Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:37:37 UTC

Tool: ETUMBOT

Names	ETUMBOT RIPTIDE HIGHTIDE Exploz Specfix
Category	Malware
Type	Backdoor
Description	(FireEye) FireEye observed APT12 utilizing RIPTIDE, a proxy-aware backdoor that communicates via HTTP to a hard-coded command and control (C2) server. RIPTIDE's first communication with its C2 server fetches an encryption key, and the RC4 encryption key is used to encrypt all further communication. In June 2014, Arbor Networks published an article describing the RIPTIDE backdoor and its C2 infrastructure in great depth. The blog highlighted that the backdoor was utilized in campaigns from March 2011 till May 2014. Following the release of the article, FireEye observed a distinct change in RIPTIDE's protocols and strings. We suspect this change was a direct result of the Arbor blog post in order to decrease detection of RIPTIDE by security vendors. The changes to RIPTIDE were significant enough to circumvent existing RIPTIDE detection rules. FireEye dubbed this new malware family HIGHTIDE.
Information	<https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html> <https://www.arbornetworks.com/blog/asert/wp-content/uploads/2014/06/ASERT-Threat-Intelligence-Brief-2014-07-Illuminating-Etumbot-APT.pdf> <https://www.zscaler.com/blogs/research/cnacom-open-source-exploitation-strategic-web-compromise>
MITRE ATT&CK	<https://attack.mitre.org/software/S0003/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.etumbot>

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

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool ETUMBOT

Changed	Name	Country	Observed	
APT groups				
	APT 12, Numbered Panda		2009-Nov 2016	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2f137525-43e3-4296-bbcd-b7d626694f4a