

Madness PRO DDoS - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:26:24 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool Madness PRO DDoS

Tool: Madness PRO DDoS

Names	Madness PRO DDoS
Category	Malware
Type	Backdoor , DDoS
Description	<p>[Google Translated]</p> <ul style="list-style-type: none">• Written in C++, easily crypt is lightweight (compressed sample < 15KB)• Full compatibility with all Windows family of NT (x86 and x64)• Boat has 7 types of attacks• Stability in the system. Indicators load on the CPU and RAM are very uniform• Do not attracted the attention of UAC and Windows Firewall• Able to establish port, referral and cookies individually for each goal• Supports up to 10 targets simultaneously• Has a very low load on the CPU with the new, complex system of parsing commands (all analogs parsing takes place inside a function in multiple threads - it's extra work load on the processor. New bot enters all data in the array before the attack on the function and come ready options address, port, referral, etc.)• Has an enormous power output of more than 1500 http (and more 30000 UDP) queries per minute through direct interaction with the network drivers, even on desktop Windows! (only using WinSock) is about 10 times more than some few analogs and more top (on this parameter) competitors.• In the control panel are: the number of requests per minute, right in the system, the version of the system.• Supports bypass CloudFlare protection (!) And many other more common.• Supports Slow GET and Slow POST modes!• In the packet header specifies disabling the cache (Cache-Control: no-cache), which increases the load on the server• The protection of dialogue bot panel spetsklyuchem
Information	< https://malware.dontneedcoffee.com/2013/10/meet-madness-pro-or-few-days-rise-of.html >

Last change to this tool card: 20 April 2020

Download this tool card in [JSON](#) format

All groups using tool Madness PRO DDoS

Changed	Name	Country	Observed
Other groups			
	Guru Spider		2014-Mar 2018

1 group listed (0 APT, 1 other, 0 unknown)

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3778840f-9989-4cbf-b6f9-a8cf4f4e7b0f>