GameOver Zeus - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:10:34 UTC

Tool: GameOver Zeus

Names	GameOver Zeus Peer-to-Peer Zeus P2P Zeus GOZ
Category	Malware
Type	Banking trojan, Info stealer, Credential stealer, Downloader, Botnet
Description	(US-CERT) GOZ, which is often propagated through spam and phishing messages, is primarily used by cybercriminals to harvest banking information, such as login credentials, from a victim's computer. Infected systems can also be used to engage in other malicious activities, such as sending spam or participating in distributed denial-of-service (DDoS) attacks. Prior variants of the Zeus malware utilized a centralized command and control (C2) botnet infrastructure to execute commands. Centralized C2 servers are routinely tracked and blocked by the security community. GOZ, however, utilizes a P2P network of infected hosts to communicate and distribute data, and employs encryption to evade detection. These peers act as a massive proxy network that is used to propagate binary updates, distribute configuration files, and to send stolen data. Without a single point of failure, the resiliency of GOZ's P2P infrastructure makes takedown efforts more difficult.
Information	<https://www.us-cert.gov/ncas/alerts/TA14-150A> <http://www.syssec-project.eu/m/page-media/3/zeus_malware13.pdf> <https://www.blackhat.com/docs/us-15/materials/us-15-Peterson-GameOver-Zeus-Badguys-And-Backends.pdf> <https://www.cert.pl/wp-content/uploads/2015/12/2013-06-p2p-rap_en.pdf> <https://krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/> <https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware>

	<https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf> <https://www.lawfareblog.com/what-point-these-nation-state-indictments>
MITRE ATT&CK	<https://attack.mitre.org/software/S0016/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.gameover_p2p>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:gameover%20zeus>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool GameOver Zeus

Changed	Name	Country	Observed	
APT groups				
	TA505, Graceful Spider, Gold Evergreen		2006-Nov 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f120d94b-15cc-4290-b899-724a4f1c2af4