Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Black Basta Ransomware Linked to Zero-Day Windows Exploit

Date of Publication

June 13, 2024

Admiralty Code

A2

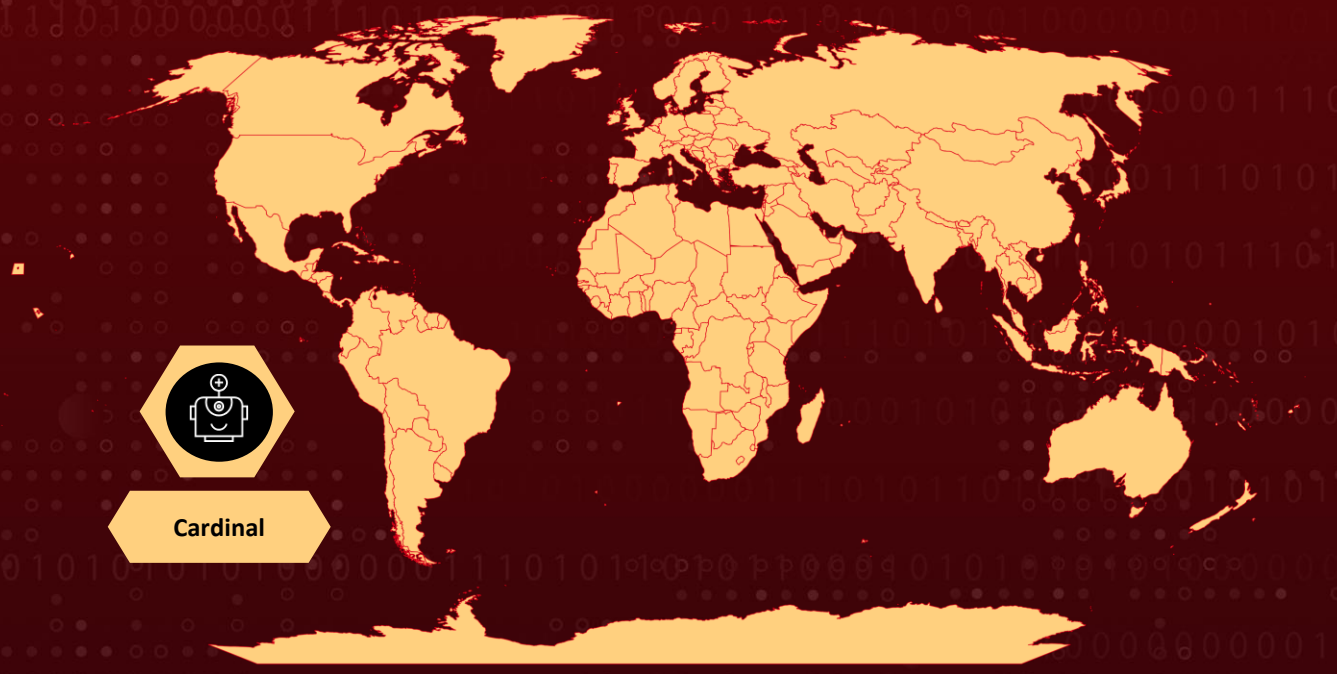
TA Number

TA2024230

Summary

First Appearance: February 27, 2024
Malware: Black Basta ransomware (aka no_name_software)
Targeted Countries: Worldwide
Threat Actor: Cardinal Threat Group (aka Storm-1811, UNC4393)
Affected Platforms: Windows
Attack: Cardinal Threat Group, known to be associated with Black Basta ransomware group, is believed to have exploited a Windows CVE-2024-26169 as zero-day, notably this flaw was fixed in March however evidence now suggests it was possibly exploited as early as February before the patch was available. The vulnerability allowed attackers to gain the highest level of access on compromised systems.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-26169	Windows Error Reporting Service Elevation of Privilege Vulnerability	Microsoft Windows	✓	✓	✓

Attack Details

#1

Attackers linked to the Black Basta ransomware group may have exploited a Windows privilege escalation vulnerability (CVE-2024-26169) as a zero-day, according to recent findings. This vulnerability, found in the Windows Error Reporting Service, allows attackers to elevate their privileges. It was patched on March 12, 2024, but evidence suggests that the Cardinal cybercrime group (aka Storm-1811, UNC4393) used the exploit before the patch was released.

#2

Recently, Cardinal has used legitimate Microsoft products, such as Quick Assist and Teams, as attack vectors to impersonate IT personnel, leading to credential theft and persistence via SystemBC. Researchers discovered an exploit tool used in a failed ransomware attack, showing tactics similar to those of Black Basta, including batch scripts disguised as software updates.

#3

The tool exploits a vulnerability in the Windows file werkernel.sys to create a registry key that starts a shell with administrative privileges. The tool's variants had compilation timestamps before the patch release, indicating possible zero-day use.

#4

Although timestamps can be altered, there seems to be little reason for the attackers to falsify them. Cardinal, which introduced Black Basta in April 2022, initially used the Qakbot botnet for distribution until its takedown in August 2023. After a temporary decline, Cardinal resumed attacks, now using the DarkGate loader to access victims.

Recommendations

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with Black Basta ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

Patch and Update Software: Keep all operating systems, applications, and firmware up to date with the latest security patches and updates. Black Basta affiliates often exploit known vulnerabilities to gain initial access to systems. By promptly applying patches, organizations can mitigate the risk of these vulnerabilities being exploited and prevent unauthorized access to their networks.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, storing them securely offline. Test restoration processes to ensure backup integrity and availability. In case of a Black Basta ransomware attack, up-to-date backups enable recovery without paying the ransom. Especially BitLocker users should secure recovery keys and maintain offline backups.

Access Control and Least Privilege: Enforce the principle of least privilege, ensuring that users and applications have only the minimum access required to perform their functions. This limits the potential impact of a ransomware attack.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0004 Privilege Escalation	TA0042 Resource Development	TA0005 Defense Evasion
TA0040 Impact	T1588.006 Vulnerabilities	T1588.005 Exploits	T1588 Obtain Capabilities
T1068 Exploitation for Privilege Escalation	T1486 Data Encrypted for Impact	T1036 Masquerading	T1059 Command and Scripting Interpreter

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	4aae231fb5357c0647483181aeae47956ac66e42b6b134f5b90da76d8ec0ac63, b73a7e25d224778172e394426c98b86215087d815296c71a3f76f738c720c1b0, a31e075bd5a2652917f91714fea4d272816c028d7734b36c84899cd583181b3d, 3b3bd81232f517ba6d65c7838c205b301b0f27572fcfef9e5b86dd30a1d55a0d, 2408be22f6184cdccec7a34e2e79711ff4957e42f1ed7b7ad63f914d37dba625, b0903921e666ca3ffd45100a38c11d7e5c53ab38646715eafc6d1851ad41b92e,

TYPE	VALUE
SHA256	71d50b74f81d27feefbc2bc0f631b0ed7fcdf88b1abbd6d104e66638993786f8, 0f9156f91c387e7781603ed716dcdc3f5342ece96e155115708b1662b0f9b4d0, 1ad05a4a849d7ed09e2efb38f5424523651baf3326b5f95e05f6726f564ccc30, 93058bd5fe5f046e298e1d3655274ae4c08f07a8b6876e61629ae4a0b510a2f7, 1cb1864314262e71de1565e198193877ef83e98823a7da81eb3d59894b5a4cfb
Domains	upd7a[.]com, upd7[.]com, upd9[.]com, upd5[.]pro, antispam3[.]com, antispam2[.]com, instance-olqdnn-relay.screenconnect[.]com, greekpool[.]com, zziveastnews[.]com, realsepnews[.]com

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26169

References

https://symantec-enterprise-blogs.security.com/threat-intelligence/black-basta-ransomware-zero-day

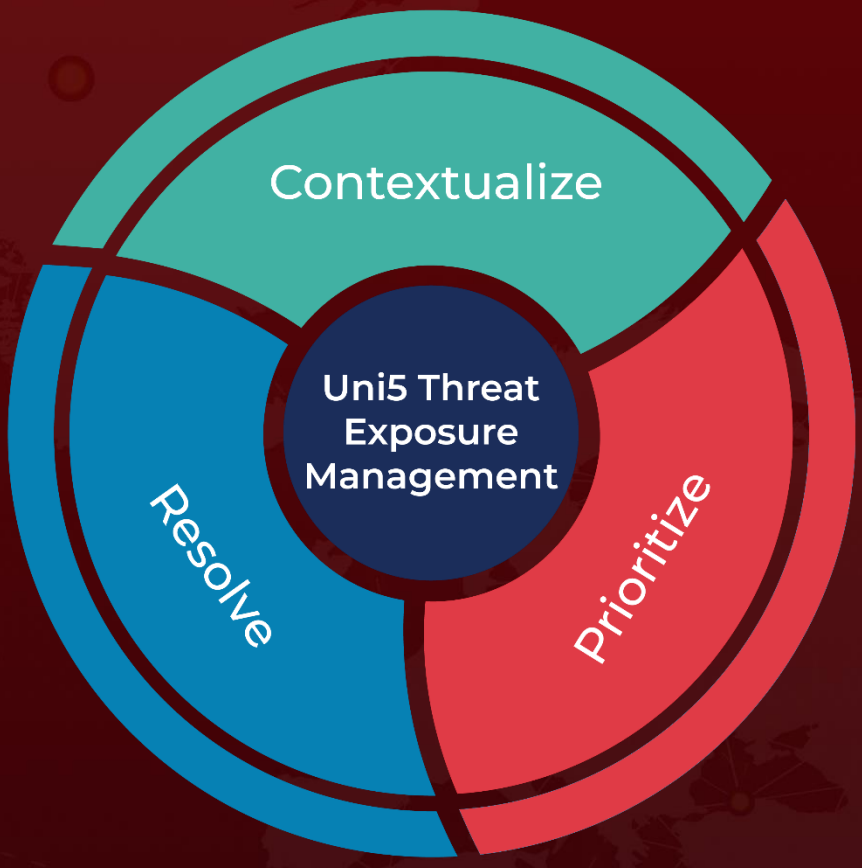
https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/

https://www.hivepro.com/threat-advisory/black-basta-ransomware-impacts-over-500-organizations-worldwide/

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

June 13, 2024 • 5:30 AM

More at www.hivepro.com