MITRE ENGENUITY | Center for Threat Informed Defense

Threat Actor Profile Report:

Exotic Lily: Prolific Initial Access Broker with Ties to Financial Crime and Ransomware

Date of Report :

March 20, 2023

EXECUTIVE SUMMARY

A prolific initial access broker, Exotic Lily has proven effective at scaling interactive phishing campaigns capable of bypassing traditional email defenses and resulting in ransomware infections. At the height of their detected operations, they were sending approximately 5,000 phishes a day. Their use of contact us forms, doppelganger domains, and interaction with the recipient prior to sending malware increase their ability to bypass traditional email defenses and standard phishing training. The group has links to ransomware operators and has been seen dropping Cobalt Strike, Sliver, and Meterpreter.

KEY POINTS

- Exotic Lily is a prolific initial access broker that specializes in high interaction operations.
- Their operations have resulted in ransomware infections.
- In one reported case, they successfully leveraged a 0day vulnerability in Windows during an operation.

ASSESSMENT

The Exotic Lily initial access group poses a unique threat to corporate networks. Their ability to both customize and scale phishing campaigns is uniquely designed to reduce the likelihood that traditional phishing countermeasures will be effective. We assess with high confidence that their deployment of novel first contact methods, a high level of victim interaction, and the deployment of a new first stage loader with aggressive anti-detection capabilities are capable of subverting most existing anti-phishing controls.

- Exotic Lily has conducted phishing campaigns that start with the use of company's contact us forms on their webpages. This method requires a high level of threat actor interaction with the intended victim, but also reduces the efficacy of phishing filters as the first contact is legitimate and from a trusted source.

- Additionally, this group will engage in email exchanges with the intended victim and leverage cloud hosting providers to send malware. This results in the phish email coming from a legitimate sender.

This group appears to work with multiple threat groups that are primarily criminally motivated. Often Exotic Lily serves as an initial access vector for ransomware although it is likely that certain networks are provided to espionage operators.

- Exotic Lily exploited a 0day vulnerability in Microsoft MSHTML (CVE-2021-40444). This is the only known instance of the group leveraging a 0day vulnerability and, unlike its other campaigns, the recipients of this targeting were selective, and a relatively small number of samples exploiting this vulnerability have been identified.

We assess with low confidence that the group operates out of Eastern Europe and has ties with pro-Russian groups.

- The deployment of their new malware happened shortly after the fracturing of Conti.
- Traditionally, the malware deployed from their initial access have ties to Eastern Europe.
- An analysis of timestamps related to their phishing campaigns shows patterns consistent with working Monday through Friday in Central or Eastern Europe.

We assess with medium confidence that the group will continue to operate in a scalable, modular way that poses significant risk for private sector entities that are enticing targets for financially motivated hacking.

THREAT ACTOR SUMMARY

Exotic Lily is a group of initial access brokers that were first identified in September 2021. The group primarily leverages phishing with a high level of user interaction for the initial intrusion method and then gains access to a victim network via one of two RATs. It is unknown where the group is located or how it markets its services, however, an analysis of timestamps indicate they might be located in Central or Eastern Europe.

Tactics, Techniques, & Procedures

Exotic Lily primarily leverages highly interactive spear phishing at scale to gain initial access to their victims. This high level of interaction comes primarily in two forms.

First, they will use a company's contact us form to establish a connection with the intended victim company. The form creates a trusted communication channel for both the recipient and for email security applications.

Second, the group will register doppelganger domains of companies that are related to the target in question. Leveraging a highly tailored spearphish, the group seeks to elicit a response before providing a malicious link.

If the group can successfully engage, they will often use legitimate file hosting tools to upload malicious files. Once hosted, they will then send a link to the file through the platform itself, thus bypassing any malicious email filter. If the malicious file is downloaded, one of two files are dropped. Historically, the group used Bazarloader to establish access on the victim network. Shortly prior to the Conti ransomware group fracturing, the group switched to a new loader commonly referred to as Bumblebee.

Follow on malware delivery is dependent on what threat actors purchase the access enabled by Bumblebee and previously Bazarloader. However, ransomware, Cobalt Strike, Sliver, and Meterpreter have all been observed in association with the loader.

In one reported case, the group was able to leverage a 0day exploit for Windows (CVE-2021-40444), but this was an aberration in how they normally operate, and there is no information regarding how the exploit was developed or obtained.

Infrastructure

The threat actor leverages known file hosting sites to send the malicious documents. File hosts include: TransferNow, TransferXL, WeTransfer, and OneDrive. Additionally, they often leverage VPS providers for the C2 of the loader.

Victims

As an initial access broker, Exotic Lily does not have a specific targeting pattern as it pertains to victims. One security company profiled their activity and “estimated Exotic Lily were sending more than 5,000 emails a day, to as many as 650 targeted organizations globally. Up until November 2021, the group seemed to be targeting specific industries such as IT, cybersecurity and healthcare, but as of late we have seen them attacking a wide variety of organizations and industries, with less specific focus.”1

Attribution

An analysis of Exotic Lily’s campaigns indicate that this is a professional outfit that primarily works a standard Monday through Friday work week likely in Central or Eastern Europe. Additionally, the group appears to have ties to the Conti ransomware group that was primarily located in Eastern Europe with interests in Russia. However, we do not have specific attribution at this time, and they appear to be mercenaries rather than affiliated or supporting any particular country or interests.

KEY INTELLIGENCE GAPS

- Attribution to a specific country or countries could change the level of risk associated with the group.Their operations have resulted in ransomware infections.
- A better understanding of how they obtained the one 0day exploit they have exploited would change our assessment of their threat.
- A better understanding of how they advertise and monetize their access would enable a better understanding of risk.

MITRE ATT&CK TABLE (BASED ON V12)

TACTICS	TECHNIQUE	SUBTECHNIQUE	PROCEDURE	D3FEND	DEPLOYED CONTROL
Reconnaissance	T1589/ Gather Victim Identity Information	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.		
Reconnaissance	T1597 / Search Closed Sources		EXOTIC LILY has searched for information on targeted individuals on business databases including RocketReach and CrunchBase.		
Reconnaissance	T1593/ Search Open Websites	T1593.001 / Search Open Websites/Domains: Social Media	EXOTIC LILY has copied data from social media sites to impersonate targeted individuals.		
Reconnaissance	T1594 / Search Victim-Owned Websites		EXOTIC LILY has used contact forms on victim websites to generate phishing e-mails.		
Resource Development	T1583/ Acquire Infrastructure	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".		
Resource Development	T1585/ Establish Accounts	T1585.001 / Establish Accounts: Social Media Accounts	EXOTIC LILY has established social media profiles to mimic employees of targeted companies.		
Resource Development	T1585/ Establish Accounts	T1585.002 / Establish Accounts: Email Accounts	EXOTIC LILY has created e-mail accounts to spoof targeted organizations.		
Resource Development	T1608/ Stage Capabilities	T1608.001 / Stage Capabilities: Upload Malware	EXOTIC LILY has uploaded malicious payloads to file-sharing services including TransferNow, TransferXL, WeTransfer, and OneDrive.		
Initial Access	T1566/ Phishing	T1566.001 / Phishing: Spearphishing Attachment	EXOTIC LILY conducted an e-mail thread-hijacking campaign with malicious ISO attachments.	LINK	Antivirus
Initial Access	T1566/ Phishing	T1566.002 / Phishing: Spearphishing Link	EXOTIC LILY has relied on victims to open malicious links in e-mails for execution.	LINK	Antivirus
Initial Access	T1566/ Phishing	T1566.003 / Phishing: Spearphishing via Service	EXOTIC LILY has used the e-mail notification features of legitimate file sharing services for spearphishing.	LINK	
Execution	T1203 / Exploitation for Client Execution		EXOTIC LILY has used malicious documents containing exploits for CVE-2021-40444 affecting Microsoft MSHTML.	LINK	
Execution	T1204/ User Execution	T1204.001 / User Execution: Malicious Link	EXOTIC LILY has used malicious links to lure users into executing malicious payloads.	LINK	User Training

TACTICS	TECHNIQUE	SUBTECHNIQUE	PROCEDURE	D3FEND	DEPLOYED CONTROL
Execution	T1204/ User Execution	T1204.002 / 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.	LINK	User Training
Command and Control	T1102 / Web Service		EXOTIC LILY has used file-sharing services including WeTransfer, TransferNow, and OneDrive to deliver payloads.	LINK	Network Intrusion Prevention

INDICATORS OF COMPROMISE MALWARE

MALICIOUS TOOL NAME	HASH TYPE	FILE HASH	ASSOCIATED FILE HASH	BRIEF DESCRIPTION	MALWARE ANALYSIS REPORT (HYPERLINK, OR N/A)	FIRST REPORTED	LAST REPORTED
BumbleBee	SHA256	a72538ba00dc95190d6919756ffce74f0b3cf60db387c6c9281a0dc892ded802		Loader used for first stage persistence	N/A	Mar 31 2022	–1 April 2022
BumbleBee	SHA256	0faa970001791cb0013416177cefebb25fbff543859bd81536a3096ee8e79127		Loader used for first stage persistence	N/A	5 April 2022	5 April 2022
BumbleBee	SHA 256	08CD6983F183EF65EABD073C01F137A913282504E2502AC34A1BE3E599AC386B		Loader used for first stage persistence	N/A	31 January 2022	10 March 2022
BumbleBee	SHA 256	9eacade8174f008c48ea57d43068dbce3d91093603db0511467c18252f60de32		Loader used for first stage persistence	N/A	March 2022	March 2022
BumbleBee	SHA 256	6214e19836c0c3c4bc94e23d6391c45ad87fdd890f6cbd3ab078650455c31dc8		Loader used for first stage persistence	N/A	March 2022	March 2022
BumbleBee	SHA 256	201c4d0070552d9dc06b76ee55479fc0a9dfacb6dbec6bbec5265e04644eebc9		Loader used for first stage persistence	N/A	March 2022	March 2022
BumbleBee	SHA 256	1fd5326034792c0f0fb00be77629a10ac9162b2f473f96072397a5d639da45dd		Loader used for first stage persistence	N/A	March 2022	March 2022

MALICIOUS TOOL NAME	HASH TYPE	FILE HASH	ASSOCIATED FILE HASH	BRIEF DESCRIPTION	MALWARE ANALYSIS REPORT (HYPERLINK, OR N/A)	FIRST REPORTED	LAST REPORTED
BumbleBee	SHA 256	01cc151149b5bf974449b00de08ce7dbf5eca77f55edd00982a959e48d017225		Loader used for first stage persistence	N/A	March 2022	March 2022
ISO Sample	SHA 256		c6ef53740f2011825dd531fc65d6eba92f87d0ed1b30207a9694c0218c10d6e0	ISO file that had Bumblebee bundled in it.	N/A	Mar 31 2022	– 1 April 2022
ISO Sample	SHA 256		77f6cdf03ba70367c93ac194604175e2bd1239a29bc66da50b5754b7adbe8ae4	ISO file that had Bumblebee bundled in it.	N/A	5 April 2022	5 April 2022
ISO Sample	SHA 256		Fe7a64dad14fe240aa026e57615fc3a22a7f5ba1dd55d675b1d2072f6262a1	ISO file that had Bumblebee bundled in it.	N/A	March 28 2022	1 April 2022
BazarLoader	SHA 256	5ceb28316f29c3912332065eeaaebf59f10d79cd9388ef2a7802b9bb80d797be		Loader used for first stage persistence	N/A	31 January 2022	Sept 2021 – March 2022
BazarLoader	SHA 256	9fdec91231fe3a709c8d4ec39e25ce8c55282167c561b14917b52701494ac269		Loader used for first stage persistence	N/A	27 January 2022	Sept 2021 – March 2022
BazarLoader	SHA 256	c896ee848586dd0c61c2a821a03192a5efef1b4b4e03b48aba18eedab1b864f7		Loader used for first stage persistence	N/A	19 January 2022	Sept 2021 – March 2022

NETWORK

NETWORK ARTIFACT	INTRUSION PHASE	DETAILS	FIRST REPORTED	LAST REPORTED
54.38.139[.]20:443	C2	Related to Bumblebee C2	N/A	March 2022
23.81.246[.]187:443	C2	Related to Cobalt Strike C2	N/A	March 2022
conlfex[.]com	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
avrobio[.]co	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022

NETWORK ARTIFACT	INTRUSION PHASE	DETAILS	FIRST REPORTED	LAST REPORTED
elemblo[.]com	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
phxmfg[.]co	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
modernmeadow[.]co	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
lsoplexis[.]com	Initial Compromise	Doppelganger domain for initial phishin	N/A	March 2022
craneveyor[.]us	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
faustel[.]us	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
lagauge[.]us	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
missionbio[.]us	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
richllndmetals[.]com	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
kvnational[.]us	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
prmflltration[.]com	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
brightlnsight[.]co	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
awsblopharma[.]com	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
amevida[.]us	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
revergy[.]us	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022

NETWORK ARTIFACT	INTRUSION PHASE	DETAILS	FIRST REPORTED	LAST REPORTED
al-ghurair[.]us	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
opontia[.]us	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022
belcolnd[.]com	Initial Compromise	Doppelganger domain for initial phishing	N/A	March 2022

SYSTEM ARTIFACTS

HOST ARTIFACT	TYPE	DETAILS	TACTIC	FIRST REPORTED	LAST REPORTED
C:\Windows\System32\cmd.exe /c powershell -WindowStyle Hidden -Command ".\7za.exe x archive.7z -pFhu$$57csa -o\"c:\programdata\" -y > $null; rundll32 c:\programdata\19a.dll,oxgdXPSGPw	Powershell command	Powershell command to extract the Bumblebee DLL and executing rundll32.	Initial intrusion	N/A	August 2022

COMMON VULNERABILITIES AND EXPOSURES (CVEs)

CVE Number	CVSS Score	Patch Available (Y/N)	Other Remediation	Date Reported	Patch Applied (Y/N/UNK/NA)
CVE-2021-40444	7.8	Y		August 2021	Y

PROBABILITY MATRIX

ALMOST NO CHANCE	VERY UNLIKELY	UNLIKELY	ROUGHLY EVEN CHANCE	LIKELY	VERY LIKELY	ALMOST CERTAINLY
remote	highly improbable	improbable (improbably)	roughly even odds	probable (probably)	highly probable	nearly certain
01-05%	05-20%	20-45%	45-55%	55-80%	80-95%	95-99%

INTELLIGENCE REQUIREMENTS

- PIR-10-002: Initial access brokers
- PIR-11-002: Email security evasion techniques

FEEDBACK

Please take a moment to provide feedback on this report by emailing EXAMPLE@companydomain.com; all comments are reviewed and used to enhance future reporting.

1. Rate the product’s overall value:
   a. Very valuable
   b. Somewhat valuable
   c. Of limited value
   d. Not valuable
2. Rate the product’s utility:
   a. Highly actionable
   b. Actionable
   c. Not actionable.
3. Rate the product’s quality of analysis:
   a. High quality analysis
   b. Acceptable quality analysis
   c. Low quality analysis
4. Rate the product’s timeliness:
   a. Very timely
   b. Timely
   c. Not timely.
5. What did you find particularly useful or lacking in the report?

DATA SOURCES

https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/

https://www.proofpoint.com/us/blog/threat-insight/bumblebee-is-still-transforming

https://unit42.paloaltonetworks.com/bumblebee-malware-projector-libra/

https://versprite.com/cybersecurity-library/bazarloader-exotic-lily-analysis/

https://www.microsoft.com/en-us/security/blog/2021/09/15/analyzing-attacks-that-exploit-the-mshtml-cve-2021-40444-vulnerability/

Threat Actor:	Exotic Lily (Projector Libra)
Actor Motivation:	NA
SECTORS:	NA
INFRASTRUCTURE USED:	NA
Actor Motivation:	CYBER CRIME