Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

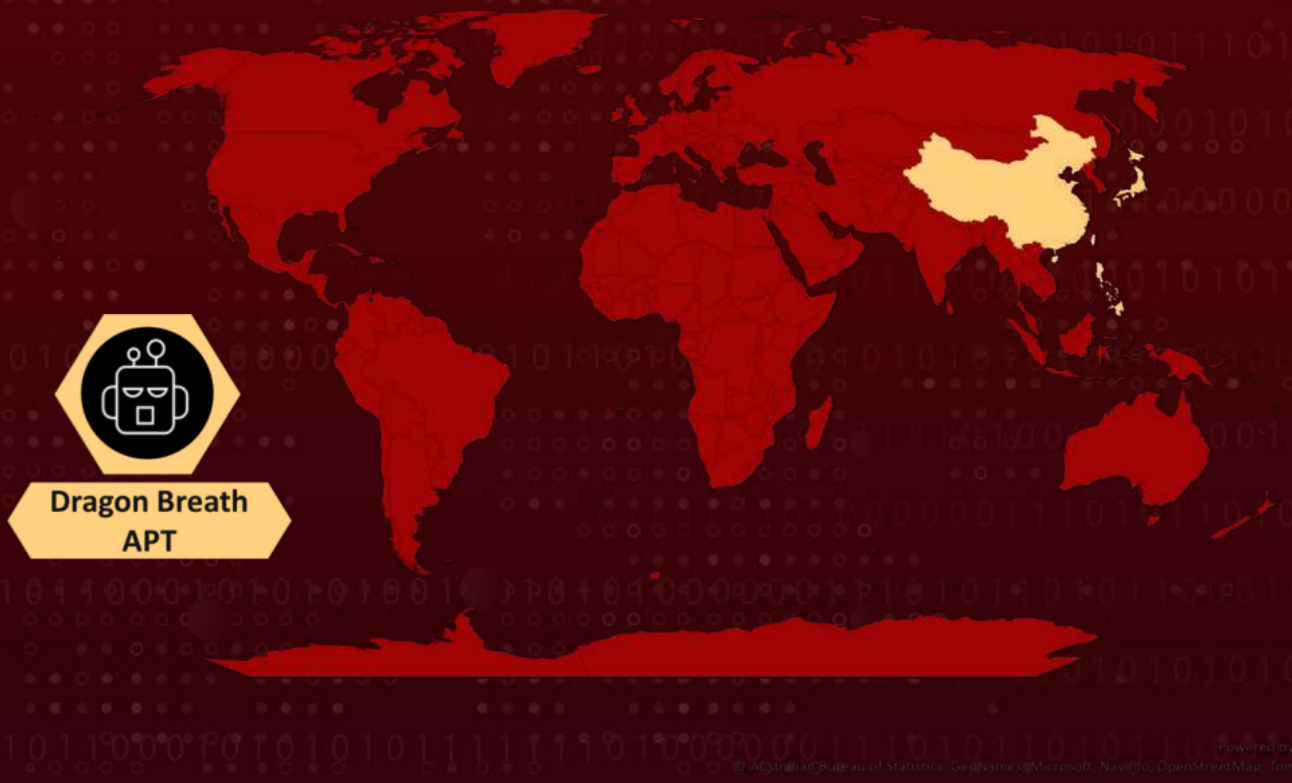
Dragon Breath APT Evolves with Double DLL Sideloading

Date of Publication	Admiralty Code	TA Number
May 8, 2023	A1	TA2023216

Summary

Attack began: 2023
Actor: Dragon Breath APT (aka Golden Eye Dog & APT-Q-27)
Affected Products: Telegram, LetsVPN, and WhatsApp for Windows
Attack Region: Philippines, Japan, Taiwan, Singapore, Hong Kong, and China
Targeted Sector: Online Gambling, Gaming
Attack: The Dragon Breath APT group has evolved its attacks, using a double-clean-app technique and novel DLL sideloading to target the gambling industry. These campaigns have targeted Chinese-speaking Windows users, and the attackers have enticed victims with trojanized versions of popular applications. Additionally, the group has added new layers of complexity to its attacks with the double DLL sideloading tactic to evade detection.

Attack Regions



Attack Details

#1 Dragon Breath, an advanced persistent threat (APT) actor, has recently been observed using a novel DLL side-loading mechanism to add more complexity to its attacks. This attack is similar to a classic sideloading attack, which involves a clean application, a malicious loader, and an encrypted payload. However, Dragon Breath has made various modifications to these components over time.

#2 The most recent attacks from Dragon Breath involve a first-stage clean application that "side"loads a second clean application and automatically executes it. This second application then sideloads the malicious loader DLL, which ultimately executes the final payload. The original campaigns focused on Chinese-speaking Windows users who were engaged in online gambling, and the initial infection vectors were distributed via Telegram.

#3 The Dragon Breath APT enticed victims by offering trojanized versions of popular applications, such as Telegram, LetsVPN, or WhatsApp for Android, iOS, or Windows, which they claimed were customized for individuals in China. These compromised applications are thought to be advertised using BlackSEO or malvertising techniques.

Recommendations

- Educate employees on the risks of downloading and installing unverified applications, especially if they claim to be customized for specific regions or languages.
- Implement network segmentation and access controls to limit the spread of malware in the event of a successful attack, and regularly test incident response plans to ensure preparedness for potential breaches.
- Implementing blocking Indicators of Compromise (IOCs) can also help organizations to defend against Dragon Breath APT's new campaign and other similar threats.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0008 Lateral Movement	T1120 Peripheral Device Discovery
T1091 Replication Through Removable Media	T1059 Command and Scripting Interpreter	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading
T1055 Process Injection	T1027 Obfuscated Files or Information	T1027.002 Software Packing	T1036 Masquerading
T1070 Indicator Removal	T1070.004 File Deletion	T1070.006 Timestomp	T1057 Process Discovery
T1082 System Information Discovery	T1083 File and Directory Discovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	097899b3acb3599944305b064667e959c707e519aef3d98be1741bbc69d56a17 34c4eda45c782e74a5f3b179961659b472c053b63eb48318a2441db2bcbbb1dc 48a35466b1a08711abcdd2cd5564164265a4ee4e2082700f2eba69e1f3bf111a 1c4ad390cf903e78571fe9c3dbc0f9ff63fda7cae449d81f743a6011e8287caf 695e0312d6612201af4b3c6d4f50f67df8614cae69e35ce2a72e68d0c587de54 9c4f42124ff130e0ff61846b2cb3d1aa6d618d65b141e466613533a350bdf278 bf19222b9eac87650db9206cee05c695b1df22499bcac310376734197ee5457c

TYPE	VALUE
SHA256	e414fc7bcd80a75d57ee4fdbb1c80a90a0993be8e8bbbe0decfc62870a2e1e86 530f01699688ab8c2bb25349a6bc398907b2adb5164d7602c28152c66851fa43 04db8e4dfecfc300a86614a2393bb768861196b18f17845b5765d06e1ba692c4 324bbcae91d4287e481ece09abe8d6d123b0c2f8ae0355c416924e4f8371661d 484fdf350c4a10c8bf0c495abf696a09f0a25258d39e81884122cb75e4432191 60f6fa45809c39ecdff4161d5925e6e8f491adedb7ed8ac67d772cd3c212b1cf af04147945915737f3f2eed7df222c0b45d7b911bf82f6176df6856514e58c08 bfb44fb2194e25eee516b431fd84892a6073735dbf510a70dfa3a344526ade97 cdb645ea97980e63b9c165ca842bad2751ce2728cc5c55329ba04e96bab3077b fe8c97f1ca9aab32b0ff4d46559f22677b3dba3c6d73c8b5d2fe9dd07c8ec64a 0b85cc5a583e94ba793a88a5184c68658eb7543bcc41deb4cf6aa633c67e538a ad7ff3ffcf4276219830228de0c0454310710011f5274f3d2436a4b699af7030 c936f1598721a9a92d7f31c6c13b55013b8a2a344e3df4156e5b033006336544 31d2076066107bd04ab24ff7bbdf8271aa16dd1d04e70bd9cc492e9aa1e6c82b 769d59d03036af86c7a9950f03ebc7b693a94d3e2f8ecd1d74cf5600ab948105 03b1df2b08999262c772b67a7bd65e9e8f6058036b5e7a382f06d3aa672854d0 a8a09d4e1ddbe4de188100b285a53b53b10677e4fbc93014e07211cdaf532e7b 0ed0f8476f0c7d7cdbdfb8935c5c012463ce2cf1e00c8fbfc1ad202366539b38 49aca2efaca973d9dea2e01c2ac63cea7cd1e0cf12aa45d98653eea46b7593c9 4bf6b4544c8584fe933eec269568d8e3dc259110b36a9376d6956980fe43a37d 4c3899f2b7be819620b5eeb6f35643043141a2e51223d56a54840b1268a6893d 5e19f77df4d5241985e94e2770b94ed6f7fbaa977d516f44bb24f2cff1bca827 79bcd6e9dadf67b771a530821abff5944a2f40019bc5e57c59cc037edebfec51

TYPE	VALUE
SHA256	ae2e145b36ab2ed129a2d34de435b76a1f4e5a4820d9d623e7018b87f24d0648 dc41b8e22c725ee4f8e04f55851b3129f0b8b6b5c2c16aaf893bfe92de440503 7fcba1dc809f39fa6b36e923af22fc7c576f3cfb49aaa7248a98d32e9bc90991 d1652c5153171fb5420a7c647888b23ab43c286eb2331ec661162cc37fb527f3 849d9e694d3e5d3f0eabcae4b722c2bbed31168d161a4f5d668f351bfa169743 1c4ad390cf903e78571fe9c3dbc0f9ff63fda7cae449d81f743a6011e8287caf be061c8bb82cd52d2f76aeb1e3ba2448c1a3230dd7eda1250d272648af4669ca 9a17c5a4f48367557f06dacd3aefaa132214cb4163bc6b6cf43e06041936a69e 99f6932e3de96d6558f37030fce5007a13bed9de8617935dcad25e7be551b2a2 11359b92b062c426d58fcf738b4f92644c7bdd7e9f47a3ab9e1cb54ad29e6dc4 49a1826a70ef6a373910ebf43bb441213ec195e68c9a242e4bead60f7e04609b 1b32c531aca954a7812c65ea41b85941e199aa78ace782f17d9307f5f51f4e43 3fc9405cfe9272323bd96aacfd082c16b392fea6e0f108545138026aa6f79137 831b6a78bc193e5bb3a112aecc385ae00a2c81b963e126d2b949140b6acf333e e50e72bf4684b2543b55234f798e728b02cafb27a70fa6f4459e68d99b988f3b f05db80e4676ffb4b4df68982f1f22b38e8054070f78b21fed1baf51e62c6853 229011ca0351dc3461b19e427b1910990dde9f268f2a361e92f728171544b589 87528e65b5c10c699edce279516f8c41c603d2382261d2d7601191e97666fa57 a21f66260427b18c5db840dca84f33a762d4089a23ff293c4ae9dcf4ef2cb90f a3e4747f878fa1959b54874d239c6170d8d3dde29b5bfbe7bfdf154a51cccdee 0e73131b428f45aa10a36e48fc8d5b30643a404125b95f9b179dd3756c6e023d 4cb3ebdc53a10c0c911fa79dd156f2d8b6c64c37f4f7c71a5ac002fd4fc8f3d5 7cd096bb8e2edd384b9cf149916b67653d07804bc0024973ee1e2e02c8d5288e

TYPE	VALUE
SHA256	da1d66610e0253a82c7ba3f2cc3e4c50d23bccee71f7a61f18f8f99937d04bdd dc758f11e768a829836e27fa265993c937fd2bb4575a3dc18c12ba4b69baa953 e07113850a83ebf58816f619f14ce142187d7e27af4025ff44bfe611e1d68820 e1e0fba8c5c14bab3d83ee18f266385d56c91b347e509cd090bdb3ef4168d91f e744f4d6ea7b88bc5e8d432f0c11b7c5cf86c0e4d22809f2df159608baf586f7 eb5b72a8a40123dfec2341414196ee11ec13c404125bb5c5ada9d70c0b2cc015 ec9083eb656234b4eb3dd5df1882046e605870975fa67ecf04bbee454a4d44ec ee07de81fd6b8896bcd128dfe9db53e9e987b9bf42e865e1f1aa7dc5b27f373d ee927ca55d06406b6dd266b286d3cfe0626308ec4193d98336e00ad509fe44e2 efacfe7cc34c5807f88296a373187a5c9324f59f476cbf07d219b6373d014f3a
IPV4	23.225.147[.]227 206.233.128[.]103
Domains	nsjdhmdjs[.]com 123[.]nsjdhmdjs[.]com 2[.]nsjdhmdjs[.]com ac2[.]nsjdhmdjs[.]com a[.]pic447[.]com b[.]pic447[.]com d[.]pic447[.]com l[.]pic447[.]com l2[.]pic447[.]com t[.]pic447[.]com v[.]pic447[.]com v2[.]pic447[.]com w[.]pic447[.]com j[.]pic6005588[.]com potatouu[.]com 2[.]potatouu[.]com

References

https://news.sophos.com/en-us/2023/05/03/doubled-dll-sideloading-dragon-breath/

https://github.com/sophoslabs/IoCs/blob/master/double-dragon-breath-iocs.csv

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

May 8, 2023 • 7:40 AM

More at www.hivepro.com