Malteiro, Group G1026 | MITRE ATT&CK®

Archived: 2026-04-05 14:18:45 UTC

Domain	ID		Name	Use
Enterprise	T1059	.005	Command and Scripting Interpreter: Visual Basic	Malteiro has utilized a dropper containing malicious VBS scripts.[1]
Enterprise	T1555		Credentials from Password Stores	Malteiro has obtained credentials from mail clients via NirSoft MailPassView.[1]
		.003	Credentials from Web Browsers	Malteiro has stolen credentials stored in the victim's browsers via software tool NirSoft WebBrowserPassView.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Malteiro has the ability to deobfuscate downloaded files prior to execution.[1]
Enterprise	T1657		Financial Theft	Malteiro targets organizations in a wide variety of sectors via the use of Mispadu banking trojan with the goal of financial theft.[1]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	Malteiro has used scripts encoded in Base64 certificates to distribute malware to victims. [2]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	Malteiro has sent spearphishing emails containing malicious .zip files.[1]
Enterprise	T1055	.001	Process Injection: Dynamic-link Library Injection	Malteiro has injected Mispadu's DLL into a process.[1]

Domain	ID		Name	Use
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	Malteiro collects the installed antivirus on the victim machine.[1]
Enterprise	T1082		System Information Discovery	Malteiro collects the machine information, system architecture, the OS version, computer name, and Windows product name. [1]
Enterprise	T1614	.001	System Location Discovery: System Language Discovery	Malteiro will terminate Mispadu's infection process if the language of the victim machine is not Spanish or Portuguese.[1]
Enterprise	T1204	.002	User Execution: Malicious File	Malteiro has relied on users to execute .zip file attachments containing malicious URLs. [1]

Source: https://attack.mitre.org/groups/G1026