Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:28:10 UTC

Tool: EvilBunny

Names	EvilBunny
Category	Malware
Type	Backdoor
Description	(Infosec Institute) EvilBunny is written in C++ and is able to detect installed antivirus and other defensive solutions. It includes a Lua 5.1 interpreter, which allows the spyware to execute Lua scripts and change its behavior at runtime. The experts discovered that EvilBunny is able to receive commands from the C&C server at least in three different ways, via HTTP, through a downloaded database file or as a scheduled task. The EvilBunny malware was initially delivered through a malicious PDF document, exploiting CVE-2011-4369. Once compromised the target the malware is loaded onto the system and infects the PC with EvilBunny malware.
Information	<https://resources.infosecinstitute.com/animal-farm-apt-and-the-shadow-of-france-intelligence/> <https://www.cyphort.com/evilbunny-malware-instrumented-lua/> <https://www.gdatasoftware.com/blog/2015/02/24270-babar-espionage-software-finally-found-and-put-under-the-microscope>
MITRE ATT&CK	<https://attack.mitre.org/software/S0396/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.evilbunny>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool EvilBunny

Changed	Name	Country	Observed

APT groups

	Snowglobe, Animal Farm		2011	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=dbcec021-bbde-487d-85e3-684c4fb7e9bb