Ferocious Kitten, Group G0137 | MITRE ATT&CK®

Archived: 2026-04-05 15:16:51 UTC

Domain	ID		Name	Use
Enterprise	T1583	.001	Acquire Infrastructure: Domains	Ferocious Kitten has acquired domains imitating legitimate sites.[1]
Enterprise	T1036	.002	Masquerading: Right-to-Left Override	Ferocious Kitten has used right-to-left override to reverse executables' names to make them appear to have different file extensions, rather than their real ones.[1]
		.005	Masquerading: Match Legitimate Resource Name or Location	Ferocious Kitten has named malicious files `update.exe` and loaded them into the compromise host's "Public" folder.[1]
Enterprise	T1588	.002	Obtain Capabilities: Tool	Ferocious Kitten has obtained open source tools for its operations, including JsonCPP and Psiphon.[1]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	Ferocious Kitten has conducted spearphishing campaigns containing malicious documents to lure victims to open the attachments.[1]
Enterprise	T1204	.002	User Execution: Malicious File	Ferocious Kitten has attempted to convince victims to enable malicious content within a spearphishing email by including an odd decoy message.[1]