ShimRatReporter, Software S0445 | MITRE ATT&CK®

Archived: 2026-04-05 18:18:37 UTC

Domain	ID		Name	Use
Enterprise	T1087		Account Discovery	ShimRatReporter listed all non-privileged and privileged accounts available on the machine.[1]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	ShimRatReporter communicated over HTTP with preconfigured C2 servers.[1]
Enterprise	T1560		Archive Collected Data	ShimRatReporter used LZ compression to compress initial reconnaissance reports before sending to the C2.[1]
Enterprise	T1119		Automated Collection	ShimRatReporter gathered information automatically, without instruction from a C2, related to the user and host machine that is compiled into a report and sent to the operators.[1]
Enterprise	T1020		Automated Exfiltration	ShimRatReporter sent collected system and network information compiled into a report to an adversary-controlled C2.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	ShimRatReporter sent generated reports to the C2 via HTTP POST requests.[1]
Enterprise	T1105		Ingress Tool Transfer	ShimRatReporter had the ability to download additional payloads.[1]

Domain	ID		Name	Use
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	ShimRatReporter spoofed itself as `AlphaZawgyl_font.exe`, a specialized Unicode font.[1]
Enterprise	T1106		Native API	ShimRatReporter used several Windows API functions to gather information from the infected system.[1]
Enterprise	T1027		Obfuscated Files or Information	ShimRatReporter encrypted gathered information with a combination of shifting and XOR using a static key.[1]
Enterprise	T1069		Permission Groups Discovery	ShimRatReporter gathered the local privileges for the infected host.[1]
Enterprise	T1057		Process Discovery	ShimRatReporter listed all running processes on the machine.[1]
Enterprise	T1518		Software Discovery	ShimRatReporter gathered a list of installed software on the infected host.[1]
Enterprise	T1082		System Information Discovery	ShimRatReporter gathered the operating system name and specific Windows version of an infected machine.[1]
Enterprise	T1016		System Network Configuration Discovery	ShimRatReporter gathered the local proxy, domain, IP, routing tables, mac address, gateway, DNS servers, and DHCP status information from an infected host.[1]

Domain	ID	Name	Use
Enterprise	T1049	System Network Connections Discovery	ShimRatReporter used the Windows function `GetExtendedUdpTable` to detect connected UDP endpoints.[1]

Source: https://attack.mitre.org/software/S0445