Jun 11 2023

NETMANAGEIT

Intelligence Report

New phishing-as-a-service tool “Greatness” already seen in the wild

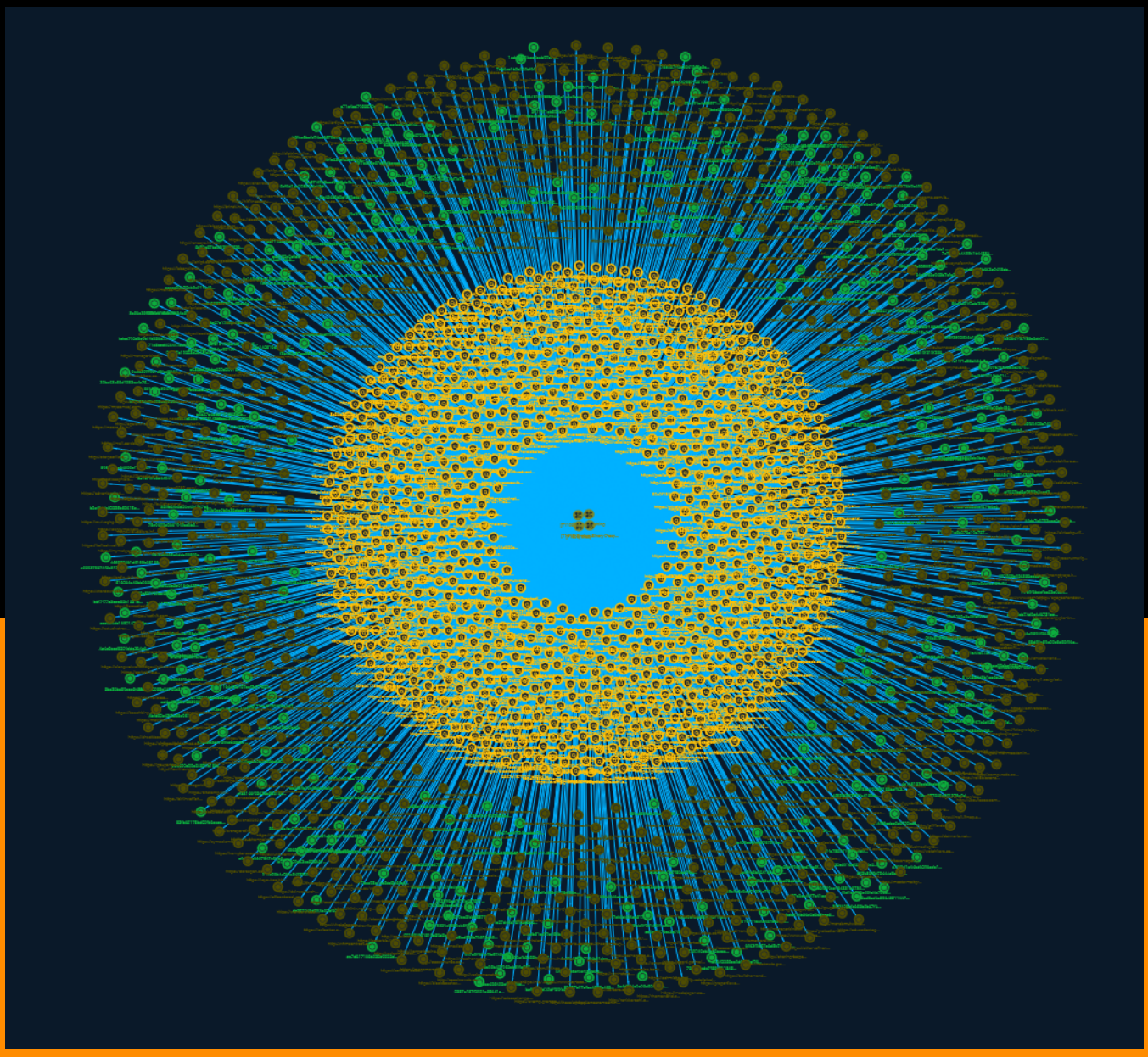

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A previously unreported phishing-as-a-service offering named Greatness has been used in campaigns targeting Microsoft 365 users, Cisco Talos has revealed in a new report from the security firm.

Confidence

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

15 / 100

Attack-Pattern

Name
Phishing
ID
T1566
Description
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Proxy

ID

T1090

Description

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name

Native API

ID

T1106

Description

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. (Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Native API functions (such as

`NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations. (Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. While invoking API functions, adversaries may also attempt to bypass defensive tools (ex: unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)).

Name

System Binary Proxy Execution

ID

T1218

Description

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands. Similarly, on Linux systems adversaries may abuse trusted binaries such as `split` to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

StixFile

Value
5e766013f476645bf6088aed86db14b65876d017918f910ec87224139ab93083
f9d1ba792a00fd4b705a9a9a9537ec2b27f57f39f798391f18817e7e3d3feffb
0f09174f1b83798abf0838cabc45bab696d95a4600f62745a6357e4822b62b56
41a53a723ea744ddf3861e3a3f152a2828cc3c47a2fe861ab78c5fe800f11322
e8aa01474d0c779a222d3c578e207f1c2a3df88c4896c35f0c67bac5015a1869
ca0ef1075ae3e79f5599b89ed37b3f806de2533a23a795020ff710b0b01058dd
a3c785c339ad70342c75a0ce902c614a8529afccb62f609a2c31567f4284523d
88ed33350c6f95666cb71e3086046717249820a11ee2db19252a02607ddc0cf5
1f7f19e1faad0a2d223efd5e00ea291078b41b4fd202e9aee5b16e8ecadb230e
b2fac5bafd74ca6570b4a4d8515b4852dbfbca84c10da3fc9f13f67baa9864dc
49de7c6733eae0c53d6bfe75b56d6cfe945e06e2972388ddc73709df6d616795
e4a37e4a5df199568b6cb76a5e4c8e7f5bdcc8a7f49c25763e6444aa3501fba2
91ff6107e6d9353b3a7d6ff6f1f2d62006a3763f3ce647d0782db7a72a3f3885

b507313abafc8f16095d9cbf8fbe980063e7e7435b66ab4c5b4b7e7c4a90e686

286e64300d13f0aa9adbef63382625c2fe73454414646038ba73b43f1353c58d

a638dd7dbbe629d20916bcb3ce66cf0877271c411d373acff5a9da60ee49c4ae

30be63a85d1383aefc7575ffbf0cd39c34a009a578c8193d19755335c43e2868

811367c503ca4d2ad64427e7f3d717bca115ba14bca6c10d00b4783a9ed1c2f5

46b44d1b1ecd0b8cc7ea742060882ca2512065ad39e432627768a3ede59ab771

11d980af0e1f9576b2b2fa319ee58a49ee72f4722e96141ce5990b37248cad42

3933ff6cc7977c057571f3d189f2cdb157c86c4477367de6f9f092e74d060753

172852899cc09d7a2cee9bef8616681929f1ab958bf8cba80daeff7e7402f7ac

135fc7231eea38524cf130b8c1b155396f26071958c04c74a985c3ec409dbca3

086ac7e2cc7c9e4df63d6330a919aed237f327b45c11241dc6f684ee8a57770e

1414f88cdcc0c6900cc5205af1b2ebaa059451221c949fada29b89a6c73f65f0

e23904e3663f2ab2d6c3a287023cff35878427d0fc1cf20692d479390437c11a

14bea33532ef39097a18360ef607b5155dcb52ef512f6a94e4a3f6efff076080

9242594acfaeb04dff433c586fb0d6a34d3bfba7f6ce788fcaf3a181a6d21056

4c5e9d4a4208b1d337f347590d8dbe271e2510f2edd4ff66fde03e3300a618aa

78ddfe73272c6604363b163b0ce2f9700e4b2c372fb9c9c2d5eafc81de0d26e6

349e751a4c1074e6ee318c68b71f03048dc141f9fe1ab27da6786825d5785e30

dfa3174b6ed50069e22a2110569ba1fd50e6f06fe1c69362ff0447fb7888f226

345c056b556265eb0bdb869c9958ec680f881396f6b78a929d7bcc67b0f34481

9715209c6b42e603438db821eeea0d8b9e46189bad4abd2c4c9e777531883be3

916732ddf94e56be6dd1eb6cc67f6d394e171e4be0a38847e2a385e9163d5f69

21db43456b0af069ceb129b477d2d5a6f70c2659364de9ec4e96146f0be291d6

215b3abf3fc8f7bbc673a2675ae08245a168c3ec92223ee861c568f6524c64d7

59692255aa9d6881ef965798dc5356fb73e52797fc837fde8e5a3adf1d6215b2

b0a51d124b2f1804d937d432e510b97febe22bb30ca4e00c632a173eddb2cd43

5d31a57bc05f56f3f236ad8748f6b1d13b6bf303d785989c7613ba6be4d97aaf

7c78425a4488b1b448866f826d4028dfd90779c8eacc2d0f897ac1d312b17214

90f05f293af5d55107c892f172ded79badc2664d48b77090c3a17385e98e7376

88b9a8d6ad01501c701bb17e5f939c57f1ae05b96b1eb201f123046831617150

ad961f773489b05eb486768bff0ff1f4383d33982003829ef996223e3b2c0428

d69b8193e33fd0792bfe4ea871f94c5eb639e0159c7c65269e4a22d29277ebb8

3f8f1ae97b722c971c27d96e60f2903608957cceff6bf033bd21a178785246aa

06b0a9f1f81abf4fb589726417ef87150b250ce312b345e5c2a5389b0cf29f59

c020373274f2b8175b9268aa53b40b62a6d2863f36803a495a400a5f4f7fc09b

72ab28cda7f85b711843dcaf14ab35a4397cd3b0181fd5906cceee930d5ce86a

ee6e20bff9694cd76a3f332ad29f244e8a68aa2ac76f4b0c7f541f1d60215249

be885b948903458a1efcc923587dcb2a2d601ef6bbee18885d96e5e7db26a8fe

217f05dfc9065ae35ca98ded67fea7e47f4c4482b7c0371cf3f7da2af8c28a66

82e2f185437e2edd4f405138463b18f94f634c9d56b16bcc4bc01afc242198fa

b300882767714afe95f0444c0196f2807c2c80c7ead8f12a8dd43a7a2683b953

468080261d5183b0810823e7c7edcacd05beab313cfccee810e4bf26f9581574

8d47f188b2346eab0c9f63693034a4d05b1c14fd6851759b112c258020293dfb

24c43e07c17580a7cecb124270d6b4ead46946572819241d6043c38e961465b5

bb2f299ec184331c978807d69d758b4e8e2fd438d7a10bd5ff584721759357f7

4bfd50c43f2e88c981fb138b49cd85edeba4aa640cfef4316ca1cfcc5b96224d

85dacd1461a6f17f0d008b9161905cab08649d88bffc5707c2480ff6dd7974d3

f2ac0644b05cccb30ffc5f338dc555f4ccd2ea391e6aabf42e70c6e5a0727cad

f7a04d7e7465237bcfb0b0e705b56fdb5ad6c0aa7c7fcdd84981fcba0b89bbde

6963f9d27e6d8b742ee73207da2024f76d9a7d1d8f156d8424f06d5fa3edc9fd

3ebf912d3577356fba7966073312b99a75a20e7c9f0ae36f6f44c30785d9e019

a13942d9ec431dfddbe727f492888e64a72abe853618462c4927e26ce141dc93

b3f084ffd8a4ef8d58b3ccb398696a496ca9c605b6ce4acdc2993d9c7ce6d3c0

0a107e19223d2a48fa0d16309435b2539993bd33653ad762452e3563f21f2de8

675456fe2dcfaaf50d24b2e5d69ba03e45a51fee5f7c86c1a98aad33be16c603

9937f4ab00c4d41c8986a4d4e5a2a4193412e031c5a33d5f88913cc8dd0b5d4f

7b81a27d46b7575cd3621d097af6f08b50c45bb5d0a4b53f459334d213f408a6

9f3cd24fa617e607e195e167c3de21dd0c33f34ffed30d4725c3a83390d9087d

ed4cd5308bf283928dfe5e3a0985e90c82014136a87fdac13670e0748482b5ed

9b9c33983cdbaa6317cde41b44b57a1df67ecc9dbd1f9de9f4bc1e2bfe09b5fb

606b4d02f36151270e0e31e2afc82359ae10b26641b77d6fce33ab96a90148ad

9a9ad6668c6dcb03502a05ac4f303adce15b0ce69aa8d848d47919eb95415cd7

39b2c18fe846f375dce3cf10640aa23d9ebb98a17b9a1ba8e9d5e8cb97814acc

b2b55f31b56c2bbdcee7f89919c28ddfb32040a96306c53775126168fbaa2593

9251da13aa26c34e51160679163990795e43d6ab703ef52c28dea2306db5937c

98636b07b82fb73a9579375fcffd53347409c4d8069cc69559c60a17ba66d2b4

ca130ace64ce6277b612c0e507a5b8e37e54b4f635b18d896992a844ca99de72

10bc277228a221378e0d1cc0e1166b6d46fd51b7134eba3694e32c398db03d24

17bae93a14e5dd3462e098bb8138c71ea027734111912184024a5e77c26c40f7

7d24830212e69b97132bf0f577cd37d66b9bf3431c10343a35636dc5e1406c19

afec48c2607847a0ffc029d53da525353abbeaa2e4f9a82463b62a8cd6fb8066

232b35fde497d4464a6e9e82ec6ed54ba9c3f076449efb24830620e29246eccf

516264a46bb062693db73ad11c963393617b83be61e63890fa213a51ffc78cea

f5f7b623c67e334beccc89a58a9f9ed63e5b90cd20d0fff4079c5955e6389f27

36179f1eb807c92a1c6aebf4006fced293e0f620ec48ceeb3845ae0f48434f49

2bf60d8b70adb392e68f4ee4f1726975fc47cb5c7ac13d6cd00d0f45574d10e3

cc26ce29c555dbd831595c805b70f89d3e6cd954911d235c8ebedcc4519fc997

c6e3558270f0fa55eb6d1f11072672a99ecfde0d80e5b8d78e387eede8f83db4

4396989d091b75cfffcdb4978cf46bd689a8a3411674e2039461eaa1eb37e5ae

c9f8cc96faf0975d35e11279004ec842f0d013974d756d35dce60701d54315b5

1d2569fdb0cc8553f351ef670fa934e989f4f7b80343645046a509ae10262c06

5bc32be89aac54560637a2b311991d20bbe7ad70fc99737f4c0652e0f12d04bd

52b41b17295c28ac5df34518cb0243772147d2a6a5074ebbf1f1ace0809a6a83

24a3782a923b7afa2f513db339469d0e0f61f1f66043554ab642fd3404bf2fd3

53b5fcdae66b940d90adc7cbf0e1a86cafeea0a44c3ffde511bd853c81902d12

cae49fe3b224160c790fec72309f1bdb8f0e1d7c8a82a49262b12707b1789ce0

83fb60178bd00fb6aacef43aa327b3f9d74424cadbf0b9d06e9d5b448bb8fbb9

6a05b407962ab39fe007c2eee5f8160bf6cc347ce7ff71dd542fc4ed345a1e5b

81098d4d8b1ea6b2e7f6bd7c690a8ef7f1e6a525e873627d8162c3f0cd60a6ce

ac70af814d4754d0eb128eeb05e60369a0a0ce0da2640728911f08a75bb31f0a

b97b88447b008cc9623d0820f8179dedf1831c88e273727186fe1f29b3d0a7f9

5f2f17cb0d454ee51727dceb48f480cfa6a3ff2ca6c8f812fd63bdfb0cc05445

62cf7ec43cd5eba4c4579c20c338fa977ea7e7380e339a14e2b2a7d7ac5efb3b

f0f0d7bb3b19f519f38653c1720afcaa6d9fbb585eb1cda835172e910a941693

9630e8af5bdc0891643faad41fc4366f88d17884b7e633219d36e7314e974192

b995c44fb0140a9e8333a27d9ec814b0ec2fd5495708ae0010453f0e08f9674d

f8b422c87ea8860bfd935a57c36da224264d93210b64e58d4c3ce1ede55b8d3e

a5a9c0543f3892536b1f07b9da1e3883ecfcd1fd36339e2daa187f2c070a2f00

a71c4ed7955570a7366a6ca87e97b96babcb3c53dc707e4489c6c4eaae65d566

867f498afe683b5b67f68b671ef95ed5c2eb77ce511708ac6d86d4f0a7ec2c55

13048f2c755d4b83d0dc63298776734855828230 3da4f9034b84bfeb85f4a71e

db2d9ab74d0c4d6731cccb53bc1e7b200bd916d34d284971e34c2c462837d2e2

5d3ee55fd11688c5bf63af51cfdade41126adf6c482dfe20e2827861b6e15f25

bfdbb76498865202ee85450cae2e7fa6654e5326a5aa489cf8281ff73171b63d

45835f8ff3781b4159de056ff1deb0a1e91679fbbfa71254b43638a8aff1a15e

cc89d07aadd55a180539489fe76774f012b5dfceeb6baf7af8e9d88f39db25e0

36545419a28143921efad747ac4db92381c790ebb6b01a3d258e099c315a2faa

214c8684ad99e01f8b4dae68f29f5e460878571d7f821ffaa96e6a8627cc1cc7

dd6fdfa23adfe2cab4fe6ff30230635956133a9813a92aab0c84da5245f85b1e

fc008fdd9f9d14891cccec3a1b15de044bcb01c00c4979807673366c4b1de3cd

638d29911e76b654ac5c6a61ca8677d65b2f958c57c8e69150d453b767ce662b

89b01ed4f734feadde058e8c9b96ac70e54a0ed1504aac8186318493610f5001

893b86f5c73444d8a2195db53ead97e7ee04b5d85626307749df7bbe1ff91fa3

1267543ca491fb06ad800faecde0256b3e41a5ee11506668e59e7936e6dcedc4

5cddda4c0b663c0498dac4590bcb9114c6d7bdd288c0add5c54a81f0adf15a0d

9ada307f961d3fad8669dd49696bdcc3f598daf064c2fe4f4f7fbfb655bb56ad

dbde614b36c2d3a3bac80ba1455b6017b33c0ec606a288783d9d133be7ca4e10

00ace99ddb54b5e52f424cd2d79865583d28b377be2eb96da5f758fb0aafb5df

276a02b09b33987a7147117f5c7d153116b3f5729b1d11622902fe50748778aa

84058f45b7a8adb5bd0a21e2e8df18f419cae98bf92eaaafabfd84aef36cbc59

492a45dd47acb19c6995acdbfce22a0cbcc135bc0263fd3efab165b1b75c9f68

2fa1dcef3e735e4b318febb517ed711410a131c7aa4cfca4669597400dd28014

f20caba9b2985dc5601e0303bf5dde61a0c4d0a7b81c8eb2b01005b342cab51d

afa98126b07b96a41840e86409354d63e7d6d207f398eb5fae60e79d58e532bb

ffaf750766f5fb62d1606cc1187672801bc389a60faff4410e83e16a6a40e6a8

0db263f9a873141d8256f783c35f244c06d490aacc3b680f99794dd8fd59fb59

071550631810c59d5ad6303b60a03ae9c7af5c125de3b846415db4a3dc45bb14

c9375f405c6409087cfabb34bdc8e9d1333f8b1f6448395a3889856a07ba3573

bc02a8c32fbe6bb91eb76863f1ea93f4e073d05050bff0e50ff1822d12ab8d98

5e4ac46f69495e7425396de054c2dc477b1ddd00aaae598b93c370fb3c847f48

f6d5b1c89ddb229c8a745100ccd152e673f6fee3aa7e161256260402e251bd29

cee6d4dd16801473af3c35142057642173235b1136b997368204725329f77e82

15e08bdc2483050d2a9e6d47b984b0fc7ca5400c3516e7d4c49313f32e691101

83587b97cfba4568b462de20a3b1a64311db7688a65fcf4a5252f8e55d52d378

eda449880905195bb311770425bd8a419d8c3ca99bec6d43e9d282b6108bd927

bd4d20ce5a3e8b9e7bf7c37c914055ebef21861670915b6b35aca07efef2e786

fa5a6700e31d0af716dafe0adb4a9b5f9af960dbab90d00d0352c88a480ef939

c546f251aa19f731f020caed4705c9aec44e54ccb5c3e94f41ddafb42290251d

fd735c409d43ae30546720f4b8ba71118508142577bb1bfc05ee4f90f46b3bd9

2998d029bbce48ec5360e8a60fe3aa1f975fe9329f9457f61cc936e7dbfd8eaa

feef56ccf25ace2beab58b52c8fbb8ef074d9c1534e4aa5309cf8f0e3e0a8044

b3a07c1a49a9737727261a22b4b9e5707f7bd740112daf997d8156cedba78d98

6a145a57bc195266965cea9f01418f0c611975a58856ecf145d69aad02085d94

dc357248d5ff4a97ef627ccb3ab1307ad4400fb844e2652865608f9dcf66b916

3807c417764ef84ea7031968fd961b802b0cb95a11ee99ccfca958ed7b1d7914

ce28143796c94eb11db68118fe5802a0d1ac7eddc3f20e954f13f4958caf0533

b745286b2aedd0d6c2ec65aff6de3128cc5741ac3705ff3c9d2279e3bc60cd7e

35e2c83c47b648df945ccf6746b04d891c0e23fbb993e219cade7fe04bfd6240

cff027bd5c9882b3aad35d69be209517e05cd61bf7aac11adf9e255da244aac7

4419f9b0680f45d0881c9b863be07af3ca5ff36ccae369d2653c1c8920dfab8a

4c168133bdd3bdcb4ee9d56e957e5f62b58724b02ed93f385aed71dad3d45037

917d05d4d2f4a34933297c5abd748007547f1813f01e56a5bf047bdc2869ad5a

6cfb18172284514ae8e79956065b5b4c4fff8ab9359f2497e25d37e3334e3f98

8567f25398c14ca530a110909e08a383df0ff94c4562f3105b59c1b84fdbf808

aa5952a0dfd52b858c4e7df965fbbc2b0fa914d83d01efdcb10e5d404d565b4e

88d52a89e00c8d52f96a96bc398b26c89fd7d197be1fe4451b032ce67e3353dd

86d2a01f2cbf398d2c139c307126be86385ff5ddd2213dc7902d3435d57bf937

33453e7a0b6c21d1c346e3b5bfb6f3d87524a5bbfcfbadf831770403f68051cf

08fe0c05b223827cfa7125d57d4cdf27ff9cc825b95363a704a236a2444a4a02

4c4c5aed8209dda364c61f36552b9e0a06cfd4ee6811cb272ae110ea9340f583

9c842c27091d336720d647b3d4da3f3f3b96ad5e1feb7250d2aeef8b6c74c0da

71c3acd403497ecb1f98ba80d9096aee7b5f17bd3775548c66e5bf18eb37a41a

ca7d617156b032d0022dd8640423cf84720f5aebaab142c7e104cbfe5f39429a

8e37f47d2aed9a22abf6a35a55aef0ff12b473236e92cdc0659c0f4577a6f4fc

56c30e5916df23ab40a23975fe8169b9d06cb0b4a6e1d413c5fec9c442c813de

7dd6cc1b3a269ef6f3058917fac34fbe00f5758dfe2b4fa945a08e8582b07e3c

cf88146f03436a5851884e1a763ae538915cc48c85dfee7c1fbc1729d4ef4fdd

184b3aac95dbc9536e205e241a9708ce1dfafa7aea05c18e50916acb7f07a21c

2b4ca60d215bd7eaf13891878ef4ddeac36354343cdc59f9f2882f8eb61b7234

58da25a3b9164b4331c0ac189892516f0c00745c69b9b8020916ff99f6262ad7

7f2ebfe5ef305ac1261422dc0a34146f6e4d79896052f97cd34c990c32c780bb

cecea22a70bb3a011a49f3ce32efadf20ad82541a259a6b220f332df3d4ac479

606cbd4d9590f26548f8b188d1a03466a446a7e8e5d57283369231895fef2c5c

64aef0c68daaf57fb6a6dea3d5a76a996a18a6a673d791ec9589ad529498464e

dcb24d7c2b11e114311aabca8b18879e891f6e71d751896a523a026922a4ee8f

859b54a6d29c494347b8b2958d76e7b267ce86c90e7ae93cba0ba9aa6e9fd35e

f20aea297c4c00e78e8059572c535b4c879b5c331f552c881ff7929d6df0f6a6

b34b9aa0b8a36deec3157f262c5be11fa705da4c4902dc50ce6f0df2b838471c

d5ba67f4242a2a158dd3f25e280cc0fe61ac92a7c9e0eb9388fe3b89b3324b4a

c26de497c199c4d85071d95049d4b92ef7c72a948f75113661f694b8155f94a2

947e0ff61af9b5740a6e440f4d76b655df348a3547aad09b96f0c6f69d4e6b1f

03037b139a6a6f1d14955c13074b59f20e166db7e09d38f93950f2f1c65f6d4c

fcf412997c3ad0ca1dd1b41d91aff09fe9d0ab363cc23b6400825f6d58bc98ae

External References

- https://otx.alienvault.com/pulse/645d1b3c88d25f37e71bb1e4
- https://blog.talosintelligence.com/new-phishing-as-a-service-tool-greatness-already-seen-in-the-wild/
- https://github.com/Cisco-Talos/IOCs/blob/main/2023/04/new-phishing-as-a-service-tool-greatness-already-seen-in-the-wild.txt