Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

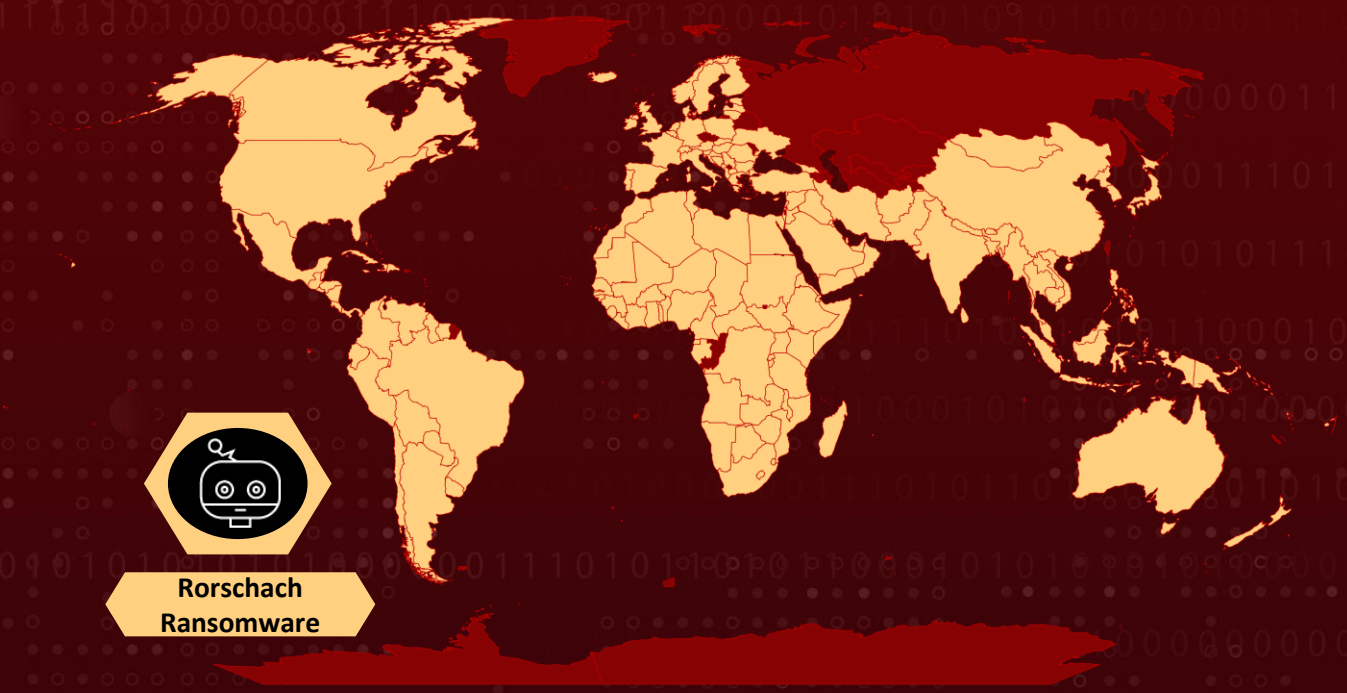
A New Rorschach Ransomware Threat Employing Hybrid-Cryptography

Date of Publication	Last Updated date	Admiralty Code	TA Number
April 06, 2023	April 07, 2023	A1	TA2023171

Summary

First Appearance: June 2022
Target Countries: Worldwide except the following CIS countries: Russia, Belarus, Kazakhstan, Azerbaijan, Moldova, Uzbekistan, Armenia, Tajikistan, Kyrgyzstan, Turkmenistan
Malware: Rorschach Ransomware (also known as BabLock)
Ransom Demands: $50,000 - $1,000,000
Affected Platforms: Windows, Linux
Attack: Rorschach is a new and highly effective ransomware that uses a hybrid-cryptography scheme and fast thread scheduling via I/O completion ports.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	PATCH	Zero-day	CISA KEV
CVE-2022-41352	Zimbra Collaboration (ZCS) Arbitrary File Upload Vulnerability	Zimbra Collaboration(ZCS)	✓	✓	✓

Attack Details

#1 The Rorschach ransomware is a new threat that employs various techniques to avoid detection and achieve high-speed encryption. The malware is delivered via a malicious email attachment disguised as a legitimate document. Upon execution, the ransomware checks the user's language settings to avoid infecting computers in CIS countries.

#2 Rorschach uses a unique hybrid cryptography scheme that blends the curve25519 and eSTREAM cipher hc-128 algorithms for encryption purposes. The malware only encrypts specific portions of the original file content instead of the entire file to increase encryption speed. The ransomware has built-in options that are hidden and obfuscated, making them inaccessible without reverse-engineering the ransomware.

#3 These options suggest networking capabilities, such as listen, srv, and hostfile. Rorschach takes inspiration from other ransomware strains such as Babuk and LockBit for some of its routines. The code used to stop services through the service control manager appears to have been directly copied from Babuk's source code and GPO creation method that closely resembles that of LockBit 2.0.

#4 The ransomware's final renaming of encrypted machine files is implemented via NtSetInformationFile using FileInformationClass FileRenameInformation, just like in LockBit v2.0. The malware leaves a ransom note with a Bitcoin wallet address and an email address for contact, offering a decryption service in exchange for payment.

Recommendations

To identify whether your system has been affected by Rorschach ransomware, it's crucial to look for the presence of cy.exe, config.ini, and taskkill.exe files, as well as any unusual activities or processes that could indicate a ransomware attack, such as encrypted files or ransom notes.

Preventive measures include keeping all security patches and antivirus software updated, using signatures or heuristics to detect malicious software, blocking code execution through application control or script blocking, managing privileged accounts, and utilizing capabilities to prevent suspicious behavior patterns. Regularly backing up data can also aid in recovery from a ransomware attack.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0002 Execution	TA0007 Discovery	TA0004 Privilege Escalation
TA0011 Command and Control	TA0009 Collection	TA0005 Defense Evasion	TA0040 Impact
T1552 Unsecured Credentials	T1106 Native API	T1569 System Services	T1027 Obfuscated Files or Information
T1055 Process Injection	T1140 Deobfuscate/Decode Files or Information	T1615 Group Policy Discovery	T1069 Permission Groups Discovery
T1083 File and Directory Discovery	T1059 Command and Scripting Interpreter	T1059.001 Power Shell	T1069.002 Domain Groups
T1190 Exploit Public-Facing Application	T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1059.004 Unix Shell
T1078 Valid Accounts	T1055.002 Portable Executable Injection	T1562 Impair Defenses	T1562.001 Disable or Modify Tools
T1564 Hide Artifacts	T1564.010 Process Argument Spoofing	T1497 Virtualization/Sandbox Evasion	T1486 Data Encrypted for Impact
T1574 Hijack Execution Flow	T1552.004 Private Keys	T1574.002 DLL Side-Loading	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	2237ec542cdcd3eb656e86e43b461cd1 4a03423c77fe2c8d979caca58a64ad6c 6bd96d06cd7c4b084fe9346e55a81cf9

TYPE	VALUE
SHA256	38c610102129be21d8d99ac92f3369c6650767ed513e5744c0cda54e68b33812 e14b88795bde45cf736c8363c71a77171aa710a4e7fa9ce38470082cb1bdadbb 7d62a33e9a2fedff6cf27aaa142ff15838a766ccd4a8d326424611e155442775 83052cc23c45ecaa09fe5c87fd650c7f8e708aea46756a2b9d452d40ce3b9c00 b711579e33b0df2143c7cb61246233c7f9b4d53db6a048427a58c0295d8daf1c De5a53131225dd97040d48221d9afd98760f7ff2f55613f0d08436891ca632b9 4874d336c5c7c2f558cfd5954655cacfc85bcfcb512a45fb0ff461ce9c38b86d 2fd264f58ba82a2675280ec8c6759612def2bcc62aa6160f5e23071f67bb67ab 03c41019faf7e4cc26ca0dd3a2c41b2115e4c4ebd561402079bc4a20256c1813 88081a21e500e831d86666ca5d7a3d348f7c03bc5c471b6d17d8b18a022f25be aa48acaef62a7bfb3192f8a7d6e5229764618ac1ad1bd1b5f6d19a78864eb31f b99d114b267ffd068c3289199b6df95a9f9e64872d6c2b666d63974bbce75bf2 66bcad0829a59c424d062b949c2a556b11c509b17515dffecb9cbf65f13f3dc6
Email	dcqyvp1@onionmail[.]org DcqYvp@onionmail[.]org dyhdsak@onionmail[.]org dyhdsak1@onionmail[.]org jzmc2t@tutanota[.]com jzmc2t@onionmail[.]org ngoueeb@onionmail[.]org ngoueeb1@onionmail[.]org vvbured@onionmail[.]org vvbured1@onionmail[.]org wvpater@onionmail[.]org wvpater1@onionmail[.]org

Patch Links

https://wiki.zimbra.com/wiki/Security_Center
https://forums.zimbra.org/viewtopic.php?t=71153&p=306532

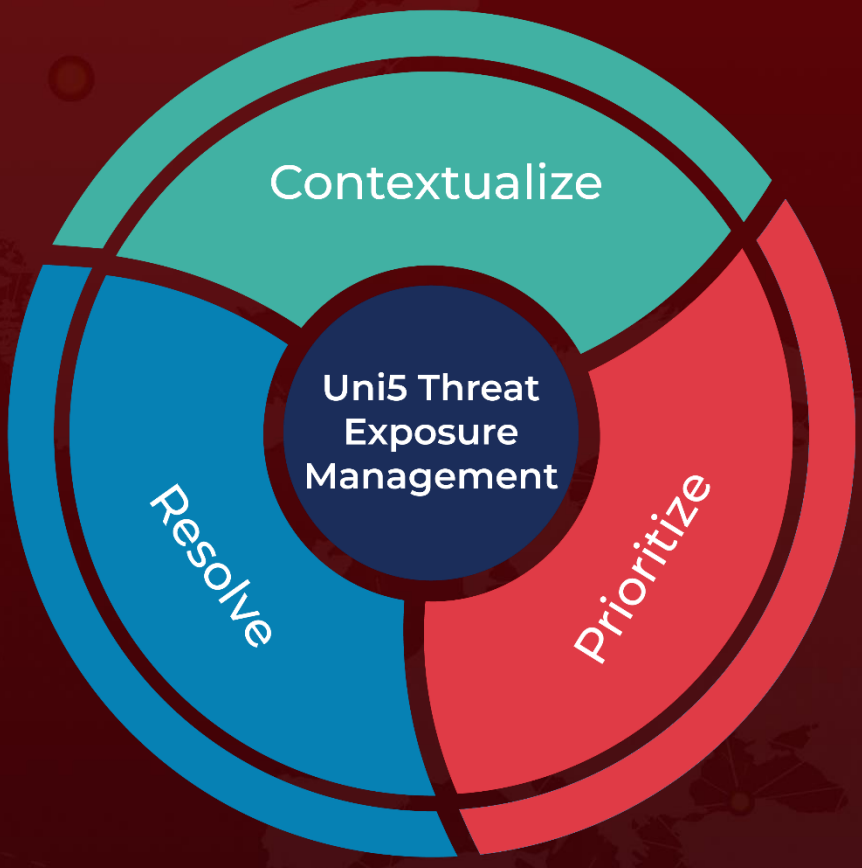
References

https://\research.checkpoint.com/2023/rorschach-a-new-sophisticated-and-fast-ransomware/
https://www.group-ib.com/blog/bablock-ransomware/

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

April 06, 2023 • 1:30 AM

More at www.hivepro.com