

PUBLICATION DATE: Tuesday, Feb. 27, 9pm ET / Wednesday, Feb. 28, 2am GMT / 3am CET / 4am

When Cats Fly: Suspected Iranian Threat Actor UNC1549 Targets Israeli and Middle East Aerospace and Defense Sectors

Authors: Ofir Rozmann, Chen Evgi, Jonathan Leathery

Summary

Today Mandiant is releasing a blog about a **suspected Iran-nexus espionage activity targeting the aerospace, aviation and defense industries in Middle East** countries, including Israel and UAE, and potentially Turkey, India and Albania.

Mandiant attributes this activity with medium confidence to the Iranian actor UNC1549, which overlaps with **Tortoiseshell** - a threat actor which has been publicly [linked](#) to **Iran's Islamic Revolutionary Guard Corps (IRGC)**. Tortoiseshell has previously attempted to compromise supply chains by targeting defense contractors and IT providers.

The **potential link between this activity and the Iranian IRGC** is noteworthy, given the focus on defense-related entities and the recent tensions with Iran, in light of the Israel-Hamas war. Notably, Mandiant observed an **Israel-Hamas war themed campaign that masquerades as the “Bring Them Home Now” movement**, which calls for the return of the Israelis kidnapped and held hostage by Hamas.

This suspected UNC1549 activity has been active since at least June 2022, and is still ongoing as of February 2024. While regional in nature and focused mostly in the Middle East, the targeting includes entities operating worldwide.

Mandiant observed this campaign deploy **multiple evasion techniques** to mask their activity, most prominently the **extensive use of Microsoft Azure cloud infrastructure**, as well as **social engineering schemes to disseminate two unique backdoors: MINIBIKE and MINIBUS**.

This blog post details the suspected UNC1549 operations since June 2022, the ongoing development of their proprietary malware, their network of over 125 Azure C2 subdomains, and their attack lifecycle which includes TTPs Mandiant has not previously seen deployed by Iran.

Attribution

Mandiant assesses with moderate confidence that this activity has ties to [UNC1549](#), an Iran-based espionage group, which overlaps with activities publicly known as [Tortoiseshell](#) and [Smoke Sandstorm/BOHRIUM](#).

Namely, a fake recruiting website (1stemployer[.]com) was observed hosting a MINIBUS payload in November 2023. The template used for the fake recruiting website had been used previously in another fake recruiting website: careers-finder[.]com, which was used by UNC1549.

- In this campaign, the MINIBUS backdoor was hosted on a fake job website (1stemployer[.]com) using the exact same written contents as careers-finder[.]com used by UNC1549 in early 2022, for example: *“After considering the career and education background we introduce you to the employer companies which are looking for the indicated skills and expertise.”*

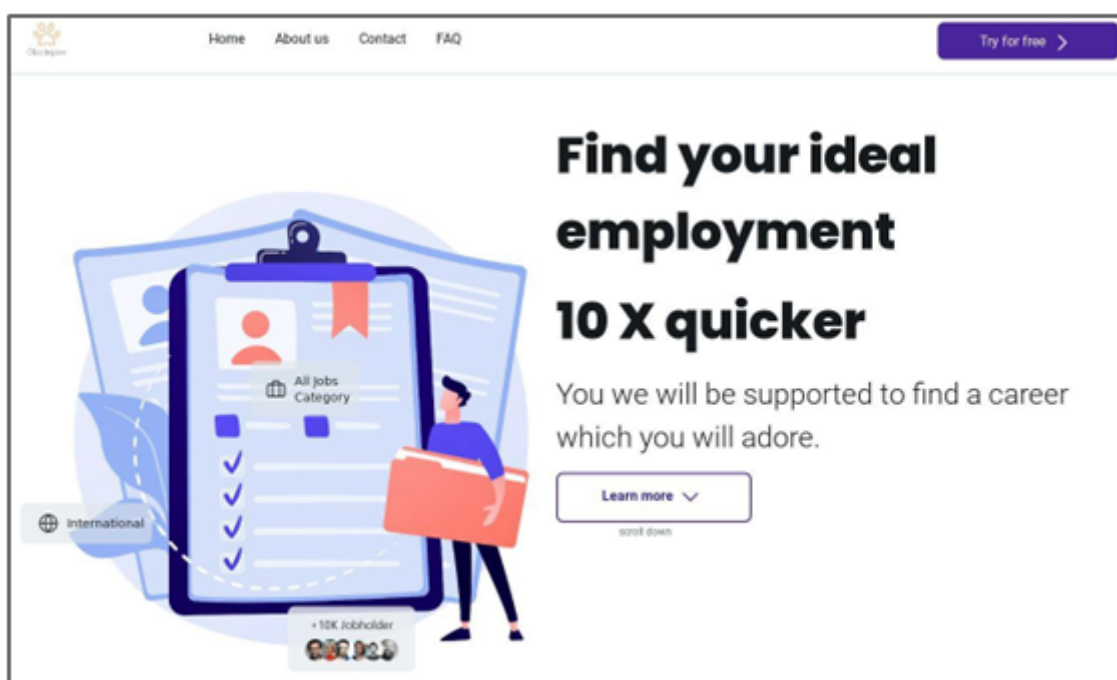


Figure 1: Fake job website 1stemployer[.]com, deploying a template similar to a previous UNC1549 website

- In addition, like in previous UNC1549 activities, this campaign leveraged .NET applications to deliver their malware - this time the attackers implemented this by using a fake Hamas-affiliated application to deliver the MINIBUS backdoor.

According to public [reporting](#) Tortoiseshell, which is tied to UNC1549, is potentially linked to the Iranian Revolutionary Guard Corps (IRGC).

In addition, **the focused targeting of Middle East entities** affiliated with the aerospace and defense sectors **is consistent with other Iran-nexus clusters of activity**, some are affiliated with the IRGC as well.

Outlook and Implications

Mandiant research indicates this campaign remains active as of February 2024, and targeted entities related to the defense, aerospace and aviation in the Middle East, and particularly in Israel and UAE, and potentially in Turkey, India and Albania as well.

The intelligence collected on these entities is of relevance to strategic Iranian interests, and may be leveraged for espionage as well as kinetic operations. This is further supported by the potential ties between UNC1549 and the Iranian IRGC.

The evasion methods deployed in this campaign, namely the tailored job-themed lures combined with the use of cloud infrastructure for C2, may make it challenging for network defenders to prevent, detect and mitigate this activity. The intelligence and indicators provided in this report may support these efforts and enhance them.

Attack Lifecycle

This suspected UNC1549 campaign uses two primary methods to achieve initial access to the targets: spear-phishing and credential harvesting. A typical chain of attack consists of several stages:

1. **Spear-phishing** emails or social media correspondence, disseminating links to **fake websites containing Israel-Hamas related content or fake job offers**. The websites would eventually lead to downloading a malicious payload.

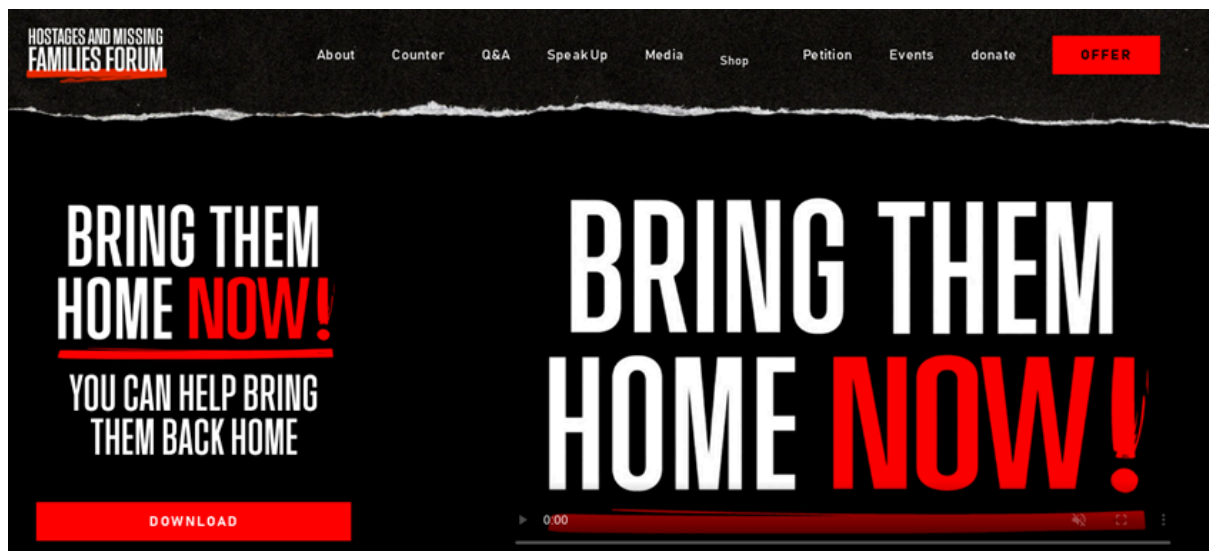


Figure 2: Fake website posing as the “Bring Them Home Now” movement (birngthemhomenow[.]co[.]il), calling for the return of Israelis kidnapped by Hamas

- The fake job offers were for **tech and defense-related positions**, specifically in the aviation, aerospace or thermal imaging sectors.
- Mandiant also observed some of the fake job websites that hosted malicious payloads were also used during 2023 to **harvest credentials**.

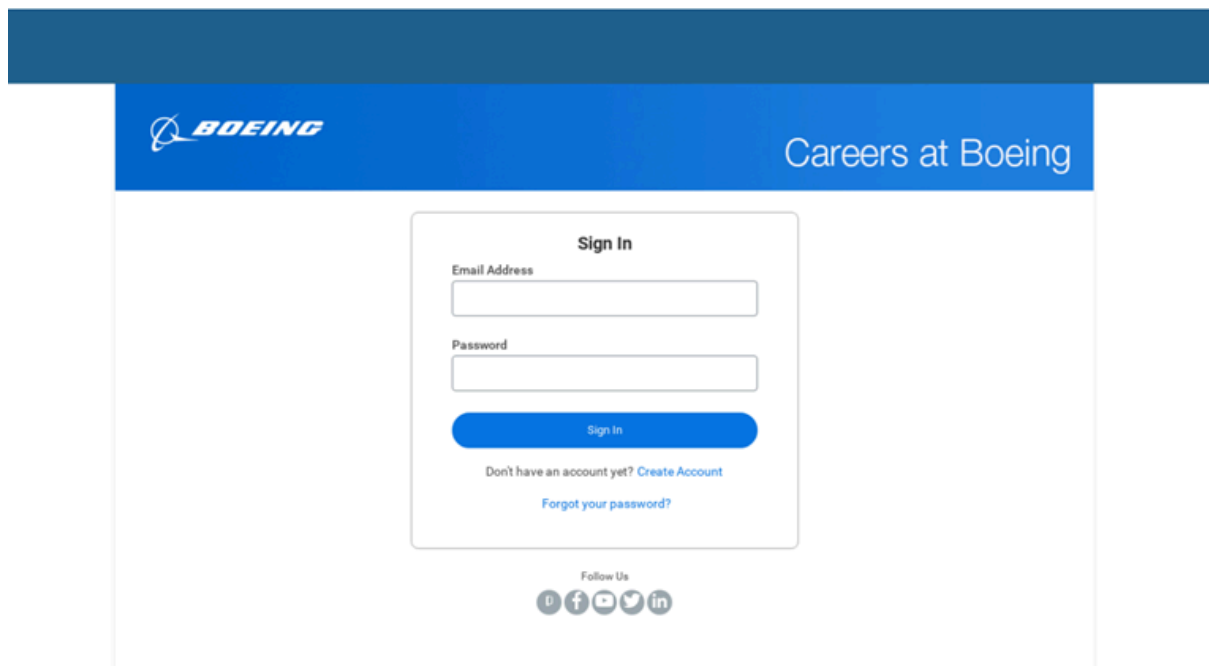


Figure 3: Fake login page masquerading as the aerospace company Boeing

2. **Payload delivery**, downloaded from the above mentioned websites to the target's computer. The payload is a compressed archive which typically includes two main bundles:
 - MINIBIKE or MINIBUS - two unique backdoors deployed at least since 2022 (MINIBIKE) and 2023 (MINIBUS), providing full backdoor functionality (see technical analysis below).
 - A benign lure in the form of an application like OneDrive (MINIBIKE) or in the case of MINIBUS, a custom application presenting content related to Israelis kidnapped by Hamas, hosted on the fake website birngthemhomenow[.]co[.]il mentioned above.

[image to follow]

Figure 4: Decoy content used by MINIBUS, related to the "Bring Them Home Now" movement

3. **Payload installation and device compromise**, achieved after the MINIBIKE or MINIBUS backdoors establish Command-and-Control (C2) communication, in most cases via Microsoft Azure cloud infrastructure.
 - The access to the device can be leveraged for multiple purposes, including intelligence collection and as a stepping stone for further access into the targeted network.
 - This stage may be supported by the use of LIGHTRAIL, a unique tunneler used in the campaign (see details below).

This suspected UNC1549 campaign **deployed several evasion techniques to mask their activity**:

- Abusing Microsoft Azure infrastructure for Command-and-Control (C2) and hosting, making it difficult to discern the activity from legitimate network traffic. In some cases, servers geolocated in the targeted countries (Israel and UAE) were used, further masking the activity.
- Using domain naming schemes that include strings that would likely seem legitimate to network defenders, like countries, organizations names, languages or descriptions related to the targeted sector. Following are several examples of indicative Azure domains:
 - ilengineeringrssfeed[.]azurewebsites[.]net (“IL Engineering RSS Feed”)
 - hiringarabicregion[.]azurewebsites[.]net (“Hiring Arabic Region”)
 - turkairline[.]azurewebsites[.]net (“Turk Airline”)
- Using job-themed lures, offering various IT and tech-related positions which are likely to be disseminated legitimately. One of these fake job offers is presented in the figure below.



Project Manager Job Description

Job Summary:

A project manager plans, organizes and oversees a project from start to finish. They should guarantee that the project is finalized to the contentment of all stakeholders, within the designated budget and timeline.

Duties/Responsibilities:

- Determine and define project scope and objectives
- Predict resources needed to reach objectives and manage resources in an effective and efficient manner
- Prepare budget based on scope of work and resource requirements
- Track project costs in order to meet budget
- Develop and manage a detailed project schedule and work plan
- Provide project updates on a consistent basis to various stakeholders about strategy, adjustments, and progress
- Manage contracts with vendors and suppliers by assigning tasks and communicating expected deliverables
- Utilize industry best practices, techniques, and standards throughout entire project execution
- Monitor progress and make adjustments as needed
- Use appropriate verification techniques to manage changes in project scope, schedule and costs
- Measure project performance using appropriate systems, tools and techniques to identify areas for improvement
- Report and escalate to management as needed
- Manage the relationship with the client and all stakeholders

Figure 5: Fake job offer on behalf of DJI, a drone manufacturing company (MD5: 4a223bc9c6096ac6bae3e7452ed6a1cd)

Malware Families

Mandiant observed the following custom malware families used in the suspected UNC1549 activity:

Malware Family	Description	First Seen	Last Seen
MINIBIKE	A custom backdoor written in C++, capable of file exfiltration and upload, command execution and more. Communicates using Azure cloud infrastructure.	June '22	Oct '23

MINIBUS	A custom backdoor which provides a more flexible code-execution interface and enhanced reconnaissance features compared to MINIBIKE.	Aug '23	Jan '24
LIGHTRAIL	A tunneler, likely based on an open-source Socks4a proxy, communicates using Azure cloud infrastructure.	Nov '22	Aug '23

MINIBIKE: When Cats Fly (Under the Radar)

MINIBIKE is a custom malware written in C++, used since at least June 2022. Once MINIBIKE is installed, it provides a full backdoor functionality, including directory and file enumeration, collection of system files and information, uploading files and running additional processes.

The MINIBIKE platform usually consists of three utilities bundled in an archive, delivered via spear-phishing:

1. The MINIBIKE backdoor, usually in the form of a .dll or a .dat file.
2. A launcher, executed via search-order-hijacking (SoH), deploying MINIBIKE and setting its persistence using registry keys.
3. A legitimate/fake executable, used to mask the malicious MINIBIKE deployment. Mandiant observed different MINIBIKE versions use three applications for this purpose: Microsoft SharePoint, Microsoft OneDrive and a fake Hamas-related .NET application.

The MINIBIKE platform has been in use since at least June 2022, gradually being developed to several versions distinct from each other in lures, features and functionality. While Mandiant did not observe any embedded version numbers, **the MINIBIKE instances can be divided to the following versions:**

Ver.	Date	Changes (compared to earlier version)	Geographies	Example MD5
------	------	---------------------------------------	-------------	-------------

1.0	06/22	<ul style="list-style-type: none"> - First version - C2 server geolocated in Iran (not Azure) - Submitted to a public malware repository from Iran - Legitimate SharePoint installation as a lure - Bundled in an IMG drive ("Screenshot.img") - Export DLL name: "update.dll" 	Iran	adef679c6aa6860aa89b775dceb6958b
1.1	10-11/22	<ul style="list-style-type: none"> - First use of Azure subdomains for C2 - three embedded, only one used - First use of OneDrive installation as a lure and as a registry key for persistence - Export DLL name: "Mini.dll" 	UAE, Turkey	409c2ac789015e76f9886f1203a73bc0
2.0	08/23	<ul style="list-style-type: none"> - Three to five Azure C2 domains used subsequently in a loop - Bundled in a ZIP file ("Survey.zip") - Additional obfuscation - Additional functionality and commands - Export DLL name: "Mini-Junked.dll" 	Israel, UAE	691d0143c0642ff783909f983ccb8ffd
2.1	08/23	<ul style="list-style-type: none"> - Uses 'Image Photo Viewer' registry key for persistence - Additional obfuscation 	Israel, India	e3dc8810da71812b860fc59aeaddcc350

		- Three Azure C2 domains		
2.2	08-10/23	<ul style="list-style-type: none"> - Four Azure C2 domains - Reverts back to OneDrive registry key for persistence - Additional functionality and commands - Additional obfuscation - Beacon communication looping over three "files": index.html, favicon.ico, icon.svg - Export DLL name: "Micro.dll" 	Israel, UAE	054c67236a86d9ab5ec80e16b884f733

MINIBUS: A RoBUST Successor?

Mandiant observed a second backdoor deployed in this campaign, which bears multiple similarities to MINIBIKE, and was therefore named MINIBUS. The MINIBUS platform has been used since at least August 2023 - likely during the same time as the latest MINIBIKE versions, though not necessarily to target the same victims.

MINIBUS is a more advanced, updated platform when compared to MINIBIKE: while similar in functionality and code base, **MINIBUS contains less built-in features and a more flexible code-execution and command interface**, in addition to more advanced reconnaissance features.

This might make the MINIBUS platform a more suitable option for an experienced operator which instead of using ready-to-use features, may require a more flexible platform. Such an operator may be concerned with operational security (OpSec), possibly as an early stage in a more elaborate operation.

Following is a more detailed list of the key differences between the MINIBIKE and MINIBUS platforms:

Functionality:

- MINIBUS has less built-in commands and features when compared with MINIBIKE. Instead, MINIBUS provides a more flexible code-execution and command interface -

including the ability to run an executable (for example, a possible next stage implant) using a single command, unlike MINIBIKE.

- MINIBUS has a process enumeration feature. A process list generated by MINIBUS may be useful to avoid detection, for example by identifying processes related to Virtual Machine (VM) utilities or security applications (such as an EDR).

Export DLL names: MINIBUS bundle contains DLLs with the names “torvaldinitial.dll” for its launcher/installer and “torvaldspersist.dll” for its payload, unlike MINIBIKE which utilizes export DLL names like “Dr2.dll” or “MspUpdate.dll” (for its launchers) and “Mini-Junked.dll” or “Micro.dll” (for its payloads).

C2 communication: MINIBUS uses a combination of Azure subdomain and unique *.com domains for C2 communications, unlike MINIBIKE which relies only on Azure infrastructure.

Lures and themes: **MINIBUS deployed lures related to the Israel-Hamas war**, including a fake .NET application with themes and contents abusing the “Bring Them Home Now” movement which calls for the return of the Israeli hostages kidnapped by Hamas.

Targeting and geography: like MINIBIKE, Mandiant observed MINIBUS targeting **Israel and possibly India and UAE**. In addition, a MINIBUS C2 domain (cashcloudservices[.]com) had a subdomain with the prefix nsalbaniahack[.]*, suggesting **an interest in Albania** as well, which is consistent with Iran interests but not yet observed in a MINIBIKE-related activity.

LIGHTRAIL: Highway to Where?

In addition to the MINIBIKE and MINIBUS backdoors, Mandiant observed a tunneler named LIGHTRAIL likely affiliated with UNC1549 as well.

LIGHTRAIL has several connections to MINIBIKE and MINIBUS in the form of (1) a shared code base; (2) Azure C2 infrastructure with similar patterns and naming; and (3) overlapping targets and victimology.

LIGHTRAIL communicates with an Azure C2 subdomain of the form **[.]*[.]cloudapp[.]azure[.]com*. Mandiant assesses with medium confidence that both LIGHTRAIL and MINIBIKE were used to target the same victim environment at least once.

LIGHTRAIL likely leverages the open source utility [“Lastenzug”](#) (“freight train” in German), a Socks4a proxy based on websockets with a “static obfuscation on [the] assembly level”. LIGHTRAIL’s export DLL is named “lastenzug.dll”, and it shares the same hardcoded User Agent as Lastenzug:

*Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36
Edge/12.10136*

Mandiant observed two LIGHTRAIL versions used at least since November 2022. Similarly to MINIBIKE, no “official” versions were embedded in LIGHTRAIL’s code, but the instances can be divided to two versions:

Ver.	Date	Changes (compared to earlier version)	Geographies	Example MD5
1.0	11/22	<ul style="list-style-type: none"> - C2 domains: tnlsowki[.]westus3[.]cloudapp[.]azure[.]com tnlsowkis[.]westus3[.]cloudapp[.]azure[.]com - Export DLL named “lastenzug.dll”, likely referring to the open source Socks4a proxy 	Turkey	36e2d9ce19ed045a9840313439d6f18d
2.0	08/23	<ul style="list-style-type: none"> - C2 domain: iaidevrssfeed[.]centralus[.]cloudapp[.]azure[.]com - Export DLL named “Lastenzug.dll” (capital ‘L’) - String obfuscation, similar to MINIBIKE 	Israel	a5fdf55c1c50be471946de937f1e46dd

Credential Harvesting and Fake Job Offers

Mandiant observed that several websites hosting MINIBIKE payloads also hosted fake login pages in mid-2023, posing as job offers on behalf of legitimate defense and technology-related companies. More specifically, the companies were affiliated with the aerospace, aviation and thermal imaging industries.

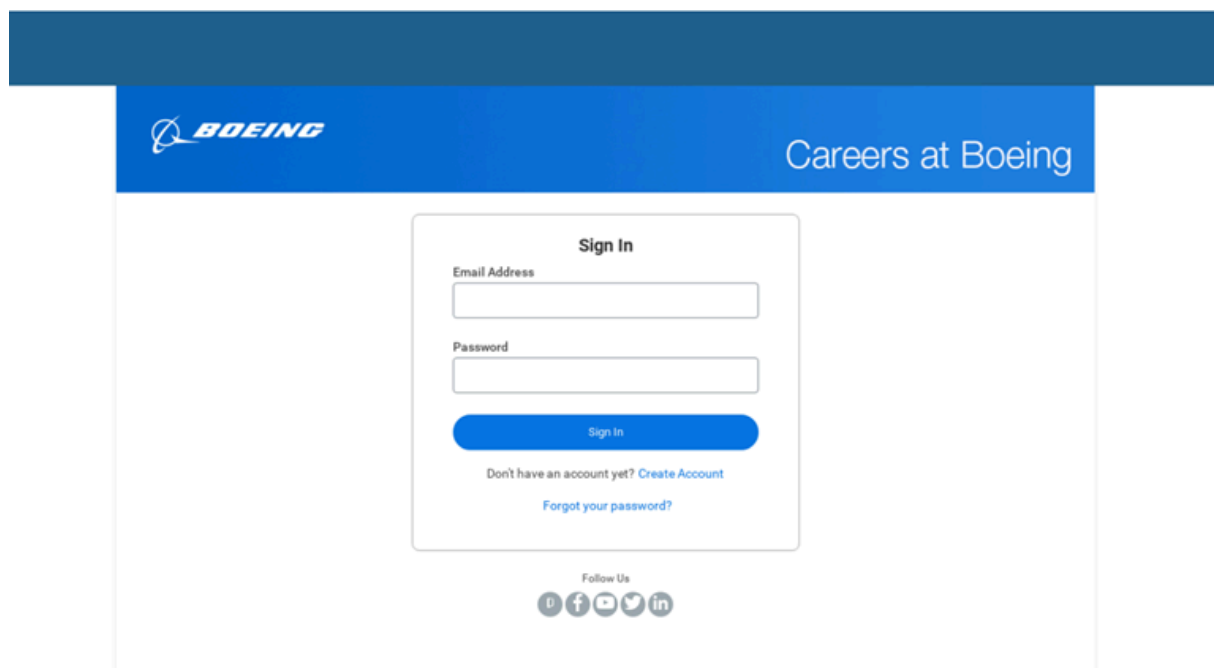
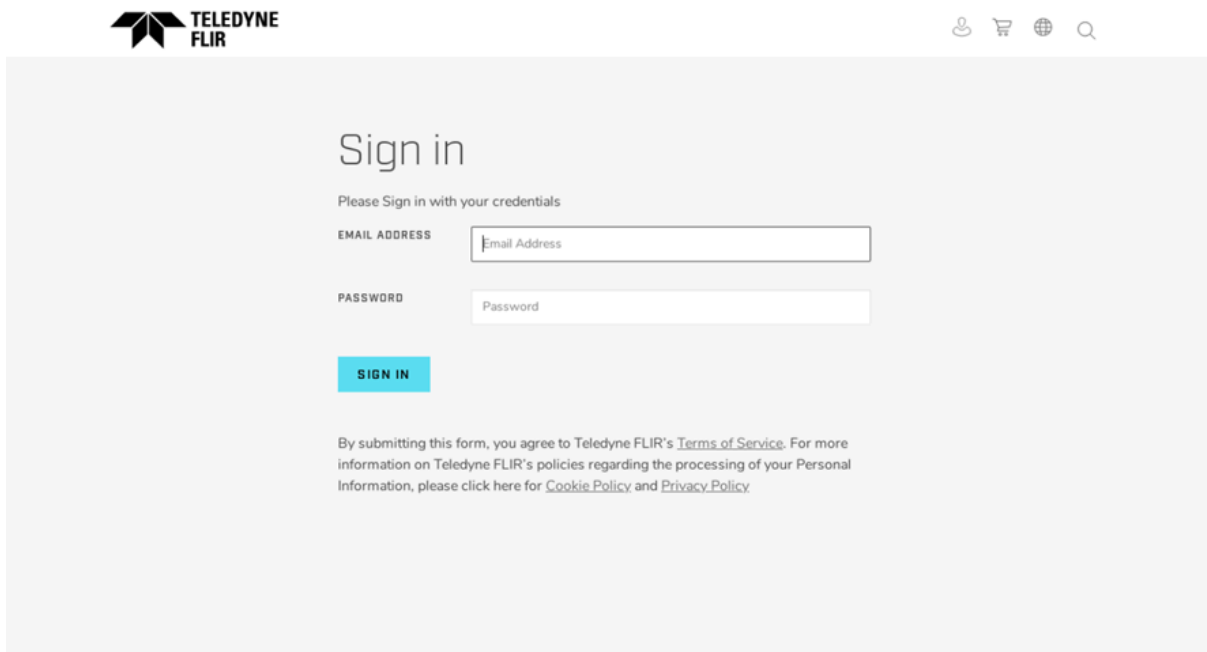


Figure 6: Fake login page masquerading as the aerospace company Boeing



The image shows a web page designed to look like the Teledyne FLIR login page. At the top left is the Teledyne FLIR logo. At the top right are four small icons: a person, a shopping cart, a globe, and a magnifying glass. The main heading is "Sign in". Below it is the text "Please Sign in with your credentials". There are two input fields: "EMAIL ADDRESS" with a placeholder "Email Address" and "PASSWORD" with a placeholder "Password". Below the password field is a blue "SIGN IN" button. At the bottom, there is a paragraph of text: "By submitting this form, you agree to Teledyne FLIR's [Terms of Service](#). For more information on Teledyne FLIR's policies regarding the processing of your Personal Information, please click here for [Cookie Policy](#) and [Privacy Policy](#)."

Figure 7: Fake login page masquerading as Teledyne FLIR, a manufacturer of thermal imaging devices

In addition, Mandiant observed a fake domain posing as DJI, a drone manufacturing company, hosting job description documents, in parallel to a MINIBIKE .zip file.

The documents were likely used as lures in social engineering efforts, either for running malicious files or harvesting credentials (see figures below):



Project Manager Job Description

Job Summary:

A project manager plans, organizes and oversees a project from start to finish. They should guarantee that the project is finalized to the contentment of all stakeholders, within the designated budget and timeline.

Duties/Responsibilities:

- Determine and define project scope and objectives
- Predict resources needed to reach objectives and manage resources in an effective and efficient manner
- Prepare budget based on scope of work and resource requirements
- Track project costs in order to meet budget
- Develop and manage a detailed project schedule and work plan
- Provide project updates on a consistent basis to various stakeholders about strategy, adjustments, and progress
- Manage contracts with vendors and suppliers by assigning tasks and communicating expected deliverables
- Utilize industry best practices, techniques, and standards throughout entire project execution
- Monitor progress and make adjustments as needed
- Use appropriate verification techniques to manage changes in project scope, schedule and costs
- Measure project performance using appropriate systems, tools and techniques to identify areas for improvement
- Report and escalate to management as needed
- Manage the relationship with the client and all stakeholders

Figure 8: Fake DJI job offer (MD5: 4a223bc9c6096ac6bae3e7452ed6a1cd)



Marketing and Sales Consultant Job Description

Job Summary:

Sales and marketing consultant advises businesses on how to develop and execute sales and marketing strategies.

Duties/Responsibilities:

- Study company profile and operations to understand its marketing needs
- Conduct marketing research to identify industry trends and commercial opportunities
- Develop and implement a marketing strategy according to objectives and budget
- Prepare detailed proposals and marketing plans
- Advise on branding, positioning, communications and other marketing issues
- Give direction to marketing efforts with the most effective methods and tools
- Liaise with marketing department and external vendors
- Monitor marketing projects and analyze results
- Write reports with suggestions for improvements and new ideas
- Provide training for search engine optimization (SEO), pay-per-click (PPC), virtual selling, e-commerce and other digital marketing strategies.

Desired Skills & Qualifications:

- 5-8 years of marketing and related experience
- Proven experience as marketing consultant or similar role

Figure 9: Fake DJI job offer (MD5: ec6a0434b94f51aa1df76a066aa05413)

Technical Annex - MINIBIKE Technical Analysis

Mandiant observed the following versions of MINIBIKE deployed since 2022:

Version 1.x - June-November 2022:

- **Payload:** IMG archive named *Screenshot.img* (example MD5: 409c2ac789015e76f9886f1203a73bc0), containing the following files:
 - *Screenshots.lnk* - a launcher LNK file (MD5: cb565b1bb128dfc20c8392974ff73e3f)
 - *Setup.exe* - a legitimate OneDrive/SharePoint executable (MD5: 400d7190012517677dd5ef2e471f2cd1)
 - *secur32.dll* - the MINIBIKE launcher, executed via search-order-hijacking (SoH) (MD5: 54848d17aa76d807e2fd6d196a01ce84)
 - *configur.dll* - the MINIBIKE backdoor (MD5: e9ed595b24a7eeb34ac52f57eeec6e2b)

Note: Most of the analysis below refers to version 1.0, but version 1.1 behaves in a similar manner.

- **Execution:** once the IMG archive is mounted, the malicious launcher is executed via SoH and copies the legitimate executable and the MINIBIKE backdoor to the following paths:

Legitimate executable: %LOCALAPPDATA%\Microsoft\OneDrive\configs\FileCoAuth.exe

MINIBIKE backdoor: %LOCALAPPDATA%\Microsoft\OneDrive\configs\secur32.dll

- **Persistence:** The loader/installer sets persistence for the MINIBIKE payload by moving it to its staging directory and setting the following Run registry key:

Key: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\OneDriveFileCoAuth.exe

Value: %LOCALAPPDATA%\Microsoft\OneDrive\configs\FileCoAuth.exe

● **Export DLL Name:**

Version 1.0: "update.dll"

Version 1.1: "Mini.dll"

● **User Agent:**

Version 1.0: Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.82 Mobile Safari/537.36

Version 1.1: Mozilla/5.0

● **C2 infrastructure:**

Version 1.0: 158.255.74[.]25

Version 1.1: homefurniture[.]azurewebsites[.]net

● **C2 URIs:**

Version 1.0:

- ☐ /api/blogs/96752 - initial beacon and request command
- ☐ /api/blogs/result/96752 - command/request response
- ☐ /api/blogs/download/ - download file
- ☐ /api/blogs/result/file/ - upload file

Version 1.1:

- */news/notifications/235722* - initial beacon and request command
- */news/update/* - command/request response
- */news/image/* - download file

● **Affected geographies:** UAE, Turkey, Iran

Version 2.x - August-October 2023:

● **Payload:** ZIP archive, usually named *Survey.zip* (example MD5: 691d0143c0642ff783909f983ccb8ffd), containing the following files:

- *Setup.exe* - a legitimate executable used to sideload the installer (MD5: ce1054d542dbd999401236f2ce20f826)
- *secur32.dll* - The MINIBIKE backdoor - (MD5: 1e7cf4c172bdabe48714b402d2255707)
- *lang.dat* - a MINIBIKE installer (MD5: 909a235ac0349041b38d84e9aab3f3a1)

● **Execution:** once the legitimate executable is run, the MINIBIKE installer is sideloaded and the files are copied to the following paths:

Legitimate executable: %LOCALAPPDATA%\Microsoft\Internet Explorer\FileCoAuth.exe

MINIBIKE backdoor: %LOCALAPPDATA%\Microsoft\Internet Explorer\secur32.dll

● **Persistence:** The loader/installer sets persistence for the MINIBIKE payload by moving it to its staging directory and setting the following Run registry key:

Key: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\OneDrive FileCoAuth

Value: %LOCALAPPDATA%\Microsoft\Internet Explorer\secur32.dll

Note: Version 2.1 uses 'Image Photo Viewer' as a registry key

● Export DLL Name:

Versions 2.0 and 2.1: *"Mini-Junked.dll"*

Version 2.2: *"Micro.dll"*

Note: In a single instance Mandiant observed the use of "devobj.dll"

● User Agent:

Version 2.0:

- *Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/539.180 (KHTML, like Gecko) Chrome/110.0.0.2 Safari/538.36*
- *Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/539.181 (KHTML, like Gecko) Chrome/111.0.0.2 Safari/538.46*

Version 2.1:

- *Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/539.181 (KHTML, like Gecko) Chrome/111.0.0.2 Safari/538.36*
- *Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/539.181 (KHTML, like Gecko) Chrome/111.0.0.2 Safari/538.46*

Version 2.2: *Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36*

Note: In a single instance Mandiant observed the use of "Mozilla/5.0" user agent.

- **C2 infrastructure:** This version of MINIBIKE communicates with three to five Azure subdomains. After every communication it uses the next C2 in a loop, for example:

- *blogvolleyballstatus[.]azurewebsites[.]net*
- *blogvolleyballstatusapi[.]azurewebsites[.]net*
- *marineblogapi[.]azurewebsites[.]net*

- **C2 URIs:**

Versions 2.0 and 2.1:

- */news/notifications/<six_digits>* - initial beacon and request command
- */news/update/* - command/request response
- */news/image/* - download file

Version 2.2:

- */assets/<six_or_eight_digits>/ {index.html / favicon.ico / icon.svg}* - initial beacon and request command
- */assets/<six_or_eight_digits>/* - command/request response
- */assets/<six_or_eight_digits>/* - download file
- */assets/<six_or_eight_digits>/* - upload file

Note: In a single instance Mandiant observed the use of URIs of the form: *blogs/<keywords>*

- **Affected geographies:** Israel, UAE, and potentially India

Technical Annex - MINIBUS Analysis

- **Payload:** ZIP archive named *bringthemhomenow.zip* (MD5: ef262f571cd429d88f629789616365e4), containing the following files:
 - BringThemeHome.exe - a benign executable (MD5: ce1054d542dbd999401236f2ce20f826)
 - A MINIBUS installer - secur32.dll (MD5: c5dc2c75459dc99a42400f6d8b455250)
 - CoreUIComponent.dll - the MINIBUS backdoor (MD5: 816af741c3d6be1397d306841d12e206)
 - essential.dat - an additional archive containing decoy content (MD5: 251894b3af0ece374ed6df223ab09cab)
- **Execution:** once the legitimate executable is run, the MINIBUS installer is installed via search-order-hijacking (SoH).

The installer DLL displays a message indicating the files are being extracted:

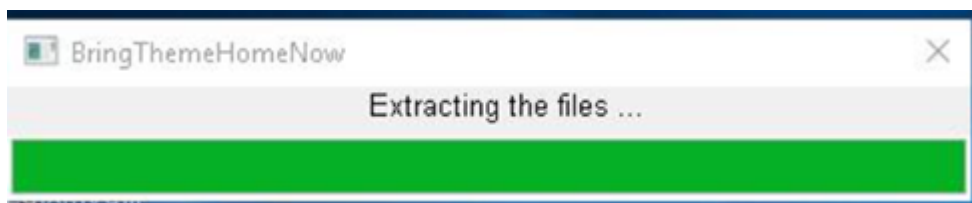


Figure 10: MINIBUS installer DLL installation message

The decoy contents are moved to their intended location on the targeted system:

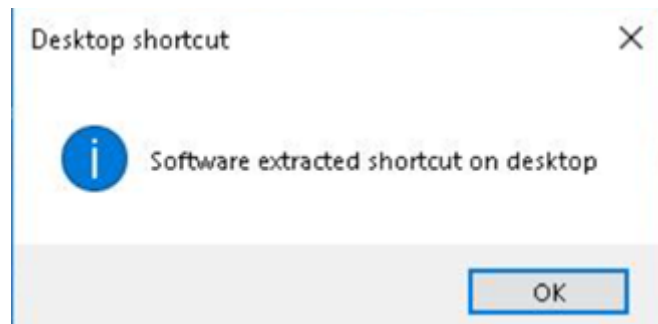


Figure 11: Installer DLL message box

Two main decoy files are contained within the ZIP archive along with some dependency files, essential.dat (MD5: 251894b3af0ece374ed6df223ab09cab):

- Decoy .NET application masquerading as an application related to Israeli hostages kidnapped by Hamas during the October 7 attack on Israel:

`<extraction_directory>\BringThemeHomeNow\BringThemeHomeNow.exe [sic]` (MD5: dfed4468dd78ad2f5d762741df4c1755)

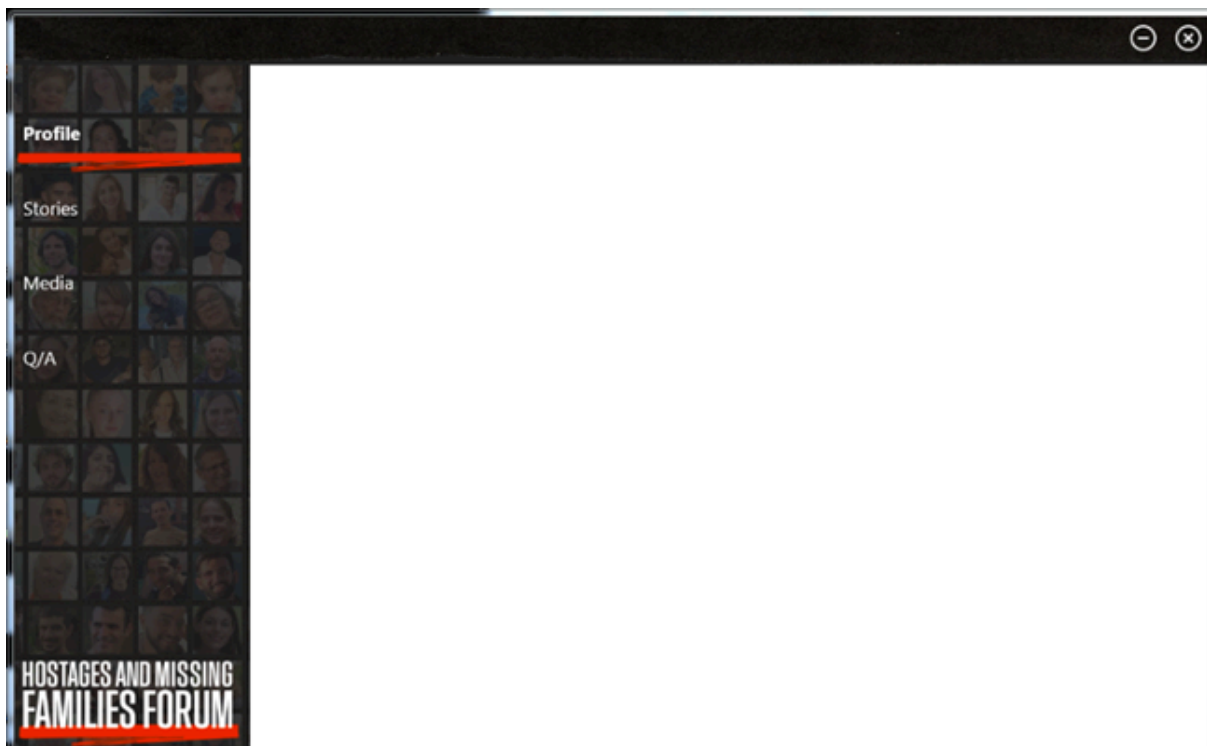


Figure 12: Fake “Bring Them Home Now”.NET application “BringThemeHomeNow.exe” [sic]

- Decoy image:

`<extraction_directory>\BringThemeHomeNow\petition.jpg (MD5:
c0060a0c26df9fed7fdcdb7d26ff921f)`

[image to follow]

Figure 13: Decoy content "petition.jpg"

Upon execution, the .NET application initially checks of the existence of a flag file that indicates if the decoy has previously run on the device: %LOCALAPPDATA%\Commons\lg

If the file does not exist, a splash screen is displayed prior to entering the application. If the file already exists, the application presents the main screen (seen in the figure above).

In addition to displaying decoy content to the victim, the installer DLL copies the backdoor and dependency files to their staging directory, and it also sets persistence for the backdoor using the following registry run key:

Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\OneDriveCoUpdate

Value: %LOCALAPPDATA%\Microsoft\OneDrive\cachellogger\FileCoAuth.exe

- **C2 infrastructure:** This version of MINIBIKE communicates with one Azure subdomain and two dedicated domains:

- `vscodeupdater[.]azurewebsites[.]net`

- *cashcloudservices[.]com*

- *xboxplayservice[.]com*

- **Affected geographies:** Israel and India, as well as possibly UAE and Albania, based on the following subdomains of cashcloudservices[.]com:

- ***dubai-ae0043[.]cashcloudservices[.]com***

- ***nsalbaniahack[.]cashcloudservices[.]com***

Detection and Mitigation

If you are a Google Chronicle Enterprise+ customer, Chronicle rules were released to your [Emerging Threats](#) rule pack and IOCs listed in this blog are available for prioritization with [Applied Threat Intelligence](#).

Indicators of Compromise (IOCs)

MINIBIKE

01cbadd7a269521bf7b80f4a9a1982f

054c67236a86d9ab5ec80e16b884f733

1d8a1756b882a19d98632bc6c1f1f8cd

2c4cdc0e78ef57b44f11f7ec2f6164cd

3b658afa91ce3327dbfa1cf665529a6d

409c2ac789015e76f9886f1203a73bc0

601eb396c339a69e7d8c2a3de3b0296d
664cfda4ada6f8b7bb25a5f50cccf984
68f6810f248d032bbb65b391cdb1d5e0
691d0143c0642ff783909f983ccb8ffd
710d1a8b2fc17c381a7f20da5d2d70fc
75d2c686d410ec1f880a6fd7a9800055
909a235ac0349041b38d84e9aab3f3a1
a5e64f196175c5f068e1352aa04bc5fa
adef679c6aa6860aa89b775dceb6958b
bfd024e64867e6ca44738dd03d4f87b5
c12ff86d32bd10c6c764b71728a51bce
cf32d73c501d5924b3c98383f53fda51
d94ffe668751935b19eae93fed1cdbe
e3dc8810da71812b860fc59aeaddcc350
e9ed595b24a7eeb34ac52f57eeec6e2b
eadbaabe3b8133426bcf09f7102088d4

MINIBUS

ef262f571cd429d88f629789616365e4
816af741c3d6be1397d306841d12e206
c5dc2c75459dc99a42400f6d8b455250

LIGHTRAIL

0a739dbdbcf9a5d8389511732371ecb4

36e2d9ce19ed045a9840313439d6f18d
aaef98be8e58be6b96566268c163b6aa
c3830b1381d95aa6f97a58fd8ff3524e
c51bc86beb9e16d1c905160e96d9fa29
a5fdf55c1c50be471946de937f1e46dd

Fake Job Offers

ec6a0434b94f51aa1df76a066aa05413
89107ce5e27d52b9fa6ae6387138dd3e
4a223bc9c6096ac6bae3e7452ed6a1cd

C2 and Hosting Infrastructure

1stemployer[.]com
birngthemhomenow[.]co[.]il
cashcloudservices[.]com
jupyternotebookcollections[.]com
notebooktextcheckings[.]com
teledyneflir[.]com[.]de
vsliveagent[.]com
xboxplayservice[.]com

Azure Subdomains

airconnectionapi[.]azurewebsites[.]net
airconnectionsapi[.]azurewebsites[.]net
airconnectionsapijson[.]azurewebsites[.]net
airgadgetsolution[.]azurewebsites[.]net
airgadgetsolutions[.]azurewebsites[.]net
altnametestapi[.]azurewebsites[.]net
answerssurveytest[.]azurewebsites[.]net
apphrquestion[.]azurewebsites[.]net
apphrquestions[.]azurewebsites[.]net
apphrquizapi[.]azurewebsites[.]net
arquestionsapi[.]azurewebsites[.]net
arquestions[.]azurewebsites[.]net
audiomanagerapi[.]azurewebsites[.]net
audioservicetestapi[.]azurewebsites[.]net
blognewsalphaapijson[.]azurewebsites[.]net
blogvolleyballstatusapi[.]azurewebsites[.]net
blogvolleyballstatus[.]azurewebsites[.]net
boeismurveyapplications[.]azurewebsites[.]net
browsercheckap[.]azurewebsites[.]net
browsercheckingapi[.]azurewebsites[.]net
browsercheckjson[.]azurewebsites[.]net
changequestionstypeapi[.]azurewebsites[.]net
changequestionstypejsonapi[.]azurewebsites[.]net
changequestiontypesapi[.]azurewebsites[.]net
changequestiontypes[.]azurewebsites[.]net
checkapicountryquestions[.]azurewebsites[.]net
checkapicountryquestionsjson[.]azurewebsites[.]net

checkservicecustomerapi[.]azurewebsites[.]net
coffeeonlineshop[.]azurewebsites[.]net
coffeeonlineshoping[.]azurewebsites[.]net
connectairapijson[.]azurewebsites[.]net
connectionhandlerapi[.]azurewebsites[.]net
countrybasedquestions[.]azurewebsites[.]net
customercareserviceapi[.]azurewebsites[.]net
customercareservice[.]azurewebsites[.]net
emiratescheckapi[.]azurewebsites[.]net
emiratescheckapijson[.]azurewebsites[.]net
engineeringrssfeed[.]azurewebsites[.]net
engineeringssfeed[.]azurewebsites[.]net
exctestcheckingapi[.]azurewebsites[.]net
exctestcheckingapihealth[.]azurewebsites[.]net
flighthelicopterahtest[.]azurewebsites[.]net
helicopterahtest[.]azurewebsites[.]net
helicopterahtests[.]azurewebsites[.]net
helicoptersahtests[.]azurewebsites[.]net
hiringarabicregion[.]azurewebsites[.]net
homefurniture[.]azurewebsites[.]net
hrapplicationtest[.]azurewebsites[.]net
humanresourcesapi[.]azurewebsites[.]net
humanresourcesapijson[.]azurewebsites[.]net
humanresourcesapiquiz[.]azurewebsites[.]net
iaidevrssfeed[.]centralus[.]cloudapp[.]azure[.]com
iaidevrssfeed[.]centrualus[.]cloudapp[.]azure[.]com
iaidevrssfeed[.]cloudapp[.]azure[.]com
iaidevrssfeedp[.]cloudapp[.]azure[.]com

identifycheckapplication[.]azurewebsites[.]net
identifycheckapplications[.]azurewebsites[.]net
identifycheckingapplications[.]azurewebsites[.]net
ilengineeringrssfeed[.]azurewebsites[.]net
integratedblognewfeed[.]azurewebsites[.]net
integratedblognewsapi[.]azurewebsites[.]com
integratedblognewsapi[.]azurewebsites[.]net
integratedblognews[.]azurewebsites[.]net
intengineeringrssfeed[.]azurewebsites[.]net
intergratedblognewsapi[.]azurewebsites[.]net
javaruntime[.]azurewebsites[.]net
javaruntimestestapi[.]azurewebsites[.]net
javaruntimetestapi[.]azurewebsites[.]net
javaruntimeversioncheckingapi[.]azurewebsites[.]net
javaruntimeversionchecking[.]azurewebsites[.]net
jupyternotebookcollection[.]azurewebsites[.]net
jupyternotebookcollections[.]azurewebsites[.]net
jupyternotebookscollection[.]azurewebsites[.]net
logsapimanagement[.]azurewebsites[.]net
logsapimanagements[.]azurewebsites[.]net
logupdatemanagementapi[.]azurewebsites[.]net
logupdatemanagementapijson[.]azurewebsites[.]net
manpowerfeedapi[.]azurewebsites[.]net
manpowerfeedapijson[.]azurewebsites[.]net
marineblogapi[.]azurewebsites[.]net
notebooktextchecking[.]azurewebsites[.]net
notebooktextcheckings[.]azurewebsites[.]net
notebooktexts[.]azurewebsites[.]net

onequestionsapi[.]azurewebsites[.]net
onequestionsapicheck[.]azurewebsites[.]net
onequestions[.]azurewebsites[.]net
openapplicationcheck[.]azurewebsites[.]net
optionalapplication[.]azurewebsites[.]net
personalitytestquestionapi[.]azurewebsites[.]net
personalizationsurvey[.]azurewebsites[.]net
qaquestionapi[.]azurewebsites[.]net
qaquestionsapi[.]azurewebsites[.]net
qaquestionsapijson[.]azurewebsites[.]net
qaquestions[.]azurewebsites[.]net
queryfindquestions[.]azurewebsites[.]net
queryquestions[.]azurewebsites[.]net
questionsapplicationapi[.]azurewebsites[.]net
questionsapplicationapijson[.]azurewebsites[.]net
questionsapplicationbackup[.]azurewebsites[.]net
questionsdatabases[.]azurewebsites[.]net
questionssurveyapp[.]azurewebsites[.]net
questionssurveyappserver[.]azurewebsites[.]net
quiztestapplication[.]azurewebsites[.]net
refaeldevrssfeed[.]centralus[.]cloudapp[.]azure[.]com
regionuaequestions[.]azurewebsites[.]net
registerinsurance[.]azurewebsites[.]net
roadmapselectorapi[.]azurewebsites[.]net
roadmapselector[.]azurewebsites[.]net
sportblogs[.]azurewebsites[.]net
surveyappquery[.]azurewebsites[.]net
surveyonlinetestapi[.]azurewebsites[.]net

surveyonlinetest[.]azurewebsites[.]net
technewsblogapi[.]azurewebsites[.]net
testmanagementapi1[.]azurewebsites[.]net
testmanagementapis[.]azurewebsites[.]net
testmanagementapisjson[.]azurewebsites[.]net
testquestionapplicationapi[.]azurewebsites[.]net
testtesttes[.]azurewebsites[.]net
tiappschecktest[.]azurewebsites[.]net
tnlsowkis[.]westus3[.]cloudapp[.]azure[.]com
tnlsowki[.]westus3[.]cloudapp[.]azure[.]com
turkairline[.]azurewebsites[.]net
uaeaircheckon[.]azurewebsites[.]net
uaeairchecks[.]azurewebsites[.]net
vscodeupdater[.]azurewebsites[.]net
workersquestionsapi[.]azurewebsites[.]net
workersquestions[.]azurewebsites[.]net
workersquestionsjson[.]azurewebsites[.]net