CoalaBot: http Ddos Bot

malware.dontneedcoffee.com/2017/10/coalabot-http-ddos-bot.html

2017-10-16 - Ddos

CoalaBot appears to be build on August Stealer code (Panel and Traffic are really alike)

I found it spread as a tasks in a Betabot and in an Andromeda spread via RIG fed by at least one HilltopAds malvertising.

2017-09-11: a witnessed infection chain to CoalaBot

A look inside :

CoalaBot: Login Screen
(August Stealer alike)

CoalaBot: Statistics

CoalaBot: Bots

CoalaBot: Tasks

CoalaBot: Tasks

CoalaBot: New Taks (list)

CoalaBot: https get task details

CoalaBot: http post task details

CoalaBot: Settings

Here is the translated associated advert published on 2017-08-23 by a user going with nick : Discomrade.
(Thanks to Andrew Komarov and others who provided help here).

Coala Http Ddos Bot

The software focuses on L7 attacks (HTTP). Lower levels have more primitive attacks.

Attack types:

• ICMP (PING) FLOOD

• UDP FLOOD

• TCP FLOOD

• HTTP ARME

• HTTP GET *

• HTTP POST *

• HTTP SLOWLORIS *

• HTTP PULSE WAVE *

* - Supports SMART mode, i.e. bypasses Cloudflare/Blazingfast and similar services (but doesn't bypass CAPTCHA). All types except ICMP/UDP have support for using SSL.

Binary:

• .NET 2.0 x86 (100% working capacity WIN XP - WIN 7, on later versions OC .NET 2.0 disabled by default)

• ~100kb after obfuscation

• Auto Backup (optional)

• Low CPU load for efficient use

• Encryption of incoming/outgoing traffic

• No installation on machines from former CIS countries(RU/UA/BL/KZ/...)

• Scan time non-FUD. Contact us if you need a recommendation for a good crypting service.

• Ability to link a build to more than one gate.

Panel:

• Detailed statistics on time online/architecture/etc.

• List of bots, detailed information

• Number count of requests per second (total/for each bot)

• Creation of groups for attacks

• Auto sorting of bots by groups

• Creation of tasks, the ability to choose by group/country

• Setting an optional time for bots success rate

Other:

• Providing macros for randomization of sent data

• Support of .onion gate

• Ability to install an additional layer (BOT => LAYER => MAIN GATE)

Requirements:

• PHP 5.6 or higher

• MySQL

• Module for MySQLi(mysqli_nd); php-mbstring, php-json, php-mcrypt extensions

Screenshots:

• Statistics- http://i.imgur.com/FUevsaS.jpg
• Bots - http://i.imgur.com/nDwl9pY.jpg
• Created tasks - http://i.imgur.com/RltiDhl.png
• Task List - http://i.imgur.com/tqEEpX0.jpg
• Settings - http://i.imgur.com/EbhExjE.jpg

Price:

• $300 - build and panel. Up to 3 gates for one build.

• $20 - rebuild

The price can vary depending on updates.

Escrow service is welcome.

Help with installation is no charge.

Sample:

VT link
MD5 f3862c311c67cb027a06d4272b680a3b
SHA1 0ff1584eec4fc5c72439d94e8cee922703c44049
SHA256 fd07ad13dbf9da3f7841bc0dbfd303dc18153ad36259d9c6db127b49fa01d08f

Emerging Threats rules :
2024531 || ET TROJAN MSIL/CoalaBot CnC Activity

Read More:
August in November: New Information Stealer Hits the Scene - 2016-12-07 - Proofpoint