Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

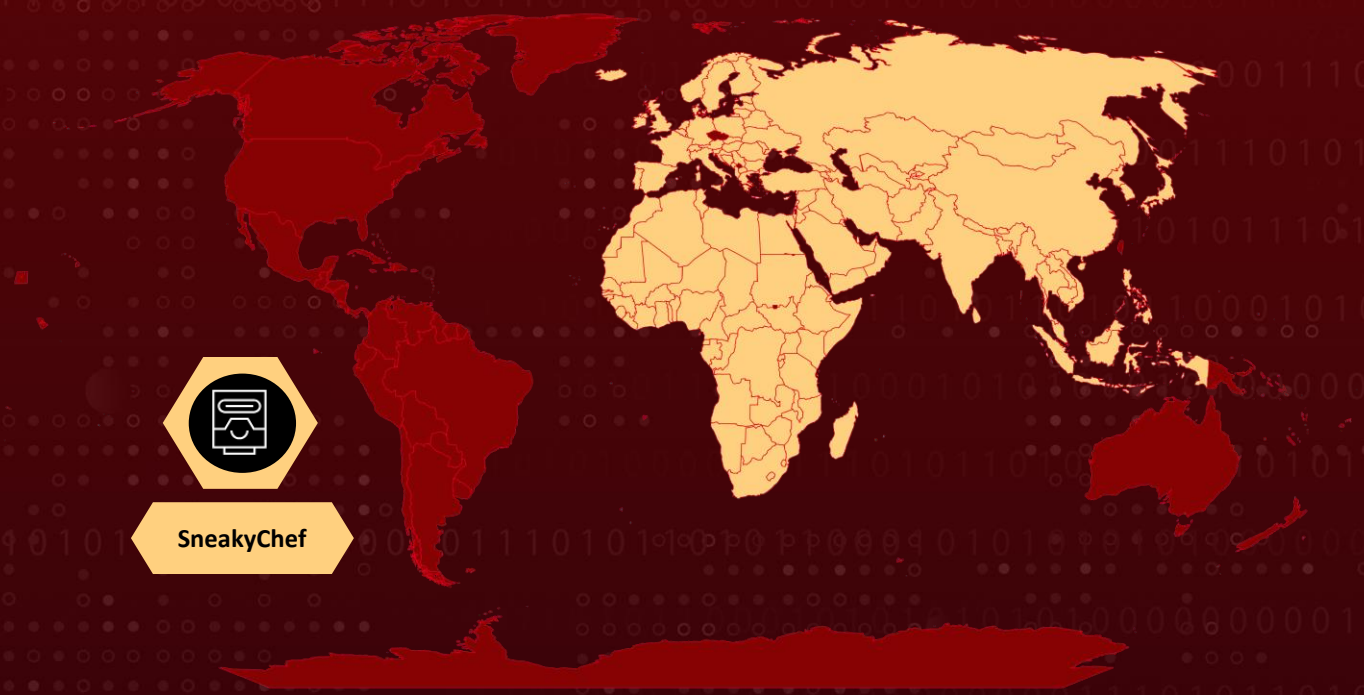
SneakyChef Group Hits Governments Using SugarGh0st and SpiceRAT

Date of Publication	Admiralty code	TA Number
June 25, 2024	A1	TA2024242

Summary

First Appearance: August 2023
Actor Name: SneakyChef
Targeted Regions: Europe, Middle East, Africa and Asia
Malware: SugarGh0st, SpiceRAT
Targeted Industry: Government

Actor Map



Attack Details

#1 A new campaign by the espionage group SneakyChef, targeting government agencies using two novel Remote Access Trojans (RATs): SugarGh0st and SpiceRAT. This malware campaign has been active since at least August 2023.

#2 SneakyChef's tactics involve deceiving victims with fake government documents. Initially, their attacks were concentrated in South Korea and Uzbekistan, but they have since expanded to target U.S. AI organizations and government bodies in Angola, India, Latvia, Saudi Arabia, and Turkmenistan.

#3 The attackers use Windows Shortcut files and self-extracting RAR archives to deliver malware. In Angola, they introduced SpiceRAT, a new trojan that employs DLL side-loading techniques. This involves using legitimate executables like ChromeDriver.exe to run malicious DLLs, thereby expanding their attack surface. SneakyChef employs various persistence methods to maintain access to compromised systems, including creating scheduled tasks and manipulating registry keys

#4 SneakyChef's operations are noted for their precision and focus on high-value targets, particularly within the EMEA (Europe, Middle East, and Africa) and Asia regions. SugarGh0st is used to gain control over infected systems, enabling data exfiltration, reconnaissance, and other malicious activities. SpiceRAT further enhances their espionage capabilities, making their toolkit even more formidable.

#5 The attack typically starts with phishing emails containing malicious attachments or links. Once opened, the malware is downloaded and executed, granting attackers remote access to the compromised system. The RATs have various capabilities, including keylogging, screen capturing, file manipulation, and executing arbitrary commands.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
SneakyChef	China **MOTIVE** Espionage and Information theft	Europe, Middle East, Africa and Asia	Government

Recommendations

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with SneakyChef. Regularly update endpoint security software to ensure protection against the latest threats.

Implement Email Security Solutions: Deploy email filtering and security solutions to detect and block phishing emails containing malicious attachments or links. Educate employees on recognizing phishing attempts.

Advanced Threat Detection and Response: Deploying advanced threat detection and response solutions is essential for identifying and mitigating sophisticated attacks. This includes using Endpoint Detection and Response (EDR) tools, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS). These tools can detect unusual activity and provide alerts on potential intrusions, allowing for quicker response times.

Network Segmentation: Segmenting the network can limit the spread of an attack and protect sensitive information. By creating isolated network segments for different parts of the infrastructure, organizations can control access more effectively and contain potential breaches. Implementing strict access controls and monitoring traffic between segments can further enhance security.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0009 Collection	TA0006 Credential Access	T1053.005 Scheduled Task
T1566 Phishing	T1027 Obfuscated Files or Information	T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter

T1036 Masquerading	T1204 User Execution	T1204.002 Malicious File	T1059.005 Visual Basic
T1574.002 DLL Side-Loading	T1574 Hijack Execution Flow	T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution
T1056.001 Keylogging	T1056 Input Capture	T1218.010 Regsvr32	T1218 System Binary Proxy Execution

Indicator of Compromise (IOCs)

TYPE	VALUE
Domains	account[.]drive-google-com[.]tk, account[.]gommask[.]online
SHA256	8a563b3091b56eb0562f5442c90b4d28d4be2946a3dc4a225b4b96134f7e447b, d6bffa45aa2448b2fb584713395b742e02ef77c1d54f125cd501240e0dd91a13, 951a54d2c61c3257447c4ff5fd451ee581c76d3d4d88fa482b99f5410d7b7b6f, 8db5a7efe1a83e43cb4acdc596b0413b4beb54f9f8e13f978c07a6eeee6b8435, 31b7e97770ffe74dad914a37a78c8f9a7286c75b62b5fae1c4ec722837ad457e, e56537d09156bb77f4821d5ce005c7840ec41890de233d88a1152f68110098cf, 06056f83e93849124dc435166c1b463bf34bbf99ea5671221ddaf6641e3db4f4, 81ded17e368abc280db4d9f83fb0aebe1ec58eb7e4103f98f0fb5269c8696551, 8190e8990bb7bc860691ce2d3ff6015d7f9a0339e77aa7c6e5e3ae5209bd6f4c, 727bcb28eb0282a389bd2c82e3fac57a9c348aedee23d18c8d136bbd8803b642, 0b6dcf9ba14096c631bd9a3f90180c5f6ad9177a8283724146425b2f08b53e02, 653c3ea0ce07880ffe3a2acd735770cc2cbedb137cb5a29d4b059af5a569f98f, 2547f1a874c552da17abf6d5f88e626ed4bda71ca0bb39b2bc13b2d748a05409, 4b1f3cc69e905137263ec8c39bbdcbccd5e33c3abffe54d77de847a998fcf17a,

TYPE	VALUE
SHA256	48cc1d2df6ea2a04201e74ce59983a0bf0964d59a0e5c5647068b653a0ec66d5, 05758a568e30b3f35092b8d43bf4f29a3e5e9b988dc541d51fc8233ebbec2874, a22e16fad2d88de1a625201408b2262d8335bef3d944f4f696ad825973af124d, 7684296728c10249f671cf80b58e04633031e1b74a88e8b4f7d31776fc643d10, 375e0b117c7e45266e9544c23e226dd791ac32d094e60b858ff823577be43acb, 944cd95eaf496ad6dd8859032c4577ad6917dec3a4c300eeca762e08a97243f5, 6b327a15877528e5e5b0891fd587cb2fc932d94404c756401af628195eb94831, 8cd0026ba4f0c8984bdb6daaddb6fa17088e3b9272859cc2c03195d36f47f334, 06ac9bcbc1d026fbe9a261afe62a1b5704dc64b89a28dae47441fa6ef6230eb9, 2432f192511fb377d69619fc7eb0612570e22e3ba88fc42e841552a66fe2dc8f, 53e7e7fce0d8fde3be0d6679193f924555df217b696f6dc201e1966e9f4efabd, ac5342050b0ec85a122846510e06f861960c45613ecc05e3951c57d7d02aa716, 21cf0efec4def4a95af75a7bfdef915bf103a9a6cd03593b4f665f49cdbe4a02, 58754bf9701a39bf13959157db5761d19a562264ac79a8ae47b82589d17a1a07, 5f40142782f5e13334caf25f3038be324b3f47a3ee465f6da4442ec6e7920d5b, 862f6f60d6c145d99fb01476708c93e72f0b905ee54aba03904e92eaf3d8b2d9, 99ab797804684699925b70bdf2ecbbb878f4a86e7b971349036700c72ad15fb1, 653281c876250878eb503e4377c3f79bdfec31e94b27e5413a1b9f8f0f84a6a4, c8bfebff63e5f227aacb3a0aebcf40c973a4fbde6d37895c76498798e925cfb6, cac8c35fd03cc8698e53cafa64941be59870380ecedd2f4998e110787224241c, 18270dd537c3e2f02513b51c3a89814f4c34aa994aa8d823bc534fa39d95dde2, 4509575df3a0a791838f13405122def4eae7f5d2d8142f4830f6944ecd913f03, 823d23f1bcc76b08773e988be209b4a2f1cf99b094732cde395bc40f0729948e, 70359e4ce398ad356fd36f1f9306a570b36c552b83310332e5bf257f21cb1e9a,

TYPE	VALUE
SHA256	70359e4ce398ad356fd36f1f9306a570b36c552b83310332e5bf257f21cb1e9a, e2a8ffe20d91720516b242d0053ae58474be4205b9926993eab13e6662cb9a91, 267eec9cd5ff136364e0346d62df0cbb0294e0fb8f672685e785bf3ffddfb76e, 7ccb9b8964391360d6e122343d714301851c2332f0d50e037fe08591bd7c139d, 7caca38b67f9f629912f21bc0d76f8a5782fc62cccb93f53d2d07fd21fd30c33, 66f2712d989950e3b6c1f56a08b2e8689ea8a48bf84c7cee93583c7e78591f3c, b9a60ea9b1ac73e333b403f8471b5111a0ba67b60c9f0d7e44e2e290fccf6f42, 837164909df9b37bc31edcdb1207954337bad59a630b44f8ea06a594bcbe4035, 4cdc33e535d07e6519b1be0520349dedaefcc464734b24d1e656414100680efe, e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855, d31b5dd937655c14caff1cca6da88dc81f9cc523e119d43a9ac38dbb302eebbd, 21123d5bf92e763c4ef34fd4f9ddcb1b3a4a2c9ab0fd5657f4f30b0964979274, 75b39e923c69b488ae6981d314075f7e423ba2236150c20d41112db8f80a4827, 6071f84650b3226f60068f5f7a1dc7c7ec819ab7b6e8dcf341638b966fda44b0, 510acd67d4c5fb45d6721283ed0eb4128347458ccb2b00feda9787f138c35278, 4f98dc3df220f41bce3c3a2714392279e68dd24a53c7c2f22a0a9850eb5d8476, 2e2aef8948f5e2d93df7f4412fadc31500feb9035ceff18cce85393c6e230088, c0230704e1ee34666c40b2a3898666ba3929283ad0a86b63ab0fad6f4a0555ec, f7de8e94f280f9b943950a75ae78032c6501261a12650a6f757107bc8df6c3c2, bc73528b391f30acdd3c3a1674bc7973d3026c367142d72684facd68915851f6, e11908adf04627812cfa721189dfa06f884ceedff2dfa3b18578494995561716, 0fcc045db0d07ea4909a487273d313f796fa19ee8095a5272dfc5d6f3484f4ec, bdcc0bc3f5d022f99a1599c7cbed3aa2b6839e1e1d05ed2448dbd8b7ab34c784, 065f10e2a92b433a779c508e4add9c096b2891f5417fa183e58c8b8f7f9f8524,

TYPE	VALUE
SHA256	87bda94d6b5ad0170c07abe540f530e797c6fec7410b30796e265cc21997d735, 401720fa24dc03cce8640b00d00c57676a8369ee49f456bd771a6ecbd81b82b6, 84572497f7022163bbb2e9885c942b1bcfa1793305c116ac898ee1b52ab6f898, 2f32e99c182f0f7cf6ff54d9d1a9d9f7e59823030d2a89e15890c2c8b1612caf, 57e3c92639027738e5a867d2f66d30a9509a96573d7a5eeee1c2a710faf9321c, 7528cf4daa8f0b4108ff220bc98f6046faf446653a3f98edc1d58350490d9fc8, b89ebfdfa9abb0ab618ebf2baf66b6cf27929d1e6599b3cb174c12e0a4c71d96, 6f8ccda88e0ff98c781ad6e027f4294eb54bff27a3ca1cd72aa83e40820138 60, 162594cdb38526300af0db4acd13dd7a5a4ac07004bf32f887b6f149236160b7, f46b2a57ee2904ded87f6db77ed4373bfd71de12879bd939348ccb8fa8cc1403, a77789f32058b879d7e3831d2d20a885996b8f07694a954e1e717f0483660ccb, 984e8b3dda2c87bc8e3d21a05b07a8f52799c99aa45584aa2671efe62b5184c2, 3f23d9ffc16c5f455f7bd02bf57667efb3d0a645ffa13fa38e0a6f5022208dd4, 4e18b57c586b3bfb6bd825ecbee2bdfcce91c8414e40c0a7655edc327d62ac0f, f4ffced2a4c7f3e48f2a43e17e58f8feb0ad6cb2ad98fafc87d9a159230810fa, 9483bccb2b0964d11b13ca01fba7ba6a21a531807d48eb3182ceaf7ed240ef2b, 26f92ea9f5eb220d9e544af757c57e5672971b9cd43b166e65c055b6978d6031, 2c8116dce38993762cdb687eab69786b9ccd1bd8c569dee8bef5a226579224bb, 4bcf097c19e18e3b3bfa4c45ebb4e67d565a0984211edf9e2fdc042b43141317, 67b648a7f0d24e5b56e83f73f9494be6a63f4d7372c960a2134054352c9c3490, 9ce558dc6af9c183d15012a5012a36184586e40f8a461a948192c3f055201766, b5953319cb28a0db7a70dff03949f1d98487456a273ac3cfb1f70f8cb3b07c18, e4b8fe0b0a87e5844deee4668d7638acd3ab9ea60a947eb1b32a4bd0691e5411, 7fffe1969dee2b4c72b4c5d0c75e493ecf6f3598a89d8538be3e7c53b898bbff,

TYPE	VALUE
SHA256	6cb99d0073d2e6b7e15b22a74b98901dccb3c328d88f6e1c38b0af0379dd388c, 5a3811aee5156d928b2b634b512d382d89f8203cb883cab743a54cbc4f3f41f1, bfcfa5e291b0c9201344a73c8ef25c2912561e32c48af0ae0d30ad8199ffc8c4, c4a912f776579aa0126bbadd9261a4cd6efb3bcb5f5c7d64e96b11f3bdbc214b, f92c275dfd051481cb03557213195647dd7c68edf9f7beddcff0aadf298f371b, 1b14de17a12cdb92210b8543e3418c16f9fe00db3394fa74ab3a8f1c5904ecf0, c4e2301615cbab9abf2d94327bb7839df64d88fc5c508a2f33c3f0fc881be7c3, 066b3631682f63b4a44ecfa5b6dfb100d8052429a7e1c5b1ba8cab4832529f26, fb76bc19e177372d210bcfe9b1f35fb296b0b7cb64f0ad5075a64d06a3c85159, 2c4356614ddeb8085367167b301a8e437166142e738adb27bf26c09da3acae56, 4b1b7257fd376286501043eb27debc850300a674962068e044a34e697381d694, 0618b63352d0ae02d0f02ce8adf02d1c16fd56b18e903622bc95e520388743e0, 792ca7508ce158e20eff7b838fafb6120afc81b3677a84eb066810544ccf1577, 49fa747eee1bebed9bbb74b7b555f8018fb4e0e11f74349c2f7ac89a225d27f8, 1b9604b50e8c0c6cf2496855a3c367d72fc447839fab708b20d649cf276f572a, 698c73f004e7f46bc371e0476193456071d9f7df9662cca7aa0e010b4fcedf57, 0986b26fcc87723d73e80c280f1bbc221fdb188ab8666f098caac6d896f1c4d1, 27ace9002f5bc7b3474ec3ec7ac72ed094fa2d29d9b2e8b5b1a787b50afd4f05, e498efd08ced0eccaebc4721cee807858d40fde428fd5ea61ce06272a25282a0, 26dfb13aea6f55e01f4dc54bb91ea7d9afd3bd73bd0c95b63345364ed149ff80, aa58e1b322877ff660961e18558488c49491a523a12373f95c41a1dfe60ad477, 43c40fe84b53b2573564331db15f5fea8cdf599d6c9c2f361dd154a9b78cd6aa, e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855, 3df795503a11b3c1a7ce3aeaf72f436ec9d7704c8189f9aa4abbc4f6db69d155,

TYPE	VALUE
SHA256	f0f587aa4eac787e4caf5f4b8795b7cc8a4c33fbb518ec2d616516076570f393, bae38315e5a6622d01b66db561efa206e698f3cb6157645dabd4f0267b8d2c91, 5779a2234b05311716259837998997847d56cdcd421cacf0a1860bbe4ba70b79, 35a9c2e8d911c8793a4b464633beaa2c6772601d6d58bf12c456e694a4adcf46, 220dd9d5ba1c6e087c8294eb01b7e0dfeb39b3a9c99567da102df44b2f04dbd7, dd4fc4760401b8dc37b0a823af19d0f7b5c2039704caf5327f8f8c6d00bd148c, d18cf366f549a8828dc02e6540a191b3625da36995806dab559d6b020fe74695, db6a8b9988ab1b83d8c1e6b5bd0a4bbf2baacf1ed84220026f9ae8a867e5eec2, e121a6c8cccecbe1a27c2003c255096f04c23f13b24a1f035775348f2aae53d0, d18cf366f549a8828dc02e6540a191b3625da36995806dab559d6b020fe74695, daed820a32723e146e762343d0a32f041d21bd2e603b355b2f91d0bc7d98927c, 41bb112c6d4c609d53111ad1bb7cc687ec8ab848b6039c7a8eb64fee311b0822, 1c1499485254acb0d94ec6b4ffcb0c33d1dc154b5d95cc433a44c8bbb66c718f, f87c6b520253d9d6b14a443ea2096baeb8cf532e9cc8843f39e6168cd873669d, 4f02b04252b268bffdc6584ced29254209fcac4ba7388527efa43786cad17aaa, 33dc74a86e72a353412da885e5e07fe64b65f1769fe7ef17aa79b6bd6b36d0dc, f7cbe4349d4f95bbf08e1d649490fffe85e345976467bd1e0a066acfd3c2bb35, 88c6525924bf306dc21aada7898084622bf6a224465123025a53b1c187ff8ae9, d18cf366f549a8828dc02e6540a191b3625da36995806dab559d6b020fe74695, 3edc38bb3ad101f6e56d99e4c9f173c16346315ec7bb36e3d7f327dbcbdcd606, 502a08fa74475ad5affeaac4a0f9e491df59a20c97796ce88284e79821ac8483, e71d4f329b7353f95f5f13f3fd33c4727f9f06f96083e199c18ad3cf1a2351fa, 6af30df6ee33ee44e93e34aed5fbe80bef0e7d1832d96f60c61e3eace5df315e, e71d4f329b7353f95f5f13f3fd33c4727f9f06f96083e199c18ad3cf1a2351fa,

TYPE	VALUE
SHA256	65d96b763572ad2a7a03ab964225414de9fc7f4b820a603ef3f94f9203fbe4b2, 502a08fa74475ad5affeaac4a0f9e491df59a20c97796ce88284e79821ac8483, d3da04c58d81445754a4a837f3784e5fa7ec54ceeb8e595a836e9b87dc0c39cd, 44bab852fa3bbaec1a03c900a8dace3c3553bf3c8289e5ffe9457633af0ea74a, b02bc37b60170d53ff9d17ae0f75e6df5cde7287cede634bcb0042545585dd90, 948ce1b8169805870338a59415ef470029323fc824a84bed9a760b2d78affb44, adfdf33b7f14b4509d1d1ec5155bb57ae381b6a04ebc97281a58d3246d7abaa3, 1a11ba0de41e053025e98f64d4b6ac044f6afd0db00fb91f97c447a4e63a5e78, 17c6aaa3efc51678cf4c269ba99e62859967c5d2a6da0303e66d60c1e04b20b6, 638ef4333b1b2993e945dbbc57f8a2a2ee0ab84bf02ef11a6a343a07f6737784a, f7cbe4349d4f95bbf08e1d649490fffe85e345976467bd1e0a066acfd3c2bb35, 502a08fa74475ad5affeaac4a0f9e491df59a20c97796ce88284e79821ac8483, 35a9c2e8d911c8793a4b464633beaa2c6772601d6d58bf12c456e694a4adcf46, 40bd419635471cf6c8df65142cb1cadfc1ed88bb6f9f921abbdaf5041503bc96, bf30f0045791417fa1e691b4974d5651ffd4310a536f30df325fe89365f1fd70, 15929ca0bf26f189592cc6f2ba7fae8d10b0d84d86ecce2f74f583f7ebf849ed, 832225013088d9619cca1bfc3192652fb434a2442ec33316342969c330b46825, 1cd45dac19c6d340f604546504393060d9b313d5b16a85f947e19daebc41dee5, 1073bf25ac3af08cf3f48c2cbaed489ef43671387211d6e63f96aa7fcf1ec0b3, 543a1c4db82edce36ae07e4836b4d4a7640355bdf728d5ed41370892bf97d8a8, f7cbe4349d4f95bbf08e1d649490fffe85e345976467bd1e0a066acfd3c2bb35, 33dc74a86e72a353412da885e5e07fe64b65f1769fe7ef17aa79b6bd6b36d0dc, e39a3ceb034e425f4554df867871bb7c5df43ba116dea05b173c4bd444789aea

References

https://blog.talosintelligence.com/sneakychef-sugarghost-rat/

https://blog.talosintelligence.com/new-spicerat-sneakychef/

https://github.com/Cisco-Talos/IOCs/blob/main/2024/06/sneakychef-sugargh0st-rat.txt

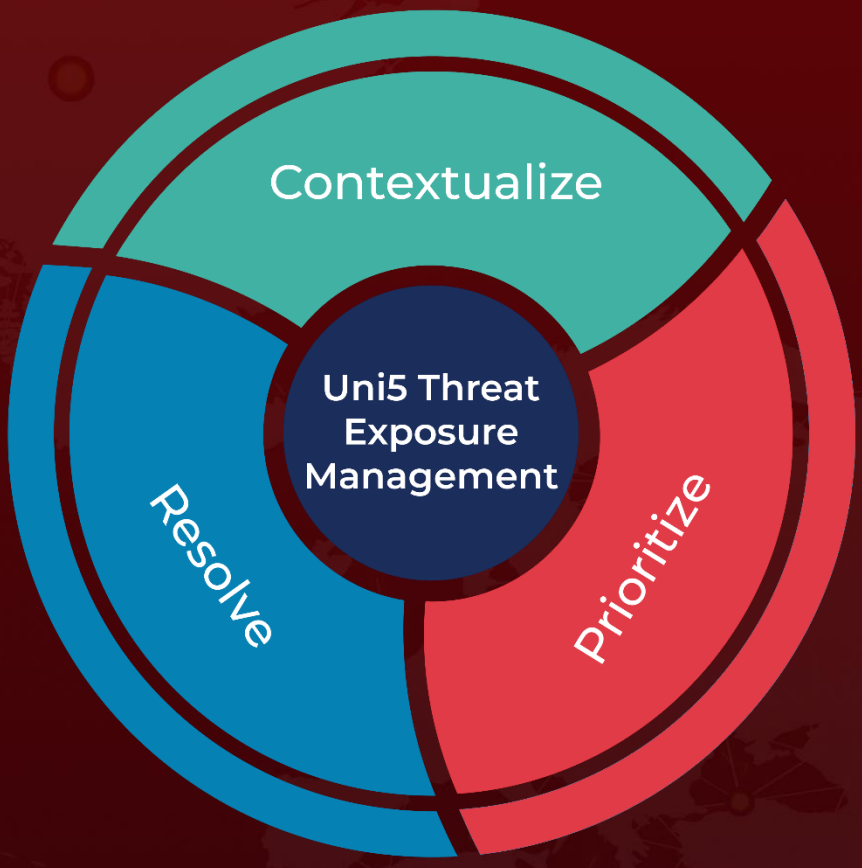
https://www.hivepro.com/threat-advisory/sugargh0st-rat-a-customized-gh0st-variant-in-cyber-espionage/

https://www.hivepro.com/threat-advisory/sugargh0st-rat-infiltrates-us-ai-sector/

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

June 25, 2024 • 4:30 AM

More at www.hivepro.com