ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
Electronic Transactions Development Agency

Threat Group Cards: A Threat Actor Encyclopedia

Tool: Ryuk

Names	Ryuk
Category	Malware
Type	Ransomware, Big Game Hunting
Description	Ryuk is a ransomware which encrypts its victim's files and asks for a ransom via bitcoin to release the original files. It is has been observed being used to attack companies or professional environments. Cybersecurity experts figured out that Ryuk and Hermes ransomware shares pieces of codes. Hermes is commodity ransomware that has been observed for sale on dark-net forums and used by multiple threat actors.
Information	<https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/> <https://www.csoonline.com/article/3541810/ryuk-ransomware-explained-a-targeted-devastatingly-effective-attack.html> <https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware> <https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/> <https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html> <https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html> <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/ryuk-ransomware-attack-rush-to-attribution-misses-the-point/> <https://thedfirreport.com/2020/10/08/ryuks-return/> <https://cofense.com/the-ryuk-threat-why-bazarbackdoor-matters-most/> <https://www.deepinstinct.com/2020/11/24/ryuk-ransomware-the-deviance-is-in-the-variance/> <https://www.cybereason.com/blog/cybereason-vs.-ryuk-ransomware> <https://www.advanced-intel.com/post/crime-laundering-primer-inside-ryuk-crime-crypto-ledger-risky-asian-crypto-traders> <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf> <https://www.darkreading.com/vulnerabilities---threats/ryuks-rampage-has-lessons-for-the-enterprise/a/d-id/1340533> <https://www.advanced-intel.com/post/adversary-dossier-ryuk-ransomware-anatomy-of-an-attack-in-2021> <https://news.sophos.com/en-us/2021/05/06/mtr-in-real-time-pirates-pave-way-for-ryuk-ransomware/> <https://securityintelligence.com/articles/ryuk-ransomware-operators-shift-tactics/> <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/new-ryuk-ransomware-sample%e2%80%aftargets-webservers/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0446/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ryuk>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Ryuk>
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=ryuk-ransomware>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Ryuk

Changed	Name	Country	Observed
APT groups			
	FIN6, Skeleton Spider	[Unknown]	2015-Oct 2021

Wizard Spider, Gold Blackburn		2014-May 2025	

Other groups

UNC1878	[Unknown]	2020

3 groups listed (2 APT, 1 other, 0 unknown)

↑

Infrastructure and Security Department
Electronic Transactions Development Agency

Follow us on

Report incidents

+66 (0)2-123-1227

helpdesk@etda.or.th