Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:12:24 UTC

Tool: Felixroot

Names	Felixroot GreyEnergy mini
Category	Malware
Type	Backdoor
Description	(FireEye) In September 2017, FireEye identified the FELIXROOT backdoor as a payload in a campaign targeting Ukrainians and reported it to our intelligence customers. The campaign involved malicious Ukrainian bank documents, which contained a macro that downloaded a FELIXROOT payload, being distributed to targets. FireEye recently observed the same FELIXROOT backdoor being distributed as part of a newer campaign. This time, weaponized lure documents claiming to contain seminar information on environmental protection were observed exploiting known Microsoft Office vulnerabilities CVE-2017-0199 and CVE-2017-11882 to drop and execute the backdoor binary on the victim's machine.
Information	<https://www.fireeye.com/blog/threat-research/2018/07/microsoft-office-vulnerabilities-used-to-distribute-felixroot-backdoor.html> <https://medium.com/@Sebdraven/when-a-malware-is-more-complex-than-the-paper-5822fc7ff257>
MITRE ATT&CK	<https://attack.mitre.org/software/S0267/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.felixroot>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:FELIXROOT>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool Felixroot

Changed	Name	Country	Observed

APT groups

	TeleBots		2015-Oct 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ebbfbe19-e146-4df3-8d7d-19cd716a94bd