Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Termite Ransomware Weaponizes Babuk's Legacy to Strike High-Profile Targets

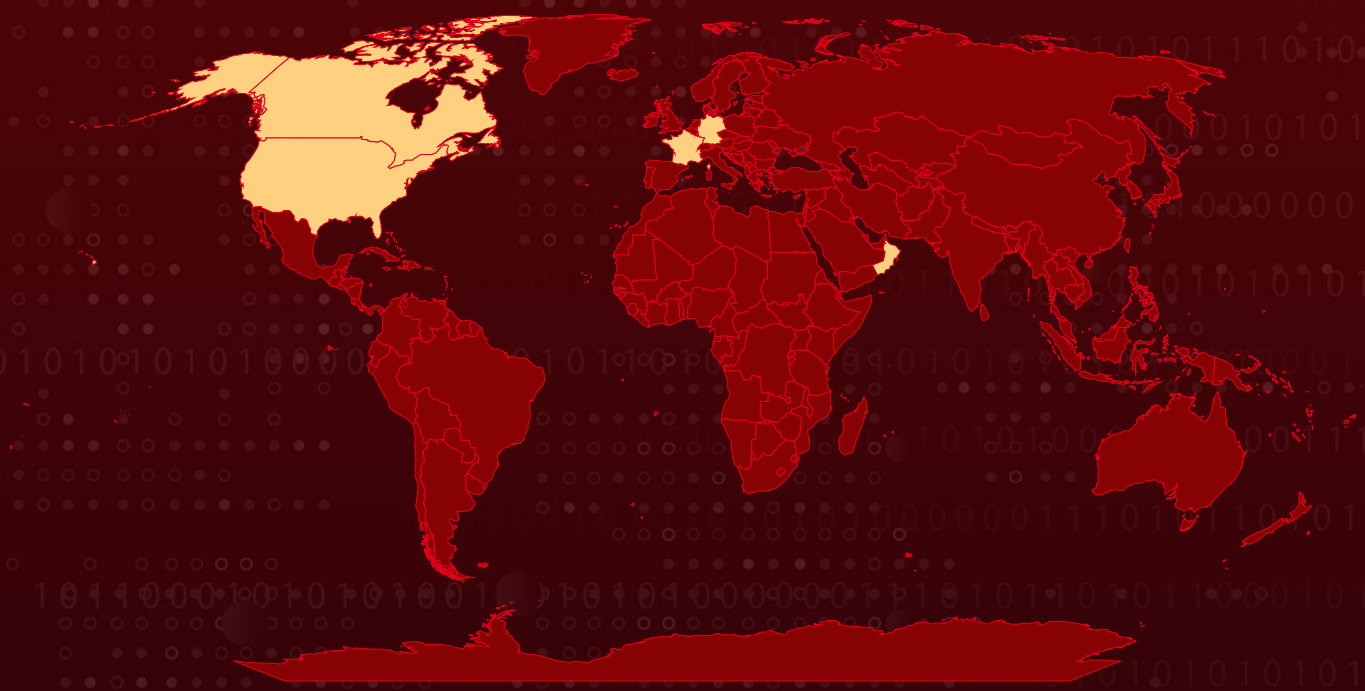
Date of Publication	Admiralty Code	TA Number
December 9, 2024	A1	TA2024455

Summary

Active Since: November 2024
Malware: Termite ransomware
Affected Platform: Windows
Targeted Countries: Canada, United States, Germany, Oman, France
Targeted Industries: Technology, Government, Education, Charitable Organizations, Food Service, Energy, Manufacturing, Environmental Services, Oil and Gas, Healthcare, Disability Support Services, Water Treatment, Automotive

Attack: Termite ransomware, a dangerous offshoot of the Babuk family, has emerged as a significant cyber threat, targeting organizations in the US, Canada, Germany, France, and Oman. It employs a sophisticated attack chain to disable recovery mechanisms, encrypt critical files, and disrupt operations. Notably, the group claimed responsibility for breaching Blue Yonder, exfiltrating 680 GB of sensitive data.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 Termite ransomware, a derivative of the **Babuk** family, has recently targeted organizations in France, Canada, Germany, Oman, and the United States. Leveraging a modified version of the Babuk encryptor, leaked in September 2021.

#2 The ransomware employs a refined attack chain designed to maximize disruption and hinder recovery. Upon execution, Termite ensures its persistence by running until the system shuts down, prioritizing file encryption. It interacts with the system's service manager to identify and terminate critical services, such as those managing backups and databases, thereby reducing resistance.

#3 To strengthen its attack, Termite halts processes that might interfere with encryption. It disables recovery mechanisms by deleting system Shadow Copies and clearing the Recycle Bin, effectively preventing the restoration of affected files. Additionally, it gathers system information to fine-tune its operations, creating encryption threads optimized for the system's hardware capabilities.

#4 The ransomware strategically excludes critical system directories and file types from encryption to maintain the machine's operability, ensuring victims can access ransom instructions. Encrypted files are appended with a unique extension and embedded markers to confirm successful encryption.

#5 Termite ransomware can propagate through network shares and connected drives, targeting shared resources for encryption. If specific targeting instructions are not found, it defaults to encrypting all local drives. After the encryption process, it leaves behind a ransom note titled 'How To Restore Your Files.txt', directing victims to its onion site for payment and decryption instructions.

#6 In November 2024, the Termite ransomware gang claimed responsibility for breaching the Arizona-based SaaS provider Blue Yonder, exfiltrating over 680 GB of sensitive data. Blue Yonder is a global leader in supply chain software for retailers, manufacturers, and logistics providers. While the Termite ransomware encryptor appears to still be under development, its growing capabilities signal a critical period for organizations to bolster their cybersecurity defenses before the group refines its tactics further.

Recommendations

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup, kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Harden Administrative Accounts: Apply additional layers of security to administrative accounts by using dedicated, isolated administrative workstations for system management tasks. Avoid using administrator accounts for routine tasks to reduce the risk of an attacker gaining access to critical systems.

Enforce Application Whitelisting: Implement strict application whitelisting policies to prevent unauthorized or malicious executables from running within your environment.

Network and File Share Security: Secure shared network resources by limiting write access and enforcing strict access controls. Isolate critical shared drives to minimize the impact of ransomware propagating across the network.

Conduct Ransomware Simulation Drills: Test the organization's resilience against ransomware attacks by conducting simulated scenarios to identify gaps in preparedness.

Regularly Test Backup Restores: Conduct frequent tests to verify the integrity of backup data and ensure that restoration processes work as intended. This practice helps identify any issues before an actual data recovery scenario arises.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion	TA0007 Discovery
TA0009 Collection	TA0040 Impact	T1204 User Execution	T1204.002 Malicious File

T1070.004 File Deletion	T1027 Obfuscated Files or Information	T1087.002 Domain Account	T1087 Account Discovery
T1083 File and Directory Discovery	T1135 Network Share Discovery	T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery
T1543.003 Windows Service	T1543 Create or Modify System Process	T1491 Defacement	T1070 Indicator Removal
T1005 Data from Local System			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	6b06aae5ec596cdbc1b9d4c457fd5f81
SHA1	a515b7d89676b1401eeb9eb776190a1179c386cf
SHA256	f0ec54b9dc2e64c214e92b521933cee172283ff5c942cf84fae4ec5b03abab55
TOR Address	termiteuslbumdge2zmfmfcsrvmvsfe4gvyudc5j6cdnisnhtftvokid[.]onion
Email	rgagfhiuehrf[@]proton[.]me

Recent Breaches

https://blueyonder.com/
https://departement974.fr/
https://csviamonde.ca/
https://www.lebenshilfe-heinsberg.de/
https://www.culligan.fr/
https://oq.com/
http://nifast.com/

References

https://cyble.com/blog/technical-look-at-termite-ransomware-blue-yonder/

https://www.pcrisk.com/removal-guides/31694-termite-ransomware

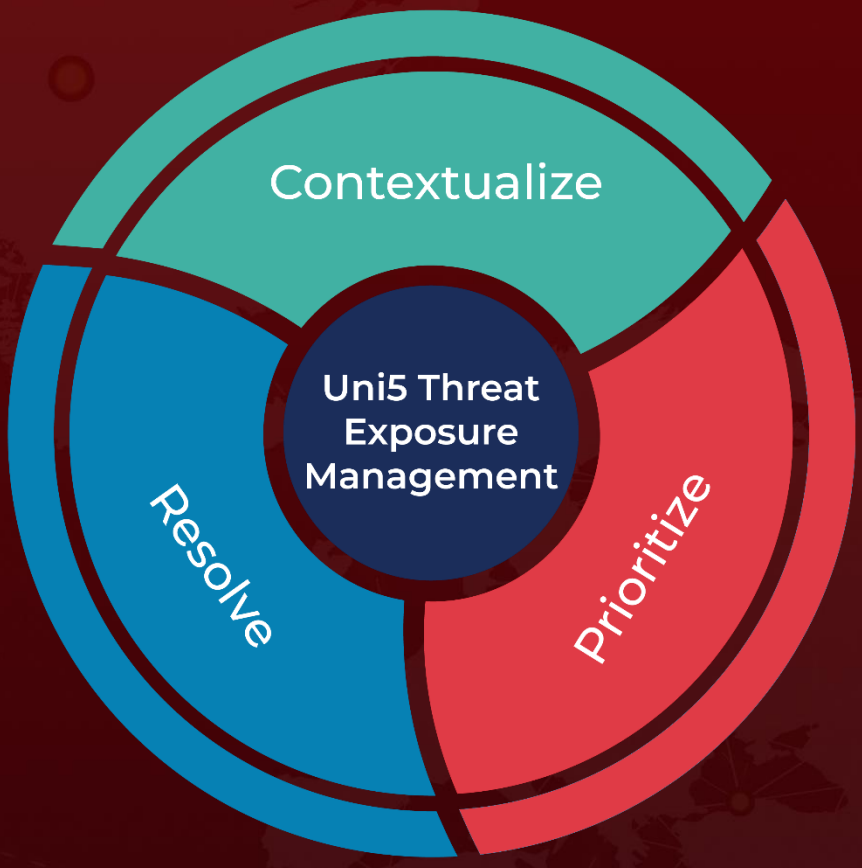
https://www.broadcom.com/support/security-center/protection-bulletin/termite-ransomware

https://hivepro.com/threat-advisory/crypt-ghouls-deployed-lockbit-and-babuk-to-paralyze-russian-firms/

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 9, 2024 . 4:30 AM

© 2024 All Rights are Reserved by Hive Pro

More at www.hivepro.com