Threat Intelligence Report
We Are Garfield (WAG)

Description

We Are Garfield (WAG) is a rapidly emerging Advanced Persistent Threat (APT) group that specifically targets industries such as finance, healthcare, and manufacturing. Their operations typically begin with gaining initial access through phishing attacks, credential stuffing, or by exploiting vulnerabilities in publicly accessible systems. Once inside, WAG conducts thorough discovery activities to identify high-value targets. Their primary objectives include stealing and exfiltrating sensitive data, as well as carrying out ransomware operations.

One peculiar characteristic of WAG's activity is their noticeable reduction in operations on Mondays.

Tools

Initial Access	Defense Evasion	Discovery	Credential Access	Command and Control	Lateral Movement	Exfiltration
Phishing	NimBlackout	SharpView	ProcDump	Havoc	RDP	WinSCP
CVE-2021-40539	Veil	Nmap	LaZagne	Metasploit	WinRM	Custom Exfiltration Binaries
CVE-2023-22515	Donut	PowerView		Sliver		

Associated IoCs

SHA-256 or URL	IoC Type
62ccdfad8431f31fea9152f863eefc1847bb3169a031ae9ae8ad4832a62346e9	Filehash of Implant Murdoc.exe
9be7df150c4eefb557a6047eef1d44da4a9fa9f1ff6439de18b571a8f1af0451	Filehash of Implant WinBackup.exe
3ccbc4776c59833006750646485b6c0985cf804bcc9ec4233384b11ec42c922b	Filehash of Implant Murloc.exe
50d6e979f3b0e90e27c8789e4346a7da30ea4ea43542b4513dd93383382527ff	PowerView
7ee5bd376de57b401153b7faad413424f103b00e03a4690a3aebf9caab82d4c8	Filehash of Exfiltration Binary
bccb122c431eeded6bea79f056ff032cfb2316487e19f8ad2b90144c0c1526ee	Filehash of Exfiltration Binary