Elderwood, Elderwood Gang, Beijing Group, Sneaky Panda, Group G0066

Archived: 2026-04-05 15:48:12 UTC

Domain	ID		Name	Use
Enterprise	T1189		Drive-by Compromise	Elderwood has delivered zero-day exploits and malware to victims by injecting malicious code into specific public Web pages visited by targets within a particular sector.[2][3][1]
Enterprise	T1203		Exploitation for Client Execution	Elderwood has used exploitation of endpoint software, including Microsoft Internet Explorer Adobe Flash vulnerabilities, to gain execution. They have also used zero-day exploits.[2]
Enterprise	T1105		Ingress Tool Transfer	The Ritsol backdoor trojan used by Elderwood can download files onto a compromised host from a remote location.[4]
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	Elderwood has packed malware payloads before delivery to victims.[2]
		.013	Obfuscated Files or Information: Encrypted/Encoded File	Elderwood has encrypted documents and malicious executables.[2]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	Elderwood has delivered zero-day exploits and malware to victims via targeted emails containing malicious attachments.[2][3]
		.002	Phishing: Spearphishing Link	Elderwood has delivered zero-day exploits and malware to victims via targeted emails

Domain	ID		Name	Use
				containing a link to malicious content hosted on an uncommon Web server.[2][3]
Enterprise	T1204	.001	User Execution: Malicious Link	Elderwood has leveraged multiple types of spearphishing in order to attempt to get a user to open links.[2][3]
		.002	User Execution: Malicious File	Elderwood has leveraged multiple types of spearphishing in order to attempt to get a user to open attachments.[2][3]

Source: https://attack.mitre.org/groups/G0066