admin@338, Group G0018 | MITRE ATT&CK®

Archived: 2026-04-05 14:07:33 UTC

Domain	ID		Name	Use
Enterprise	T1087	.001	Account Discovery: Local Account	admin@338 actors used the following commands following exploitation of a machine with LOWBALL malware to enumerate user accounts: `net user >> %temp%\download` `net user /domain >> %temp%\download` [1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Following exploitation with LOWBALL malware, admin@338 actors created a file containing a list of commands to be executed on the compromised computer.[1]
Enterprise	T1203		Exploitation for Client Execution	admin@338 has exploited client software vulnerabilities for execution, such as Microsoft Word CVE-2012-0158.[1]
Enterprise	T1083		File and Directory Discovery	admin@338 actors used the following commands after exploiting a machine with LOWBALL malware to obtain information about files and directories: `dir c:\ >> %temp%\download` `dir "c:\Documents and Settings" >> %temp%\download` `dir "c:\Program Files\" >> %temp%\download` `dir d:\ >> %temp%\download` [1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	admin@338 actors used the following command to rename one of their tools to a benign file name: `ren "%temp%\upload" audiodg.exe` [1]
Enterprise	T1069	.001	Permission Groups Discovery: Local Groups	admin@338 actors used the following command following exploitation of a machine with LOWBALL

Domain	ID		Name	Use
				malware to list local groups: `net localgroup administrator >> %temp%\download` [1]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	admin@338 has sent emails with malicious Microsoft Office documents attached.[1]
Enterprise	T1082		System Information Discovery	admin@338 actors used the following commands after exploiting a machine with LOWBALL malware to obtain information about the OS: `ver >> %temp%\download` `systeminfo >> %temp%\download` [1]
Enterprise	T1016		System Network Configuration Discovery	admin@338 actors used the following command after exploiting a machine with LOWBALL malware to acquire information about local networks: `ipconfig /all >> %temp%\download` [1]
Enterprise	T1049		System Network Connections Discovery	admin@338 actors used the following command following exploitation of a machine with LOWBALL malware to display network connections: `netstat -ano >> %temp%\download` [1]
Enterprise	T1007		System Service Discovery	admin@338 actors used the following command following exploitation of a machine with LOWBALL malware to obtain information about services: `net start >> %temp%\download` [1]
Enterprise	T1204	.002	User Execution: Malicious File	admin@338 has attempted to get victims to launch malicious Microsoft Word attachments delivered via spearphishing emails.[1]