Silent Librarian, TA407, COBALT DICKENS, Group G0122

Archived: 2026-04-05 13:16:21 UTC

Domain	ID		Name	Use
Enterprise	T1583	.001	Acquire Infrastructure: Domains	Silent Librarian has acquired domains to establish credential harvesting pages, often spoofing the target organization and using free top level domains .TK, .ML, .GA, .CF, and .GQ.[1][2][5][4][6][3]
Enterprise	T1110	.003	Brute Force: Password Spraying	Silent Librarian has used collected lists of names and e-mail accounts to use in password spraying attacks against private sector targets.[1]
Enterprise	T1114		Email Collection	Silent Librarian has exfiltrated entire mailboxes from compromised accounts.[1]
		.003	Email Forwarding Rule	Silent Librarian has set up auto forwarding rules on compromised e-mail accounts.[1]
Enterprise	T1585	.002	Establish Accounts: Email Accounts	Silent Librarian has established e-mail accounts to receive e-mails forwarded from compromised accounts.[1]
Enterprise	T1589	.002	Gather Victim Identity Information: Email Addresses	Silent Librarian has collected e-mail addresses from targeted organizations from open Internet searches.[1]
		.003	Gather Victim Identity Information: Employee Names	Silent Librarian has collected lists of names for individuals from targeted organizations.[1]
Enterprise	T1588	.002	Obtain Capabilities: Tool	Silent Librarian has obtained free and publicly available tools including SingleFile and HTTrack to

Domain	ID		Name	Use
				copy login pages of targeted organizations.[4][6]
		.004	Obtain Capabilities: Digital Certificates	Silent Librarian has obtained free Let's Encrypt SSL certificates for use on their phishing pages.[2][6]
Enterprise	T1598	.003	Phishing for Information: Spearphishing Link	Silent Librarian has used links in e-mails to direct victims to credential harvesting websites designed to appear like the targeted organization's login page.[1][2][5][4][6][3]
Enterprise	T1594		Search Victim-Owned Websites	Silent Librarian has searched victim's websites to identify the interests and academic areas of targeted individuals and to scrape source code, branding, and organizational contact information for phishing pages.[1][2][4]
Enterprise	T1608	.005	Stage Capabilities: Link Target	Silent Librarian has cloned victim organization login pages and staged them for later use in credential harvesting campaigns. Silent Librarian has also made use of a variety of URL shorteners for these staged websites.[6][3][4]
Enterprise	T1078		Valid Accounts	Silent Librarian has used compromised credentials to obtain unauthorized access to online accounts.[1]