EXOTIC LILY, Group G1011 | MITRE ATT&CK®

Archived: 2026-04-05 17:55:26 UTC

Enterprise T1583 .001 Acquire Infrastructure: Domains

EXOTIC LILY has registered domains to spoof targeted organizations by changing the top-level domain (TLD) to ".us", ".co" or ".biz".[1]

Enterprise T1585 .001 Establish Accounts: Social Media Accounts

EXOTIC LILY has established social media profiles to mimic employees of targeted companies.[1]

.002 Establish Accounts: Email Accounts

EXOTIC LILY has created e-mail accounts to spoof targeted organizations.[1]

Enterprise T1203 Exploitation for Client Execution

EXOTIC LILY has used malicious documents containing exploits for CVE-2021-40444 affecting Microsoft MSHTML.[1]

Enterprise T1589 .002 Gather Victim Identity Information: Email Addresses

EXOTIC LILY has gathered targeted individuals' e-mail addresses through open source research and website contact forms.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

EXOTIC LILY conducted an e-mail thread-hijacking campaign with malicious ISO attachments.[1][2]

.002 Phishing: Spearphishing Link

EXOTIC LILY has relied on victims to open malicious links in e-mails for execution.[1]

.003 Phishing: Spearphishing via Service

EXOTIC LILY has used the e-mail notification features of legitimate file sharing services for spearphishing.[1]

Enterprise T1597 Search Closed Sources

EXOTIC LILY has searched for information on targeted individuals on business databases including RocketReach and CrunchBase.[1]

Enterprise T1593 .001 Search Open Websites/Domains: Social Media

EXOTIC LILY has copied data from social media sites to impersonate targeted individuals.[1]

Enterprise T1594 Search Victim-Owned Websites

EXOTIC LILY has used contact forms on victim websites to generate phishing e-mails.[1]

Enterprise T1608 .001 Stage Capabilities: Upload Malware

EXOTIC LILY has uploaded malicious payloads to file-sharing services including TransferNow, TransferXL, WeTransfer, and OneDrive.[1]

Enterprise T1204 .001 User Execution: Malicious Link

EXOTIC LILY has used malicious links to lure users into executing malicious payloads.[1]

.002 User Execution: Malicious File

EXOTIC LILY has gained execution through victims clicking on malicious LNK files contained within ISO files, which can execute hidden DLLs within the ISO.[1][2]

Enterprise T1102 Web Service

EXOTIC LILY has used file-sharing services including WeTransfer, TransferNow, and OneDrive to deliver payloads.[1]
