SslMM, Software S0058 | MITRE ATT&CK®

Archived: 2026-04-02 11:27:39 UTC

Domain	ID		Name	Use
Enterprise	T1134		Access Token Manipulation	SslMM contains a feature to manipulate process privileges and tokens.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	To establish persistence, SslMM identifies the Start Menu Startup directory and drops a link to its own executable disguised as an "Office Start," "Yahoo Talk," "MSN Gaming Z0ne," or "MSN Talk" shortcut.[1]
		.009	Boot or Logon Autostart Execution: Shortcut Modification	To establish persistence, SslMM identifies the Start Menu Startup directory and drops a link to its own executable disguised as an "Office Start," "Yahoo Talk," "MSN Gaming Z0ne," or "MSN Talk" shortcut.[1]
Enterprise	T1008		Fallback Channels	SslMM has a hard-coded primary and backup C2 string.[1]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	SslMM identifies and kills anti-malware processes.[1]
Enterprise	T1056	.001	Input Capture: Keylogging	SslMM creates a new thread implementing a keylogging facility using Windows Keyboard Accelerators.[1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	To establish persistence, SslMM identifies the Start Menu Startup directory and drops a link to its own executable disguised as an "Office Start,"

Domain	ID	Name	Use
			"Yahoo Talk," "MSN Gaming Z0ne," or "MSN Talk" shortcut.[1]
Enterprise	T1082	System Information Discovery	SslMM sends information to its hard-coded C2, including OS version, service pack information, processor speed, system name, and OS install date.[1]
Enterprise	T1033	System Owner/User Discovery	SslMM sends the logged-on username to its hard-coded C2.[1]

Source: https://attack.mitre.org/software/S0058