# About the malware family:

PsiXBot is a modular piece of software which was found first in 2017 but this has undergone significant developments of its core and modules, which include the logging of keystrokes and stealing of Outlook and browser credentials.

File Type : PEXE - PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

PE Packer : .NET executable

MD5 : e524d8066aa47ae1da9a73ee3eeb2262

SHA1 : dc7cf5808417cd8d271e8270f44a1beb95c23ec0

SHA256 : ca30c42334fcc693320772b4ce1df26fe5f1d0110bc454ec6388d79dffea4ae8

IMPHASH : 72779b978cbe963afc19d5595ff38c1f

PEHASH : ddf47f62197f859ddfa2561cc1f0f9dc91374e34

MD5 : b9f3f4d8f493617d347d633fa9104b12

SHA1 : 6e83f8913871d30f04154c5ca84362c68278d8f4

SHA256 : d2ee07bf04947cac64cc372123174900725525c20211e221110b9f91b7806332

IMPHASH : f34d5f2d4577ed6d9ceec516c1f5a744

PEHASH : dcb667b24dbdea5aee451b4a36f54318e2e0351f

MD5 : 154cc6ee7de3f085a4bb18145fb49117

SHA1 : 0cb776aa118e9014c480fe19f1e94b254f4318a0

SHA256 : ce0e46fa1c5b463ed4a070a05594a79203ed2dd5df96cece9f875e2957fda4fa

IMPHASH : 1d8a37f2c80392d743f9173bfa9c98c9

PEHASH : [f80ddd98f22537a335780b65a41bd9ed](https://www.virustotal.com/gui/search/rich_pe_header_hash%253Af80ddd98f22537a335780b65a41bd9ed)

# Sandbox Reports:

Any.run report

<https://any.run/report/d2ee07bf04947cac64cc372123174900725525c20211e221110b9f91b7806332/983b8adc-e60f-4fe4-b461-a37fa8142c6d>

<https://any.run/report/ce0e46fa1c5b463ed4a070a05594a79203ed2dd5df96cece9f875e2957fda4fa/3033dabd-9034-45a1-bbf9-8d3809005a0a>

<https://any.run/report/ca30c42334fcc693320772b4ce1df26fe5f1d0110bc454ec6388d79dffea4ae8/3e2e76e9-1b47-44c4-81da-7c89bd1f63eb>

Hybrid analysis report

<https://www.hybrid-analysis.com/sample/d2ee07bf04947cac64cc372123174900725525c20211e221110b9f91b7806332>

<https://www.hybrid-analysis.com/sample/ca30c42334fcc693320772b4ce1df26fe5f1d0110bc454ec6388d79dffea4ae8?environmentId=100>

Alienvault Report :

<https://otx.alienvault.com/indicator/file/ca30c42334fcc693320772b4ce1df26fe5f1d0110bc454ec6388d79dffea4ae8>

<https://otx.alienvault.com/indicator/file/d2ee07bf04947cac64cc372123174900725525c20211e221110b9f91b7806332>

# YARA rule constructed:

rule psixbot

{

meta:

created = "21/08/2021 11:15:00 AM IST"

modified = "28/08/2021 10:15:00 AM IST"

author = "vijayabharathi"

description = "To find PSIXBot files using strings"

strings:

$str1 = "VirtualAllocEx"

$str2 = "ModifyBootConfig"

$str3 = "acledit.dll"

$str4 = "crypt32.dll"

condition:

$str1 or $str2 or $str3 or $str4

}

# Output:



# References:

<https://malpedia.caad.fkie.fraunhofer.de/details/win.psix>

<https://blog.fox-it.com/2019/03/27/psixbot-the-evolution-of-a-modular-net-bot/>

<https://blog.katastros.com/a?ID=b09d294c-427d-4652-87c5-8aa9c4766f0f>

<https://vxcube.com/recent-threats-ioc/5c9da5c7a39bb56c09651b59/detail>

<https://vxcube.com/tools/domain/manage-shope.com/relate_iocs>

<https://manalyzer.org/report/e524d8066aa47ae1da9a73ee3eeb2262>

<https://www.malware-traffic-analysis.net/2019/03/16/index.html>

<http://en.hackdig.com/09/83333.htm> (not opening now)

<https://www.hackfence.com/w/psixbot-the-evolution-of-a-modular-net-bot/>

<https://www.proofpoint.com/us/threat-insight/post/psixbot-now-using-google-dns-over-https-and-possible-new-sexploitation-module>

<https://www.proofpoint.com/us/threat-insight/post/psixbot-continues-evolve-updated-dns-infrastructure>