LockerGoga, Software S0372 | MITRE ATT&CK®

Archived: 2026-04-05 16:35:20 UTC

Domain	ID		Name	Use
Enterprise	T1531		Account Access Removal	LockerGoga has been observed changing account passwords and logging off current users.[2][1]
Enterprise	T1486		Data Encrypted for Impact	LockerGoga has encrypted files, including core Windows OS files, using RSA-OAEP MGF1 and then demanded Bitcoin be paid for the decryption key.[2][1][3]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	LockerGoga installation has been immediately preceded by a "task kill" command in order to disable anti-virus.[3]
Enterprise	T1070	.004	Indicator Removal: File Deletion	LockerGoga has been observed deleting its original launcher after execution.[2]
Enterprise	T1570		Lateral Tool Transfer	LockerGoga has been observed moving around the victim network via SMB, indicating the actors behind this ransomware are manually copying files form computer to computer instead of self-propagating.[1]
Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	LockerGoga has been signed with stolen certificates in order to make it look more legitimate.[3]
Enterprise	T1529		System Shutdown/Reboot	LockerGoga has been observed shutting down infected systems.[3]

Domain	ID	Name	Use
ICS	T0827	Loss of Control	Some of Norsk Hydro's production systems were impacted by a LockerGoga infection. This resulted in a loss of control which forced the company to switch to manual operations. [4] [5]
ICS	T0828	Loss of Productivity and Revenue	While Norsk Hydro attempted to recover from a LockerGoga infection, most of its 160 manufacturing locations switched to manual (non-IT driven) operations. Manual operations can result in a loss of productivity. [4][5]
ICS	T0829	Loss of View	Some of Norsk Hydro's production systems were impacted by a LockerGoga infection. This resulted in a loss of view which forced the company to switch to manual operations. [4] [5]
