Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:20:52 UTC

Tool: COMpfun

Names	COMpfun Reductor RAT
Category	Malware
Type	Backdoor, Keylogger, Info stealer
Description	(G-Data) G DATA SecurityLabs experts discovered a new Remote Administration Tool, which we dubbed COMpfun. This RAT supports 32-bit and 64-bit Windows versions, up to the Windows 8 operating system. The features are rather common for today's espionage tools: file management (download and upload), screenshot taking, Keylogger functionality, code execution possibility and more. It uses the HTTPS and an asymmetric encryption (RSA) to communicate with the command and control server. The big novelty is the persistence mechanism: the malware hijacks a legitimate COM object in order to be injected into the processes of the compromised system. And it is remarkable, that this hijacking action does not need administrator rights. With this RAT, Attackers could spy on an infected system for quite a long time, as this detection evasion and persistence mechanism is indeed pretty advanced!
Information	<https://www.gdatasoftware.com/blog/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence> <https://securelist.com/compfun-successor-reductor/93633/> <https://securelist.com/compfun-http-status-based-trojan/96874/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.compfun>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool COMpfun

Changed	Name	Country	Observed
APT groups			

	Turla, Waterbug, Venomous Bear		1996-2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=bf661fd5-7355-48f3-ae5b-bd692345b4bb