Threat Group Cards: A Threat Actor Encyclopedia

Tool: Duqu

Names	Duqu Tilded
Category	Malware
Type	ICS malware, Backdoor, Keylogger, Info stealer, Wiper
Description	(Wikipedia) Duqu is a collection of computer malware discovered on 1 September 2011, thought to be related to the Stuxnet been created by Unit 8200. The Laboratory of Cryptography and System Security (CrySyS Lab) of the Budapest University c Economics in Hungary discovered the threat, analysed the malware, and wrote a 60-page report naming the threat Duqu. Duq from the prefix '~DQ' it gives to the names of files it creates.
Information	<https://en.wikipedia.org/wiki/Duqu> <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_ <https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf> <https://securelist.com/blog/research/70504/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns> <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2
MITRE ATT&CK	<https://attack.mitre.org/software/S0038/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.duqu>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Duqu>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Duqu

Changed	Name	Country	Observed	
APT groups				
	Equation Group		2001-Aug 2016	

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