# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:38:12 UTC



## Tool: GreyEnergy

| | |
|---|---|
| Names | GreyEnergy |
| Category | Malware |
| Type | ICS malware, Backdoor, Downloader, Tunneling |
| Description | (ESET) This malware requires administrator privileges, which must already have been obtained before this stage is reached. According to our research, the GreyEnergy actors deploy this backdoor mainly on two types of endpoints: servers with high uptime, and workstations used to control ICS environments.<br><br>To make communication with command and control (C&C) servers stealthier, the malicious actors may deploy additional software on internal servers in the compromised network, so each server would act as a proxy. Such a proxy C&C redirects requests from infected nodes inside the network to an external C&C server on the internet. This way, it might be less suspicious to a defender who notices that multiple computers are “talking” to an internal server, rather than to a remote server. This technique can be also used by attackers to control the malware in different segments of a compromised network. A similar technique using internal servers as C&C proxies was used by the Duqu 2.0 APT.<br><br>If an affected organization has public-facing web servers connected to an internal network, the attackers may deploy “backup” backdoors onto these servers. These backdoors are used to regain access to the network in the event that the main backdoors are detected and removed. |
| Information | <https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf><br><https://www.eset.com/int/greyenergy-exposed/><br><https://www.nozominetworks.com/2019/02/12/blog/greyenergy-malware-research-paper-maldoc-to-backdoor/><br><https://securelist.com/greyenergys-overlap-with-zebrocy/89506/><br><https://github.com/NozomiNetworks/greyenergy-unpacker> |
| MITRE ATT&CK | <https://attack.mitre.org/software/S0342/> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.grey_energy> |

| | |
|---|---|
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:greyenergy> |

Last change to this tool card: 13 June 2020

Download this tool card in JSON format

### All groups using tool GreyEnergy

| 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=a0fb90eb-ee97-4be7-a141-64b5d0a2d223