Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:36:07 UTC

Tool: Filerase

Names	Filerase
Category	Malware
Type	Wiper
Description	(Symantec) Unlike previous Shamoon attacks, these latest attacks involve a new, second piece of wiping malware (Trojan.Filerase). This malware will delete and overwrite files on the infected computer. Shamoon itself will meanwhile erase the master boot record of the computer, rendering it unusable. The addition of the Filerase wiper makes these attacks more destructive than use of the Shamoon malware alone. While a computer infected by Shamoon could be unusable, files on the hard disk may be forensically recoverable. However, if the files are first wiped by the Filerase malware, recovery becomes impossible. Filerase is spread across the victim's network from one initial computer using a list of remote computers. This list is in the form of a text file and is unique to each victim, meaning the attackers likely gathered this information during an earlier reconnaissance phase of the intrusion. This list is first copied by a component called OCLC.exe and passed on to another tool called Spreader.exe. The Spreader component will then copy Filerase to all the computers listed. It will then simultaneously trigger the Filerase malware on all infected machines.
Information	<https://symantec-blogs.broadcom.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.filerase>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Filerase

Changed	Name	Country	Observed

APT groups

	APT 33, Elfin, Magnallium		2013-Apr 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=6fdf99c2-8299-484b-a70a-ca2534092fde