Aug 18 2023

NETMANAGEIT

Intelligence Report

Old exploit kits still kicking around in 2023

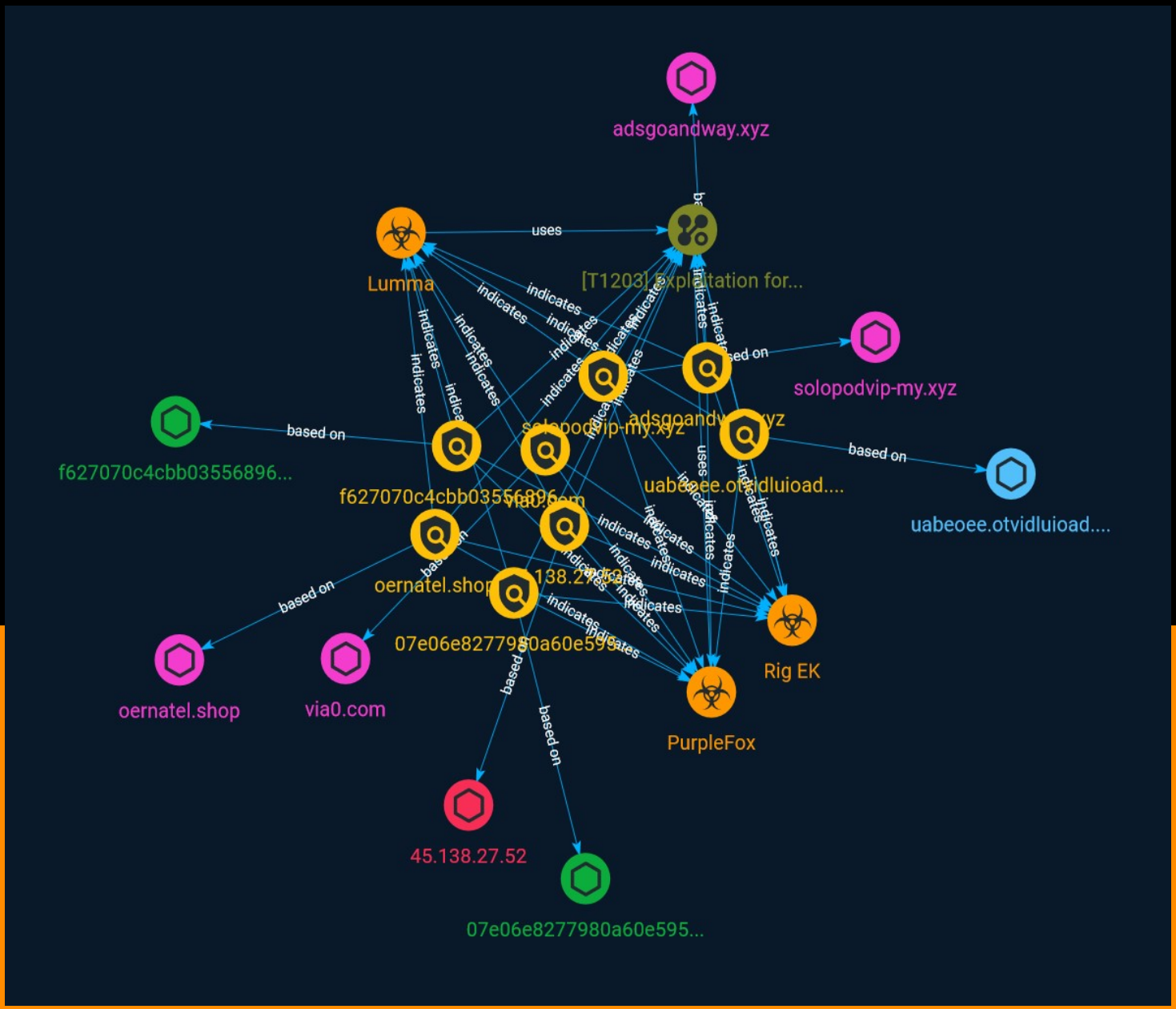

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Malwarebytes provides a comprehensive guide to how to protect against attacks using Internet Explorer, and the threat actors who use it are still using it to deliver malware. the year after the 9/11 attacks.

Confidence

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

15 / 100

Indicator

Name

45.138.27.52

Description

ISP: ITGLOBAL.COM NL B.V. **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_9.2p1 Debian-2 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBM10gjIVD0bhG6ZOtVeUcRiLMJYIchEfKBgfrIHYHH3b+B1GWyL0SAzAGXU5qyzNiwmF1fGNvcDcPXXwGqQtBz0= Fingerprint: 46:67:5f:28:cc:c7:8b:f6:b1:34:08:e4:ca:98:98:f7 Kex Algorithms: sntrup761x25519-sha512@openssh.com 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-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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx/1.22.1 Date: Sat, 12 Aug 2023 11:26:28 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: keep-alive ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.138.27.52']

Name

07e06e8277980a60e595da9cd9e03a4ecd2e8f8bdbd3cf5c930ab878ac5b0836

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '07e06e8277980a60e595da9cd9e03a4ecd2e8f8bdbd3cf5c930ab878ac5b0836']

Name

f627070c4cbb03556896601870cf575b1c8f47b062fdfef5c3516ff5a07db40c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f627070c4cbb03556896601870cf575b1c8f47b062fdfef5c3516ff5a07db40c']

Name

adsgoandway.xyz

Pattern Type

stix

Pattern
[domain-name:value = 'adsgoandway.xyz']
Name
oernatel.shop
Pattern Type
stix
Pattern
[domain-name:value = 'oernatel.shop']
Name
via0.com
Pattern Type
stix
Pattern
[domain-name:value = 'via0.com']
Name
uabeoee.otvidluioad.online
Pattern Type
stix

Pattern
[hostname:value = 'uabeoee.otvidluioad.online']
Name
solopodvip-my.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'solopodvip-my.xyz']

Malware

Name
PurpleFox
Name
Lumma
Name
Rig EK

Attack-Pattern

Name
Exploitation for Client Execution
ID
T1203
Description
Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility. Several types exist: ### Browser-based Exploitation Web browsers are a common target through [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) and [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed. ### Office Applications Common office and productivity applications such as Microsoft Office are also targeted through [Phishing](https://attack.mitre.org/techniques/T1566). Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run. ### Common Third-party Applications Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise

environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

Domain-Name

Value
via0.com
adsgoandway.xyz
solopodvip-my.xyz
oernatel.shop

StixFile

Value
07e06e8277980a60e595da9cd9e03a4ecd2e8f8bdbd3cf5c930ab878ac5b0836
f627070c4cbb03556896601870cf575b1c8f47b062fdfef5c3516ff5a07db40c

Hostname

Value
uabeoee.otvidluioad.online

IPv4-Addr

Value
45.138.27.52

External References

- https://otx.alienvault.com/pulse/64de06ea3bfe29b3fe0d6490
- https://www.malwarebytes.com/blog/threat-intelligence/2023/08/old-exploit-kits-still-kicking-around-in-2023