Product Solutions Resources Open Source Enterprise Pricing

Sign in   Sign up

eset / malware-ioc   Public

Notifications   Fork 263   Star 1.6k

<> Code   Issues   Pull requests   Security   Insights

Files

master

Go to file

> ace_cryptor
> agrius
> amavaldo
> animalfarm
> apt_c_60
> aridspy
> asylum_ambuscade
> attor
> backdoordiplomacy
> badiis
> ballisticbobcat
> bandook
> blacklotus
> blackwood
> buhtrap
> casbaneiro
> cdrthief
> ceranakeeper
> cloudmensis
> cosmicbeetle
> danabot
> dark_iot
> dazzlespy
> deprimon
> dnsbirthday
> donot
> dukes
> embargo
> emotet
> especter
> evasive_panda
> evilnum
> evilvideo
> exchange_exploitation
> famoussparrow
> gamaredon

malware-ioc / oceanlotus /

marc-etienne   Add some missing hashes in samples.* files   7a0483e · 5 years ago   History

Name	Last commit message	Last commit date
..		
README.adoc	Added IoCs for OceanLotus' latest macOS…	5 years ago
oceanlotus-macOS.misp.event.json	Added IoCs for OceanLotus' latest macOS…	5 years ago
oceanlotus-rtf_ocx_campaigns.mis…	Added IoCs for the OceanLotus RTF and …	5 years ago
oceanlotus-wateringhole-2018.mi…	Added IoCs for OceanLotus 2018's wateri…	6 years ago
oceanlotus.misp.event.json	Added IoCs for OceanLotus	6 years ago
samples.md5	Add some missing hashes in samples.* files	5 years ago
samples.sha1	Add some missing hashes in samples.* files	5 years ago
samples.sha256	Add some missing hashes in samples.* files	5 years ago

README.adoc

OceanLotus — Indicators of Compromise

Table of Contents

OceanLotus New Backdoor Indicators of Compromise

For a description of OceanLotus' latest campaign (using side-loaded binaries such as rastls.exe) please see the article OceanLotus article and for a detailed explanation the paper

gamarue

gelsemium

glupteba

gmera

goldenjackal

grandoreiro

[OceanLotus whitepaper](#).

Registry

- `HKCU\SOFTWARE\Classes\AppXc52346ec40fb4061ad96be0e6cb7d16a\`

- `HKCU\SOFTWARE\Classes\AppX3bbba44c6cae4d9695755183472171e2\`

- `HKCU\SOFTWARE\Classes\CLSID{E3517E26-8E93-458D-A6DF-8030BC80528B}\`

- `HKCU\SOFTWARE\Intel\Display\igfxcui\igfxtray\;[NUMBER];[DWORD]`

Hashes

Initial Dropper

SHA1	Filename	ESE
`fdcb35cd9cb8dc1474cbcdf1c9bb03200dcf3f18`	RobototFontUpdate.exe	Win32/T
`a40ee8ff313e59aa92d48592c494a4c3d81449af`	Firefox Installer.exe	Win32/T
`c2eb1033bc01ab0fd732a7ba4967be02c0690bf0`	20170905-Evaluation Table.xls.exe	Win32/T
`d35695f2366a43628231e73ffa83ca106306a8fa`	CV_LeHoangThing.doc.exe	Win32/T
`fe0161fb8a26a0bf4afad746c7ebf89499dcd3a7`	Chi tiet don khieu nai gui saigontel.exe	Win32/T
`032ef58b7978d079287874044dc516af624ae5f5`	Mi17 Technical issues - Phonesack Grp.exe	Win32/T
`2a387d7d47a63d6e47d9cc92d3dc69a53816c2c0`	Sorchornor_with_PM_-_Sep_2017.exe	Win32/T
`7105caa6d4fd8a2c67523d385277528e556ae4f6`	Updated AF MOD contract - Jan 2018.exe	Win32/T
`f96bcd875836da89800912de1e557891697c7cf4`	remove_pw_Reschedule of CISD Regular Meeting.exe	Win32/T

Sideloaded libraries

SHA1	Filename	ESET Detection name
`82e579bd49d69845133c9aa8585f8bd26736437b`	rastls.dll	Win32/Salgorea.BD
`202fb56edb2fb542e05c845d62ffbdcfbebed9ec`	McUtil.dll	Win32/Korplug.MK

Network

IP addresses

- `46.183.220.81`

- `46.183.220.82`

- `46.183.222.82`

- `46.183.222.83`

- `46.183.222.84`

- `46.183.223.106`

- `46.183.223.107`

- `74.121.190.130`

- `74.121.190.150`
- `79.143.87.230`
- `79.143.87.233`
- `84.38.132.226`
- `84.38.132.227`
- `149.56.180.243`
- `158.69.100.199`
- `164.132.45.67`
- `192.34.109.163`
- `192.34.109.173`
- `198.50.191.194`
- `198.50.191.195`
- `198.50.234.96`
- `198.50.234.111`

Domains

- `adineohler.com`
- `aisicoin.com`
- `alicervois.com`
- `anessallie.com`
- `antenham.com`
- `arinaurna.com`
- `arkoimmerma.com`
- `aulolloy.com`
- `avidilleneu.com`
- `avidsontre.com`
- `aximilian.com`
- `biasatts.com`
- `braydenhateaub.com`
- `carosseda.com`
- `chascloud.com`
- `dreyoddu.com`
- `dwarduong.com`
- `eckenbaue.com`
- `eighrimeau.com`
- `errellawle.com`
- `erstin.com`
- `frahreiner.com`

- `hieryells.com`
- `hristophe.com`
- `ichardt.com`
- `icmannaws.com`
- `iecopeland.com`
- `irkaimboeuf.com`
- `jamedalue.com`
- `jamyer.com`
- `jeanessbinder.com`
- `jeffreyue.com`
- `keoucha.com`
- `laudiaouc.com`
- `lbertussbau.com`
- `loridanase.com`
- `marrmann.com`
- `meroque.com`
- `moureuxacv.com`
- `myolton.com`
- `nasahlaes.com`
- `ntjeilliams.com`
- `omasicase.com`
- `onnaha.com`
- `onteagle.com`
- `orinneamoure.com`
- `orresto.com`
- `orrislark.com`
- `rackerasr.com`
- `rcuselynac.com`
- `sanauer.com`
- `stopherau.com`
- `tefanie.com`
- `tefanortin.com`
- `tephens.com`
- `traveroyce.com`
- `tsworthoa.com`
- `ucaargo.com`
- `ucairtz.com`

- `urnage.com`
- `venionne.com`
- `virginiaar.com`

OceanLotus WateringHole 2018 Indicators of Compromise

The blog post about this watering hole campaign is available on WeLiveSecurity at https://www.welivesecurity.com/2018/11/20/oceanlotus-new-watering-hole-attack-southeast-asia/.

Network

Compromised website	1st stage	IP	
baotgm[.]net	arabica.podzone[.]net	178.128.103.24	10c
cnrp7[.]org	utagscript[.]com	206.189.88.50	opt
conggiaovietnam[.]net	lcontacts.servebbs[.]net	178.128.219.207	img
daichungvienvinhthanh[.]com	sskimresources[.]com	178.128.90.102	sec imr
danchimviet[.]info	wfpscripts.homeunix[.]com	178.128.223.102	cdn am
danviet[.]vn	cdnscr.thruhere[.]net	178.128.98.139	io.b
danviethouston[.]com	your-ip.getmyip[.]com	178.128.103.74	Unl
fvpoc[.]org	gui.dnsdojo[.]net	178.128.28.93	cdn
gardencityclub[.]com	figbc.knowsitall[.]info	178.128.103.207	iche che
lienketqnhn[.]org	tips-renew.webhop[.]info	159.65.7.45	cyh
mfaic.gov[.]kh	tcog.thruhere[.]net	178.128.107.83	wel
mfaic.gov[.]kh	s0-2mdn[.]net	104.248.144.178	p-ty
mod.gov[.]kh	static.tagscdn[.]com	206.189.95.214	pag
mtgvinh[.]net	metacachecdn[.]com	178.128.209.153	boc
nguoitieudung.com[.]vn	s-adroll[.]com	128.199.159.127	play cne
phnompenhpost[.]com	tiwimg[.]com	206.189.89.121	tiqc
raovatcalitoday[.]com	widgets-wp[.]com	178.128.90.107	cdn
thongtinchongphandong[.]com	lb-web-stat[.]com	159.65.128.57	ber
tinkhongle[.]com	cdn1.shacknet[.]us	142.93.127.120	scd
toithichdoc.blogspot[.]com	assets-cdn.blogdns[.]net	178.128.28.89	cart
trieudaiviet[.]com	html5.endofinternet[.]net	178.128.90.182	effe azu
triviet[.]news	ds-aksb-a.likescandy[.]com	159.65.137.144	labs
Unknown	nav.neat-url[.]com	142.93.116.157	stra acto
Unknown	pixel1.dnsalias[.]net	142.93.116.157	ad-
Unknown	trc.webhop[.]net	178.128.90.223	stat add

File

Description	SHA-1	
First stage script	2194271C7991D60AE82436129D7F25C0A689050A	1EDA0DE280713470878
Second stage script	996D0AC930D2CDB16EF96EDC27D9D1AFC2D89CA8	8B824BE52DE7A872312

OceanLotus : RTF and SFX archives decoys

For a description of OceanLotus' latest campaign (using rtf exploits and sfx archives) please see the article [OceanLotus article](#).

Registry

- `HKCU\SOFTWARE\Classes\CLSID{E08A0F4B-1F65-4D4D-9A09-BD4625B9C5A1}\Model`
- `HKLM\SOFTWARE\App\AppXbf13d4ea2945444d8b13e2121cb6b663\Application`
- `HKLM\SOFTWARE\App\AppXbf13d4ea2945444d8b13e2121cb6b663\DefaultIcon`
- `HKCU\SOFTWARE\App\AppXbf13d4ea2945444d8b13e2121cb6b663\Application`
- `HKCU\SOFTWARE\App\AppXbf13d4ea2945444d8b13e2121cb6b663\DefaultIcon`
- `HKLM\SOFTWARE\App\AppX70162486c7554f7f80f481985d67586d\Application`
- `HKLM\SOFTWARE\App\AppX70162486c7554f7f80f481985d67586d\DefaultIcon`
- `HKCU\SOFTWARE\App\AppX70162486c7554f7f80f481985d67586d\Application`
- `HKCU\SOFTWARE\App\AppX70162486c7554f7f80f481985d67586d\DefaultIcon`
- `HKLM\SOFTWARE\App\AppX37cc7fdccd644b4f85f4b22d5a3f105a\Application`
- `HKLM\SOFTWARE\App\AppX37cc7fdccd644b4f85f4b22d5a3f105a\DefaultIcon`
- `HKCU\SOFTWARE\App\AppX37cc7fdccd644b4f85f4b22d5a3f105a\Application`
- `HKCU\SOFTWARE\App\AppX37cc7fdccd644b4f85f4b22d5a3f105a\DefaultIcon`

Hashes

RTF documents

SHA1	ESET Detection name
D1357B284C951470066AAA7A8228190B88A5C7C3	Win32/Exploit.Agent.LT
49DFF13500116B6C085C5CE3DE3C233C28669678	Win32/Exploit.CVE-2017-11882.BU
9DF3F0D8525EDF2B88C4A150134C7699A85A1508	Win32/Exploit.CVE-2017-11882.BU
50A755B30E8F3646F9476080F2C3AE1347F8F556	Win32/Exploit.CVE-2017-11882.A
BB060E5E7F7E946613A3497D58FBF026AE7C369A	Win32/Exploit.Agent.KT
E2D949CF06842B5F7AE6B2DFFAA49771A93A00D9	Win32/Exploit.CVE-2017-11882.EI

SFX archives and .ocx files

SHA1	ESET Detection name
AC10F5B1D5ECAB22B7B418D6E98FA18E32BBDEAB	Win32/Agent.ZUR
7642F2181CB189965C596964D2EDF8FE50DA742B	Win32/Agent.ZUR

CD13210A142DA4BC02DA47455EB2CFE13F35804A	Win32/Agent.ZUR
377FDC842D4A721A103C32CE8CB4DAF50B49F303	Win32/Agent.ZUR
B4E6DDCD78884F64825FDF4710B35CDBEAABE8E2	Win32/Agent.ZUR
BD39591A02B4E403A25AAE502648264308085DED	Win32/Agent.ZUR
B998F1B92ED6246DED13B79D069AA91C35637DEC	Win32/Agent.ZUR
CC918F0DA51794F0174437D336E6F3EDFDD3CBE4	Win32/Agent.ZUR
83D520E8C3FDAEFB5C8B180187B45C65590DB21A	Win32/Agent.ZUR
EFAC23B0E6395B1178BCF7086F72344B24C04DCC	Win32/Agent.ZUR
8B991D4F2C108FD572C9C2059685FC574591E0BE	Win32/Agent.ZUR
B744878E150A2C254C867BAD610778852C66D50A	Win32/Agent.ZUR
3DFC3D81572E16CEAAE3D07922255EB88068B91D	Win32/Agent.ZUR
77C42F66DADF5B579F6BCD0771030ADC7AEFA97C	Win32/Agent.ZUR

Network

Domains

- aliexpresscn.net
- andreagahuvrauvin.com
- andreagbridge.com
- aol.straliaenollma.xyz
- beaudrysang.xyz
- becreybour.com
- byronorenstein.com
- chinaport.org
- christienoll.xyz
- christienollmache.xyz
- cloud.360cn.info
- dieordaunt.com
- dns.chinanews.network
- illagedrivestralia.xyz
- karelbecker.com
- karolinblair.com
- lauradesnoyers.com
- ntop.dieordaunt.com
- office.ourkekwiciver.com
- ourkekwiciver.com
- sophiahoule.com
- stienollmache.xyz
- straliaenollma.xyz

- `ursulapapst.xyz`

MITRE ATT&CK matrix

ID	Description
T1009	Binary Padding
T1094	Custom Command and Control Protocol
T1073	DLL Side-Loading
T1002	Data Compressed
T1022	Data Encrypted
T1041	Exfiltration Over Command and Control Channel
T1203	Exploitation for Client Execution
T1083	File and Directory Discovery
T1112	Modify Registry
T1050	New Service
T1027	Obfuscated Files or Information
T1012	Query Registry
T1060	Registry Run Keys / Start Folder
T1117	Regsvr32
T1053	Scheduled Task
T1035	Service Execution
T1193	Spearphishing Attachment
T1082	System Information Discovery
T1099	Timestomp
T1065	Uncommonly Used Port
T1204	User Execution

OceanLotus : macOS backdoor update

For a description of OceanLotus' latest macOS update please see the article OceanLotus article.

Hash

SHA1	ESET Detection name
E615632C9998E4D3E5ACD8851864ED09B02C77D2	OSX/OceanLotus.D

File paths

File path
`~/Library/SmartCardsServices/Technology/PlugIns/drivers/snippets.ecgML`
`/Library/Storage/File System/HFS/25cf5d02-e50b-4288-870a-528d56c3cf6e/pivtoken.appex`
`/tmp/store`

Network

Domains

- `daff.faybilodeau.com`

- `sarc.onteagleroad.com`

- `au.charlineopkesston.com`

URI

- `/dp/B074WC4NHW/ref=gbps_img_m-9_62c3_750e6b35`

MITRE ATT&CK matrix

ID	Description
T1158	Hidden Files and Directories
T1107	File Deletion
T1222	File Permissions Modification
T1027	Obfuscated Files or Information
T1099	Timestomp
T1082	System Information Discovery
T1022	Data Encrypted
T1094	Custom Command and Control Protocol

- `daff.faybilodeau.com`

- `sarc.onteagleroad.com`

- `au.charlineopkesston.com`

- `/dp/B074WC4NHW/ref=gbps_img_m-9_62c3_750e6b35`