Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

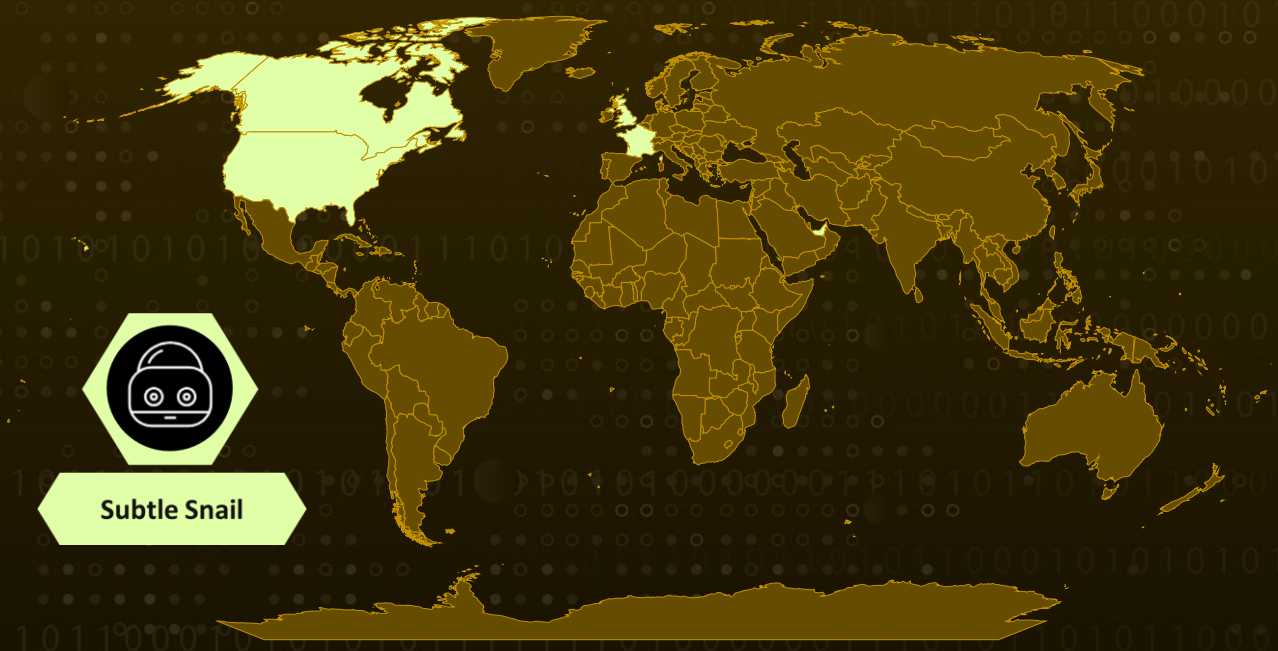
Subtle Snail's Silent Espionage Across Europe

Date of Publication	Admiralty Code	TA Number
September 23, 2025	A1	TA2025292

Summary

Attack Discovered: 2025
Targeted Countries: Canada, USA, UK, France, UAE
Targeted Industries: Telecommunications, Aerospace, Defense
Actor: Subtle Snail (aka UNC1549, TA455, Smoke Sandstorm, Bohrium, DEV-0056, Yellow Dev 13)
Affected Platform: Windows
Malware: MINIBIKE
Attack: Subtle Snail (UNC1549), an Iran-linked espionage group, has been quietly crawling into Europe's telecom, aerospace, and defense sectors by posing as LinkedIn recruiters and offering fake job opportunities. Behind these convincing fronts hides the MINIBIKE backdoor, a custom tool that steals credentials, monitors communications, and exfiltrates sensitive files while blending into trusted applications and cloud traffic. With signed binaries, DLL sideloading, and clever use of Microsoft Azure services, Subtle Snail has turned everyday job hunting into a gateway for long-term espionage.

Attack Regions



Attack Details

#1 Subtle Snail (aka UNC1549), an Iran-linked espionage group active since 2022, has been quietly infiltrating Europe's most critical industries. The group has compromised 34 devices across 11 organizations in the telecommunications, aerospace, and defense sectors. Their method is deceptively simple yet effective, posing as HR recruiters on LinkedIn and offering fake job opportunities. Behind these staged recruitment campaigns lies the **MINIBIKE** backdoor, a custom malware built to ensure long-term access and espionage inside targeted environments.

#2 Once engagement begins, Subtle Snail escalates with precision. They collect detailed intelligence on their targets from public sources such as LinkedIn, validate information through spear-phishing, and eventually deliver malicious ZIP files disguised as legitimate job materials. These archives contain signed binaries that, when executed, exploit DLL sideloading to inject malicious code into trusted applications.

#3 At the core of their toolkit is the MINIBIKE backdoor, which enables reconnaissance, credential theft, and stealthy execution of attacker commands. Subtle Snail develops unique DLLs for each victim, leveraging Windows' DLL search order hijacking for persistence and privilege escalation. With modules for keylogging, browser data theft, and credential harvesting, the group siphons off sensitive communications, authentication details, and even files from centralized storage systems.

#4 The group's ability to remain undetected is one of its greatest strengths. By routing command-and-control traffic through Microsoft Azure services and Virtual Private Servers, they camouflage malicious activity within legitimate cloud communications. Their malware encrypts data, fragments large files for discreet exfiltration, and stores logs in public user folders to avoid detection. Combined with registry-based persistence, these measures allow Subtle Snail to maintain a resilient foothold across system reboots and security scans.

#5 There is an overlap with another Iran-linked actor, Nimbus Manticore, which has focused on similar industries as those of Subtle Snail in Denmark, Sweden, and Portugal. While sharing infection techniques with Subtle Snail, Nimbus Manticore deploys an updated backdoor named MiniJunk and a stealer called MiniBrowse. Although related in tradecraft, Nimbus Manticore distinguishes itself with a specialized malware suite, a different command-and-control infrastructure, and narrower targeting preferences. For European organizations, the message is clear: defending against such advanced threats requires more than standard security controls.

Recommendations

- **Be cautious with job offers online:** If you receive an unexpected job offer on LinkedIn or email, especially from an unknown recruiter, verify it directly through the company's official website or HR department before opening any files or links.
- **Check file sources before opening:** Avoid downloading ZIP files, PDFs, or executables from unknown or unverified senders. Subtle Snail relies heavily on fake recruitment files to deliver malware.
- **Watch for suspicious signs:** Emails with mismatched sender names, login pages asking for unusual credentials, or job postings that feel "too perfect" should raise red flags.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0042** Resource Development	**TA0001** Initial Access	**TA0002** Execution
TA0003 Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0010** Exfiltration	**TA0011** Command and Control
T1589 Gather Victim Identity Information	**T1591** Gather Victim Org Information	**T1598** Phishing for Information	**T1598.003** Spearphishing Link
T1583 Acquire Infrastructure	**T1583.001** Domains	**T1583.003** Virtual Private Server	**T1587** Develop Capabilities

T1587.001 Malware	T1585 Establish Accounts	T1585.001 Social Media Accounts	T1585.002 Email Accounts
T1585.003 Cloud Accounts	T1588 Obtain Capabilities	T1588.003 Code Signing Certificates	T1566 Phishing
T1566.002 Spearphishing Link	T1566.001 Spearphishing Attachment	T1204 User Execution	T1204.001 Malicious Link
T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell	T1016 System Network Configuration Discovery
T1070 Indicator Removal	T1574 Hijack Execution Flow	T1574.001 DLL	T1055 Process Injection
T1055.012 Process Hollowing	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1497 Virtualization/Sandbox Evasion
T1622 Debugger Evasion	T1140 Deobfuscate/Decode Files or Information	T1027 Obfuscated Files or Information	T1027.007 Dynamic API Resolution
T1036 Masquerading	T1036.003 Rename Legitimate Utilities	T1070.004 File Deletion	T1056 Input Capture
T1056.001 Keylogging	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1539 Steal Web Session Cookie
T1552 Unsecured Credentials	T1552.001 Credentials In Files	T1552.004 Private Keys	T1552.003 Bash History
T1555.005 Password Managers	T1087 Account Discovery	T1016 System Network Configuration Discovery	T1033 System Owner/User Discovery
T1082 System Information Discovery	T1069 Permission Groups Discovery	T1069.002 Domain Groups	T1083 File and Directory Discovery

T1057 Process Discovery	T1217 Browser Information Discovery	T1005 Data from Local System	T1119 Automated Collection
T1560 Archive Collected Data	T1560.001 Archive via Utility	T1114 Email Collection	T1114.001 Local Email Collection
T1025 Data from Removable Media	T1039 Data from Network Shared Drive	T1115 Clipboard Data	T1071 Application Layer Protocol
T1071.001 Web Protocols	T1020 Automated Exfiltration	T1041 Exfiltration Over C2 Channel	T1029 Scheduled Transfer

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	b40533e67e70b7ff7bb53d34a4b9170e, 67e09818d1aa650896a432b1de54d376, 63080b45ca4978fb5d2d71387dbaf610, 25d3a014c332aaa3adce429d0e714e31, 424f887f651371aa3058cf7c8e908d2a, 8db7338c487143a4d43ed1a22fec49a7, 7d887893a6107d7ae902e6771f30e080, a933c623e3b047292efd55e0e424c732
SHA256	0e4ff052250ade1edaab87de194e87a9afeff903695799bcbc3571918b131100, 23c0b4f1733284934c071df2bf953a1a894bb77c84cff71d9bfcf80ce3dc4c16, 0b2c137ef9087cb4635e110f8e12bb0ed43b6d6e30c62d1f880db20778b73c9a, 6780116ec3eb7d26cf721607e14f352957a495d97d74234aade67adbdc3ed339, 41d60b7090607e0d4048a3317b45ec7af637d27e5c3e6e89ea8bdcad62c15bf9, 4260328c81e13a65a081be30958d94b945fea6f2a483d051c52537798b100c69, a37d36ade863966fb8520ea819b1fd580bc13314fac6e73cb62f74192021dab9,

TYPE	VALUE
SHA256	5d832f1da0c7e07927dcf72d6a6f011bfc7737dc34f39c561d1457af83e04e70, ffeacef025ef32ad092eea4761e4eec3c96d4ac46682a0ae15c9303b5c654e3e, c22b12d8b1e21468ed5d163efbf7fee306e357053d454e1683ddc3fe14d25db5, 4da158293f93db27906e364a33e5adf8de07a97edaba052d4a9c1c3c3a7f234d, 061c28a9cf06c9f338655a520d13d9b0373ba9826a2759f989985713b5a4ba2b, bc9f2abce42141329b2ecd0bf5d63e329a657a0d7f33ccdf78b87cf4e172fbd1, e69c7ea1301e8d723f775ee911900fbf7caf8dcd9c85728f178f0703c4e6c5c0, e77b7ec4ace252d37956d6a68663692e6bde90cdbbb07c1b8990bfaa311ecfb2, b43487153219d960b585c5e3ea5bb38f6ea04ec9830cca183eb39ccc95d15793, 1b629042b5f08b7460975b5ecabc5b195fcbdf76ea50416f512a3ae7a677614a, f8a1c69c03002222980963a5d50ab9257bc4a1f2f486c3e7912d75558432be88, 954de96c7fcc84fb062ca1e68831ae5745cf091ef5fb2cb2622edf2358e749e0, afe679de1a84301048ce1313a057af456e7ee055519b3693654bbb7312083876, 9ec7899729aac48481272d4b305cefffa7799dcdad88d02278ee14315a0a8cc1, 3b4667af3a3e6ed905ae73683ee78d2c608a00e566ae446003da47947320097f, a4f5251c81f080d80d1f75ad4cc8f5bc751e7c6df5addcfca268d59107737bd0, cf0c50670102e7fc6499e8d912ce1f5bd389fad5358d5cae53884593c337ac2e, 3b58fd0c0ef8a42226be4d26a64235da059986ec7f5990d5c50d47b7a6cfadcd, 7c77865f27b8f749b7df805ee76cf6e4575cbe0c4d9c29b75f8260210a802fce, d2db5b9b554470f5e9ad26f37b6b3f4f3dae336b3deea3f189933d007c17e3d8, b9b3ba39dbb6f4da3ed492140ffc167bde5dee005a35228ce156bed413af622d, 53ff76014f650b3180bc87a23d40dc861a005f47a6977cb2fba8907259c3cf7a, b405ae67c4ad4704c2ae33b2cf60f5b0ccdaff65c2ec44f5913664805d446c9b,

TYPE	VALUE
SHA256	5985bf904c546c2474cbf94d6d6b2a18a4c82a1407c23a5a5eca3cd828f03826, 8e7771ed1126b79c9a6a1093b2598282221cad8524c061943185272fbe58142d, f54fccb26a6f65de0d0e09324c84e8d85e7549d4d04e0aa81e4c7b1ae2f3c0f8, 054483046c9f593114bc3ddc3613f71af6b30d2e4b7e7faec1f26e72ae6d7669, 95d246e4956ad5e6b167a3d9d939542d6d80ec7301f337e00bb109cc220432cf, 9b186530f291f0e6ebc981399c956e1de3ba26b0315b945a263250c06831f281
Domains	asylimed[.]azurewebsites[.]net, clinichaven[.]azurewebsites[.]net, healsanctum[.]azurewebsites[.]net, mediasylum[.]azurewebsites[.]net, therashelter[.]azurewebsites[.]net, arabiccountriestalent[.]com, arabiccountriestalenthr[.]azurewebsites[.]net, arabiccountriestalents[.]azurewebsites[.]net, arabiccountriestalentshr[.]azurewebsites[.]net, talenthumanresourcestalent[.]com, carebytesolutions[.]azurewebsites[.]net, medicoreit[.]azurewebsites[.]net, smartmediq[.]azurewebsites[.]net, vitatechlink[.]azurewebsites[.]net, biolinksystems[.]azurewebsites[.]net, digicura[.]azurewebsites[.]net, healthcarefluent[.]com, hivemedtech[.]azurewebsites[.]net, neurocloudhq[.]azurewebsites[.]net, marsoxygen[.]azurewebsites[.]net, nanobreathe[.]azurewebsites[.]net, turbulencemd[.]azurewebsites[.]net, zerogmed[.]azurewebsites[.]net, virgomarketingsolutions[.]com, virgomarketingsolutions[.]comtions[.]com, airtravellog[.]com, masterflexiblecloud[.]azurewebsites[.]net, storagewiz[.]co[.]azurewebsites[.]net, thecloudappbox[.]azurewebsites[.]net, arabiccountriestalent[.]azurewebsites[.]net, focusfusion[.]eastus[.]cloudapp[.]azure[.]com, frameforward[.]azurewebsites[.]net, tacticalsnap[.]eastus[.]cloudapp[.]azure[.]com, thetacticstore[.]com,

TYPE	VALUE
Domains	lensvisionary[.]azurewebsites[.]net, wellnessglowluth[.]azurewebsites[.]net, activehealthlab[.]azurewebsites[.]net, ehealthpsuluth[.]com, grownehealth[.]eastus[.]cloudapp[.]azure[.]com, activespiritluth[.]eastus[.]cloudapp[.]azure[.]com, createformquestionshelper[.]com[.]net, collaboromarketing[.]com, cloudaskquestioning[.]eastus[.]cloudapp[.]azure[.]com[.]net, cloudaskquestionanswers[.]com[.]net, cloudaskquestionanswers[.]azurewebsites[.]net[.]net, cloudaskingquestions[.]eastus[.]cloudapp[.]azure[.]com[.]net, cloudaskingquestions[.]azurewebsites[.]net[.]net, cloudaskingquestioning[.]azurewebsites[.]net[.]net, vitatechlinks[.]azurewebsites[.]net, mojavemassageandwellness[.]com, airmdsolutions[.]azurewebsites[.]net, ventilateainest[.]azurewebsites[.]net, aeroclinicit[.]azurewebsites[.]net, exchtestcheckingapijson[.]azurewebsites[.]net, exchtestcheckingapihealth[.]com, exchtestchecking[.]azurewebsites[.]net, maydaymed[.]azurewebsites[.]net, traveltipspage[.]com, smartapptools[.]azurewebsites[.]net, createformquestionshelper[.]com, cloudaskquestioning[.]eastus[.]cloudapp[.]azure[.]com, cloudaskquestionanswers[.]com, cloudaskquestionanswers[.]azurewebsites[.]net, cloudaskingquestions[.]eastus[.]cloudapp[.]azure[.]com, cloudaskingquestioning[.]azurewebsites[.]net, healthbodymonitoring[.]azurewebsites[.]net, healthcare-azureapi[.]azurewebsites[.]net, healthdataanalyticsrecord[.]azurewebsites[.]net, medical-deepresearch[.]azurewebsites[.]net, medicalit-imaging[.]azurewebsites[.]net, mentalhealth-support-portal[.]azurewebsites[.]net, patient-azureportal[.]azurewebsites[.]net, pharmainfo[.]azurewebsites[.]net, symptom-recordchecker[.]azurewebsites[.]net, systemmedicaleducation[.]azurewebsites[.]net, acupuncturebentonville[.]com, cardiomedspecialists[.]azurewebsites[.]net, digithealthplatform[.]azurewebsites[.]net, medicpathsolutions[.]azurewebsites[.]net, nextgenhealthtrack[.]azurewebsites[.]net, sulumorbusinessservices[.]com,

TYPE	VALUE
Domains	telehealthconnectpro[.]azurewebsites[.]net, totalcaremedcenter[.]azurewebsites[.]net, trustedcarehub360[.]azurewebsites[.]net, virtualcliniczone[.]azurewebsites[.]net, wellnessfirstgroup[.]azurewebsites[.]net, yourfamilymdclinic[.]azurewebsites[.]net, doctorconsult-app.azurewebsites[.]net, managetools-platform.azurewebsites[.]net, msnotetask-insights.azurewebsites[.]net, mstrakcer-tools.azurewebsites[.]net, olemanage-dashboard.azurewebsites[.]net, oletask-tracker.azurewebsites[.]net, patientcare-portal.azurewebsites[.]net, rpcconnection.azurewebsites[.]net, backsrv66.azurewebsites[.]net, backsrv74.azurewebsites[.]net, datasheet96.azurewebsites[.]net, mainrepo10.azurewebsites[.]net, services-update-check[.]azurewebsites[.]net, send-feedback[.]azurewebsites[.]net, send-feedback-413[.]azurewebsites[.]net, send-feedback-838[.]azurewebsites[.]net, send-feedback-296[.]azurewebsites[.]net, check-backup-service[.]azurewebsites[.]net, check-backup-service-288[.]azurewebsites[.]net, check-backup-service-179[.]azurewebsites[.]net, check-backup-service-736[.]azurewebsites[.]net, boeing-careers[.]com, rheinmetallcareer[.]org, rheinmetallcareer[.]com, airbus[.]global-careers[.]com, airbus[.]careersworld[.]org, airbus[.]usa-careers[.]com, airbus[.]germanywork[.]org, airbus[.]careers-portal[.]org, rheinmetall[.]careersworld[.]org, rheinmetall[.]careers-hub[.]org, rheinmetall[.]theworldcareers[.]com, rheinmetall[.]gocareers[.]org, flydubaicareers[.]ae[.]org, global-careers[.]com, careers-hub[.]org, careersworld[.]org, usa-careers[.]com, germanywork[.]org, careers-portal[.]org, theworldcareers[.]com, gocareers[.]org

References

https://catalyst.prodaft.com/public/report/modus-operandi-of-subtle-snail/overview#heading-1000

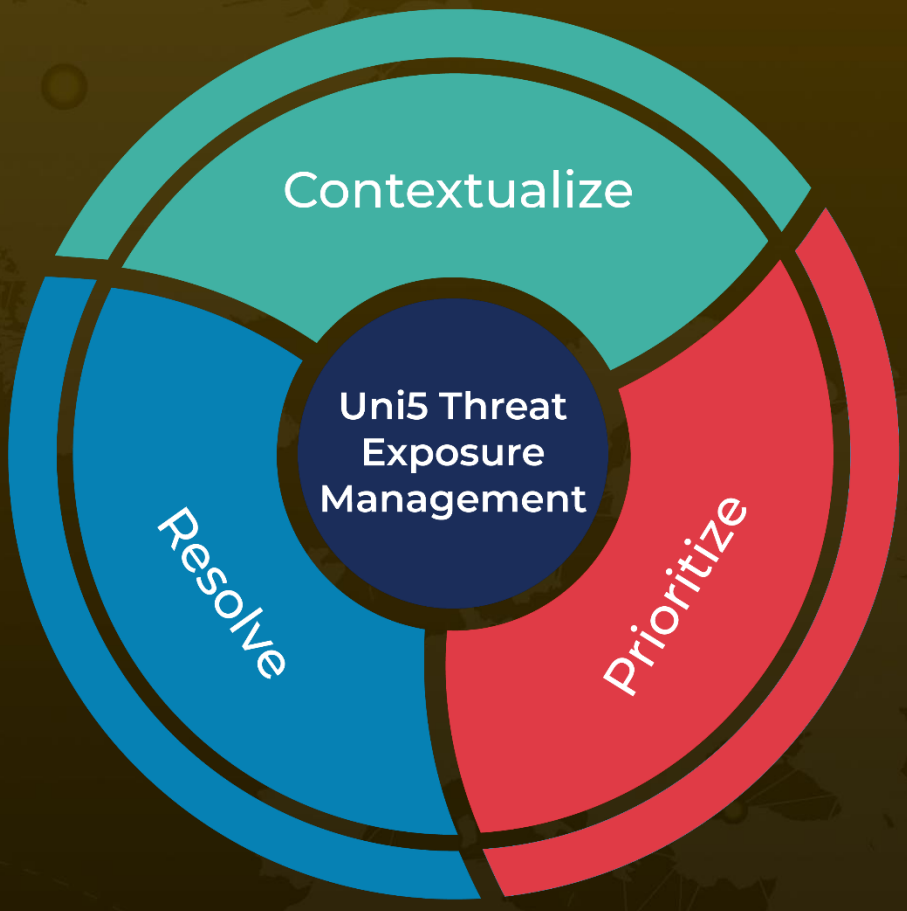
https://research.checkpoint.com/2025/nimbus-manticore-deploys-new-malware-targeting-europe/

https://www.hivepro.com/threat-advisory/iranian-hackers-soar-into-the-defense-sectors-of-the-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

September 23, 2025 . 7:30 AM

More at www.hivepro.com