Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:02:33 UTC

APT group: TeleBots

Names	TeleBots *(ESET)*
Country	Russia
Sponsor	State-sponsored, GRU
Motivation	Sabotage and destruction
First seen	2015
Description	(ESET) In the second half of 2016, ESET researchers identified a unique malicious toolset that was used in targeted cyberattacks against high-value targets in the Ukrainian financial sector. We believe that the main goal of attackers using these tools is cybersabotage. This blog post outlines the details about the campaign that we discovered. We will refer to the gang behind the malware as TeleBots. However it's important to say that these attackers, and the toolset used, share a number of similarities with the BlackEnergy group, which conducted attacks against the energy industry in Ukraine in December 2015 and January 2016. In fact, we think that the BlackEnergy group has evolved into the TeleBots group. This group appears to be closely associated with, or evolved from, Sandworm Team, Iron Viking, Voodoo Bear.
Observed	Sectors: Financial, Transportation and Software companies. Countries: Ukraine and Worldwide (NotPetya).
Tools used	BadRabbit, BlackEnergy, CredRaptor, Exaramel, FakeTC, Felixroot, GreyEnergy, KillDisk, NotPetya, TeleBot, TeleDoor, Living off the Land.
Operations performed	Dec 2016: These recent ransomware KillDisk variants are not only able to target Windows systems, but also Linux machines, which is certainly something we don't see every day. This may include not only Linux workstations but also servers, amplifying the damage potential. <https://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/>

	Mar 2017	In 2017, the TeleBots group didn't stop their cyberattacks; in fact, they became more sophisticated. In the period between January and March 2017 the TeleBots attackers compromised a software company in Ukraine (not related to M.E. Doc), and, using VPN tunnels from there, gained access to the internal networks of several financial institutions. <https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/>
	May 2017	XData ransomware making rounds amid global WannaCryptor scare A week after the global outbreak of WannaCryptor, also known as WannaCry, another ransomware variant has been making the rounds. Detected by ESET as Win32/Filecoder.AESNI.C, and also known as Xdata ransomware, the threat has been most prevalent in Ukraine, with 96% of the total detections between May 17th and May 22th, and peaking on Friday, May 19th. ESET has protected its customers against this threat since May 18th. <https://www.welivesecurity.com/2017/05/23/xdata-ransomware-making-rounds-amid-global-wannacryptor-scare/>
	Jun 2017	NotPetya ransomware <https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/> ThaiCERT's whitepaper: <https://www.dropbox.com/s/hksfa7zzc17jgrq/Whitepaper Petya Ransomware.pdf?dl=0>
	Oct 2017	Bad Rabbit ransomware <https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/> ThaiCERT's whitepaper: <https://www.dropbox.com/s/tb8qmb98082p9e7/Whitepaper BadRabbit Ransomware.pdf?dl=0>
Counter operations	Jul 2020	EU imposes the first ever sanctions against cyber-attacks <https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/>
	Oct 2020	Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>

Information	<https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/> <https://blog.trendmicro.com/trendlabs-security-intelligence/timeline-of-sandworm-attacks/>

Last change to this card: 22 June 2023

Download this actor card in PDF or JSON format
