Threat Group Cards: A Threat Actor Encyclopedia

Tool: ELMER

Names	ELMER Elmost
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(FireEye) The exploit documents delivered during the December campaigns dropped a binary containing an embedded variant of a backdoor we refer to as ELMER. ELMER is a non-persistent proxy-aware HTTP backdoor written in Delphi, and is capable of performing file uploads and downloads, file execution, and process and directory listings. To retrieve commands, ELMER sends HTTP GET requests to a hard-coded CnC server, and parses the HTTP response packets received from the CnC server for an integer string corresponding to the command that needs to be executed. Table 2 lists the ELMER backdoors observed during the December campaigns.
Information	<https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0064/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.elmer>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool ELMER

Changed	Name	Country	Observed
APT groups			

	APT 16, SVCMONDR		2015	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b2351a30-d7be-4309-8f5d-9818164c9811