ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
Electronic Transactions Development Agency

Threat Group Cards: A Threat Actor Encyclopedia

Tool: EnvyScout

Names	EnvyScout ROOTSAW
Category	Malware
Type	Dropper
Description	EnvyScout is a dropper that has been used by APT29 since at least 2021.
Information	<https://mrtiepolo.medium.com/sophisticated-apt29-campaign-abuses-notion-api-to-target-the-european-commission-200188059f58> <https://blogs.blackberry.com/en/2023/03/nobelium-targets-eu-governments-assisting-ukraine> <https://go.recordedfuture.com/hubfs/reports/cta-2022-0503.pdf> <https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing> <https://blog.bushidotoken.net/2022/06/overview-of-russian-gru-and-svr.html> <https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/> <https://www.sekoia.io/en/nobeliums-envyscout-infection-chain-goes-in-the-registry-targeting-embassies/> <https://cert.pl/posts/2023/04/kampania-szpiegowska-apt29/> <https://cert-agid.gov.it/news/il-malware-envyscout-apt29-e-stato-veicolato-anche-in-italia/> <https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_nobelium_2022_v1.pdf> <https://www.mandiant.com/resources/blog/apt29-wineloader-german-political-parties>
MITRE ATT&CK	<https://attack.mitre.org/software/S0634>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.envyscout>

Last change to this tool card: 22 April 2024

Download this tool card in JSON format

All groups using tool EnvyScout

Changed	Name	Country	Observed
APT groups			
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025

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

↑

Infrastructure and Security Department
Electronic Transactions Development Agency

Report incidents

Follow us on

+66 (0)2-123-1227

helpdesk@etda.or.th