Mustard Tempest, DEV-0206, TA569, GOLD PRELUDE, UNC1543, Group G1020

Archived: 2026-04-05 18:06:30 UTC

Domain	ID		Name	Use
Enterprise	T1583	.004	Acquire Infrastructure: Server	Mustard Tempest has acquired servers to host second-stage payloads that remain active for a period of either days, weeks, or months.[5]
		.008	Acquire Infrastructure: Malvertising	Mustard Tempest has posted false advertisements including for software packages and browser updates in order to distribute malware.[1]
Enterprise	T1584	.001	Compromise Infrastructure: Domains	Mustard Tempest operates a global network of compromised websites that redirect into a traffic distribution system (TDS) to select victims for a fake browser update page.[3][4][5][6]
Enterprise	T1189		Drive-by Compromise	Mustard Tempest has used drive-by downloads for initial infection, often using fake browser updates as a lure.[4][5][6][3]
Enterprise	T1105		Ingress Tool Transfer	Mustard Tempest has deployed secondary payloads and third stage implants to compromised hosts.[1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	Mustard Tempest has used the filename `AutoUpdater.js` to mimic legitimate update files and has also used the Cyrillic homoglyph characters C `(0xd0a1)` and a `(0xd0b0)`, to produce the filename `Chrome.Update.zip`.[6][4]

Domain	ID		Name	Use
Enterprise	T1566	.002	Phishing: Spearphishing Link	Mustard Tempest has sent victims emails containing links to compromised websites.[4]
Enterprise	T1608	.001	Stage Capabilities: Upload Malware	Mustard Tempest has hosted payloads on acquired second-stage servers for periods of either days, weeks, or months.[5]
		.004	Stage Capabilities: Drive-by Target	Mustard Tempest has injected malicious JavaScript into compromised websites to infect victims via drive-by download.[4][5][6][3]
		.006	Stage Capabilities: SEO Poisoning	Mustard Tempest has poisoned search engine results to return fake software updates in order to distribute malware.[1][4]
Enterprise	T1082		System Information Discovery	Mustard Tempest has used implants to perform system reconnaissance on targeted systems.[1]
Enterprise	T1204	.001	User Execution: Malicious Link	Mustard Tempest has lured users into downloading malware through malicious links in fake advertisements and spearphishing emails.[1][4]

Source: https://attack.mitre.org/groups/G1020