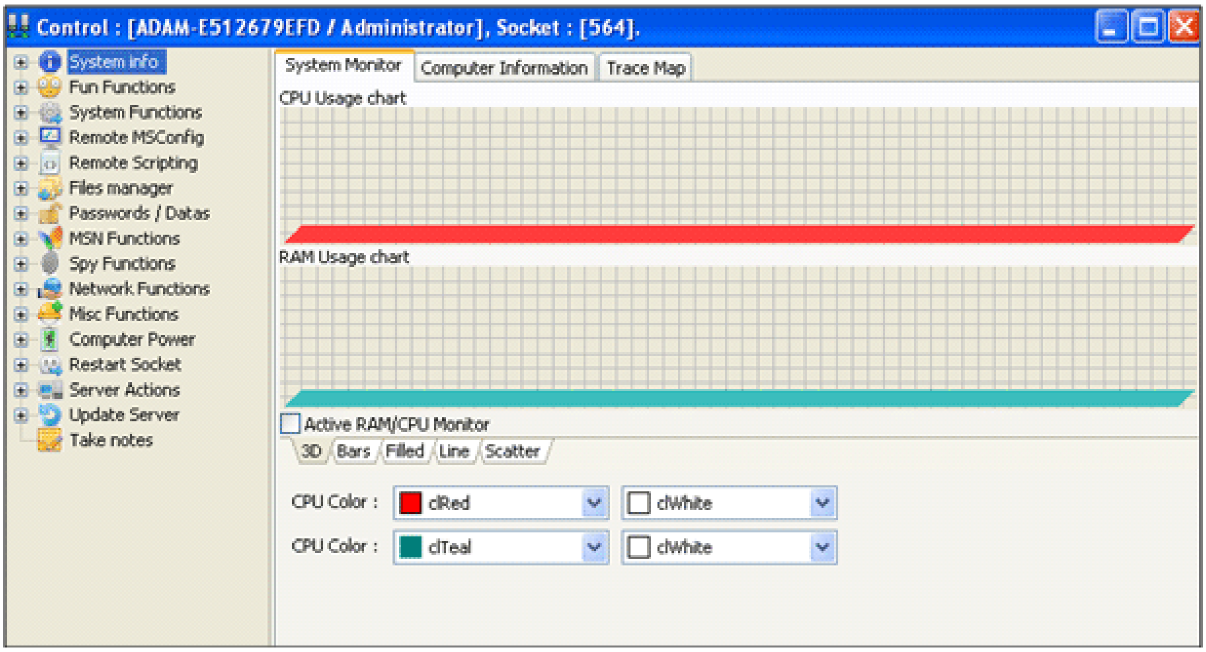


Unclassed users

ID	IP Wan/[L...	Computer...	OS . SP	% RAM Used	Language/Country	A	C	Ping	Idle
DC_Serv...	127.0.0.1 ...	ADAM-E51...	Windows X...	40%	English (United St...	x		63Ms	1s

DarkComet is connected an infected computer in the US

Double clicking and right clicking gives various control options over the remote computer connected to the client manager. For example, double-clicking reveals a wealth of options to triage the system and remotely control it:


Control : [ADAM-E512679EFD / Administrator], Socket : [564].

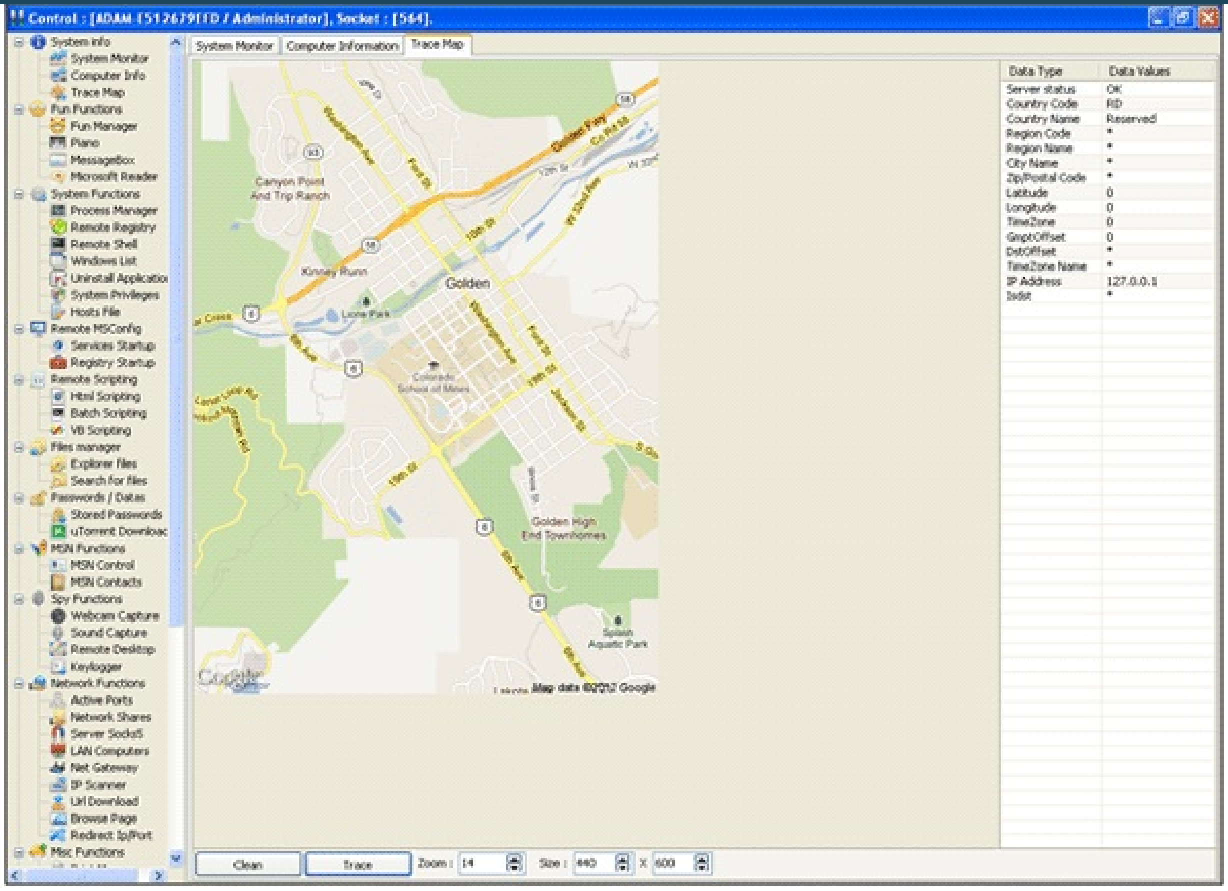
☐ Active RAM/CPU Monitor

CPU Color : 🟥 clRed | ☐ clWhite

CPU Color : 🟩 clTeal | ☐ clWhite

Control options for a remotely infected computer

DarkComet makes it easy to immediately identify the reported IP geolocation and other data about an infected computer:



Data Type	Data Values
Server status	OK
Country Code	RD
Country Name	Reserved
Region Code	*
Region Name	*
City Name	*
Zip/Postal Code	*
Latitude	0
Longitude	0
TimeZone	0
GmptOffset	0
DstOffset	*
TimeZone Name	*
IP Address	127.0.0.1
Isdst	*

Geolocation of an infected computer

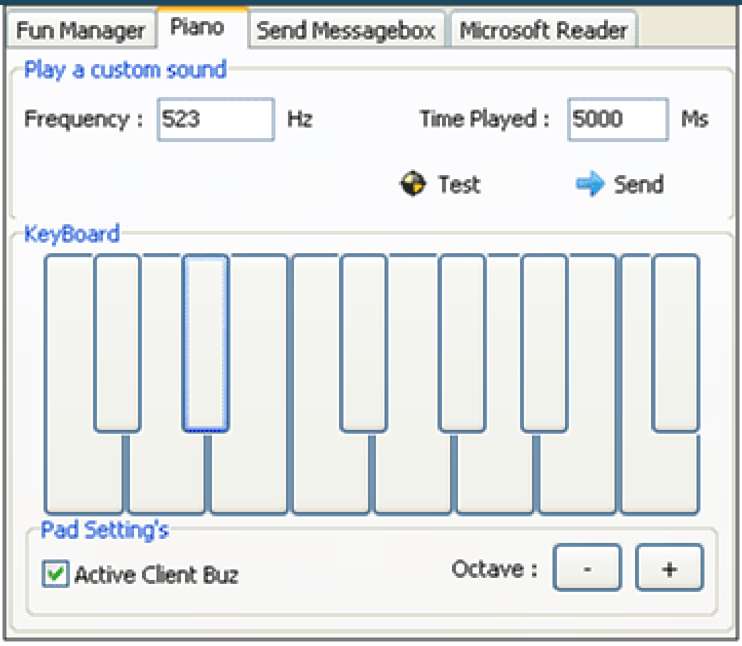
If tracing is enabled and performed, communications may take place from the client manager computer to a website managed by the Trojan's author:

```
GET /scripts/traceroute.php?ip=127.0.0.1 HTTP/1.1

User-Agent: ipget

Host: unremote[.]org



HTTP/1.1 200 OK
```

```
Date: Fri, 24 Feb 2012 17:04:46 GMT

Server: Apache/2.2.19 (Unix) mod_ssl/2.2.19 OpenSSL/0.9.8o

X-Powered-By: PHP/5.2.13-pl1-gentoo

Vary: Accept-Encoding,User-Agent

Content-Length: 39

Content-Type: text/html



OK|RD|Reserved|||||0|0|0|0|||127.0.0.1|
```

This is also associated with a Google Maps request, used to generate the map seen inside the client manager window. This may be a method by which the Trojan's author is able to track all requests made for Trojan infection locations, via his centralized website. How the code's author uses this bot reporting is unclear and unconfirmed, but this behavior was seen in packets related to lab tests.

A variety of "fun" options exists, such as disabling or swapping mouse buttons and more. DarkComet also has a unique remote digital piano that can be played on an infected computer if desired:



Frequency : 523 Hz

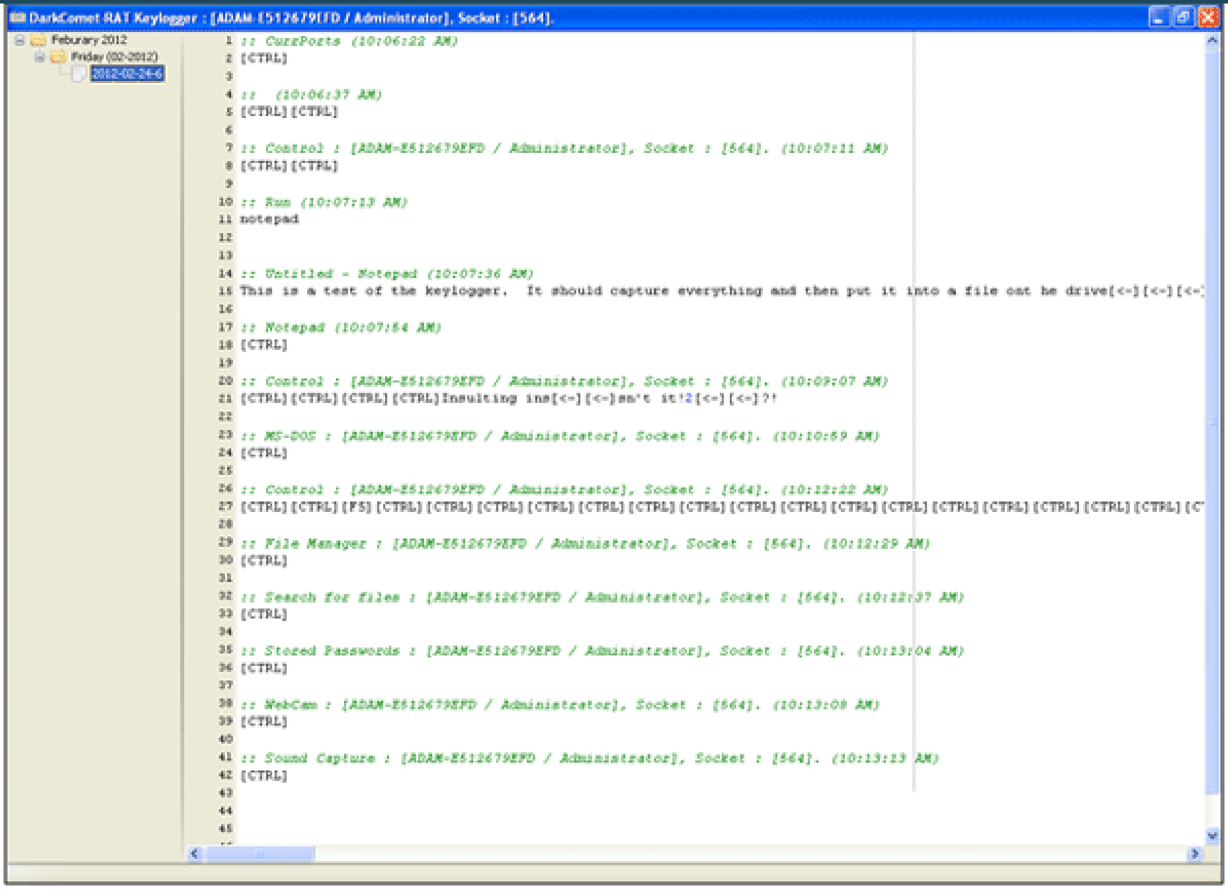
Time Played : 5000 Ms

☑ Active Client Buz

Remote digital piano for fun

Of course, an actor can remotely control anything on the computer desired with a robust interface for managing installed application, services, HOST file data, stealing data from a webcam and sound and more. This includes the ability to install new payloads if desired.

Stolen log files are organized as shown below:

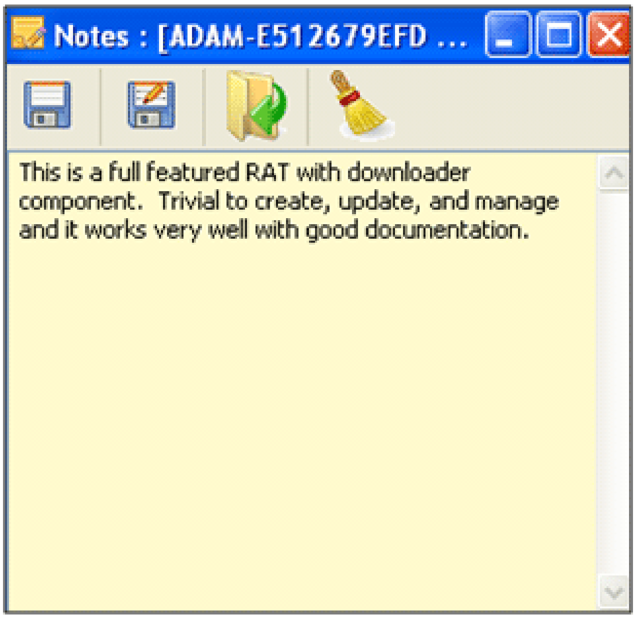


DarkComet-RAT Keylogger : [ADAM-E512679EFD / Administrator], Socket : [564].

```
:: CurrPorts (10:06:22 AM)
[CTRL]

::  (10:06:37 AM)
[CTRL][CTRL]

:: Control : [ADAM-E512679EFD / Administrator], Socket : [564]. (10:07:11 AM)
[CTRL][CTRL]

:: Run (10:07:13 AM)
notepad


:: Untitled - Notepad (10:07:36 AM)
This is a test of the keylogger.  It should capture everything and then put it into a file ont he drive[<-][<-][<-

:: Notepad (10:07:54 AM)
[CTRL]

:: Control : [ADAM-E512679EFD / Administrator], Socket : [564]. (10:09:07 AM)
[CTRL][CTRL][CTRL][CTRL]Insulting ins[<-][<-]sn't it!2[<-][<-]?!

:: MS-DOS : [ADAM-E512679EFD / Administrator], Socket : [564]. (10:10:59 AM)
[CTRL]

:: Control : [ADAM-E512679EFD / Administrator], Socket : [564]. (10:12:22 AM)
[CTRL][CTRL][F5][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][C

:: File Manager : [ADAM-E512679EFD / Administrator], Socket : [564]. (10:12:29 AM)
[CTRL]

:: Search for files : [ADAM-E512679EFD / Administrator], Socket : [564]. (10:12:37 AM)
[CTRL]

:: Stored Passwords : [ADAM-E512679EFD / Administrator], Socket : [564]. (10:13:04 AM)
[CTRL]

:: WebCam : [ADAM-E512679EFD / Administrator], Socket : [564]. (10:13:08 AM)
[CTRL]

:: Sound Capture : [ADAM-E512679EFD / Administrator], Socket : [564]. (10:13:13 AM)
[CTRL]
```

Keylogger data is organized and easily viewable using the client manager of DarkComet

Finally, there is a notes section where an actor may take notes on an infected client if desired:



Notes : [ADAM-E512679EFD ...

This is a full featured RAT with downloader component. Trivial to create, update, and manage and it works very well with good documentation.

Notes taken in the client manager

Behavioral Details of DarkComet

This RAT can clearly be highly customized by actors and typically runs a hidden instance of Internet Explorer, visible in memory via Task Manager and Process Explorer. Default settings store the DarkComet Trojan in a sub-directory of TEMP, such as "dc." Registry changes such as the following may take place, as configured by an actor:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run "MicroUpdate"

Data: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\dc\fun.exe

Keylogger data is often stored in a TEMP file location, such as "Temp\dclogs\2012-02-24-6.dc," using a unique date and naming strategy for tracking and unique names.

DarkComet may also use encrypted RC4-256 strategies for command and control (C&C) communications, if selected by an actor during the builder process. The default encryption key for version 3 is reportedly "#KCMDDC2#-890" and for version 4 reportedly "#KCMDDC4#-890." A default password for version 4 encrypted communications is reportedly "#KCMDDC4#-8900123456789."

Aliases

Krademok
Finlosky
Fynloski
DarkComet

Aliases

Krademok
Finlosky
Fynloski
DarkComet

First Version Publish Date

February 29, 2012 05:49:00 AM

Tags	MEDIUM

Threat Intelligence Tags

Malware Family

- DarkComet

Technical Indicators & Warnings

SHA1:	c63c7b83441768c9a2909125754491ec054139de
Fuzzy Hash:	24:ZHGStGBsEEKlAClUU1WpVCfJZ+5H/vBjaNAMd4dH:ZvtCEKmfU1x6BjQAMd2H
File Name:	downloader.exe
File Size:	3072
Identifier:	Victim
MD5:	352120954900ea4d037adb8fe704491a
SHA1:	06da45940133008f3312559015873f4517e874c2
Fuzzy Hash:	12288:H8UaT9XY2siA0bMG09xD7I3Gg8ecgVvfBoCDBOQQYbVXpuy1f/gORixUl:cUKoN0bUxgGa/pfBHDb+y1HgZ
File Name:	server.exe
File Size:	694784
Identifier:	Attacker
MD5:	f3672f20d3b1e19f9d0f25a8cecb86a9

Version Information

Version:1.0, February 29, 2012 05:49:00 AM
Analysis of DarkComet RAT

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/12-18880