NOKKI, Software S0353 | MITRE ATT&CK®

Archived: 2026-04-02 11:18:18 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	NOKKI has used HTTP for C2 communications.[1]
		.002	Application Layer Protocol: File Transfer Protocols	NOKKI has used FTP for C2 communications.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	NOKKI has established persistence by writing the payload to the Registry key `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`. [1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	NOKKI can collect data from the victim and stage it in `LOCALAPPDATA%\MicroSoft Updatea\uplog.tmp`.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	NOKKI uses a unique, custom de-obfuscation technique. [1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	NOKKI can delete files to cover tracks.[1]
Enterprise	T1105		Ingress Tool Transfer	NOKKI has downloaded a remote module for execution. [1]
Enterprise	T1056	.004	Input Capture: Credential API Hooking	NOKKI uses the Windows call SetWindowsHookEx and begins injecting it into every GUI process running on the victim's machine.[1]

Domain	ID		Name	Use
Enterprise	T1680		Local Storage Discovery	NOKKI can gather information on drives on the victim’s machine.[1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	NOKKI is written to %LOCALAPPDATA%\MicroSoft Updatea\svServiceUpdate.exe prior being executed in a new process in an apparent attempt to masquerade as a legitimate folder and file.[1]
Enterprise	T1027		Obfuscated Files or Information	NOKKI uses Base64 encoding for strings.[1]
Enterprise	T1218	.011	System Binary Proxy Execution: Rundll32	NOKKI has used rundll32 for execution.[1]
Enterprise	T1082		System Information Discovery	NOKKI can gather information on the operating system on the victim’s machine.[1]
Enterprise	T1016		System Network Configuration Discovery	NOKKI can gather information on the victim IP address.[1]
Enterprise	T1033		System Owner/User Discovery	NOKKI can collect the username from the victim’s machine.[1]
Enterprise	T1124		System Time Discovery	NOKKI can collect the current timestamp of the victim's machine.[1]