Dec 22 2023

NETMANAGEIT

Intelligence Report

Operation HamsaUpdate: A Sophisticated Campaign Delivering Wipers Puts Israeli Infrastructure at Risk

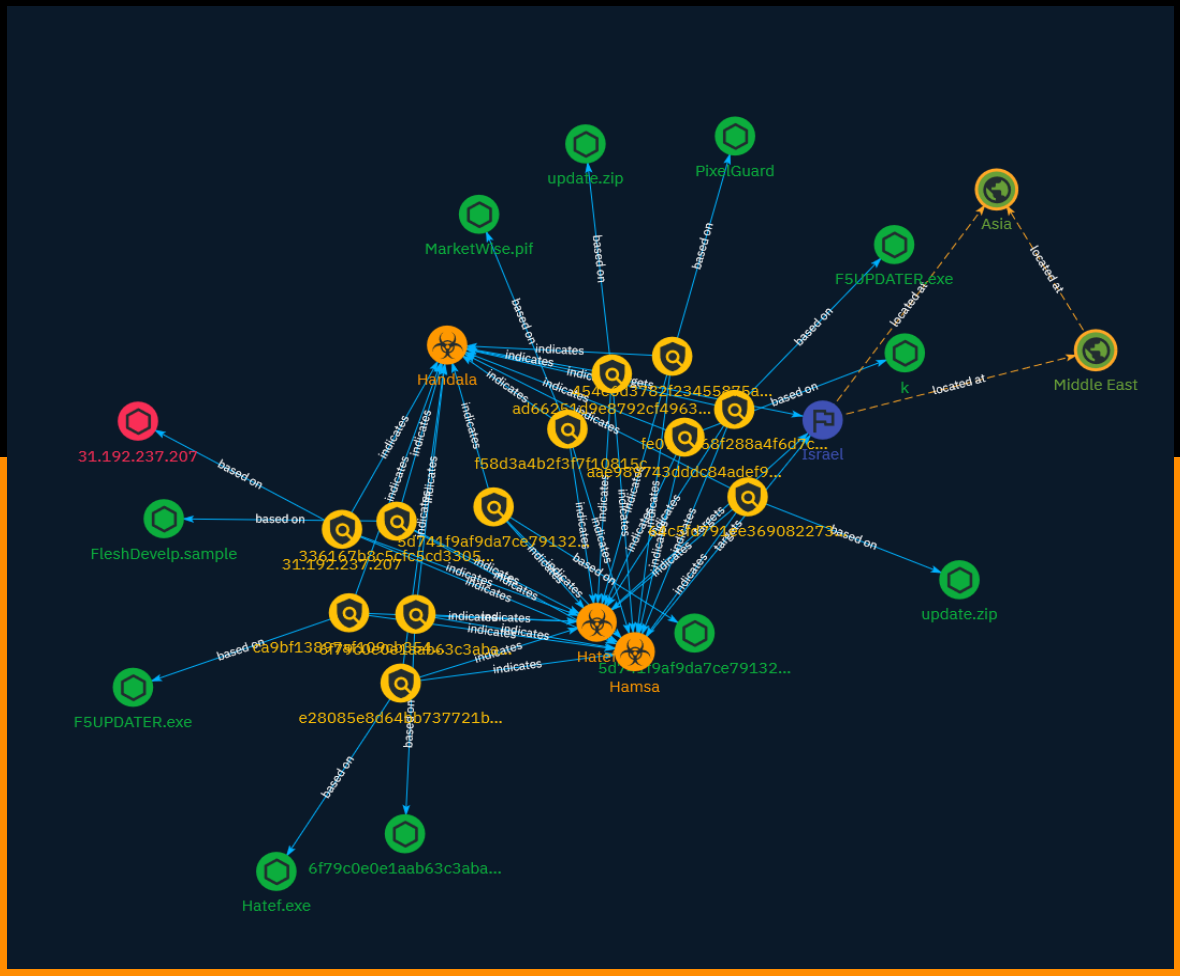

Table of contents

Overview

Entities

Observables

External References

Overview

Description

On December 19th, the Israel National Cyber Directorate released an urgent alert warning regarding a phishing campaign actively targeting Israeli customers using F5's network devices. Intezer has labeled this campaign Operation HamsaUpdate. It features the deployment of a newly developed wiper malware that targets both Windows and Linux servers. The campaign leverages a convincingly written email in Hebrew and utilizes sophisticated social engineering techniques, pressuring victims to execute the harmful code residing on their servers. The final attack delivers a complex, multi-stage loader or a destructive wiper, each variant customized for either Linux or Windows environments.

Confidence

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

15 / 100

Content

N/A

Indicator

Name

64c5fd791ee369082273b685f724d5916bd4cad756750a5fe953c4005bb5428c

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '64c5fd791ee369082273b685f724d5916bd4cad756750a5fe953c4005bb5428c']

Name

336167b8c5cfc5cd330502e7aa515cc133656e12cbedb4b41ebbf847347b2767

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '336167b8c5cfc5cd330502e7aa515cc133656e12cbedb4b41ebbf847347b2767']

Name

fe07dca68f288a4f6d7cbd34d79bb70bc309635876298d4fde33c25277e30bd2

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fe07dca68f288a4f6d7cbd34d79bb70bc309635876298d4fde33c25277e30bd2']

Name

f58d3a4b2f3f7f10815c24586fae91964eeed830369e7e0701b43895b0cefbd3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f58d3a4b2f3f7f10815c24586fae91964eeed830369e7e0701b43895b0cefbd3']

Name

aae989743dddc84adef90622c657e45e23386488fa79d7fe7cf0863043b8acd4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aae989743dddc84adef90622c657e45e23386488fa79d7fe7cf0863043b8acd4']

Name

e28085e8d64bb737721b1a1d494f177e571c47aab7c9507dba38253f6183af35

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e28085e8d64bb737721b1a1d494f177e571c47aab7c9507dba38253f6183af35']

Name

6f79c0e0e1aab63c3aba0b781e0e46c95b5798b2d4f7b6ecac474b5c40b840ad

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6f79c0e0e1aab63c3aba0b781e0e46c95b5798b2d4f7b6ecac474b5c40b840ad']

Name

ad66251d9e8792cf4963b0c97f7ab44c8b68101e36b79abc501bee1807166e8a

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ad66251d9e8792cf4963b0c97f7ab44c8b68101e36b79abc501bee1807166e8a']

Name

ca9bf13897af109cb354f2629c10803966eb757ee4b2e468abc04e7681d0d74a

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ca9bf13897af109cb354f2629c10803966eb757ee4b2e468abc04e7681d0d74a']

Name

5d741f9af9da7ce79132daa37a200afed1cb0c28e47de35d127113d69cbab13d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5d741f9af9da7ce79132daa37a200afed1cb0c28e47de35d127113d69cbab13d']

Name

454e6d3782f23455875a5db64e1a8cd8eb743400d8c6dadb1cd8fd2ffc2f9567

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '454e6d3782f23455875a5db64e1a8cd8eb743400d8c6dadb1cd8fd2ffc2f9567']

Name

31.192.237.207

Description

ISP: Chelyabinsk-Signal LLC **OS:** None ------------------------- Hostnames: - kiston277.pserver.space ------------------------- Domains: - pserver.space ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDMsc79utJFMfOhQZqjoYq2GPYLToVQ4KKaMGzm0M/1k/t8 flTdu6oaVvNEJ/AXZbFn25hpLr9SehwkHUe69qJTGSFhJycrctYtOv94e/Rsd5WC6jysUyYwJYYETKuCY96FbXBKcb+DJekOfXEtEbfDcl6ZUY+GmZ6hct6aNqCRQ4qx4WXsPDXQ2/9kCe2KTqrqrO/o5O5KH4N4LmBTz4ZHypPWhdvsGuvpJtKOtYO5VvfTGzBQqC0/DX1WhSVJ89AzM28mbjo6hTlbQJFQ 2Mp6IVbR+gLhKvknHYxPbof6wBho93t0/hnrFF9gGFthcRK3evuNVCW3BxQ/bcbDibOH Fingerprint: 3f:a5:f7:23:de:8d:cb:40:d7:47:b7:7f:e8:f0:3d:ef 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '31.192.237.207']

Country

Name
Israel

Region

Name
Asia
Name
Middle East

Malware

Name
Hatef
Name
Handala
Name
Hamsa

StixFile

Value
f58d3a4b2f3f7f10815c24586fae91964eeed830369e7e0701b43895b0cefbd3
6f79c0e0e1aab63c3aba0b781e0e46c95b5798b2d4f7b6ecac474b5c40b840ad
454e6d3782f23455875a5db64e1a8cd8eb743400d8c6dadb1cd8fd2ffc2f9567
64c5fd791ee369082273b685f724d5916bd4cad756750a5fe953c4005bb5428c
336167b8c5cfc5cd330502e7aa515cc133656e12cbedb4b41ebbf847347b2767
aae989743dddc84adef90622c657e45e23386488fa79d7fe7cf0863043b8acd4
e28085e8d64bb737721b1a1d494f177e571c47aab7c9507dba38253f6183af35
ad66251d9e8792cf4963b0c97f7ab44c8b68101e36b79abc501bee1807166e8a
5d741f9af9da7ce79132daa37a200afed1cb0c28e47de35d127113d69cbab13d
ca9bf13897af109cb354f2629c10803966eb757ee4b2e468abc04e7681d0d74a
fe07dca68f288a4f6d7cbd34d79bb70bc309635876298d4fde33c25277e30bd2

IPv4-Addr

Value
31.192.237.207

External References

- https://otx.alienvault.com/pulse/6584316b9546f2e5af862d6f
- https://intezer.com/blog/research/stealth-wiper-israeli-infrastructure/