Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:12:26 UTC

Tool: SunCrypt

Names	SunCrypt
Category	Malware
Type	Ransomware, Big Game Hunting
Description	(Intezer) SunCrypt is a Ransomware as a Service (RaaS) that uses a closed affiliate program on the dark web. The history of this RaaS can be traced back to circa October 2019. In October 2019, a new ransomware was found in-the-wild (5657abdb9d99cd5aec433099f8d6f53d). The new ransomware was written in Go and targeted Windows machines. This version of SunCrypt was not reported in many attacks and it wasn't until mid-2020 when a new version of the ransomware written in C/C++ was discovered, that attacks started to increase. It is an interesting shift of retooling from Go to C/C++ when other groups are instead retooling from C/C++ to Go. While the RaaS didn't appear until October 2019, these ransomware share connections with another ransomware, called QNAPCrypt (also known as eCh0raix), that was used to target Network Attached Storage (NAS) devices back in July 2019. Both families share identical code logic for the file encryption, which we can conclude with high certainty has been compiled from the same source code.
Information	<https://www.intezer.com/blog/malware-analysis/when-viruses-mutate-did-suncrypt-ransomware-evolve-from-qnapcrypt/> <https://securityboulevard.com/2020/09/the-curious-case-of-suncrypt/> <https://www.acronis.com/en-us/blog/posts/suncrypt-adopts-attacking-techniques-netwalker-and-maze-ransomware> <https://blog.minerva-labs.com/suncrypt-ransomware-gains-new-abilities-in-2022>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.suncrypt>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:suncrypt>

Last change to this tool card: 04 April 2022

Download this tool card in JSON format

All groups using tool SunCrypt

Changed	Name	Country	Observed	
APT groups				
	SunCrypt Gang	[Unknown]	2019-Oct 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=878abf22-c447-4e44-8df7-1a63625de2e9