PLATINUM, Group G0068 | MITRE ATT&CK®

Archived: 2026-04-02 10:48:34 UTC

Domain	ID		Name	Use
Enterprise	T1189		Drive-by Compromise	PLATINUM has sometimes used drive-by attacks against vulnerable browser plugins.[1]
Enterprise	T1068		Exploitation for Privilege Escalation	PLATINUM has leveraged a zero-day vulnerability to escalate privileges.[1]
Enterprise	T1105		Ingress Tool Transfer	PLATINUM has transferred files using the Intel® Active Management Technology (AMT) Serial-over-LAN (SOL) channel.[2]
Enterprise	T1056	.001	Input Capture: Keylogging	PLATINUM has used several different keyloggers.[1]
		.004	Input Capture: Credential API Hooking	PLATINUM is capable of using Windows hook interfaces for information gathering such as credential access.[1]
Enterprise	T1036		Masquerading	PLATINUM has renamed rar.exe to avoid detection.[3]
Enterprise	T1095		Non-Application Layer Protocol	PLATINUM has used the Intel® Active Management Technology (AMT) Serial-over-LAN (SOL) channel for command and control.[2]
Enterprise	T1003	.001	OS Credential Dumping: LSASS Memory	PLATINUM has used keyloggers that are also capable of dumping credentials.[1]

Domain	ID		Name	Use
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	PLATINUM has sent spearphishing emails with attachments to victims as its primary initial access vector.[1]
Enterprise	T1055		Process Injection	PLATINUM has used various methods of process injection including hot patching.[1]
Enterprise	T1204	.002	User Execution: Malicious File	PLATINUM has attempted to get users to open malicious files by sending spearphishing emails with attachments to victims.[1]

Source: https://attack.mitre.org/groups/G0068/