Threat Group Cards: A Threat Actor Encyclopedia

Tool: Dridex

Names	Dridex Bugat v5
Category	Malware
Type	Banking trojan, Credential stealer, Worm
Description	OxCERT blog describes Dridex as 'an evasive, information-stealing malware variant; its goal is to acquire as many credentials as possible and return them via an encrypted tunnel to a Command-and-Control (C&C) server. These C& servers are numerous and scattered all over the Internet, if the malware cannot reach one server it will try another. F reason, network-based measures such as blocking the C&C IPs is effective only in the short-term.' According to MalwareBytes, 'Dridex uses an older tactic of infection by attaching a Word document that utilizes ma install malware. However, once new versions of Microsoft Office came out and users generally updated, such a thre subsided because it was no longer simple to infect a user with this method.' IBM X-Force discovered 'a new version of the Dridex banking Trojan that takes advantage of a code injection techr called AtomBombing to infect systems. AtomBombing is a technique for injecting malicious code into the 'atom tab almost all versions of Windows uses to store certain application data. It is a variation of typical code injection attacl take advantage of input validation errors to insert and to execute malicious code in a legitimate process or applicatic Dridex v4 is the first malware that uses the AtomBombing process to try and infect systems.'
Information	<https://www.us-cert.gov/ncas/alerts/aa19-339a> <https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-similar-loader/> <https://securelist.com/analysis/publications/78531/dridex-a-history-of-evolution/> <https://blogs.it.ox.ac.uk/oxcert/2015/11/09/major-dridex-banking-malware-outbreak/> <https://securityintelligence.com/dridexs-cold-war-enter-atombombing/> <https://www.blueliv.com/downloads/documentation/reports/Network_insights_of_Dyre_and_Dridex_Trojan_bank <https://www.govcert.admin.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps> <https://www.cert.pl/en/news/single/talking-dridex-part-0-inside-the-dropper/> <https://viql.github.io/dridex/> <https://www.flashpoint-intel.com/blog-dridex-banking-trojan-returns/> <https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/> <https://securityintelligence.com/posts/dridex-campaign-propelled-by-cutwail-botnet-and-powershell/> <https://www.fortinet.com/blog/threat-research/new-dridex-variant-being-spread-by-crafted-excel-document> <https://www.bleepingcomputer.com/news/security/log4j-vulnerability-now-used-to-install-dridex-banking-malwar <https://news.sophos.com/en-us/2022/02/23/dridex-bots-deliver-entropy-ransomware-in-recent-attacks/> <https://unit42.paloaltonetworks.com/excel-add-ins-dridex-infection-chain/> <https://www.trendmicro.com/en_us/research/23/a/-dridex-targets-macos-using-new-entry-method.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0384/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.dridex>

Last change to this tool card: 15 February 2023

Download this tool card in JSON format

All groups using tool Dridex

Changed	Name	Country	Observed	
APT groups				
	Indrik Spider		2007-Oct 2024	
	TA505, Graceful Spider, Gold Evergreen		2006-Nov 2022	
	TA530	[Unknown]	2016-Nov 2016	

3 groups listed (3 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=be7578fe-e99f-4c53-bac4-db27ddbe2d2b