Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

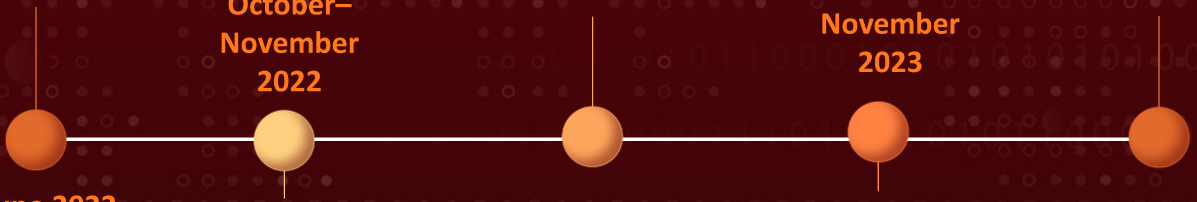
Iranian hackers soar into the defense sectors of the Middle East

Date of Publication	Admiralty Code	TA Number
March 1, 2024	A1	TA2024083

Summary

Active Since: June 2022
Malware: MINIBIKE, MINIBUS, LIGHTRAIL
Threat Actor: UNC1549
Attack Region: Akrotiri and Dhekelia, Albania, Bahrain, Cyprus, Egypt, India, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirates, Yemen
Targeted Industries: Aerospace, Aviation, and Defense
Attack: Since June 2022, the hacking group UNC1549, potentially connected to Tortoiseshell (aka Imperial Kitten) and linked with the Iranian IRGC, has implemented distinct backdoors known as MiniBike and MiniBus. Their primary focus lies in targeting defense-related entities in the Middle East.

Attack Timeline



June 2022

The suspected activity attributed to **UNC1549** initiates, with the **MINIBIKE** backdoor having been active since.

October–November 2022

First employment of Azure subdomains for Command and Control (C2).

November 2022

LIGHTRAIL, a tunneling tool, has been identified and is likely linked to UNC1549. **MINIBIKE** version 1.0 has been observed.

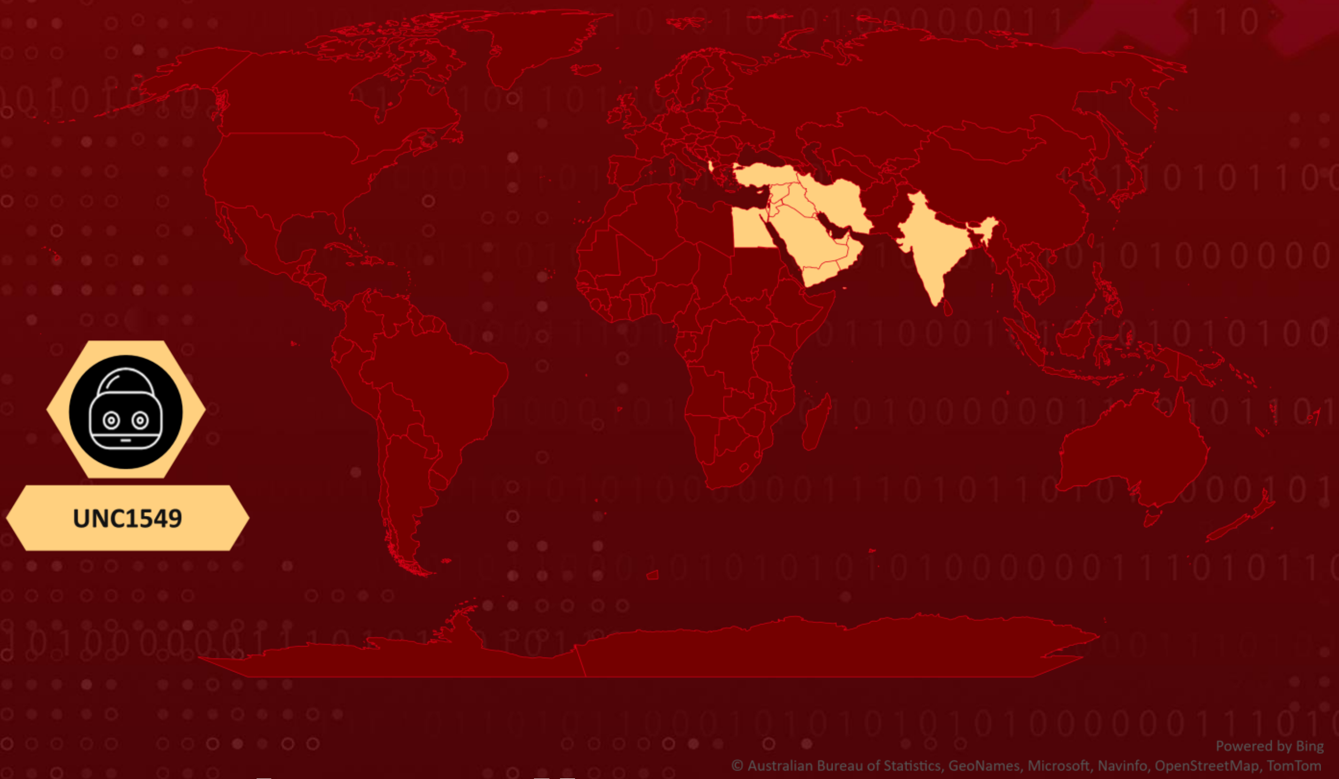
November 2023

The counterfeit recruitment site persists in hosting a **MINIBUS** payload.

February 2024

The campaign continues, focusing on **defense**, **aerospace**, and **aviation** entities, particularly in **Israel** and the **UAE**.

Attack Regions



© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 As part of an ongoing campaign since at least June 2022, the suspected hacking group identified as UNC1549 has been utilizing two distinctive backdoors, namely MiniBike and MiniBus, to conduct espionage on organizations in the Middle East. UNC1549, believed to be associated with Tortoiseshell (aka Imperial Kitten), is of particular interest due to its potential connection to the Iranian IRGC.

#2 This interest is heightened by the group's focus on defense-related entities, especially given the recent tensions with Iran in the context of the Israel-Hamas conflict. The latest series of attacks targets aerospace, aviation, and defense industries in Israel and the U.A.E., with additional potential targets including Turkey, India, and Albania.

#3 UNC1549 employs spear phishing and watering-hole attacks to harvest credentials and deploy malware. In November 2023, a MINIBUS payload was observed on a fake recruiting website, using a template previously employed by UNC1549 in another deceptive recruiting site. These attacks involve the use of Microsoft Azure cloud infrastructure for command-and-control (C2) operations, utilizing job-related lures for social engineering. Two backdoors, MINIBIKE and MINIBUS, are deployed in these operations.

#4 MINIBIKE, a custom C++ backdoor first identified in June 2022, facilitates file exfiltration, command execution, and more, communicating through Azure cloud infrastructure. MINIBUS, documented in August 2023, offers a more versatile code-execution interface and enhanced reconnaissance features compared to MINIBIKE.

#5 Once C2 access is established, these custom backdoors serve as conduits for intelligence collection and further access into the targeted network. Another tool in use is LIGHTRAIL, a tunneling software first seen in November 2022, communicating via Azure cloud. Notably, the MINIBUS backdoor was hosted on a fake job website, replicating written content used by UNC1549 in early 2022.

#6 The evasion tactics employed in this campaign, particularly the use of tailored job-themed lures and reliance on cloud infrastructure for C2 operations, pose challenges for network defenders in preventing, detecting, and mitigating this cyber espionage activity.

Recommendations

Email Security and Document Verification: Employ advanced email security measures to detect and filter malicious attachments, especially those masquerading as invitation letters. Implement document verification processes to ensure the authenticity of official communications.

Heighten Awareness: Familiarize yourself with common social engineering tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Zero Trust Architecture: Adopt a Zero Trust security architecture, where trust is never assumed and continuous authentication and authorization mechanisms are implemented, reducing the risk of unauthorized access.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Implement Network Security Measures: Employ robust network security measures, including firewalls and intrusion detection/prevention systems, to help prevent unauthorized access and the spread of ransomware within the network.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0007 Discovery
TA0011 Command and Control	TA0040 Impact	T1055 Process Injection	T1204.002 Malicious File
T1562 Impair Defenses	T1059 Command and Scripting Interpreter	T1057 Process Discovery	T1083 File and Directory Discovery
T1027 Obfuscated Files or Information	T1598.002 Spearphishing Attachment	T1070 Indicator Removal	T1574.002 DLL Side-Loading
T1041 Exfiltration Over C2 Channel	T1036 Masquerading	T1001 Data Obfuscation	T1027.010 Command Obfuscation
T1555.003 Credentials from Web Browsers	T1578 Modify Cloud Compute Infrastructure		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	01cbaddd7a269521bf7b80f4a9a1982f, 054c67236a86d9ab5ec80e16b884f733, 1d8a1756b882a19d98632bc6c1f1f8cd, 2c4cdc0e78ef57b44f11f7ec2f6164cd, 3b658afa91ce3327dbfa1cf665529a6d, 409c2ac789015e76f9886f1203a73bc0, 601eb396c339a69e7d8c2a3de3b0296d, 664cfda4ada6f8b7bb25a5f50cccf984, 68f6810f248d032bbb65b391cdb1d5e0, 691d0143c0642ff783909f983ccb8ffd, 710d1a8b2fc17c381a7f20da5d2d70fc,

TYPE	VALUE
MD5	75d2c686d410ec1f880a6fd7a9800055, 909a235ac0349041b38d84e9aab3f3a1, a5e64f196175c5f068e1352aa04bc5fa, adef679c6aa6860aa89b775dceb6958b, bfd024e64867e6ca44738dd03d4f87b5, c12ff86d32bd10c6c764b71728a51bce, cf32d73c501d5924b3c98383f53fda51, d94ffe668751935b19eaeb93fed1cdbe, e3dc8810da71812b860fc59aeadcc350, e9ed595b24a7eeb34ac52f57eeec6e2b, eadbaabe3b8133426bcf09f7102088d4, ef262f571cd429d88f629789616365e4, 816af741c3d6be1397d306841d12e206, c5dc2c75459dc99a42400f6d8b455250, 05fcace605b525f1bece1813bb18a56c, 4ed5d74a746461d3faa9f96995a1eec8, f58e0dfb8f915fa5ce1b7ca50c46b51b, 0a739dbdbcf9a5d8389511732371ecb4, 36e2d9ce19ed045a9840313439d6f18d, aaef98be8e58be6b96566268c163b6aa, c3830b1381d95aa6f97a58fd8ff3524e, c51bc86beb9e16d1c905160e96d9fa29, a5fdf55c1c50be471946de937f1e46dd, ec6a0434b94f51aa1df76a066aa05413, 89107ce5e27d52b9fa6ae6387138dd3e, 4a223bc9c6096ac6bae3e7452ed6a1cd
C2	1stemployer[.]com, birngthemhomenow[.]co[.]il, cashcloudservices[.]com, jupyternotebookcollections[.]com, notebooktextcheckings[.]com, teledyneflir[.]com[.]de, vsliveagent[.]com, xboxplayservice[.]com
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,

TYPE	VALUE
Subdomains	arquestions[.]azurewebsites[.]net, audiomanagerapi[.]azurewebsites[.]net, audioservicetestapi[.]azurewebsites[.]net, blognewsalphaapijson[.]azurewebsites[.]net, blogvolleyballstatusapi[.]azurewebsites[.]net, blogvolleyballstatus[.]azurewebsites[.]net, boeisurveyapplications[.]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, exchtestcheckingapi[.]azurewebsites[.]net, exchtestcheckingapihealth[.]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,

TYPE	VALUE
Subdomains	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, questionsurveyapp[.]azurewebsites[.]net, questionsurveyappserver[.]azurewebsites[.]net, quiztestapplication[.]azurewebsites[.]net, refaeldevrssfeed[.]centralus[.]cloudapp[.]azure[.]com, regionuaequestions[.]azurewebsites[.]net,

TYPE	VALUE
Subdomains	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

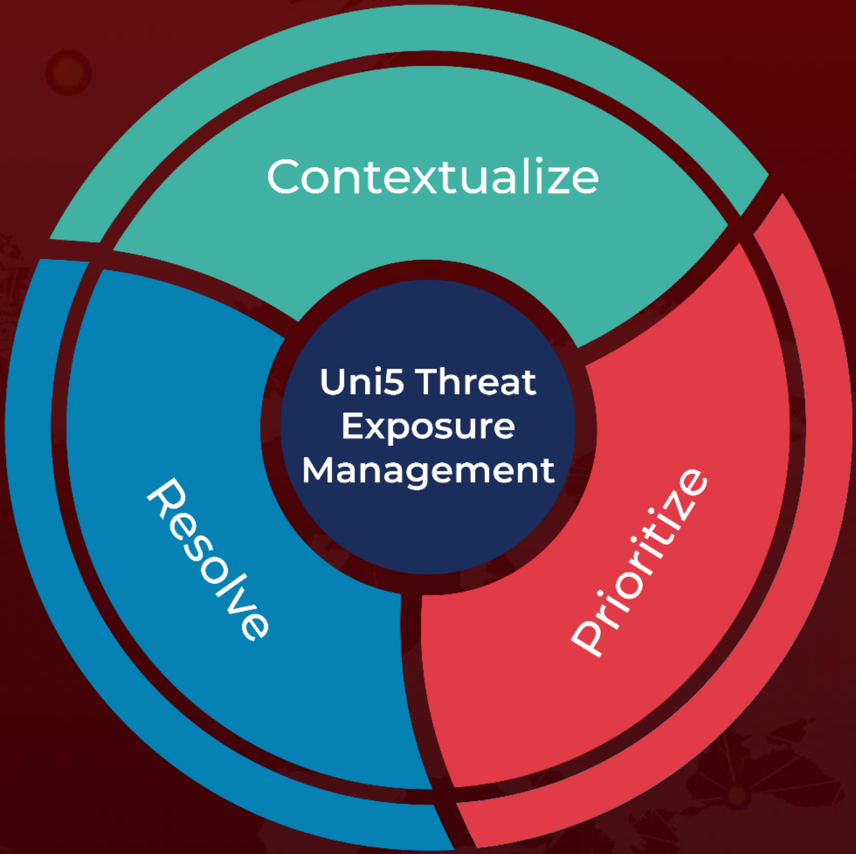
References

https://www.mandiant.com/resources/blog/suspected-iranian-unc1549-targets-israel-middle-east

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 1, 2024 • 6:00 AM

More at www.hivepro.com