Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:01:32 UTC

Tool: Industroyer

Names	Industroyer Crash CrashOverride CRASHOVERRIDE Win32/Industroyer
Category	Malware
Type	ICS malware, Backdoor
Description	(ESET) Industroyer is a particularly dangerous threat, since it is capable of controlling electricity substation switches and circuit breakers directly. To do so, it uses industrial communication protocols used worldwide in power supply infrastructure, transportation control systems, and other critical infrastructure systems (such as water and gas). These switches and circuit breakers are digital equivalents of analogue switches; technically they can be engineered to perform various functions. Thus, the potential impact may range from simply turning off power distribution, cascading failures and more serious damage to equipment. The severity may also vary from one substation to another, as well. Needless to say, disruption of such systems can directly or indirectly affect the functioning of vital services. Industroyer's dangerousness lies in the fact that it uses protocols in the way they were designed to be used. The problem is that these protocols were designed decades ago, and back then industrial systems were meant to be isolated from the outside world. Thus, their communication protocols were not designed with security in mind. That means that the attackers didn't need to be looking for protocol vulnerabilities; all they needed was to teach the malware "to speak" those protocols.
Information	<https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/> <https://dragos.com/blog/crashoverride/CrashOverride-01.pdf> <https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf> <https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-

	industroyer-notpetya/> <https://en.wikipedia.org/wiki/Industroyer>
MITRE ATT&CK	<https://attack.mitre.org/software/S0604/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.industroyer>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Industroyer>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Industroyer

Changed	Name	Country	Observed	
APT groups				
	Energetic Bear, Dragonfly		2010-Mar 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=1b2b82e5-fac6-4864-bdca-2a55695dbed4