Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

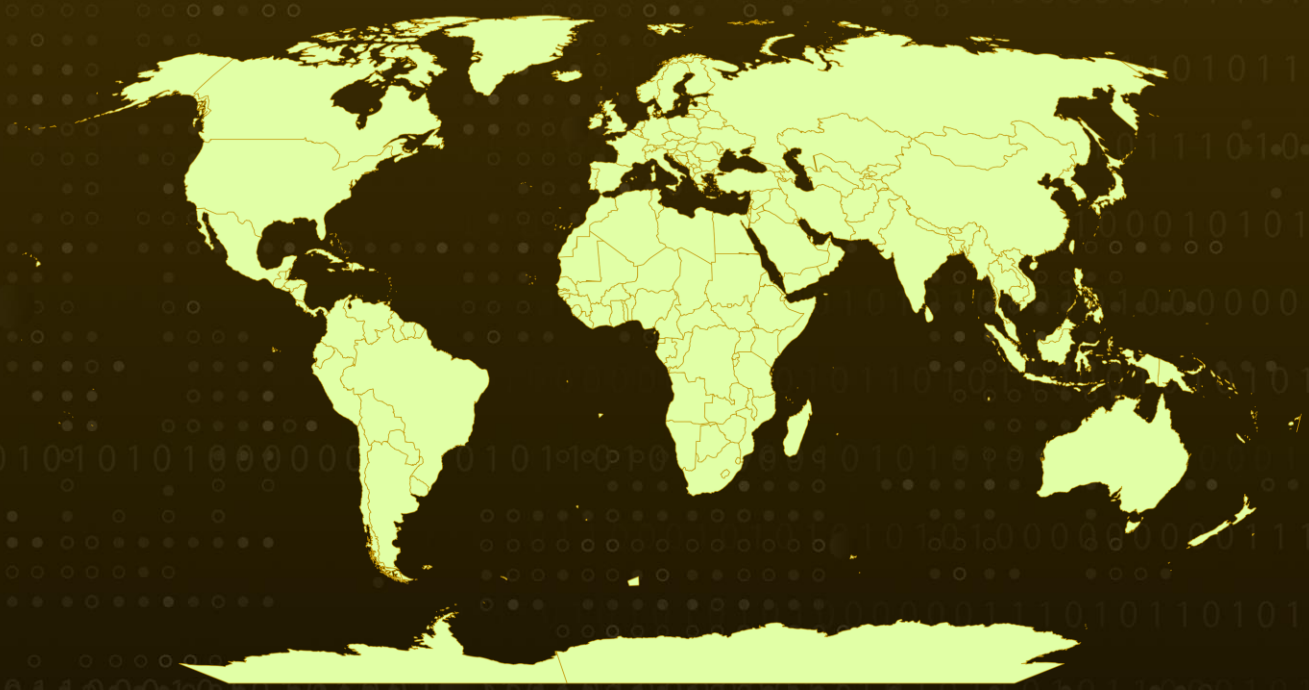
Ekipa RAT: A High-Priced and Evolving Threat for Targeted Attacks

Date of Publication	Admiralty Code	TA Number
December 23, 2022	A1	TA2022313

Summary

First appeared: February 2022
Attack Region: Worldwide
Attack: Ekipa RAT, which has been designed by Russian hackers to exfiltrate system information, execute commands, and upload files remotely, has been sold for 3900$ on the darkweb.

Attack Regions



Attack Details

#1 Ekipa is a remote access trojan (RAT) that is used for targeted attacks and can be purchased on underground forums for a high price of $3,900. It primarily spreads and operates through the use of Microsoft Office and Visual Basic for Applications. The trojan also comes with a control panel and tools for creating malicious macros in MS Word, Excel add-ins, and MS Publisher.

#2 A remote access trojan (RAT) is able to gather information about a targeted system, such as basic system information, installed antivirus products, GPU and CPU information, and more. It can also browse and download files from attached drives, drop files, and execute files and commands.

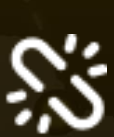
#3 When used in conjunction with malicious Word documents, the trojan's primary functions are activated through a one-time VBA macro template. When the document is reopened, the server denies requests to download the macro template and any subsequent requests for installation actions.

#4 The Ekipa RAT illustrates how threat actors are constantly evolving their techniques in order to stay ahead of defenders. According to research, the creators of this malware are aware of changes in the security industry, such as Microsoft's block on macros from the internet, and alter their tactics accordingly.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.



Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0011 Command and Control	**T1566** Phishing	**T1102** Web Service	**T1548** Abuse Elevation Control Mechanism
T1104 Multi-Stage Channels	**T1059** Command and Scripting Interpreter	**T1204** User Execution	**T1036** Masquerading

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	03eb08a930bb464837ede77df6c66651d526bab1560e7e6e0e8466ab23856bac, 0661fc4eb09e99ba4d8e28a2d5fae6bb243f6acc0289870f9414f9328721010a, 8336260aa342272f92b12050772e56b4012c848f58707e704a32ea3705de30b4, 0b76f4c321ac5193890c4ae32f542e0d95fce42ff9aa5bb0ec4b7d4be932d2ec, 2826e891fb9d9076513005f39e036a9d470b59d6eeaafb71e7ccbd039f349ba5, 3e74c248a6e2272e0fc9365ce79188241ed3d3924bfbac7ae31caf5ae336b4cb, 46b899d25e3ee77572a302859e1177cd0cd4a474e4b31e4f1e2cfc0e9a753a98, 535561be76de14d3d6724ad11ed1cdbe914388d549579fd7f7f0c6fb09431d47, 563537a99531e62a4e8b7c7e9a15f966e3d22c724d4b83e994a074539ff10159, 624ea33f8b92dbc98ff07d9c225863ac323a4cc08a5f3599d753efe0c9332409, 64b131ff403c716d4ff9d4c749e8c7152e6c42f6eddf78c307b0da5f1321fc1e, 7324f089604e2722860322ce2178692ce9c20c409f31bda6be08e2467bef1d1d, 765a06387e3da1b3870328eb062864a97b02d047f5d2f08ee39890f8d77dc61d, b91e10c2c01b398dbf27df0274604b8efe78e0a51f947ade9ad6d198df5c31e5, c117df5fe9bd83998c1e2cc1f0bc0bc4ac8a567b355c1fab515f1381c4c0e52e,

TYPE	VALUE
SHA256	7a03e24535fd73a9e0f98ea692ea802c1e0af3067ae1205a3bcd44314666c393, 881f38d91652fade6494e59cc8baf4f64508a8daf0f5bfba5328da1d409f107d, 8c6cfb7e620d57864cbbd55a982c2002a9bf2e6691a40bd08faf53288c54444d, b10b48212b256951e69161a4978e5f32a4e402e3a3f69afa67cb4a0546cb62b5, b841d0004f4692dd7ec85e661e2e5295199da11ff8d1013ecacdcbf36c33623b, ba7c39cc4e349a852241b929c6046734ab3a8a94d19d0b8abb8f25023bbebfa0, c380a287cc6198feba0e707049031a2f3c606dba1402a9dc3842d861e9023de1, c9d2ddf2bf879d165329c5768e256175e972cf5dca589d9ac35e46a037c22877, dbb7f05e55fa575cba2c51f2507278ee1e97d92bec8839501e9fef5ffb261c4f, e03d018812cab38bd0bf1ac6dfce0131638ce809e2070df4e80546a1635a8159, e20effff374b2a9c9422d438c833d875232f30f55e21e359b18a8801b905058e, e345e15b73778cb5739cb8d5cb3d1697c825904490c2c57c95b33a12d5219cca, e617877f439eaa4fed535e05afae96d91d7e483ae7d3a5b64d487a74f2071461, e6ecb28f57fff1548b46869a15d5e684ba21fd724f833292438bdbc11b43666e, f07946d42ae26e19657c0e13b58650bc003d4232238198d0edf870181c3015dc, f95c757e7bfe75f440120f60671f6d00c7a94f588e5d5fda0081dd819e685060, ff18d3bb78b00e501628725dfa4b1ec1e4e65ba48f45b442142ccf420993a4e1, 619564eb8a89522cadaba85060221052612bf04c3199c10580317a1e7b1ac381, 8c45ef0dc9b48205924b93c0c30e617bd6b5daa5672d67a72504d2c8e586f84c, c18b825130accac6ec129c59ba06e74350b0255856f7f59b437ff20f2a789c78, d77ac3175bfa0c7832111099be004b06ca9569101b07611d151c845ddb268db6, e7434bb1a8f57230f689f0809aee05340af46ff8e8c05b6a7a266dc57b6f14cc, 5d12d567c4d85657cce63bf73868eda9b98f76b91cea6cb1ada4840a53314061

TYPE	VALUE
SHA256	ce792512a4a2a19f2c43582a6f44cb11a9f33afa5f6cda9e4e78529ce1c653de, 72933000d4e210b981de3f768af24bcb6e545087ba36ca0c4bbf9c27a4962fc6, aa25233e5566d73102fa499f1ffb928af566c172ee89218ed9aa42e4edefcece, e587b272d96ab772dada266f8f580e342fcb84e9611b7961f3e1aa7dfbc37415, e7b68ee7b73b4d0debc5342fcadfd64598769d67af6b13909dffeee0c284ee47, 9bfb2393b5985577ba223360e24a398fdc93914243414a3350d3faee809135f5
IPV4	146[.]70[.]87[.]218, 146[.]70[.]87[.]148, 146[.]70[.]87[.]186, 193[.]47[.]61[.]182, 185[.]246[.]220[.]149, 185[.]246[.]220[.]148, 85[.]208[.]136[.]130
URLs	hxxp://146[.]70[.]87[.]218/load/6.bat, hxxp://146[.]70[.]87[.]218/load/doc.dll, hxxp://193[.]47[.]61[.]182/load/powerDEF.bat, hxxp://193[.]47[.]61[.]182/load/uac.bat, hxxp://193[.]47[.]61[.]182/load/1.bat, hxxp://193[.]47[.]61[.]182/load/2.bat, hxxp://193[.]47[.]61[.]182/load/4.bat, hxxp://185[.]246[.]220[.]149:10443/work6, hxxp://185[.]246[.]220[.]148:10443/work5, hxxp://85[.]208[.]136[.]130:80/work2
SHA1	9f8b39480505b822c0a34f60f0604a681c25e329b603f8b8088d7f291c308b39e322156d6b142647e61f22c6929a2c0850433cf9c4fe37db367e9741b36b58d8c236ba55a7e3513fd59d39c75356a52f4ad293fe645ca18db71273771418f44045246a95de6022d3bd254f4e8f4604364896024921a0b23d84f75e845452759d

References

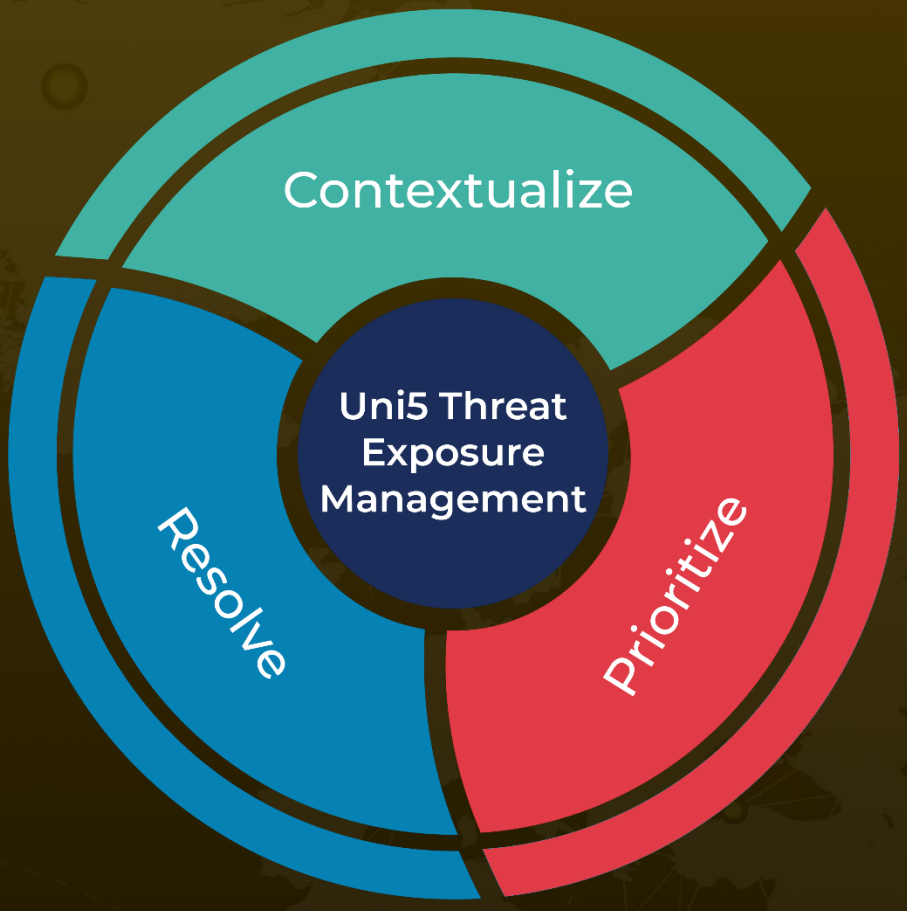
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/malicious-macros-adapt-to-use-microsoft-publisher-to-push-ekipa-rat/

https://cloudsek.com/threatintelligence/ekipa-remote-access-trojan-designed-by-russian-hacktivists-for-targeted-attacks/

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

December 23, 2022 . 1:30 AM

More at www.hivepro.com