Sep 16 2023

NETMANAGEIT

Intelligence Report

Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets | Microsoft Security Blog

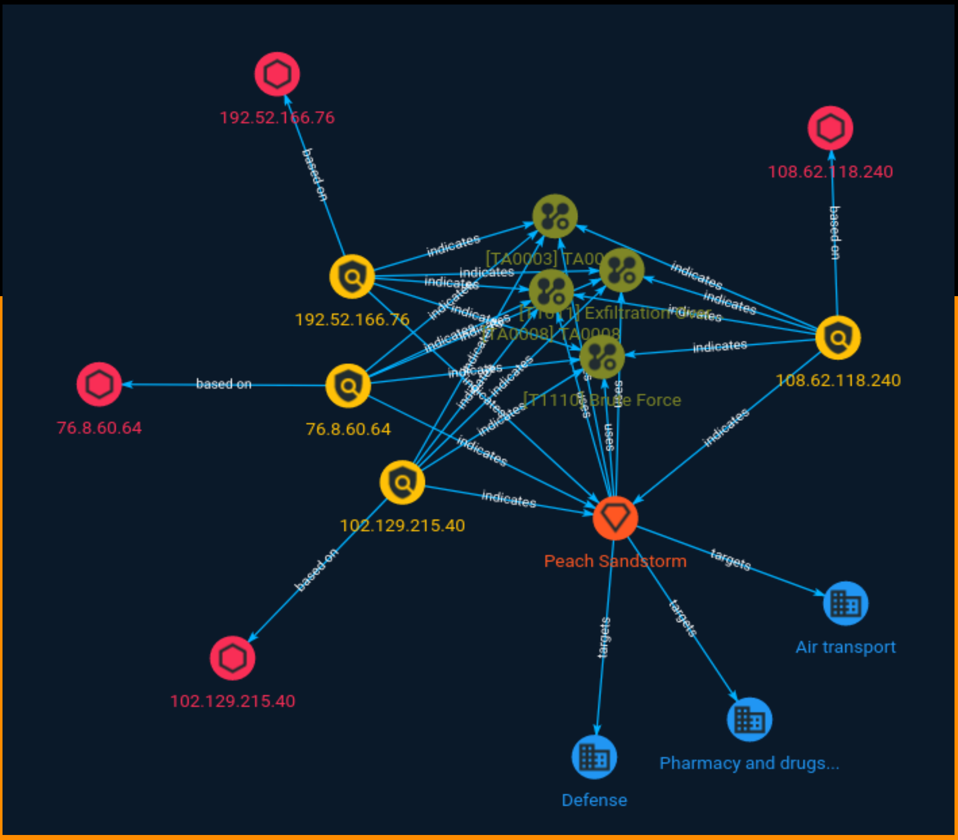

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Since February 2023, Microsoft has observed password spray activity against thousands of organizations carried out by an actor we track as Peach Sandstorm (HOLMIUM)

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Attack-Pattern

Name
TA0008
ID
TA0008
Name
Brute Force
ID
T1110
Description
Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy

Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

Name

TA0003

ID

TA0003

Name

Exfiltration Over Other Network Medium

ID

T1011

Description

Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel. Adversaries may choose to do this if they have sufficient access or proximity, and the connection might not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

Sector

Name

Pharmacy and drugs manufacturing

Description

Public and private entities involved in producing and selling medicinal products and drugs.

Name

Defense

Description

Public and private entities involved in the conception and production of weapons and the planning and conducting of military operations.

Name

Air transport

Description

All entities transporting people or goods by plane, managing or exploiting airports and structures, traffic authorities and plane manufacturers. Includes all civilian space activities.

Indicator

Name
76.8.60.64
Description
CC=US ASN=AS397384 LAUNCHVPS
Pattern Type
stix
Pattern
[ipv4-addr:value = '76.8.60.64']
Name
108.62.118.240
Description
CC=US ASN=AS30633 LEASEWEB-USA-WDC
Pattern Type
stix

Pattern

[ipv4-addr:value = '108.62.118.240']

Name

102.129.215.40

Description

ISP: NextArray LLC. **OS:** None ------------------------- Hostnames: - concernedguid.sbs ------------------------- Domains: - concernedguid.sbs ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDDIzvafZJL9UmTiMEW28to/nkLII3Bgp+uqGFpEWAvTyEjtT8ABkr9QqcEqad4tjO/XF3MzSpt7B76ImE16EBCkO2y8blY1oxgU13ePE8B9qAQwpWR+mIpoViLAXkoL7C4V5yps1uAAEZlgX5oQC/RT0h2gBG5qKzc7B/7XfYoKLYPT6NI/xkUhYQvtJMv85Jhr6/uuNfq/pXv0PoEkZwjcO/QzfqNSrEshp61EeHjACkQHa2RKfow0gHHFT7Y7hrnWU5kfOX0RWcp10rx5i7ACnKihq25DIJDZQEByGmpih2cQltSp3KrSITZIdBwDAi2nnwNvYznEDxWT4GhAEeD Fingerprint: 9a:c9:08:9f:68:5a:21:e1:d4:1a:4c:0e:94:dd:f6:7b Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ------------------ **80:** ``` HTTP/1.1 200 OK Date: Fri, 15 Sep 2023 05:12:30 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.33 X-Powered-By: PHP/7.1.33 Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 ``` ------------------ **443:** ``` HTTP/1.1 200 OK Date: Thu, 14 Sep 2023 15:46:14 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.33 Content-Length: 481 Content-Type: text/html;charset=ISO-8859-1 ``` HEARTBLEED: 2023/09/14 15:46:39 102.129.215.40:443 - SAFE ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '102.129.215.40']

Name

192.52.166.76

Description

CC=US ASN=AS8100 ASN-QUADRANET-GLOBAL

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.52.166.76']

Intrusion-Set

Name
Peach Sandstorm

IPv4-Addr

Value
192.52.166.76
76.8.60.64
108.62.118.240
102.129.215.40

External References

- https://otx.alienvault.com/pulse/6504b11fccc9665a33f44a6d
- https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/