Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:51:08 UTC

Tool: Uroburos

Names	Uroburos Urouros Turla Snake
Category	Malware
Type	Rootkit, Backdoor, Info stealer, Exfiltration
Description	(G Data) Uroburos is a rootkit, composed of two files, a driver and an encrypted virtual file system. The rootkit is abl control of an infected machine, execute arbitrary commands and hide system activities. It can steal information (most files) and it is also able to capture network traffic. Its modular structure allows extending it with new features easily, makes it not only highly sophisticated but also highly flexible and dangerous. Uroburos' driver part is extremely com is designed to be very discrete and very difficult to identify.
Information	<https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_E <https://www.gdatasoftware.com/blog/2014/02/23968-uroburos-highly-complex-espionage-software-with-russian-ro <https://www.gdatasoftware.com/blog/2014/03/23966-uroburos-deeper-travel-into-kernel-protection-mitigation> <https://www.gdatasoftware.com/blog/2014/05/23958-uroburos-rootkit-belgian-foreign-ministry-stricken> <https://www.gdatasoftware.com/blog/2014/06/23953-analysis-of-uroburos-using-windbg> <https://www.gdatasoftware.com/blog/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence> <https://www.gdatasoftware.com/blog/2014/11/23937-the-uroburos-case-new-sophisticated-rat-identified> <https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/november/turla-png-dropper-is-back/> <https://www.carbonblack.com/2017/08/18/threat-analysis-carbon-black-threat-research-dissects-png-dropper/> <https://blog.fox-it.com/2017/05/03/snake-coming-soon-in-mac-os-x-flavour/> <https://blog.malwarebytes.com/threat-analysis/2017/05/snake-malware-ported-windows-mac/> <https://www.circl.lu/pub/tr-25/> <https://www.lastline.com/labsblog/dissecting-turla-rootkit-malware-using-dynamic-analysis/> <https://www.lastline.com/labsblog/turla-apt-group-gives-their-kernel-exploit-a-makeover/> <https://unit42.paloaltonetworks.com/acidbox-rare-malware/> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a>
MITRE ATT&CK	<https://attack.mitre.org/software/S0022/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/osx.uroburos> <https://malpedia.caad.fkie.fraunhofer.de/details/win.uroburos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:uroburos>

Last change to this tool card: 21 June 2023

Download this tool card in JSON format

All groups using tool Uroburos

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=6f442433-7a6d-4492-b57e-5e69266de853