Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

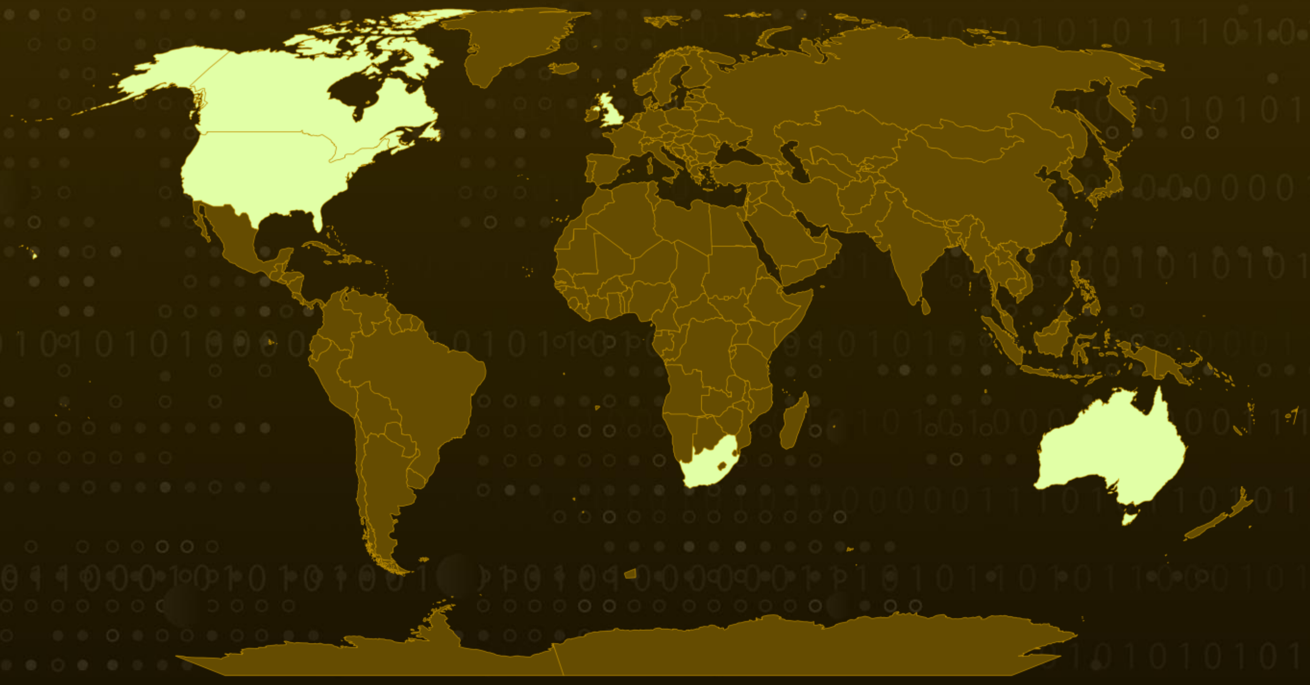
Greatness a Growing Threat to Microsoft 365 Users

Date of Publication	Admiralty Code	TA Number
May 12, 2023	A1	TA2023227

Summary

Attack Began: November 2022
Phishing-as-a-service (PaaS): Greatness
Affected Platform: Microsoft 365
Attack Region: United States, United Kingdom, Australia, South Africa, and Canada.
Targeted Sector: Manufacturing, Healthcare, Technology, Education, Real Estate, Construction, Finance, Business Services, Non-Profit, Retail, Automotive, Energy, Legal, Transportation, Marketing, Agriculture, and Food & Beverage
Attack: The Phishing-as-a-Service (PaaS) platform named 'Greatness' has experienced a surge in its operations, which target organizations utilizing Microsoft 365 in the United States, United Kingdom, Australia, South Africa, and Canada.

Attack Regions



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

Attack Details

#1

The Phishing-as-a-service (PaaS) platform, Greatness, has been leveraged in multiple phishing campaigns since mid-2022, with notable increases in activity observed during December 2022 and March 2023. The majority of targets were business entities, with over 50% being located in the United States.

#2

The next most frequently targeted countries were the United Kingdom, Australia, South Africa, and Canada. Greatness is specifically engineered to infiltrate Microsoft 365 users, rendering phishing pages that are highly persuasive and successful in compromising corporate entities.

#3

Greatness encompasses functionalities of the most sophisticated PaaS platforms, including MFA bypass, IP filtering, and integration with Telegram bots. Greatness exclusively concentrates on constructing Microsoft 365 phishing pages, empowering its affiliates with an attachment and link builder that fabricates convincing login pages. To utilize Greatness, affiliates must install and adjust a supplied phishing kit to serve as a proxy to the Microsoft 365 authentication system, conducting a 'man-in-the-middle' attack and siphoning the victim's authentication credentials or cookies.

Recommendations

Regular phishing simulations, education, and awareness training are vital. Also, verifying the authenticity of email attachments and untrusted links before opening them is crucial to prevent attacks.

Regularly back it up offline to protect critical data and install reliable anti-virus and internet security software on all connected devices. Enable automatic software updates whenever possible and practical. Additionally, consider implementing proactive security measures, such as blocking indicators of compromise (IoCs), to stay ahead of potential threats.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0011 Command and Control
T1090 Proxy	T1106 Native API	T1218 System Binary Proxy Execution	T1566 Phishing

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//bluecheckcommunication[.]com/finale/host8/admin/js/mj[.]php hxxps[:]//thesslcgroup[.]org/host10/admin/js/mj[.]php hxxps[:]//cliffordandblu[.]com/wp-includes/SimplePie/Parse/pate/procs/admin/js/mj[.]php hxxps[:]//avenzzi[.]com/ayoo/host7/admin/js/mj[.]php hxxps[:]//at[.]benconcept[.]com/wp-content/plugins/TOPXOH/offe/host6/admin/js/mj[.]php hxxps[:]//cp3955[.]com/host8/admin/js/mj[.]php hxxps[:]//schneidera[.]ga/[.]well-known/off/host8/admin/js/mj[.]php hxxp[:]//bbqpro[.]za[.]com/fb/host7/admin/js/mj[.]php hxxps[:]//www[.]c2tec[.]com[.]br/today/host16/admin/js/mj[.]php hxxps[:]//cedarcreeklabradoodles[.]com/host6/admin/js/mj[.]php hxxps[:]//whitesomcponwmc[.]com/wnclrm/andlw/admin/js/mj[.]php hxxps[:]//hihin[.]net/wp-content/plugins/backwpup/k/host7/admin/js/mj[.]php hxxps[:]//hansarobotics[.]com/host7/admin/js/mj[.]php hxxp[:]//cloudnewsdaily[.]sa[.]com/img/host8/admin/js/mj[.]php hxxps[:]//pog[.]flylineaeru[.]com/html/admin/js/mj[.]php hxxp[:]//whitesomcponwmc[.]com/wnclrm/andlw/admin/js/mj[.]php hxxps[:]//manimot[.]ca/wp-includes/dump/host8/admin/js/mj[.]php hxxps[:]//ochrelandscapes[.]com[.]au/host9/admin/js/mj[.]php hxxps[:]//fanningcpaz[.]com/jumpjumping/host15/admin/js/mj[.]php hxxp[:]//mail[.]sorderatoluca[.]com/wp-content/host7/admin/js/mj[.]php
SHA256	c5b29072d28e35c3992015fcbedc29540dd5ffc2931257a71866affae9de31f4 d07a2aa49f7b41eac954cd917aeedad3309d2856f63d51410da10dd5ff5847ce

TYPE	VALUE
SHA256	bbf7f77c3aca82b1531ba295cb5edb700777325dec9533d0c0341b66ddd073e3 d587c80ba12878146cfcb62262608c4a09f8b4d8647f9819ee3a5a94874b0205 492a45dd47acb19c6995acdbfce22a0cbcc135bc0263fd3efab165b1b75c9f68 61c094210d25d2e501234cc45b399b556d9bc95bc18f81c9ef4f433cc96b431a 9937f4ab00c4d41c8986a4d4e5a2a4193412e031c5a33d5f88913cc8dd0b5d4f c9375f405c6409087cfabb34bdc8e9d1333f8b1f6448395a3889856a07ba3573 8619111ae4e427ce31eea0dd4e3b1ec5fa728438b64fdbff3351256cc52d5831 ca130ace64ce6277b612c0e507a5b8e37e54b4f635b18d896992a844ca99de72 2b4ca60d215bd7eaf13891878ef4ddeac36354343cdc59f9f2882f8eb61b7234 3216d8ad022b72512c65756c4272e897d8669faa8f3fbf8c4788fd41d67477f1 Ed4cd5308bf283928dfe5e3a0985e90c82014136a87fdac13670e0748482b5ed 02212ba142819acd27377cf8fa627e230ad44f0ff9f4a31a9a1fc7d17b74c88b 11d980af0e1f9576b2b2fa319ee58a49ee72f4722e96141ce5990b37248cad42 8567f25398c14ca530a110909e08a383df0ff94c4562f3105b59c1b84fdbf808 cccfdf7ba2c5f740a0ddfee6d273cf286d48765334e8e66ca1d8834fb4426af7 f20aea297c4c00e78e8059572c535b4c879b5c331f552c881ff7929d6df0f6a6 fcee0c8773ecc95b846e4b45dd1364d42796387d831f7203e50e116d1ed5a750 b34b9aa0b8a36deec3157f262c5be11fa705da4c4902dc50ce6f0df2b838471c cae49fe3b224160c790fec72309f1bdb8f0e1d7c8a82a49262b12707b1789ce0

References

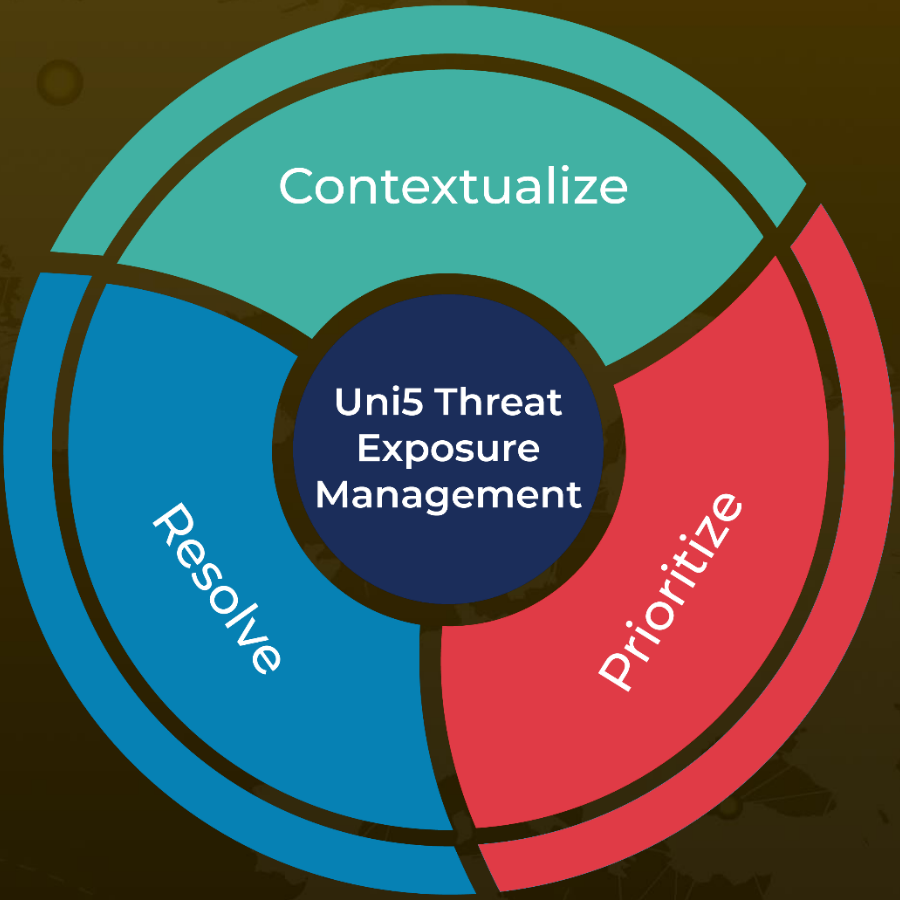
https://blog.talosintelligence.com/new-phishing-as-a-service-tool-greatness-already-seen-in-the-wild/

https://github.com/Cisco-Talos/IOCs/blob/main/2023/04/new-phishing-as-a-service-tool-greatness-already-seen-in-the-wild.txt

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 12, 2023 • 4:24 AM

More at www.hivepro.com