Jul 03 2023

NETMANAGEIT

Intelligence Report

GuLoader Campaign Targets Law Firms in the US

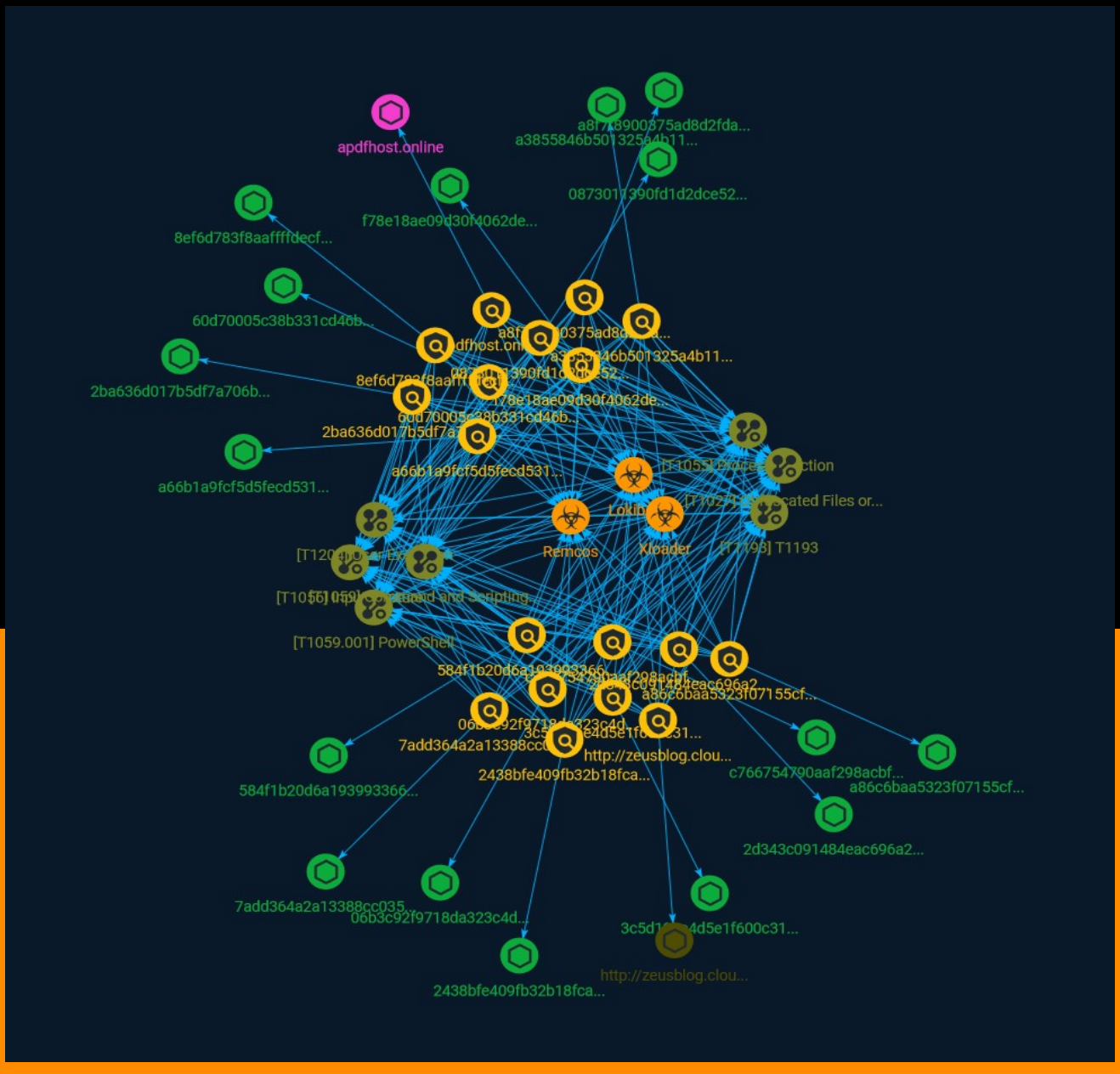

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A security researcher from Morphisec Labs has identified the source of GuLoader, a malware that targets law firms in the United States and healthcare and investment firms, as the target of an active campaign.

Confidence

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

15 / 100

Indicator

Name
c766754790aaf298acbf85229096d8f0493fa9ee64d429facd425e30ceceaa4b
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'c766754790aaf298acbf85229096d8f0493fa9ee64d429facd425e30ceceaa4b']
Name
60d70005c38b331cd46b8af0f8e3d8cf181bdf43fb685a1962b1e26e085a6e2a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '60d70005c38b331cd46b8af0f8e3d8cf181bdf43fb685a1962b1e26e085a6e2a']
Name

f78e18ae09d30f4062de466afb5e1de5041b6cda445b15a3cca912a3294f731a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f78e18ae09d30f4062de466afb5e1de5041b6cda445b15a3cca912a3294f731a']

Name

06b3c92f9718da323c4d3a18d69629696dc5f799a7ddaef4e7415d117b345af4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '06b3c92f9718da323c4d3a18d69629696dc5f799a7ddaef4e7415d117b345af4']

Name

apdfhost.online

Pattern Type

stix

Pattern

[domain-name:value = 'apdfhost.online']

Name

a86c6baa5323f07155cf414cdfd667216fb2816ec999ad240042c78b86175492

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a86c6baa5323f07155cf414cdfd667216fb2816ec999ad240042c78b86175492']

Name

584f1b20d6a1939933663dd57e13603c7fe664f81a117f0d5456b4d448506b7d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '584f1b20d6a1939933663dd57e13603c7fe664f81a117f0d5456b4d448506b7d']

Name

a8f7f8900375ad8d2fda626f098cdda95bb4e42855cbae91c290d3f020bfd45f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a8f7f8900375ad8d2fda626f098cdda95bb4e42855cbae91c290d3f020bfd45f']

Name

3c5d19be4d5e1f600c31f837b9650ad8c7508d6691f6cd4889d2178809703de7

Description

invalid_trailer_structure

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c5d19be4d5e1f600c31f837b9650ad8c7508d6691f6cd4889d2178809703de7']

Name

2ba636d017b5df7a706b4dfede215733807fff6db5fea202e4a5b6bf515ba8b4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2ba636d017b5df7a706b4dfede215733807fff6db5fea202e4a5b6bf515ba8b4']

Name

2d343c091484eac696a23418f04df81c35bc538a10d25193ad014d11c4422907

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2d343c091484eac696a23418f04df81c35bc538a10d25193ad014d11c4422907']

Name

7add364a2a13388cc035e5f082f7adbb76c1e60d82748acd3eb30d6c9b3ce5be

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7add364a2a13388cc035e5f082f7adbb76c1e60d82748acd3eb30d6c9b3ce5be']

Name

0873011390fd1d2dce527a726607255693c306774dfed8ac6b5b88efd4920d48

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0873011390fd1d2dce527a726607255693c306774dfed8ac6b5b88efd4920d48']

Name

http://zeusblog.cloud/Adobe.pdf

Pattern Type

stix

Pattern

[url:value = 'http://zeusblog.cloud/Adobe.pdf']

Name

a66b1a9fcf5d5fecd53152ecf68be150028109f484ad349d7029d72b3c5c9564

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a66b1a9fcf5d5fecd53152ecf68be150028109f484ad349d7029d72b3c5c9564']

Name

a3855846b501325a4b11cbc27fac9f845a56c91e088edbd75fb5ab651f913ede

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a3855846b501325a4b11cbc27fac9f845a56c91e088edbd75fb5ab651f913ede']

Name

2438bfe409fb32b18fca95f95fff85a778502553ce627d0f25e54653c84e0e0c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2438bfe409fb32b18fca95f95fff85a778502553ce627d0f25e54653c84e0e0c']

Name

8ef6d783f8aaffffdecfa13bcc20b4f1a18f6c4c3c4cc22e93fb5c8d753ca338

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8ef6d783f8aaffffdecfa13bcc20b4f1a18f6c4c3c4cc22e93fb5c8d753ca338']

Malware

Name
Xloader
Name
Remcos
Name
Lokibot
Description
[Lokibot](https://attack.mitre.org/software/S0447) is a widely distributed information stealer that was first reported in 2015. It is designed to steal sensitive information such as usernames, passwords, cryptocurrency wallets, and other credentials. [Lokibot](https://attack.mitre.org/software/S0447) can also create a backdoor into infected systems to allow an attacker to install additional payloads.(Citation: Infoblox Lokibot January 2019)(Citation: Morphisec Lokibot April 2020)(Citation: CISA Lokibot September 2020)

Domain-Name

Value
apdfhost.online

StixFile

Value
3c5d19be4d5e1f600c31f837b9650ad8c7508d6691f6cd4889d2178809703de7
a66b1a9fcf5d5fecd53152ecf68be150028109f484ad349d7029d72b3c5c9564
584f1b20d6a1939933663dd57e13603c7fe664f81a117f0d5456b4d448506b7d
60d70005c38b331cd46b8af0f8e3d8cf181bdf43fb685a1962b1e26e085a6e2a
06b3c92f9718da323c4d3a18d69629696dc5f799a7ddaef4e7415d117b345af4
a86c6baa5323f07155cf414cdfd667216fb2816ec999ad240042c78b86175492
8ef6d783f8aaffffdecfa13bcc20b4f1a18f6c4c3c4cc22e93fb5c8d753ca338
a3855846b501325a4b11cbc27fac9f845a56c91e088edbd75fb5ab651f913ede
2438bfe409fb32b18fca95f95fff85a778502553ce627d0f25e54653c84e0e0c
f78e18ae09d30f4062de466afb5e1de5041b6cda445b15a3cca912a3294f731a
c766754790aaf298acbf85229096d8f0493fa9ee64d429facd425e30ceceaa4b
2ba636d017b5df7a706b4dfede215733807fff6db5fea202e4a5b6bf515ba8b4
7add364a2a13388cc035e5f082f7adbb76c1e60d82748acd3eb30d6c9b3ce5be

0873011390fd1d2dce527a726607255693c306774dfed8ac6b5b88efd4920d48

2d343c091484eac696a23418f04df81c35bc538a10d25193ad014d11c4422907

a8f7f8900375ad8d2fda626f098cdda95bb4e42855cbae91c290d3f020bfd45f

Url

Value
http://zeusblog.cloud/Adobe.pdf

External References

- https://otx.alienvault.com/pulse/64a2f8202cb39e7c1a90cd3b
- https://blog.morphisec.com/guloader-campaign-targets-law-firms-in-the-us