Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:02:43 UTC

Tool: LockerGoga

Names	LockerGoga
Category	Malware
Type	Ransomware, Big Game Hunting
Description	(Fortinet) The binary for this particular variant of LockerGoga does not utilize any type of security evasion or obfuscation. Instead, the binary only goes as far as encoding the RSA public key that is used in its later stages for file encryption. It's possible to speculate that the attackers may have already been fully aware of the target companies' security measures, and were therefore confident that their malware would not be intercepted even without any obfuscation. Another interesting fact is that the malware uses open-source Boost libraries for its filesystem, and inter-process communication and Crypto++ (Cryptopp) for file encryption. One of the advantages of using these libraries is easier development and implementation since developers only need to work with wrapper functions instead of calling individual native APIs to achieve the same goal. And since this utilizes a higher level of programming, statically and dynamically analysing the application without source code is more complicated than just reading a straight sequence of Windows APIs. However, since they do not use standard libraries, they need to be manually linked and the functions need to be physically added to the final binary, which results a larger file size than usual.
Information	<https://www.fortinet.com/blog/threat-research/lockergoga-ransomeware-targeting-critical-infrastructure.html> <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware> <https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html> <https://www.abuse.io/lockergoga.txt> <https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880>

	<https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0372/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.lockergoga>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:LockerGoga>
Playbook	<https://www.bleepingcomputer.com/news/security/bitdefender-releases-free-decryptor-for-lockergoga-ransomware/>

Last change to this tool card: 18 November 2022

Download this tool card in JSON format

All groups using tool LockerGoga

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

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8cdd2a40-7ddd-4caf-b7d0-94af5984a979