Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

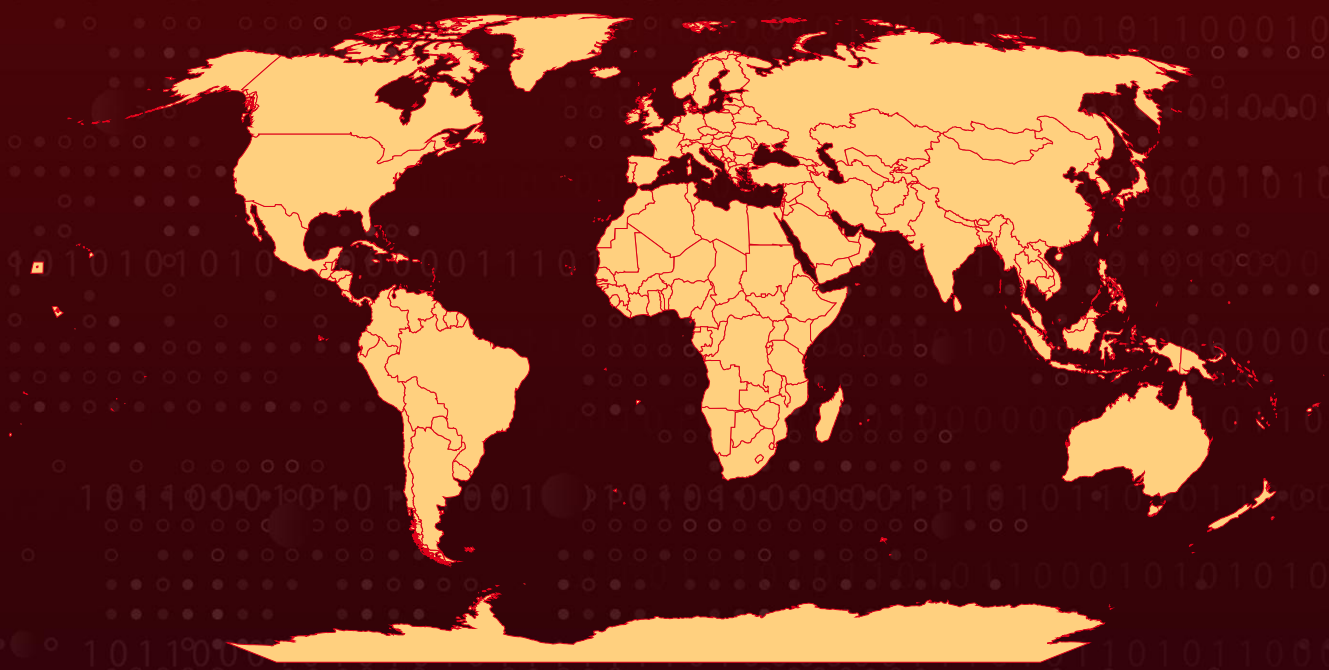
Betruger Backdoor: How RansomHub is Redefining Ransomware Strategies

Date of Publication	Admiralty Code	TA Number
March 21, 2025	A1	TA2025090

Summary

Attack Commenced: March 2024
Targeted Countries: Worldwide
Malware: RansomHub, Betruger
Targeted Platform: Windows
Attack: RansomHub, a ransomware-as-a-service operation, has been deploying a custom backdoor named Betruger. This multi-functional malware consolidates capabilities such as keylogging, network scanning, credential dumping, and privilege escalation into a single tool, minimizing the need for multiple attack components. By masquerading under benign filenames like "mailer.exe," Betruger evades detection, enhancing the stealth of ransomware attacks. This development underscores the evolving sophistication of ransomware tactics, highlighting the necessity for robust cybersecurity measures.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-24521	Microsoft Windows CLFS Driver Privilege Escalation Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2023-27532	Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability	Veeam Backup & Replication	✗	✓	✓

Attack Details

#1

RansomHub, a prominent ransomware-as-a-service (RaaS) operation, has recently been observed leveraging a custom backdoor known as Betruger. Unlike many ransomware campaigns that rely on widely available tools, this operation has developed a bespoke malware solution that consolidates multiple attack capabilities into a single payload. This strategy not only streamlines the attack process but also reduces the digital footprint left by the attackers.

#2

The Betruger backdoor is engineered to perform a variety of functions that are typically spread across several distinct tools. It can capture screenshots, log keystrokes, scan the network for vulnerable systems, dump credentials, and even escalate privileges within the compromised environment. This multi-functionality allows the threat actors to gather crucial information and maintain persistent access, setting the stage for a full-scale ransomware deployment without the need to drop multiple specialized tools.

#3

To further complicate detection, attackers disguise the backdoor by using file names like “mailer.exe” and “turbomailer.exe,” which suggest benign or routine applications. This clever masquerade not only helps the malware blend in with legitimate processes but also delays the recognition of its true malicious intent by security systems. The design choices behind Betruger indicate a focus on operational stealth, enabling the threat actors to remain undetected while they prepare their ransomware attack.

#4

In addition to deploying Betruger, RansomHub affiliates have been exploiting known vulnerabilities to enhance their attack capabilities. The evolution of such custom tools signals a significant shift in the tactics of ransomware operators. By developing specialized malware like Betruger, ransomware groups are lowering the technical barriers for affiliates and increasing their overall efficiency.

Recommendations

Apply Security Patches and Updates Promptly: Regularly update all software, operating systems, and applications to address known vulnerabilities that RansomHub can exploit. Automated patch management systems can assist in ensuring timely updates.

Deploy Endpoint Detection and Response (EDR) Solutions: Utilize EDR tools to monitor and analyze endpoint activities, enabling the detection and swift response to suspicious behaviors indicative of ransomware attacks.

Restrict User Privileges and Network Access: Apply the principle of least privilege by limiting user access rights to only what is necessary for their roles. Implement network segmentation to contain potential ransomware spread and regularly audit privileged accounts.

Strengthen Email Security and Filtering: Implement advanced email filtering solutions to block malicious attachments, links, and phishing attempts. Technologies such as SPF, DKIM, and DMARC can authenticate senders and reduce the risk of email-based attacks.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of an RansomHub ransomware attack, up-to-date backups enable recovery without paying the ransom.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0040 Impact	TA0002 Execution	TA0011 Command and Control	TA0043 Reconnaissance
TA0042 Resource Development	TA0010 Exfiltration	T1486 Data Encrypted for Impact	T1041 Exfiltration Over C2 Channel

T1113 Screen Capture	T1056.001 Keylogging	T1056 Input Capture	T1595 Active Scanning
T1068 Exploitation for Privilege Escalation	T1003 OS Credential Dumping	T1589.001 Credentials	T1589 Gather Victim Identity Information
T1036 Masquerading	T1219 Remote Access Software	T1040 Network Sniffing	T1027 Obfuscated Files or Information

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	ae7c31d4547dd293ba3fd3982b715c65d731ee07a9c1cc402234d8705c01dfca, b058c128c801e2ee03874e183239ff369c599f3a2324905ff73f99d16d3b1a16, 9e0a89c1b98f448865a73049a2b90bdfcd1b9846c4506441cfa6f0e429c1b329, 0ad9ab7aa9ecbc79bca0bfce5be58e0aa2606bdab3898daac43a6fa1231af164, 290b3fe64fd0875b2dc6bc0ad77dd52a70ad91a81dc24220523d38bf6c538afa, 35e853cc67bf1869127ed341ea7b1a5cbf7032523288d514dc4685924f898db2, 9e0274c4e57381e97ccceadba37b64da35cfc379f80abc53e40f310a5e6b690b, a46c3639ba099953def013430063ea018f616c10e4b1cb4fe9a26d261f9dab0d, bd82216f1341159e950e9e7a68015c54c4995c8fd7c12c28a839c5068b0919ad, df4c29cce2cf1a158ed0cefc860dc54f6fbb9bdafdc3bf5af60b506f78e69e4f, 6d215534002fe7627763f5dd971d529d2f2186431244108d1fd8b5e9e2c9a3b2, 2d4fa520c03b358223d8210f2e9bad572e4914efd6e70cb7db85a377e891e69a, 24be73b64509dbad476b2873edf500554fed5885826b21e2f538993900d9a364,

TYPE	VALUE
SHA256	24be73b64509dbad476b2873edf500554fed5885826b21e2f538993900d9a364, 84099559a6d1dd1fec8a5c065da9f0747fab8ebb7368c197224fa33035eabe8d, 3c9f0907304f7af7a7b88f931b6733698e86492d02e98e440e87e3ffe2153dbc, c4d51f5a4dc95b0ac4b4f44a74d282d84898ddf56293a7dfddd5cb5eb90ec989, 262a4dff66ceb25d35d5ca8d8d148c1fee88ea2ee1187877a5a0c8d6a0dd24b5, de4d1f58fa8fa9eb156a37a8d9a3396d58e804f92e5eee25878a36a116f66362, ab84aeee213b902fde9740c466cd53af4bae6d5ea81a2b84c4d534b08b2fa049, 1f1d3587e458dd883f9ca282fbf559115334a993ba111ec2296e94de8a6fab83, 6af2283337104fac154c26c7c55f274f4c36a231497af96f414897dfbeb6691c, 76964c6e8283101383a5a99f7a0bd8a7c170e44752a73ce034558c43a19207af, a8806944ff6cad0d45d956972c32e93f44da7e251352d63c1f058df8384b78d1, aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9, 8dc79c12fe1e8aefb870049c16fd1d62051207310702b99428cd73987e299ca3, 05633246aeee0959414cf3b4d5482df728cb798b838963270cf416783ef0db7b, cf87a44c575d391df668123b05c207eef04b91e54300d1cbbec2f48f5209d4a4, 57f58fd5c140fd86fda11c8f7aae1b53479e1510fbcabe7bee795dc01929285c, a96a0ba7998a6956c8073b6eff9306398cc03fb9866e4cabf0810a69bb2a43b2, 9fa315259cc627b17a0d99864cd1bf54667bd26ccef5ce50ba412fa8911b10e5, d37a023b809ef9ec024be3976344813a4b860aa9104e298d5d5d4805381ff3a5, e14ba0fb92e16bb7db3b1efac4b13aee178542c6994543e7535d8efaa589870c, 7c0f223f585b9c9b64d4ac8c04724edbffa43b95fa997912960c9c5332ede18b, d04bd76a2710fc35b3a445b5db241f13f199763e38b8fbe5316063c36a27a931,

TYPE	VALUE
SHA256	41abfef1ac0b9700700a9b42cb39cdd79b39a1a5b0eb3d3929e82c650b84bac6, c3405d9c9d593d75d773c0615254e69d0362954384058ee970a3ec0944519c37, 80a2ae9d5189c55aeb838b651a712e70045d8e45bd95678c61109e6183fe3607, edc9222aece9098ad636af351dd896ffee3360e487fda658062a9722edf02185, f402d9eb5158adac54ab9f4f564051a39a8d817dd66bd46bbb373e80f08a4a08, 5f08f5d3732bc019c80277ab6d8d4a4bd49709958e7a1ee8879ddcea21751cbb, 32d8971ce5d541b1eb8863ea66dfd1aee0cb9fdaeb47990991ed301912bffa78, 67d99f3afaa21d470f354dade1fa19320cc36d51e7023be64d4daa25af6f5def, 6ff9eac3b4272e81a3b89f709fba4dba6544db22e72dcb114ba27e10970420ad, f9c5d479ead9d36af0dc3389774fa2af85d490d93ff91620b1f9390783247cae, 3d7658c7db34650db12f11c0f2621c08a80aa0ffb5443a944519b4da0236e446, 03fec698a64c49f2650b064f0ba61266b22cae4a8eb8e07959bfc07c9180b905, 91c8b02b1fa9d1d555b56e50b091d4c5493b907e18b794f3280682d8d30b96f3, 494123779a6edf73807f549b6cd1bffd3bfd660dacb027af66600eaad66f8fb1, 7985fbd052906a1cd963d42987ac5c840ddbf920b6c9b274aa5f428021830902, 7d7d6c292c05920d8272960c62acb8ab5c000f4c6cf3ed9f5e1edd70f7f33c91, 479c27daa3b3bc10de1cde10c54d62f71eed0cb922d32b58fa4083204fecc050, 90b9a10809bae2db28b585f9a4fc5f40f474b76db7aa936d2059a1244f955908, aaf985a5817a693f92a2775ce65ef57ddd2425b38533ec95062940d475c5568d

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24521

https://www.veeam.com/kb4424

Recent Breaches

https://georghay.co.uk
https://janvier-labs.com
https://ccktech.com
https://www.mslglobalexp.com
https://controlledair.com
https://www.jhayber.com
https://baxterlaboratories.com
https://www.ameda.com
https://idcconstruction.com
https://jennyyoo.com
https://www.dtrglaw.com
https://myraymond.com
https://www.v1.co.uk
https://www.hexosys.com
https://dcarosolutions.com
https://wheats.com
https://srmg.com.au
https://jpwindustries.com
https://total-ps.com
https://hickorylaw.com
https://lovesac.com
https://mitchellmcnutt.com
https://black-star.fr

References

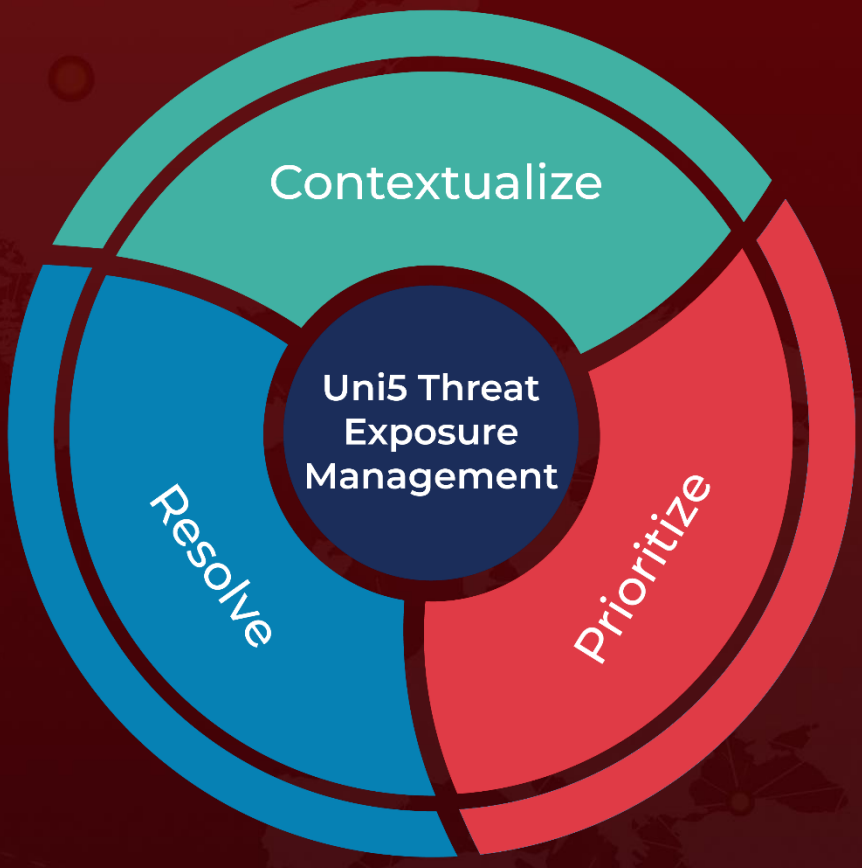
https://www.security.com/threat-intelligence/ransomhub-betruger-backdoor

https://hivepro.com/threat-advisory/ransomhub-the-raas-powerhouse-exploiting-200-victims/

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 21, 2025 • 6:30 AM

More at www.hivepro.com