Jul 25 2023

NETMANAGEIT

Intelligence Report

PurpleFox Distributed to MS-SQL Servers

Table of contents

Overview

- Description 3
- Confidence 3

Entities

- Indicator 4

Observables

- StixFile 6
- IPv4-Addr 7

External References

- External References 8

Overview

Description

Developing a new version of MS-SQL, which allows users to access the code directly from the web, has been described as “unprecedented" by its creator, Yoko Ono.

Confidence

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

15 / 100

Indicator

Name

64.227.152.193

Description

ISP: DigitalOcean, LLC **OS:** Windows Server 2012 R2 (build 6.3.9600) ---------- Hostnames: ---------- Domains: ---------- Services: **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Fri, 07 Jul 2023 14:11:37 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: TEDDY2012 NetBIOS Domain Name: TEDDY2012 NetBIOS Computer Name: TEDDY2012 DNS Domain Name: TEDDY2012 FQDN: TEDDY2012 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '64.227.152.193']

Name

0a970e58599c403de3ef186fff03565913e47b5c22f9bdf55b84a9f497b10520

Description

Trojan:Win32/Tiggre!rfn SHA256 of f725bab929df4fe2626849ba269b7fcb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0a970e58599c403de3ef186fff03565913e47b5c22f9bdf55b84a9f497b10520']

Name

46ba198ec579d4a968e9b7760e615a097c0de8889e7f3acb081dcc11de17f432

Description

SLFPER:PsObfus.A SHA256 of d88a9237dd21653ebb155b035aa9a33c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '46ba198ec579d4a968e9b7760e615a097c0de8889e7f3acb081dcc11de17f432']

StixFile

Value
46ba198ec579d4a968e9b7760e615a097c0de8889e7f3acb081dcc11de17f432
0a970e58599c403de3ef186fff03565913e47b5c22f9bdf55b84a9f497b10520

IPv4-Addr

Value
64.227.152.193

External References

- https://otx.alienvault.com/pulse/64bfca997135d1348a7563c8
- https://asec.ahnlab.com/ko/55302/