Ragnar Locker, Software S0481 | MITRE ATT&CK®

Archived: 2026-04-05 14:33:11 UTC

Domain	ID		Name	Use
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Ragnar Locker has used cmd.exe and batch scripts to execute commands.[1]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Ragnar Locker has used sc.exe to create a new service for the VirtualBox driver.[1]
Enterprise	T1486		Data Encrypted for Impact	Ragnar Locker encrypts files on the local machine and mapped drives prior to displaying a note demanding a ransom.[1][2]
Enterprise	T1564	.006	Hide Artifacts: Run Virtual Instance	Ragnar Locker has used VirtualBox and a stripped Windows XP virtual machine to run itself. The use of a shared folder specified in the configuration enables Ragnar Locker to encrypt files on the host operating system, including files on any mapped drives.[1]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	Ragnar Locker has attempted to terminate/stop processes and services associated with endpoint security products.[1]
Enterprise	T1490		Inhibit System Recovery	Ragnar Locker can delete volume shadow copies using `vssadmin delete shadows /all /quiet`.[1]
Enterprise	T1120		Peripheral Device Discovery	Ragnar Locker may attempt to connect to removable drives and mapped network drives.[1]

Domain	ID		Name	Use
Enterprise	T1489		Service Stop	Ragnar Locker has attempted to stop services associated with business applications and databases to release the lock on files used by these applications so they may be encrypted.[1]
Enterprise	T1218	.007	System Binary Proxy Execution: Msiexec	Ragnar Locker has been delivered as an unsigned MSI package that was executed with `msiexec.exe`.[1]
		.010	System Binary Proxy Execution: Regsvr32	Ragnar Locker has used regsvr32.exe to execute components of VirtualBox.[1]
		.011	System Binary Proxy Execution: Rundll32	Ragnar Locker has used rundll32.exe to execute components of VirtualBox.[1]
Enterprise	T1614		System Location Discovery	Before executing malicious code, Ragnar Locker checks the Windows API `GetLocaleInfoW` and doesn't encrypt files if it finds a former Soviet country.[3]
Enterprise	T1569	.002	System Services: Service Execution	Ragnar Locker has used sc.exe to execute a service that it creates.[1]

Source: https://attack.mitre.org/software/S0481/