Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

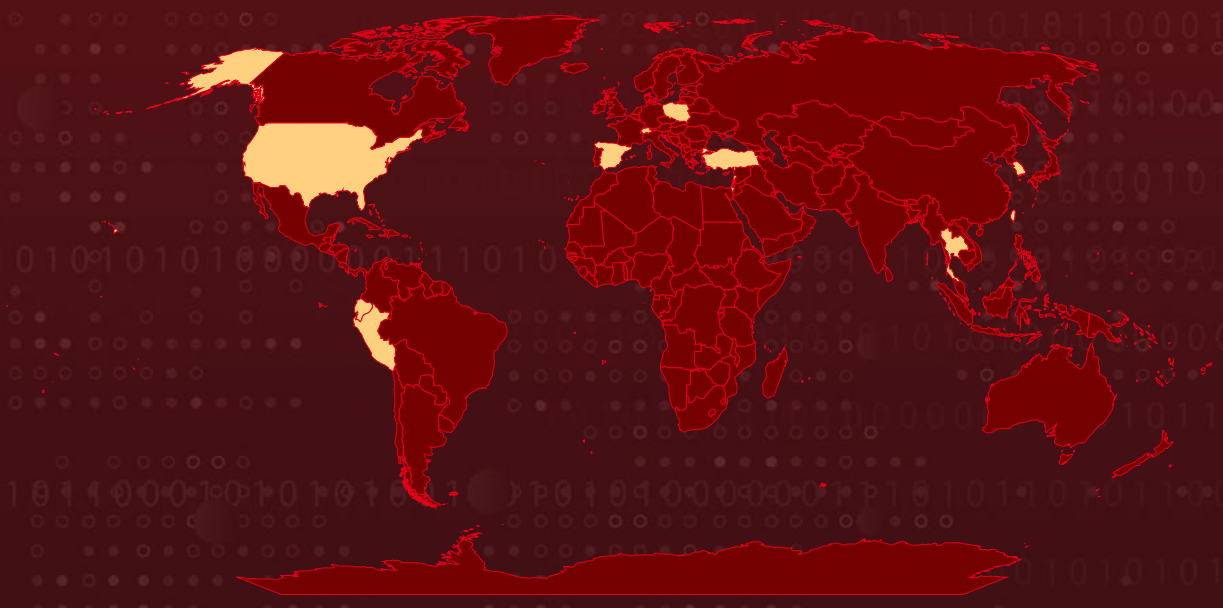
CopyRh(ight)adamantys: Unmasking a Phishing Campaign with the Latest Rhadamanthys Stealer

Date of Publication	Admiralty Code	TA Number
November 8, 2024	A1	TA2024422

Summary

Attack Discovered: July 2024
Targeted Countries: US, Spain, Poland, Czech Republic (Czechia), Switzerland, Malta, Andorra, Liechtenstein, Monaco, San Marino, Bahrain, Israel, Lebanon, Hong Kong, Macau, Taiwan, Chile, Ecuador, Peru, Thailand, South Korea, Turkey
Targeted Industries: Entertainment, Media and Technology, Software sectors
Malware: Rhadamanthys stealer
Campaign: CopyRh(ight)adamantys
Attack: An extensive, highly sophisticated phishing campaign, dubbed "CopyRh(ight)adamantys," is currently underway, deploying the latest version (0.7) of the Rhadamanthys stealer which uses AI in its latest advancements. This campaign skillfully impersonates numerous companies, with each phishing email customized for specific targets and sent from distinct Gmail accounts. The campaign's adaptability is notable, tailoring both the impersonated brand and the language to align closely with each intended victim, maximizing its deceptive effectiveness.

Attack Regions



Attack Details

#1 Since July 2024, a large-scale phishing campaign has deployed the latest version of the Rhadamanthys stealer (v0.7) through sophisticated, targeted attacks. Known as "CopyRh(ight)adamantys," this campaign leverages brand impersonation to deceive recipients, alleging copyright infringement on social media accounts. Victims are instructed to download an archive file to “resolve” the violation, which triggers a DLL side loading infection chain.

#2 The campaign has launched a fresh wave of spear-phishing emails posing as legal notices from well-known companies, mainly in Entertainment, Media, Technology, and Software. These emails claim recipients have misused a brand on social media and demand they remove specific images or videos. An attached, password-protected archive supposedly contains removal instructions, with a link directing users to Dropbox or Discord to download it.

#3 Phishing emails and Gmail accounts are generated quickly, likely using an AI-powered tool. The attached archive contains a legitimate executable, a DLL, and a decoy file. The malware quietly loads by adding a modified DLL to the victim’s Documents folder, disguised as a Firefox file, using random padding to change its hash, allowing it to bypass hash-based detection. Rhadamanthys modules are then injected into system32 processes. In Stage 2, anti-detection checks are run before connecting to a C2 server to retrieve the final Stage 3 payload, which is equipped with advanced data-stealing functions.

#4 Stage 3 brings Rhadamanthys’ latest advancements, notably the ImgDat module, which implements basic OCR capabilities for extracting text from images via a local, pre-trained machine learning model. However, it has limitations in precision, lacking support for handwritten text and only recognizing common fonts.

#5 Rhadamanthys has connections to both nation-state actors and financially driven cybercriminals, but its broad, global targeting suggests a financial motive. The continuous evolution in tactics makes Rhadamanthys a growing threat to organizations worldwide.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Limit DLL Side-loading Opportunities: Deploy security solutions and policies that detect and prevent DLL side-loading. Use application whitelisting to restrict legitimate applications from loading external DLLs that aren't explicitly approved.

Monitor for Unusual Network Traffic: Track connections to known file-sharing and storage services (e.g., Dropbox, Discord) that could be used to distribute malicious archives, and apply controls to prevent unauthorized downloads.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0011** Command and Control	**T1566** Phishing	**T1566.002** Spearphishing Link
T1204 User Execution	**T1204.001** Malicious Link	**T1204.002** Malicious File	**T1574** Hijack Execution Flow
T1574.002 DLL Side-Loading	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1036** Masquerading
T1027 Obfuscated Files or Information	**T1588** Obtain Capabilities	**T1588.007** Artificial Intelligence	**T1656** Impersonation

T1218 System Binary Proxy Execution	T1218.011 Rundll32	T1001 Data Obfuscation	T1001.002 Steganography

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	198[.]135[.]48[.]191, 139[.]99[.]17[.]158, 103[.]68[.]109[.]208, 95[.]169[.]204[.]214, 15[.]235[.]138[.]155, 15[.]235[.]176[.]166
SHA256	d285677cba6acf848aa4869df74af959f60ef1bc1271b4032000fcdd44f407f2, 2be6ad454fa9e87f78dea80d2855f1c14df81a881093a1a0d57f348377f477a8, 9ef9c88cef51ee0fb77ea9a78dbe60651603ef807ddb6c44d5bda95cc9026527, e8aa9a061c6ea803faaf4c8d7a80c6886b4ee73d9a89a9dc6e87e3fecf7a6851, b1ac4ad92045e935c132214015188d27ec4382f930d0152dfb303695b708b38d, 00086cf4f35b6fb7f897cfa2f0d5ad9876aa9819cdc87416c798005ce901d3a1, 05e02f0f9b8625fe3959ae1219f31b0167d787fefc0a9d152edf6524d6859590, 0a3dfe260dd7b038ddb8911689c899541391c188aff966261e7bd9d0280d153d, 0b9bd95d815af9ea4a59840ef6fcdc7ccfd0e239c40974334cb4cfb41df530db, 0de8d2d3217cebd37a2fe488713d1c288ae5a63d3d3b2a3495e2e636ba6a1f89, 10eafd75429ffadee2384acd37b0d4e7ca26b83666e6786f2acaf1b1c29c3f17, 12b7390835f30c1bcdeddd258e49684c98133cee4a6a2ccab869785567deae4f, 2a276ca5b2e095cdac7b24e58b3f7a67cee7db2fb5c1568e4775909265c7e914,

TYPE	VALUE
SHA256	2aa58fa8d71bd2b4fd1ffac16a6461191bbf6f4b2c97455ae52800cce929a0f2, 2e0c99758432a3759b5af6f190ec5cb72a5a84c977d8883dcf041c4de003f3d3, 324dfc7bb75f27e6fba8d67dea67a63525efbe947bf8e29ef39980c6efc1c3f6, 3448005600ccb0ae52443a4c227a657de9cd767b389e9a1ed75ef074709981bd, 3de252c9023bc8920d77570acdfe21813532727af3f91d59af35fa8abcd3700f, 3ecf2838b2e07e6d329d45cde7d0162ba47fea4b94bacb24838358314daed756, 415ee9b12002f17ca4f36bef794fdb19884e22980e21bf8a15043258624c439b, 416f3fa48b75ab168e3373dae77cab7f4702de5158835d23a02629e8c1d20156, 41a3edb3a8e8d5cf093cbd02791911f6ee26df39a377fceb6b101d66a7b7aff2, 4b33219c5cadb4d741044874f6f0184d45f43891d28ad5b489716d4da21310fd, 4bbe0f6b5488a51295b15d8144d0a1c9b41bb86384299b88ea48e88c76704f52, 4cbcfa2a8d56976eff1e8ac0ef4d7703d0b802f227975a0cc36f3dcd3a90e73e, 5cec33e8f47855da3c4ce1f3953d750275864714b16e08a94605bc3889867caf, 6044e08402d1abd52991f5c6a4749ba6aa29a0587ff196edf60b38862392e855, 623bb3f1f476c37afc309d6c0ab89e216aaedc03b8a7ec1aaec5fb5085d78a97, 741dfdae8948f3e430a5b7b66c8fb4b8a750695b67a84a12abc0b6089e8fba31, 7990765022c4400a45f996046971b9e6b69cca5b06f8d2adb61bc267fd362197, 7d7a3e254b7968400a301d83fcd44a69f655386b9b95998a36113cfb2e542720, 7dc07b8aa268485e40ab78bfbb03a367d80ebd7b2c6c74961dc6842cae7086e1, 7e270a80cd0f04f245309e8c75cfc2cb46dc075ba01a00b30f66cb8b5deaaf3f, 865a4f2583679f7a40357b61301d75567cf516a5b8295dc8155e6d4aa2ce244a, 878917b6a8d241031fc330eff771f416a9fffaecab42c39d57e58ac2d8f38f11, 970e199e40511e90d6dd5d6f3c9f3701215fd881b1273fe2617bd44444b0bee9,

TYPE	VALUE
SHA256	9a249dfdc2c16700bc5add2455f2ed00e47a2610b7779cc33e40aac576a2a74d, 9abf9fb94e2529d8819a3873f2025bdd90d14e75fe4af81e489f6d0560809f9c, 9d10835f7717c89d17886b7e59cc2dfc9133bfaa044bad5f070e1c8e1212e257, a03d2956ff8d0ae4d96c9e6cced79b335b70eef10feb0f7202609cb8652179f6, a064bbc4b58642ab4d7118abc55fb81db6584cbc633800ad14048e8370a95ef2, a15d0aedc8b4e54a170b6ecc3d9a06835cc499f07b05c6ca261081ace505debf, a72083974e886856b7d985bdc79888234c8cd9012ed39b2566851fb0d86cca50, a8729621ca4310e8e1a7ad3e1426708f1e1954a16af420cd3ce46c501e9692ab, a9896a8f96407a5eedda08a63dd40967f0fe0b3926e7002b6e1abc11f6ab81cc, aa04c9307a9087455d21dfac02d7f322ab337cd5978f9161285a9c79379efecc, b36205464ead176a473ab43ea7b5e0c2b8749b3eb9549d65609be2337dce25db, b529c6df6164ff8badf30f942220a3126f99e3fc2c2ea1494aa3e305b3b53c1f, b9c4c8343ba75081954b2db54940585c6c0c9bb47e053ac1b9229b4fa8fc9293, be9c3feed5f6e81ccd375902c8c92616f77694b6cd14f69896d44dd4b1ea4990, c5bb808a88f9e729484c05a1bc3097157bbfbd28469e502f2ebc4c6e6135df42, c622c0f67eb5d9a90008e5e120065cd5a1a6e25c6e758e8205d377596059b8fe, ccb539bf17d479d9707ee717d0afb03cd57e9b6f023becf1abf9cdbd88e1b06c, cd3040c88a6fd71ed1ce8c2a5d0b13ed8e25e49835932a39891c514ef946dd29, ce2f00f1d0e71287e746d5a3507547f355297a3e45a7c2cc0322015916a0137c, d00d3adf81bf95ff4994dcbd2ae1305a6ee6b0edfad6eb55b87217f85645651a, d0e3f547e3efcc9d9794774a765b9c3950955e7ad752f3e630ebd5ab9425bcdc, d452461f3527d674de3e9b680026ceb2b02c56d6d3f7c94da3aab65c05f52c03,

TYPE	VALUE
SHA256	d57f45096e646837dec51129222fcbe79981c595721164009aec68be09bf5dcf, dbb4f7e6354621c316fbba7e7a15f59cf229684e16ab6d21027f310beecaf49b, dbdeede6f39936305c4c5bd8e4f7bfccb0b823c025130e7f8fa285e80383be0f, dc3d72f72247141efeba3c2ffd498025f68e0c4b34c9a4dc2686ffec09b6d401, de933f7b47707f4bf8d5a4aaef8b31f5059d3b8f465bcaae3e22438466e8390b, e6315b24e0311758da1c25daa5f2724da4f534ed7ed644cbf43f3cc64c4676a7, e9a18755312011e30081e7ce0fcc1db3e3aec3b9f3ed3a776dd38498830a2738, eb4e39d44ad016b8d6d1dc8dc25a9ea3d3e18df87516922fdbd995de15b68f54, ebd167ca477af620065548a9e55567682b0750625b3e078fc4498dd5adeabdc6, f2536e520d37512d868a418797974a5c11e67742824a5477100b7e3f5b2efbc3, f4fcba1c9d7f4ae8e3868f901035ea1e0e9e1122a362a83afd3d111c17a97d7a, f7eef906c7dc1ce2ffe586d4b7f316a5f5c6761b5cdbf22d892fbc87a5ee2f6f, fe55c1d263e0ea356d86afd8b2b1cedff570568e45b8a3810e05ea482b8a9329, fefba5ce20c71a71cfe35dd8ff06c514bf6ffde60356babf4f4bba66dd904b78, cf9d93951e558ed22815b34446cfa2bd2cf3d1582d8bd97912612f4d4128a64e, 48aaa2dec95537cdf9fc471dbcbb4ff726be4a0647dbdf6300fa61858c2b0099, 00fc4b8a4c65c06766608f3ef3f92385c8e147f5991dabe290e33dd14b39ad44, 0ad65fd0897a6547f6febf398708ab2d423a8f8834b53136219cb490ec3ebd13, 11ba24d023b544e28c37b6cb8afe27d06638175d7f56c2e4d4ff97bf7bd813b6, 1a2399ecc38f3288206c75b55762d125d3d75254062a2c0d85c86e7f896736ac, 258ffcc13dbe110bcce21b91f7f075995719791fdd3c9f55ea5934984fa4373d, 2cbc1e8a4cb5d18a867666adbd3417bc88d48a74ae6500593959aec1a1c92d2d, 342a5c7df2bdd040570f4b83c74366d4c96a90d6418149d432cb5e8577f2f6b1,

TYPE	VALUE
SHA256	3648e89e7449ea433a8b3ef0e5b605b5dc4157048c03b20dedc5e3b920fa8552, 5418e42706bca4712ff2a3db67853eb42a2310660c51cff2f9020586cffedeb3, 69573694d16b7ccadfa208ff976bfe1b3e36837aba3e5dc4dfc80e66341ef61e, 6de4f65b1d738d84f8e825613092bbd360194195fe8a1c986e12a9bb704217c1, 751f149665f87dd20cc8dff743f28e5da1ff2a5f04874d4b8569b9afceeedfec, 78200cd816acbd39b6664c6582e06500f6d46085b62b49d2f914bea5a004197a, 783c7f4bf23072343f6247ee14e54e4af0b147553ad1ef42b4e7fb44386d667c, 7f99e506c17676b98dcc08e6a19f100ef933cde3e0423c6d4072f6802a9196bb, 8d0b1174cbda6b102bb98c91ba123e9f404b9fad23b49a4e29f3cfd8d20a577a, 90c7688e0dc23ba4530bac1d567bad920c4ef1c06cbf4b2d867eeb363271eefe, 9102e564c3262b2c291e8ca3d67f8a55c06650aa86f617c919916f6053c03c9b, 9327aa03760431b6d86eeb2f1a3efc36aa443b842b5116fbbe0f2a7794c4e70e, 97286b6f3a6535ff1172ef65172e6967e3670c6b14a3313c3bf0d6c171b1fc85, 98e28d3423f5d414effe3c0ed6fd0f1c8154942e5e127ecee5f051e1196ffc75, 99c0bebdc8cb7b0948000a601f510fc70487f9da532be199b8641512a2db9839, 9bdf49b27fd4d80ef087f63e0bfa0a0822686814863eca09ac506404ad76dfda, b2588061ba5ee9948bbccd320b40c6d7b8d6a693d181f3bce61e5e267f53aa7e, b936853a0c50a0cd0bc8b33103b55bd88e19c6c28768d990b954c11d714286ca, F2429f4bd09897653d0ffa41206a14cafa55356d5edc04dc0915c116867f8c27, bea558e8129fcb647e6f42c8beda4464e109dd3cd546342c0337dbd50616f991, 4fd469d08c051d6997f0471d91ccf96c173d27c8cff5bd70c3f2c5008faa786f, 633b0fe4f3d2bfb18d4ad648ff223fe6763397daa033e9c5d79f2cae89a6c3b2, b97dd0279e112e0591b38064f59077102ab188b07a069cb104e66e4756e2570a,

TYPE	VALUE
SHA256	13872271ee511aa83f3f27d5db248516652b10a079ad01f78ed734cd2a87ec77, d96ec4b08c08b81ba9075423d5e83bf330de09866066b4bdb459bcbac389a350, a905226a2486ccc158d44cf4c1728e103472825fb189e05c17d998b9f5534d63, 44f3936ee158d2846664bf5cd795fd90a99441186b20b90ff241ba1b38a6a3e9, 219a6387d91c4b2c8e91c8613192af950bd9c790114a238eb0e1e7c878f6e728, 37438095a5e7be0ce12997dc23d1ff117912989d2f24beab95284f9380f65834, aeba4ece8c4bf51d9761e49fad983967e76c705a06999c556c099f39853f737c, 3ca87045da78292a6bba017138ff9ee42b4e626b64d0fee6d86a16cc3258c8c3, 3737501bbd4abd0844da016c0263399e3c670ae52952b30ca46c6c96cf4e318d, 6012386eab453f4fb1cfb88fb5b05ba9ec71a838029ea51bcff4c0b5a2fbfad2, c0b319bb19092fe3c193e5139fcdf599502b669143b06c676e81f46ab50fb4ed, 18273fa35c54332d8763cb17a5ae92de5636f3a05c507ce18d9d6a77c3139deb, d97aa65123c26509e3fc1a9963962b7f707a50ddca44a9a12fd03e654ab5aa66, fd9fbfa809450415e8d0d79199ec8686cb7071d6e13a5b76f0ce1b03a2a61302, a87032195e38892b351641e08c81b92a1ea888c3c74a0c7464160e86613c4476, 3d010e3fce1b2c9ab5b8cc125be812e63b661ddcbde40509a49118c2330ef9d0, fcb00beaa88f7827999856ba12302086cadbc1252261d64379172f2927a6760e, 2625d99af56c79de32f9fba2332f63eb9c88707e9ea83985bce5df9022ced99a, ffb264a19af7c8a8dd5357b62c45fcd3063ca946aa2710740c4e8b21f8e697d9, 24ce42c2fd4a95c1b86bbee9bce1e1cf255bd0022e19bab6bd591afd68b7efdb

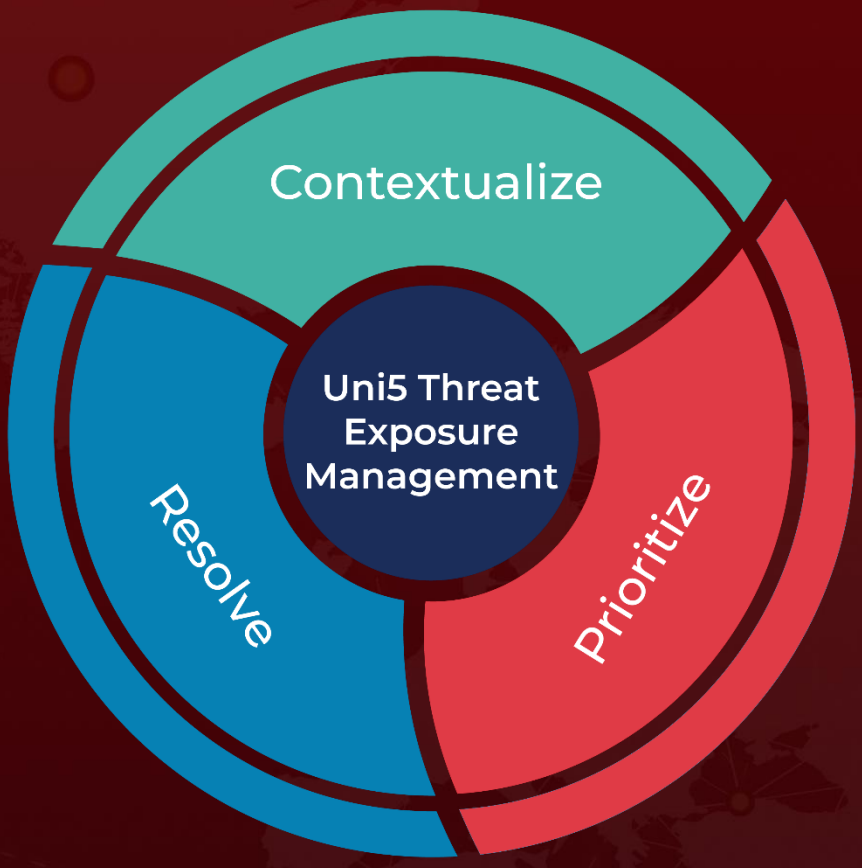
References

https://research.checkpoint.com/2024/massive-phishing-campaign-deploys-latest-rhadamanthys-version/#single-post

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

November 8, 2024 • 5:45 AM

More at www.hivepro.com