Oct 05 2023

NETMANAGEIT

Intelligence Report

Qakbot-affiliated actors distribute Ransom Knight malware despite infrastructure takedown

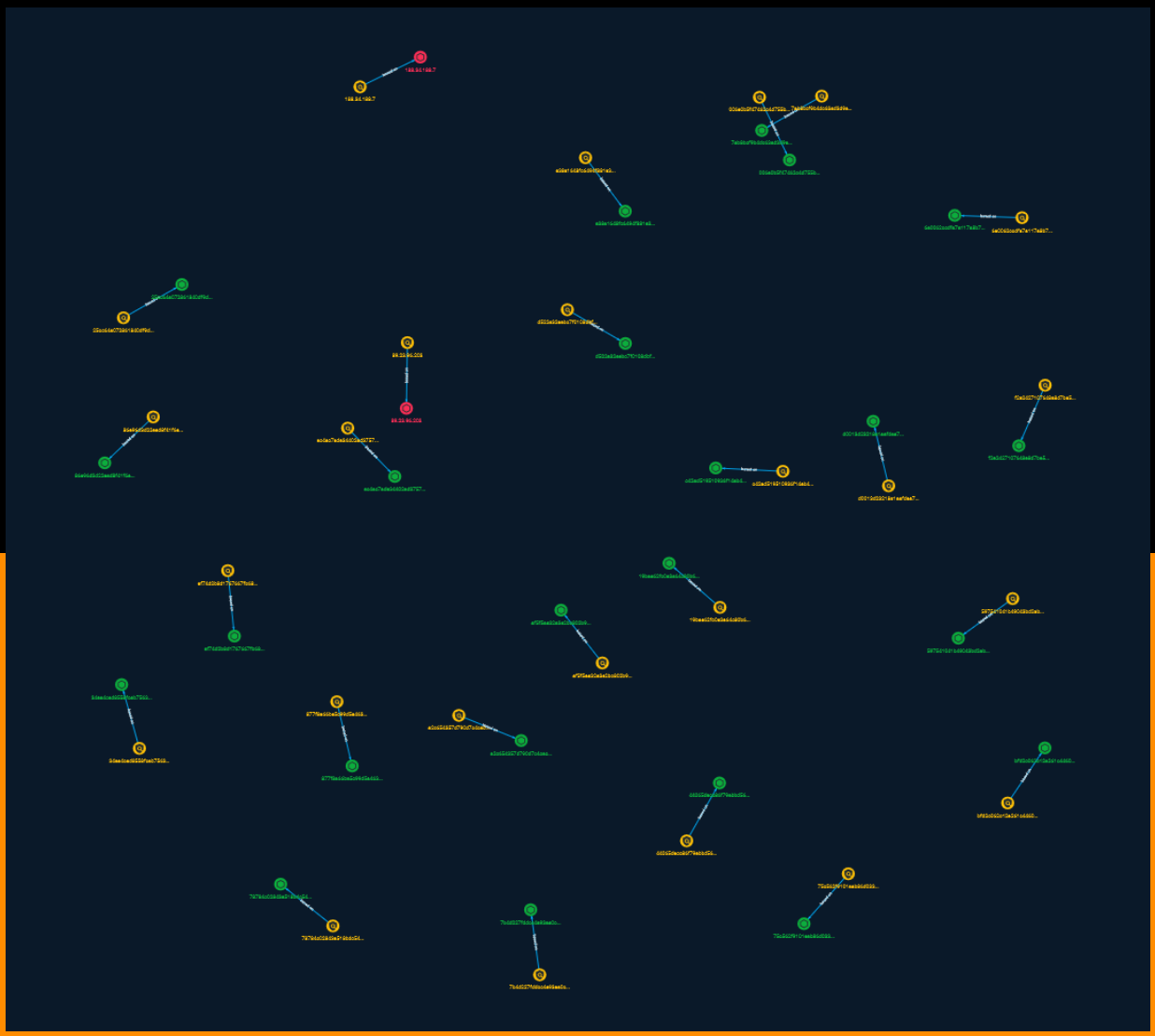

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The threat actors behind the Qakbot malware have been conducting a campaign since early August 2023 in which they have been distributing Ransom Knight ransomware and the Remcos backdoor via phishing emails.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
e38a1648fc6494f881e3b793688ef4d69e925137c4c7494f4dd6c6604142a2bc
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'e38a1648fc6494f881e3b793688ef4d69e925137c4c7494f4dd6c6604142a2bc']
Name
19bae62fc0a3a64c80b666237c2f04706e3b89c5a6ea6be055df22122e5f8a63
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '19bae62fc0a3a64c80b666237c2f04706e3b89c5a6ea6be055df22122e5f8a63']
Name

ec4ac7ade34402ad3757e97d03de7aa3dfee0ed53f28f32c99d8dbbb96958dcb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ec4ac7ade34402ad3757e97d03de7aa3dfee0ed53f28f32c99d8dbbb96958dcb']

Name

f2e2427107648e8d7be5f4e42341c702ceddb442191434128cbbf15c0325d8e9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f2e2427107648e8d7be5f4e42341c702ceddb442191434128cbbf15c0325d8e9']

Name

78784c02843a518bdc546534759dcdb3ea523c54751858a51f39e0f9d1492868

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '78784c02843a518bdc546534759dcdb3ea523c54751858a51f39e0f9d1492868']

Name

d522a32eebc7f0108dbff116b7fa9dd457bf9f062465060115ec423c567c5115

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd522a32eebc7f0108dbff116b7fa9dd457bf9f062465060115ec423c567c5115']

Name

d0013d23218a1aafdea792a0599b746af6966f765181c8c1dbfe7257be0cb022

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd0013d23218a1aafdea792a0599b746af6966f765181c8c1dbfe7257be0cb022']

Name

25cc64a072861840df9dfa7b2449165e4c37d57c542da8ec4ea4fffa10f1be39

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '25cc64a072861840df9dfa7b2449165e4c37d57c542da8ec4ea4fffa10f1be39']

Name

7ab8bcf9b4dc63ad3d9e1fe8eb2e8292a1545871fb2e3b5dd83c96a2b7e33b41

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7ab8bcf9b4dc63ad3d9e1fe8eb2e8292a1545871fb2e3b5dd83c96a2b7e33b41']

Name

44065decc86f79ebbd56b27f1db8c7bd5843147f3fa8e577604c0ed45317b016

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '44065decc86f79ebbd56b27f1db8c7bd5843147f3fa8e577604c0ed45317b016']

Name

86e96d3d22ead8f41f6a29f7bfe4b35c0d4ae5bd8da046ff0d01d9c6ea678dc2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '86e96d3d22ead8f41f6a29f7bfe4b35c0d4ae5bd8da046ff0d01d9c6ea678dc2']

Name

c42ad519510936f14ab46fbad53606db8132ea52a11e3fc8d111fbccc7d9ab5a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c42ad519510936f14ab46fbad53606db8132ea52a11e3fc8d111fbccc7d9ab5a']

Name

34ea4cad8558fcab75631a44eae492a54e1cf9ae2f52e7d5fa712686acd06437

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '34ea4cad8558fcab75631a44eae492a54e1cf9ae2f52e7d5fa712686acd06437']

Name

89.23.96.203

Description

ISP: LLC Smart Ape **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 403 Forbidden Date: Thu, 07 Sep 2023 06:36:56 GMT Server: Apache/2.4.6 (CentOS) Content-Length: 202 Content-Type: text/html; charset=iso-8859-1 ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10 (version 1809)/Windows Server 2019 (version 1809) OS Build: 10.0.17763 Target Name: WIN-LIVFRVQFMKO NetBIOS Domain Name: WIN-LIVFRVQFMKO NetBIOS Computer Name: WIN-LIVFRVQFMKO DNS Domain Name: WIN-LIVFRVQFMKO FQDN: WIN-LIVFRVQFMKO ``` ---------- **5357:** ``` HTTP/1.1 503 Service Unavailable Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Thu, 05 Oct 2023 08:05:46 GMT Connection: close Content-Length: 326 ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Sun, 01 Oct 2023 08:01:39 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2019 (version 1809) OS Build: 10.0.17763 Target Name: WIN-LIVFRVQFMKO NetBIOS Domain Name: WIN-LIVFRVQFMKO NetBIOS Computer Name: WIN-LIVFRVQFMKO DNS Domain Name: WIN-LIVFRVQFMKO FQDN: WIN-LIVFRVQFMKO ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '89.23.96.203']

Name

bfd2c062c12a261c4460cdc59cc9f7e80b72b455e852d08c106f12a3d657a575

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bfd2c062c12a261c4460cdc59cc9f7e80b72b455e852d08c106f12a3d657a575']

Name

877f8a66be5c99d5a4636d74c566d61ebc1951049be5fa8968c132922ca4ba18

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '877f8a66be5c99d5a4636d74c566d61ebc1951049be5fa8968c132922ca4ba18']

Name

6e0062ccdfa7a117a8b76d4056ac144fdf91f3a2811b32d5a3b7f31ac326181b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6e0062ccdfa7a117a8b76d4056ac144fdf91f3a2811b32d5a3b7f31ac326181b']

Name

7b4d227fddcc4e93ea0cdf017026ff2dad6efd6bc7de71b689dc0595a2a4fb4d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7b4d227fddcc4e93ea0cdf017026ff2dad6efd6bc7de71b689dc0595a2a4fb4d']

Name

188.34.188.7

Description

ISP: Hetzner Online GmbH **OS:** None ---------- Hostnames: - static.7.188.34.188.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.3 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPB1wfdXpuk6zC0Yb8QIq2zjUVvUn23XOb5snFkyK79PlGhfE/APkVuDDqqHrXA2Ib+uiWI3/wfvHBuW/+stK84= Fingerprint: 5d:9d:97:f6:63:18:bb:ea:d6:ea:b9:86:e6:cf:a8:2a Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: 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 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 ``` ---------- **9100:** ``` HTTP/1.1 400 Bad Request Content-Type: text/plain; charset=utf-8 Connection: close 400 Bad Request Prometheus Node Exporter: node_exporter_build_info: branch: HEAD goversion: go1.19.3 revision: 1b48970ffcf5630534fb00bb0687d73c66d1c959 version: 1.5.0 node_os_info: id: centos id_like: rhel fedora name: CentOS Linux pretty_name: CentOS Linux 7 (Core) version: 7 (Core) version_id: 7 node_uname_info: domainname: (none) machine: x86_64 nodename: mail.glonass-tm.com release: 3.10.0-1160.95.1.el7.x86_64 sysname: Linux version: #1 SMP Mon Jul 24 13:59:37 UTC 2023 node_dmi_info: bios_date: 11/11/2017 bios_vendor: Hetzner bios_version: 20171111 board_name: Standard PC (i440FX + PIIX, 1996) board_vendor: KVM board_version: pc-i440fx-6.2 chassis_vendor: QEMU chassis_version: NotSpecified product_name: vServer product_serial: 37084117 product_uuid: DD7076F9-A89B-4DD0-8AA5-5DFC01652011 product_version: 20171111 system_vendor: Hetzner node_network_info: lo: address: 00:00:00:00:00:00 broadcast: 00:00:00:00:00:00 device: lo operstate: unknown eth0: address: 96:00:02:8a:73:ee broadcast: ff:ff:ff:ff:ff:ff device: eth0 operstate: up ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '188.34.188.7']

Name

75c562f9101eab86d03386fcf0ddfe3cdebec0008c2c5b5a94047c06ddeb2566

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '75c562f9101eab86d03386fcf0ddfe3cdebec0008c2c5b5a94047c06ddeb2566']

Name

a2c654357d790d7c4cec619de951649db31ecdb63935f38b11bb37f983ff58de

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a2c654357d790d7c4cec619de951649db31ecdb63935f38b11bb37f983ff58de']

Name

006e0b5f47462c4d755b3f84e22b90f09fb6b369032a3ca72f39180e5395ed17

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '006e0b5f47462c4d755b3f84e22b90f09fb6b369032a3ca72f39180e5395ed17']

Name

af5f5aa32a3e2bc802b9863c20de2eac0ca14e1002c02396e63e2aa38eb351c6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'af5f5aa32a3e2bc802b9863c20de2eac0ca14e1002c02396e63e2aa38eb351c6']

Name

ef74d2b8d1767667fb6817916f7d2d2c998358e07422a6af246151e0299f26aa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ef74d2b8d1767667fb6817916f7d2d2c998358e07422a6af246151e0299f26aa']

Name

597541041b49043bd2abd482b3bf4dd233a0dbb47d5ef704ea9ee28705d2764b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '597541041b49043bd2abd482b3bf4dd233a0dbb47d5ef704ea9ee28705d2764b']

StixFile

Value
e38a1648fc6494f881e3b793688ef4d69e925137c4c7494f4dd6c6604142a2bc
7b4d227fddcc4e93ea0cdf017026ff2dad6efd6bc7de71b689dc0595a2a4fb4d
44065decc86f79ebbd56b27f1db8c7bd5843147f3fa8e577604c0ed45317b016
ec4ac7ade34402ad3757e97d03de7aa3dfee0ed53f28f32c99d8dbbb96958dcb
34ea4cad8558fcab75631a44eae492a54e1cf9ae2f52e7d5fa712686acd06437
006e0b5f47462c4d755b3f84e22b90f09fb6b369032a3ca72f39180e5395ed17
597541041b49043bd2abd482b3bf4dd233a0dbb47d5ef704ea9ee28705d2764b
19bae62fc0a3a64c80b666237c2f04706e3b89c5a6ea6be055df22122e5f8a63
f2e2427107648e8d7be5f4e42341c702ceddb442191434128cbbf15c0325d8e9
78784c02843a518bdc546534759dcdb3ea523c54751858a51f39e0f9d1492868
7ab8bcf9b4dc63ad3d9e1fe8eb2e8292a1545871fb2e3b5dd83c96a2b7e33b41
877f8a66be5c99d5a4636d74c566d61ebc1951049be5fa8968c132922ca4ba18
af5f5aa32a3e2bc802b9863c20de2eac0ca14e1002c02396e63e2aa38eb351c6

a2c654357d790d7c4cec619de951649db31ecdb63935f38b11bb37f983ff58de

75c562f9101eab86d03386fcf0ddfe3cdebec0008c2c5b5a94047c06ddeb2566

d0013d23218a1aafdea792a0599b746af6966f765181c8c1dbfe7257be0cb022

d522a32eebc7f0108dbff116b7fa9dd457bf9f062465060115ec423c567c5115

c42ad519510936f14ab46fbad53606db8132ea52a11e3fc8d111fbccc7d9ab5a

6e0062ccdfa7a117a8b76d4056ac144fdf91f3a2811b32d5a3b7f31ac326181b

ef74d2b8d1767667fb6817916f7d2d2c998358e07422a6af246151e0299f26aa

25cc64a072861840df9dfa7b2449165e4c37d57c542da8ec4ea4fffa10f1be39

bfd2c062c12a261c4460cdc59cc9f7e80b72b455e852d08c106f12a3d657a575

86e96d3d22ead8f41f6a29f7bfe4b35c0d4ae5bd8da046ff0d01d9c6ea678dc2

IPv4-Addr

Value
89.23.96.203
188.34.188.7

External References

- https://otx.alienvault.com/pulse/651ec74c1af711eb36638ce7
- https://blog.talosintelligence.com/qakbot-affiliated-actors-distribute-ransom/