Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:15:31 UTC

Tool: OnionDuke

Names	OnionDuke
Category	Malware
Type	Dropper, Loader, Info stealer
Description	(F-Secure) The OnionDuke toolset includes at least a dropper, a loader, an information stealer trojan and multiple modular variants with associated modules. OnionDuke first caught our attention because it was being spread via a malicious Tor exit node. The Tor node would intercept any unencrypted executable files being downloaded and modify those executables by adding a malicious wrapper contained an embedded OnionDuke. Once the victim finished downloading the file and executed it, the wrapper would infect the victim's computer with OnionDuke before executing the original legitimate executable. The same wrapper has also been used to wrap legitimate executable files, which were then made available for users to download from torrent sites. Again, if a victim downloaded a torrent containing a wrapped executable, they would get infected with OnionDuke. Finally, we have also observed victims being infected with OnionDuke after they were already infected with CozyDuke. In these cases, CozyDuke was instructed by its C&C server to download and execute OnionDuke toolset.
Information	<https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf> <http://contagiodump.blogspot.com/2014/11/onionduke-samples.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0052/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.onionduke>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:onionduke>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool OnionDuke

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

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=4b23da0a-7140-4fc2-b9fa-cc896215964e