ZLAB

Malware Analysis Report

Dissencting GandCrab v5

01/10/2018

CSE CybSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

Table of Contents

CSE CybSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

Introduction

A new version of the infamous GandCrab ransomware,version 5.0, was recently spotted in the wild. According to the experts from several cybersecurity firms, the ransomware mainly targeted users in Central Europe, as shown in the following images published by the Italian Cert-PA.

Figure 1 - Malware spread

The ransomware is spread through different attack vectors, including spam emails, exploit-kits or malicious links. We analyzed a sample that was hosted on a server located in Ukraine.

Samples Information

“o.exe”

MD5	b5de1da74b3420b9cefbc94638592b52
SHA-1	ffa8aa05c745db4915369392a368888829369796
SHA-256	623f558a50bb665a15f50121d0b7a8b54d90108c35e2787f2576016f3fe74dd8
File Size	200 KB

Malware behavior

Once executed, the ransomware begins to encrypt all the files on the machine. We noticed, the malware uses a different pseudo-randomic extension (5 characters long) for each encrypted file (i.e. “.txvpq”, “.rttmc”, “.mcbot”, etc.).

The malware also replaces the desktop image with a custom one used to threaten the victims, and drops a TXT ransom note in every folder of the machine.

Figure 2 - Ransomware's desktop image

The ransom note contains the instructions to proceed with the payment of the ransomware:

```
---= GANDCRAB V5.0 =---


Attention!

All your files, documents, photos, databases and other important files are encrypted and have the extension: .TXVPQ

The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover your files.

The server with your key is in a closed network TOR. You can get there by the following ways:

-------------------------------------------------------------------------------------------

| 0. Download Tor browser - https://www.torproject.org/

| 1. Install Tor browser
| 2. Open Tor Browser
| 3. Open link in TOR browser:   http://gandcrabmfe6mnef.onion/fed0a66240f8743f
| 4. Follow the instructions on this page

-------------------------------------------------------------------------------------------

On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.

ATTENTION!

IN ORDER TO PREVENT DATA DAMAGE:

* DO NOT MODIFY ENCRYPTED FILES
* DO NOT CHANGE DATA BELOW

---BEGIN GANDCRAB KEY---
lAQAAErWrq9/Kh4Co2/coCN/NQJOh3FlanYyE9SyuHn+uAZ3cIN2Y5oma3gm79SE0mBtk7KYx8AK4TMQ29SgISqowPBh3U0GdaOZTPTqHDTysRuEzmb6NORxlGbPHKBlVx99gRdqXlgsAsAl
CarpqQrQhRvCSLX9JrRFQHac2FUBxMr5bAFht2jAR7Rf4lzLKawcK0qcm9q6s2U8aPLu4dJa9AjnpYyWj3TUeFafsQMtmiENeeBQg0mhV6HAAHTPLBODSGmku+9G9xHZWf8+f3Xw68ZUMJm
zH8lRwhqvf5X4jS8nCLm/nOZXyTzujC2F7INvLGEuMSkI13gNgrJ4AZmxZu2qNAL+KASHQLy6DanxSlYj422UZjRNVOtMEIXkDYxuYcPXoIvMHyYH3Bn7QvEE4GjbaQw38N5gXBL5mHtmDA
---END GANDCRAB KEY---

---BEGIN PC DATA---
wfKD6iudumBkmpL8IRr4U6exEVaoOXLtwDwmOrT1y1YWvOiWMx5GYaRdvZZWTpNRs3YW7nZWyLfFTGKHhh5qBJzzs9MC7736UkGSDDniUJJG8/LFF//kmGmoAZAGLo2j5/wd2UrxMJK+iqKl
---END PC DATA---
```

Figure 3 - Ransom note

This file contains some information related to the infection: an ID ("fed0a66240f8743f", in the image above) and a "GANDCRAB KEY", required to restore the original files.
The txt also keeps some encrypted information related to the victim machine (in the "PC DATA" section), such as the username, the PC name, the domain, the operative system and the language, as shown in the following screen:

o.exe	lstrlenW ("C:FIXED_42842714112/34181365760,")
o.exe	lstrlenW ("admin")
o.exe	lstrlenW ("pc_user")
o.exe	lstrlenW ("ADMIN-PC")
o.exe	lstrlenW ("pc_name")
o.exe	lstrlenW ("WORKGROUP")
o.exe	lstrlenW ("pc_group")
o.exe	lstrlenW ("it-IT")
o.exe	lstrlenW ("pc_lang")
o.exe	lstrlenW ("0")
o.exe	lstrlenW ("pc_keyb")
o.exe	lstrlenW ("Windows 7 Ultimate")
o.exe	lstrlenW ("os_major")
o.exe	lstrlenW ("x64")
o.exe	lstrlenW ("os_bit")
o.exe	lstrlenW ("C:FIXED_42842714112/34181365760")
o.exe	lstrlenW ("hdd")
o.exe	VirtualAlloc (NULL, 1396, MEM_COMMIT | MEM_RESERVE, PAGE_READWRITE
KERNELBASE.dll	NtAllocateVirtualMemory (GetCurrentProcess(), 0x003bfc00, 0, 0x003bf...
o.exe	lstrcatW ("", "pc_user")
o.exe	lstrcatW ("pc_user", "=")
o.exe	lstrcatW ("pc_user=", "admin")
o.exe	lstrcatW ("pc_user=admin", "&")
o.exe	lstrcatW ("pc_user=admin&", "pc_name")
o.exe	lstrcatW ("pc_user=admin&pc_name", "=")

Figure 4 - The retrieved info

The file extensions that are targeted in the encryption phase are the following ones:

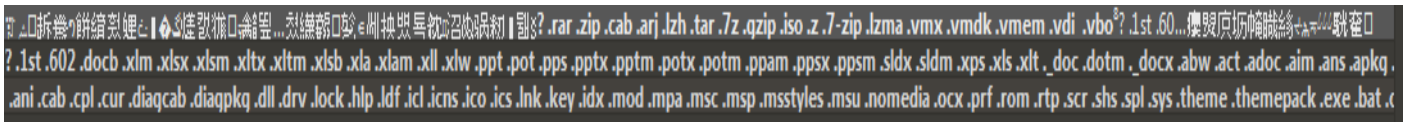

Figure 5 - List of file extensions considered by the malware

the information necessary to encrypt the files are saved as Registry Key values:

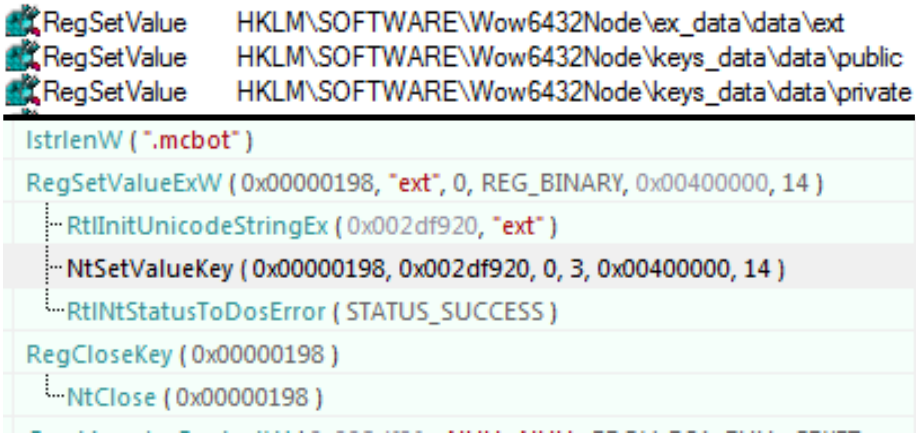

Figure 6 - Temporary information used by the malware

The key value “ext” (containing the extension generated by the malware for the encryption phase) is deleted after the file encryption, while the key values “private” and “public” are permanently stored in the key registry.

The research of the active processes

Unlike GandCrab v4, this version is able to kill the processes related to some popular applications, such as Word, Excel, SQLServer etc., with the purpose of encrypt also the temporary files opened by these applications.

Figure 7 - List of killed processes

CSE CybSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

A list of hard-coded URLs

As well as GandCrab v4, version 5 has got a hard-coded list of URLs that it contacts, sending them encrypted “PC DATA” information. The purpose of this behavior is not clear at the time of the analysis, probably it could be an attempt to make harder the analysis and mislead the analysts during their activities. The complete URLs list is reported in the IOCs section.

```
13.57.63.201        HTTP    858 POST /static/imgs/momoam.bmp HTTP/1.1
13.210.138.91       HTTP    864 POST /content/images/fukasemeheso.jpg HTTP/1.1
94.46.169.98        HTTP    865 POST /data/graphic/imheso.bmp HTTP/1.1
103.113.93.100      HTTP    861 POST /content/imgs/thkeesimim.gif HTTP/1.1
91.146.100.130      HTTP    918 POST /wp-content/image/kaamkehe.jpg HTTP/1.1
209.99.64.52        HTTP    859 POST /wp-content/pics/dase.png HTTP/1.1
209.99.64.52        HTTP    859 POST /wp-content/pics/dase.png HTTP/1.1
185.104.45.7        HTTP    856 POST /static/tmp/keru.jpg HTTP/1.1
124.217.241.112     HTTP    862 POST /uploads/tmp/karuamda.gif HTTP/1.1
164.132.235.17      HTTP    937 POST /includes/image/kemees.bmp HTTP/1.1
185.104.45.25       HTTP    860 POST /content/imgs/dasethda.png HTTP/1.1
142.4.198.208       HTTP    865 POST /content/image/ruzufuimam.gif HTTP/1.1
186.202.153.14      HTTP    861 POST /includes/tmp/zukezudeam.png HTTP/1.1
205.134.252.150     HTTP    865 POST /content/image/momeruheam.jpg HTTP/1.1
34.196.246.251      HTTP    882 POST /content/image/ammekada.png HTTP/1.1
198.136.59.58       HTTP    906 POST /includes/tmp/kamode.bmp HTTP/1.1
46.29.49.1          HTTP    869 POST /uploads/image/rudede.bmp HTTP/1.1
109.232.217.150     HTTP    858 POST /news/assets/damoheam.png HTTP/1.1
216.55.141.157      HTTP    862 POST /data/assets/imamsezuamda.gif HTTP/1.1
89.187.152.97       HTTP    870 POST /uploads/graphic/mothka.gif HTTP/1.1
91.134.164.164      HTTP    861 POST /includes/pictures/mefuka.png HTTP/1.1
109.199.108.126     HTTP    867 POST /uploads/tmp/kaamhesefu.png HTTP/1.1
185.68.16.17        HTTP    865 POST /includes/graphic/daketh.png HTTP/1.1
172.82.166.194      HTTP    872 POST /wp-content/assets/moimdeka.gif HTTP/1.1
66.96.149.20        HTTP    866 POST /uploads/imgs/dadekaes.bmp HTTP/1.1
153.92.8.183        HTTP    868 POST /content/pics/kaesheda.gif HTTP/1.1
66.96.149.32        HTTP    859 POST /content/assets/zuthketh.jpg HTTP/1.1
66.96.147.201       HTTP    913 POST /news/pictures/moes.gif HTTP/1.1
13.89.185.110       HTTP    868 POST /content/pics/seheruzu.gif HTTP/1.1
70.39.235.246       HTTP    913 POST /static/pictures/daes.bmp HTTP/1.1
179.188.11.20       HTTP    867 POST /includes/pics/damode.jpg HTTP/1.1
213.186.33.40       HTTP    913 POST /content/tmp/kehe.gif HTTP/1.1
89.44.138.158       HTTP    865 POST /wp-content/imgs/medese.png HTTP/1.1
67.210.244.162      HTTP    865 POST /wp-content/images/esmeimruru.jpg HTTP/1.1
89.252.186.195      HTTP    860 POST /includes/graphic/heth.jpg HTTP/1.1
203.146.170.42      HTTP    916 POST /content/pictures/seamhe.gif HTTP/1.1
173.236.53.234      HTTP    926 POST /includes/graphic/imthzufukafu.gif HTTP/1.1
46.30.215.72        HTTP    861 POST /static/graphic/zuth.bmp HTTP/1.1
185.104.45.27       HTTP    853 POST /data/tmp/meamdamo.bmp HTTP/1.1
```

Figure 8 – Part of URLs contacted by the malware

GandCrab saves Russia

GandCrab v5 does not infect the Russian users, like the previous version. In fact, the malware checks if the keyboard layout is set to Russian or if the user interface language is set to one of:

- Russian (0x419)
- Ukrainian (0x422)
- Belarusian (0x423)
- Tajik (0x428)
- Armenian (0x42B)
- Azerbaijani (0x42C/0x82C)
- Georgian (0x437)
- Kazakh (0x43F)
- Kyrgyz (0x440)
- Turkmen (0x442)
- Uzbek (0x843)
- Tatar (0x444)
- Romanian (0x818)
- Moldova(0x819)

GandCrab v5 Web Panel

In order to allow victims to pay the ransom and proceed with the decryption phase, the attacker implemented a web site on the darknet, at the URL hxxp://gandcrabmfe6mnef[.]onion, which is the same of the previous version of the malware.

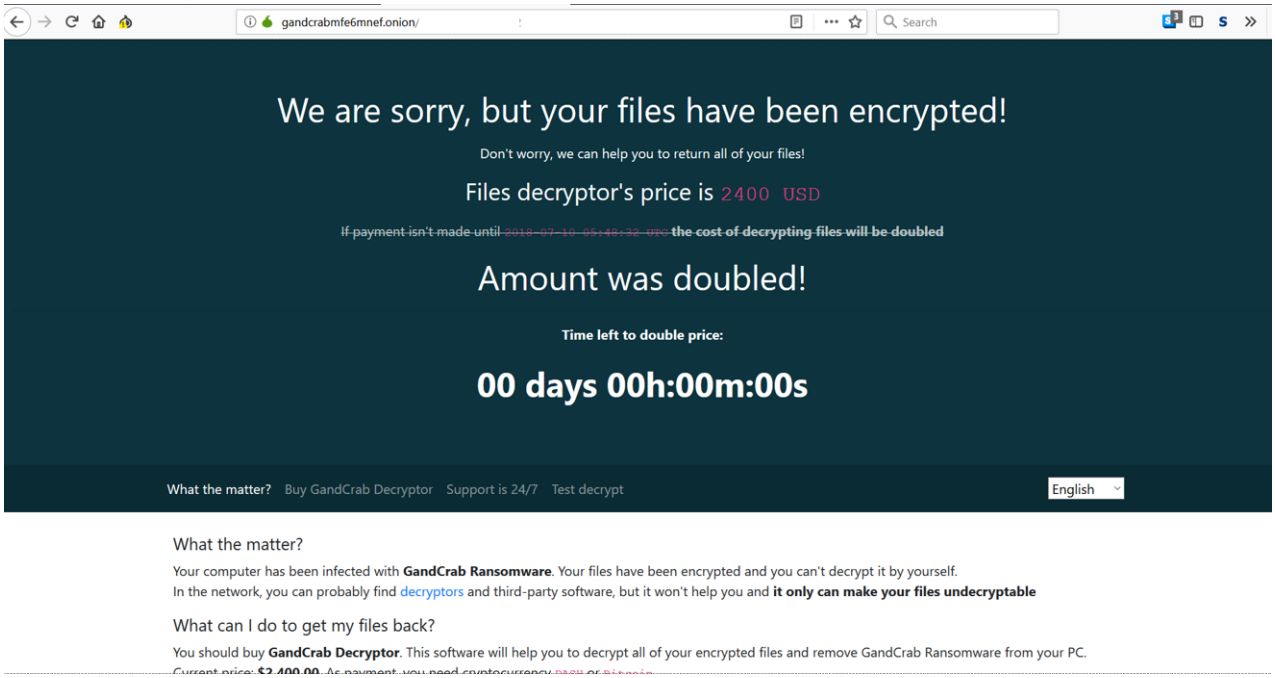

Figure 9 - Web site

However, in this case, the attacker asks for $2400 (more than the previous version, that was $1000) to decrypt all the user files. A test decrypt panel is still present, with which the user can test the effectiveness of the decryptor.

IOCs

URLs

www.billerimpex.com
www.macartegrise.eu
www.poketeg.com
perovaphoto.ru
asl-company.ru
www.fabbfoundation.gm
www.perfectfunnelblueprint.com
www.wash-wear.com
pp-panda74.ru
cevent.net
bellytobabyphotographyseattle.com
alem.be
boatshowradio.com
dna-cp.com
acbt.fr
wpakademi.com
www.cakav.hu
www.mimid.cz
6chen.cn
goodapd.website
oceanlinen.com
tommarmores.com.br
nesten.dk
zaeba.co.uk
www.n2plus.co.th
koloritplus.ru
h5s.vn
marketisleri.com
www.toflyaviacao.com.br
www.rment.in
www.lagouttedelixir.com
www.krishnagrp.com
big-game-fishing-croatia.hr
mauricionacif.com
www.ismcrossconnect.com
aurumwedding.ru
test.theveeview.com
relectrica.com.mx
bethel.com.ve
vjccons.com.vn
bloghalm.eu
cyclevegas.com
low-carb-rezept.com
cscig.ase.ro
lucianocellitancredi.com
lloyd.www.creative-platform.net
kinhmatgiao.com
khabardarexpress.com
kiemdinh345.com
imazineex.com
marbleentreprise.dk
bsp.co.id
klangplaza.com
marcora.it
masp.pro
ma-redactrice-web.com
kittipakdee.com
marmet.cba.pl
life.demobb.com
kssyn.com
meditec.ma
mellon.ir
mainlis.pt
maxibud.cba.pl
merittur.com
luatsuhaiduong.com
lgg.adv.br
mranalyz.com
moika.kg
muaithai.pl
jupiter.csit.rmit.edu.au
mugituz.com
modivi.hu
nahalbazr.com
lanxiaoyang.com
mengxiao7.com
mygembest.com
mskcontracting.ca
novosti-danasnje.info
mazjackson.com
grupoperfetto.com.br
ncrjobs.info
icebergillusion.com
nazareimoveis.vistatemporario.com.br
oscar-event.com.ua
www.closedguardthemovie.com
www.appleupdate.ir
back2backpt.com
www.ortaklarpaslanmaz.com
64.91.241.0
esancharpati.com
polyblow.com.br
braner.com.ua
adquiz.io
cultnet.eu
melloweb.com
yodthipiwater.com
www.hipervi.com.br
poly.polyblow.com.br
lecircuit.fr
dazzlecarpentry.training
trueadv.ru
www.wschyderabad.com
www.linkcoaching.com.au
www.hanumansena.co.in
www.yuvamnakliye.com
crossoceans-td.com
humae.fr
rgdh.fr
kiabod.com
openveda.info
kidathon.org
ayrintitabela.com
www.yekglass.com
www.rafaelimports.com.br
lesracinesdedemain.com
www.tvtekrarcisi.com
robfilios.com
www.cempakalaptop.com
slipandset.com
cctvvietnam.com
ciencia-ciudadana.es
asjbkk.com
bourget-pascal.fr
klinikkingcare.com
uterku.ru

CSE CybSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

royal.by
www.himmerlandgolf.dk
hoteltravel2018.com
picusglancus.pl
unnatimotors.in
krasnaypolyana123.ru
smbardoli.org
blokefeed.club
evotech.lu
devdev.com.br
graftedinn.us
top-22.ru
simetribilisim.com
sherouk.com
lucides.co.uk
hanaglobalholding.com
diadelorgasmo.cl
www.groupwine.fr
mrngreens.com
www.cognitiasystems.com
canhoopalcity.top
greatmiddleeastgate.com
xn--80adsn2ag7e.xn--p1ai
www.reusa.com.br
xn--80avc1e.xn--p1acf
www.christinapetrou.co.uk
www.lyonwood.co.uk
www.urstoothfully.com
faculdadesenacpe.edu.br
dijitalharf.com
www.maraeeventos.com.br
www.chanandeayrs.com
idclamart.fr
www.batisigortaaydin.com
muxtay.com
kubatom.com
sweetthirty.pl
onstaheerd.nl
kakaocorp.link
jamgonkongtrul.org.tw
barbochos.com
rayanaco.ir
obed-service.ru
500flats.com
www.lasertag.kiev.ua
gstelecom.cf
nilhair.com
oral.co.il
orthodontics.ir
ldm.littlerocknews.org
naizamdistributor.com
noahs-earth.com
openricostruzioneabruzzo.piattaforma.eu
oceanstockfilms.com
onlineitshop.com
naraveesurgerythailand.com
njrior.cn
peakmedia.se
haircb.com
nuzululmastah.com
nurfian.ukmforum.com
plataformacontralaprivatizaciondelcyii.org
ps-photo.ru
omahpoetih.com
paytrenkeren.xyz
ralienglish.com
phuongthaoland.com
nordestinasat.com.br
ratmfan.cba.pl
postit.angryventures.com
pittsburghbbq.com
saadetankaravekil.com
sahandnetcctv.com
shalvak.com
saids-edu.com
plasaponsel.com
shakingflames.com
shop.istest.ir
skutsje-gruttepier.nl
skbyd.cba.pl
sokolenko.dp.ua
protesesdeflex.com.br
saudigeriatrics.org
snejankagd.com
social.takeshopv.pp.ua
erikherrstrom.com
san-kelloff-italy.web5s.com
kuatsolar.kz
skilldealer.fr
lemdik.polri.go.id
studiodelcarratore.it
sportsohio.pbd-dev.com
www.caringtouch.uk.com
www.laori.co.il
www.espaces-interieurs.net
geacann.com
institut-journalisme.fr
www.ixbat.com
shacaram.com
gurkhali.fi
pigeondeck.com
travellow.world
138.68.99.104
www.hashpatal.com
massclap.com
unifiedgoals.com
emmlallagosta.cat
kinderwood.store
marcelinoadvogados.com.br
perleyfund.org
piipmgr.com
presencetalentos.com.br
jeo-graphics.com
www.marketopic.ru
mdlgroup.co.uk
avi-investforum.com
spondilos.ru
www.chestersskn.com
www.casademare.it
xn--80aanbmdrdpayqtg1d7h.xn--p1ai
www.mabnapouyesh.com
topavi.es
galaxyonetransportation.com
ittran.com.br
www.esteticaderma.com
hyroadradio.com
www.rcmgdevten.xyz
www.namikik.com
chayxana.ru
ravben.com
sman43-jkt.sch.id
galaxycorp.es
rintio.com
www.vivalavie.fr
www.greenwolfales.com
anpingstay.com
e-crimea.biz
elektro-beckers.de

CSE CybSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

Cyber Security Strategists

www.ikebana.cat
gites-les-noisetiers.fr
www.kia1.ir
m-award.com
intervener.org
sxhfhr.ga
soldiergym.nl
fitforms.mx
www.cornishinn.com
riib.com.pl
evaskinclinic.com
www.kuntoaskel.net
ecart.nu
www.phammemviet.com
www.clarusdent.com
www.lasthotel.it
www.htsinteriors.com
kwanho.com.au
importec.com.mx
www.xn--narmdnsalonlar-fjb55aa34dpkdo.com
klongpleng.com
cocnguyetsanthaomeo.com
wakeupwithmakeup.co.uk
www.jtaobk.com
mundololita.es
denaseguridad.com
inescogroup.com
www.velvet.travel
myartstudio.com.my
www.financetoit.fr
sigillum.com.ua
www.friends-for-kids.de
www.pgregoire.com
babiceresa.com
vinhomescangio.viethomes.land
heartsongroup.com
top-prodazha.ru
kalemon.net
www.tikura.com.br
www.riadtroiscours.com
videirafilho.com.br
vtr.kz
peritocaligrafosevilla.es
umrezamani.net
www.bsecure.fr
www.setiri.com
megexinc.com
sinergiindonesia.co.id
smmakcreation.com
solardosing.ir
stoveworlddirect.co.uk
sinfonia.vn
tala.today
locnuockimnguyenphat.com.vn
test.assistia.se
test.indigo-experten.be
saberes.cl
test.mirari.pl
test.patemucevherat.com
thepinspire.co.uk
syjingermei.xyz
sulawan.com
torstenbygger.se
sites.blueskydigital.com.au
theaceexports.com
stivesofminthill.com
unicef-int.karibuni.be
uatwebsite.aithent.com
villagevanguard.co.uk
atelierdupain.it
violetdecor.net
vancouvereventvideo.com
vuraldirek.com
vlawcourse.com
white-power-music.cba.pl
worldgamifier.com
visahousebangladesh.com
wp.mmitest.fr
vietx.us
weihnachts-pyramide.tk
workcompoptions.com
wp.actions.men
webmarketing.cinfoway.in
ustunbey.com
whmhost.tk
voiceyouropinions.net
vipyouxi.net
www.armangarayan.com
mas-expert.com
vitoriainvest.com.br
www.consulpyme.biz
www.equi.nl
ctrl-r.ro
feveda.com.ve
camhanhtrinh.net
tt-plus.ir
sailtrans.com
codifet.com
franckcrepelle.com
paulbloodgood.com
landmarkscalifornia.org
softshine.kiev.ua
zspm.ovh
fmcfamily.org
tonight-hobby.com
swimmik.com
greentradecorp.com
baskinbeyenal.com
www.eurosystemsrl.net
soledadmanzi.com
aquastarscooter.com
alsafas.org
politicsamongus.com
tonerplenka.ru
www.asped.cz
kidsportvn.com
gharkulconstructions.in
dogotoanquoc.com
essential-campinggear.com
thepostatrockwells.com
dogcartusa.com
hanhtrinhkientaocuocdoi.com
softsj.org
saffronali.com
www.friv.news
batdongsanhuyphat68.com
vazquezdelamorena.com
www.adecbrasil.com
irserver.net
www.nissinfrozen.com.hk
samsafadi.com
bcachc.org
www.ankarentacars.com
xkld24h.net
vlatec.com
faceok.online
cliniqueesthetiquepasteur.com
hablabonito.com

Cyber Security Strategists

CSE CybSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

www.fondsbn.com
optikchrtek.yourcloud.cz
www.sva-co.ir
www.classtransport.fr
pearlandshandyman.com
toponlinegames.pro
www.interiorideas9.com
www.cyrillecharro.com
www.romanjews.com
alatkeselamatankerja.co
mcsiweb.com
www.monei.co
www.conversants.com
pro-markservicesinc.com
thtcannabis.com
novocentropetrolina.com
bharatfolks.com
www.cheriehavetoshine.com
www.ossainicholasossai.com
www.sgfcomputers.ro
sinuverde.com
www.senteks.com
www.megawheyprotein.com
www.speardigitalweb.com
www.101.sr
dutchtraditions.nl
barvybud.com
thillaikalavathi.info
parsmoviez.com
ogenconsult.com
mdc-coaching.fr
finamlight.ru
atayastore.com
www.thatscomfortable.com
www.colorshotevents.com
ananas.kiev.ua
www.bitwiseacademy.com
sbobetcasinoterpercaya.com
upm-apply.com
carillon7tanphu.com
gofootball24h.com
miriamkapner.com
onedev.ro
www.alanya.co.uk
unitedctg.com
ioae.com.vn
keller-fenster.ch
www.anhphuoc.com.vn
roue.com.mx
www.cerespire.com
www.fratelliditalia.it
www.asiapointpl.com
www.dpsdhuri.edu.in
www.aftvec.com
www.eudel-albania.com
www.hidroser.pt
www.ivanotaola.com
www.kabiledans.com
www.broadbandimperatives.org
www.fp360.us
www.lavariable.club
www.meditec.ma
www.bdot.co.kr
www.mainlis.pt
www.modainfantilvalencia.com
www.ijzsz.com
www.jlyingshi.cn
www.envischool.vn
www.hopcentury.com
www.maaitsolutionsbd.com
www.oxfordpharmassist.com
www.dorsalsistemas.com.br
www.paginaturistului.com
www.klikidnews.com
www.michelleshairlounge.ca
feeltwenty.com
www.rcinformatica.pt
trnhomes.in
www.pushmyprofile.com
www.petsfoodbd.com
www.pizzeriarepentigny.ca
www.ruzgarchat.com
www.socialconcepts-cm.com
www.rl-treasure.com
www.fog911.com
www.kovezaagricola.com.br
www.spimol.com
www.synturfmats.com
todeschinipassofundo.com.br
www.setebr.com
www.tourmelaybasket.fr
www.urproject.fr
eurosystemsrl.net
mentoriaparacoaches.com.br
armureries-acl-37.fr
getcardonationtoday.com
safaaldan.es
dekalbchamber.org
shorecrestschools.com
rancherssupply.us
www.archives-zoliennes.fr
yogabody.com.br
winspeedy.ru
babyclickphotography.es
promenadedeflandre.com
www.hospeem.org
tweko.org.ua
www.painpoint.online
amotsouverts.org
haroldlopezr.com
inebolushipyard.com
khodtarash.ir
nebiogluavm.com
getsharkeynow.com
sevenpillars.org.uk
trudyhuisman.com
descriptivevideoproductions.com
congressodesignam.com.br
xpress.ltd
autostate.com.ua
cekicix.com
anandcontractors.com.au
stovnerkameratene.no
meatit.com.ua
fadaate.com
testing.tallawang.com
gvio.ir
www.ganlogis.com
isginsaat.com.tr
metaland.me
eviphoto.ru
escort-girls.services
interlab.com.sg
iamzaigham.com
mbztusa.com
nathaliedesperchesboukhatem.fr
arsaraiya.com
onlinebusinesskhabar.com

CSE CybSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

Cyber Security Strategists

startcomputer.com.br
aldrovanaluxe.lviv.ua
meblivdim.org
www.transento.com
www.parthabarua.com
rbctoken.com
sonnewton.com
www.santischerd.com
0123porno.com
5.77.60.222
180.211.99.165
aldirgayrimenkul.com
103.253.1.219
abidhandicraft.com
androsoft.in
128.199.96.238
argedalatpars.ir
179.188.17.9
basketkids.com.ua
avangardstone.com
autumnnight.cz
alauddintakeaway.com
androturk.club
badmos.top
barquestest9.uk
boucherie.lemarchefrais.com
baranacarpet.com
anowaragroupbd.com
blog.betzest.com
anvatbinhduong.com
bmafrique.com
amardin.com
airybd.com
cadretoiles.com
awrbloooomdevserver.com
bluebellhdb.com
ce-clp.fr
charm.andreea.alexandroni.ro
atlantisbuildcon.com
blog.raztype.com
chatrashow.com
blog.swingtaiwan.com
call4soft.com
bloomingrosebd.com
bhbeautyempire.com
acasadocarro.com.br
www.weil-weil.de
www.realsun.com
www.textual.com
www.sjmama.cn
www.veronicasantiago.com.br
xn----7sbcfeovaaet2bacdygacidsedek.xn--p1acf
www.tecnisoft.hn
www.theloveassembly.com
www.tajcellars.com
yomyat-group.com
www.tanthewa.com
www.versaseo.com
www.thaiphonecenter.com
xmarkcity.com
sundaysbestphotography.com
www.theparco.com
www.zannee.com
www.tokokuaja.com
www.amana.tn
yunuso.com
yellowcreativeco.com
www.webhtm.cn
yanchengguoji.com
www.tenqube.com
bookingbmoredjsteve.com
egelihasar.com
bookamodelbastarr.com
imperia-quest.com.ua
gremlin.studio
codamarketing.agency
freelancemarketingtraining.com
approbuilder.com
biruisblue.com
kavehsanatco.com
erturkgrup.com.tr
www.metanoiatravel.in
mystroi24.ru
emaclick.com
www.maheshsharma.live
mikenibg.com
www.yolandapalhanoimoveis.com.br
imliu.com
gr34tstore.com
www.zhainanle.com
nek-voda.ru
metodoresultado.com
www.lionsindustries.org
bettercom-berlin.de
idestinostours.com
cronicadelsureste.com
hardsoftbay.ru
mtt.com.kw
hastanetaksi.net
kayannou.be
www.rubeehandmade.com
www.stipenda.com
eduleka.com
refahnovin.ir
presentseitai.com
electrictrainproductions.com
cms.ghs-schachundkulturstiftung.de
wellnesslifescience.com
www.theatlanticseafoodcompany.com
charleswadefinance.co.uk
www.theadaptables.com
clinicadentaldelgado.es
kerryaclark.com
tr-ghods.ir
www.mci.com.sg
reiso.com.br
thegioiwebvn.com
qsgroup.vn
bishopschell.com
formametal.net
avuedepieds.be
update.com.br
nathyrealty.com
pedefigo.com
bdteacherstech.com
netoconstructioncorp.com
yesletsdrive.com
www.simsimint.com
uniquemedia.cf
bc2match.com
pardisesofe.com
roompride.es
spilbas.dk
skf-technik.de
tarhkade.info
derbydays.ru
ungpott.se
weissgallery.ru

CSE CybSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

Cyber Security Strategists

casualflirtings.com
blog.damngood.mx
carlylevanlines.com
conexa.no
cashback.ncplinc.net
creditmarketplace.eu
brightenceiling.com.hk
asiapointpl.com
cityclosetselfstorage.com
customroms.cba.pl
daoudi-services.com
cleartripcustomercare.com
dejting.party
coreserv.pixelsco.com
dneprsemena.com
azulproducciones.com.gt
drummelo.altervista.org
danialent.com
deneme2.bokshaber.net
bdot.co.kr
efacile.biz
dymoetiketler.com
dev.beverlywilshiremedical.com
electrobox.org
e-przepisy.cba.pl
doktergigimuda.com
dsc.integralmea.info
envirobostad.se
establecimientos.sintinovoy.sevapp20.com
doglabs.com.br
eyh.org.tr
conthoi.ga
enestar.es
aistockpick.com
farynskiprzemek.cba.pl
ethrx.org
emilyshope.org
103.254.113.170
eye-doctor.mobi
freespiritgroup.altervista.org
cnctechservicos.com.br
flows.mobi
dogcatpetshop.life
gabinetszott.cba.pl
gianlucafiorino1.altervista.org
chinhung.info
stripperin-duisburg.net
tagiloro.ru
www.erikherrstrom.com
test-my-work.ru
nadinidea.com
videokurs-tut.ru
rixos.top
ucjcfundacion.es
hieuvekhoemanhtunhien.com
ucjcfundacion.eu
ucjcfoundation.es
traineeship.top
www.nictoys.com.cn
www.mellbyhorsepower.se
www.yokydesign.com
thetravelnext.com
tiffintownbooks.com
sitpermatabunda.com
intercnetwork.com.ng
wallcraftcustom.com
whippetrealty.com
jcondotel.com
tdhriverview.com.vn
zeleader.com
sanxecu.vn
test.webing.io
mariamiler.com
gomoney.org.in
nossoacordo.com
muoubing.cn
elektropastuh.ru
conferencesdiary.com
schoolapp.be
hopeodisha.com
finestjodi.com
acconsultibrasil.com.br
hashpatal.com
tamanpesona.com
contentsbank.cc
www.trilogiaexpeditionsperu.com
baydarhukuk.com
4fishingbrazil.com
virtualisseta.com
sukamoviedrama.online
espinascompany.com
120.138.17.237
green-world-md.ru
serrurierparis75.ovh
tagil-spectehnika.ru
ldcpharma.com
rotaract3272.org
www.teabungalowstay.in
startkartingnow.com
www.wordpresspractice.cf
www.voirfilm.ga
www.sistemasapex.mx
uniquecollege.com.au
vehiculosbenimar.es
xn----7sbb5ad1beecki5h.xn--p1ai
physiqapparel.no
apartime.ru
www.artenkundig.at
wraytek.com
xuanduocnam.com
reueltravel.com
wingznthangz.com
willybarroy.fr
questraworld.signupvideo.com
www.palyacopapi.com
churritoshow.com
rizal.world
beautybride.net
lachongtrans.com
ultraformervn.com
sunshine-city-ciputra.net
nayahanenda.com
thecellarsisters.ca
thuexephamgia.com
lgf.dk
olindaschool.com.br
hemorrhoidsorted.com
dplusmedia.com
www.chandrobindumcltd.com
andco.mx
sun-casa.com
www.tromelin2014.com
www.jesuisunenfantterrible.com
www.ussclb.org
mrlumberjack.com
crystalhilldesign.com
oralgem.com
loboevents.com

CSE CybSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

Cyber Security Strategists

eunos8.com
fotopsy.cba.pl
faraos.foco.cl
gmstroy.com
giargianes.altervista.org
flccgilumbria.it
francis-china.com
hariominteriordecorators.com
fertilidadpma.com
giftmaster.ml
goleelanau.com
ebsolute.com
grilledcheesereviews.com
getagriptraction.com
editoraplanmark.com.br
blog.ruichuangfagao.com
gypsysoulsonfire.com
datalystsystems.com
hourliapp.com
35.184.187.178
featherenterprising.com
interflower.ee
hownottocatchacold.com
irantbt.com
jak-sie-opalac.cba.pl
istanbul212tesisat.com
jeeping-ug.ru
aesimoveis.imb.br
jiletlitelmakinasi.com
kabiledans.com
hopcentury.com
gfj.adv.br
kameleon-restauracja.cba.pl
kaffekanna.no
kancelaria-crm.pl
informatica.uss.cl
harrisheatpumps.nz
kekti.com
homemingjiang.com
karatstreet.com
krdstud.ru
kmpoznan.cba.pl
hrd.gov.co
ijzsz.com
cqfsbj.cn
graminrajasthan.allappshere.in
advokatessa.com
xn----7sbbax1aamaagfpjbdc3dm.xn--p1ai
citrus.kiev.ua
joyeriadeplata23.com
www.suvorkin.com
redmix.com.ua
kayceemarketing.com
everythingsale.com
iphotobooth.com.au
energy-utama.com
afyonkampustaksi.com.tr
www.reseptifbumipersada.com
camranhcondotel.site
200questions.ru
ideograms.ir
music-360.pl
triumphoh.com
vannadesign.ru
kunefecizade.com.tr
agrovesna.com.ua
ecodom-vent.ru
timtamduc.info
dvrsa.com.br
www.misyah.com.my
kyadapt.org
www.thatstevenrice.com
xecogioivietnam.com
freynutrition.com.tr
etkenkalip.com
heartfulness.com.ua
www.rainbowwaffle.xyz
www.ides.space
robochampsnorth.robomateplus.com
mukenageulis.com
firstbasepromotions.co.za
nashpersonal.com.ua
roketdev.com
dfinformatique.ca
update13.hospedagemdesites.ws
217.61.17.155
blessedlife.in
lealengenharia.hospedagemdesites.ws
gerothermocaldeiras.com.br
vibexpro.com
www.nissingroup.com.hk
tribratanewsende.com
tampacardiologist.com
eaglesturf.org
panoramafoto.com
www.recubrimos.com
sgtrainingzone.com
canopyunited.com
enviziondezigns.com
www.centrixs.biz
leewesley.com
naturecarelandscape.com
atlasgroupllc.com
www.doctoradodai.com
www.nestingbits.com
www.mchurley.com
motoir.com
interiors-by-catherine.com
marydonnelly.com
mvaentertainment.com
nolinenyc.com
hillcountrycamo.com
webunbox.com
www.holgatecenter.org
arantxaevents.com
hisdesignonline.com
www.apartmanipisak.com
www.internationalmoversboston.com
motorcityphotoworkshops.com
dulcethings.com
desertdawnschool.com
bebetalk.ca
massagenirvana.com
www.cnergy.com.br
citetek.com
jlashmore.com
harjudesign.com
rbcreativemg.com
ntouchgroup.com
mintmgtllc.com
www.safranmobilyadekorasyon.com
heartlandrestaurantgroup.com
www.okyanusdavetorganizasyon.com
robertallenentertainment.com
www.donorservicesgroup.com
www.saadetorganizasyon.com
wizfy.com
enzoaudiovisual.com

CSE CybSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

harryfang.com	easyenergy.co.nz	barossadental.com.au
itsupplier.com.au	ashleyfeder.com	zerophage_pedik.com

Yara rules

```
rule gandGrab_v5 {

    meta:
      description = "Yara Rule for gandCrab ransomware v5"
      author = "CSE CybSec Enterprise - Z-Lab"
      last_updated = "2018-10-01"
      tlp = "white"
      category = "informational"

    strings:
        $a1 = "@hashbreaker Daniel J. Bernstein let's dance salsa <3"
        $a2 = "jopochlen"
        $a3 = "%X ahnlab http://memesmix.net/media/created/dd0doq.jpg"
        $b = {55 8B EC E8 00 00 00 00 3E 83 04 24 11 75 05 74 03}


    condition:
        1 of ($a*) and $b

}
```

Cyber Security Strategists

CSE CybSec Enterprise SPA
Via G.B. Martini 6, Rome, Italy 00100, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com