Threat Spotlight: Locky Ransomware

cylance.com/en_us/blog/threat-spotlight-locky-ransomware.html

The BlackBerry Cylance Threat Research Team

Apparently Locky always comes back.

A persistent threat, Locky ransomware apparently has no plans of disappearing anytime soon. Locky has caused issues recently when it was used to attack Hollywood Presbyterian Medical Center during February 2016 where it claimed nearly 400,000 victims in the very first week of its detection. It was about this time that we first looked at Locky.

The largest publicly admitted ransom was paid by the Hollywood Hospital, $17,000 in Bitcoin. The second largest sum was $1,600 in Bitcoin paid by the Methodist Hospital. Since then, we have seen a lot of variants of the ransomware, named for the file extensions given to the encrypted files. Other variants we’ve seen have included zepto, thor, and osiris. Now we have Diablo6.

Little Changes in Known Malware Make it Fresh and New Again

Endpoint security is improving by the day but so are cybercriminals; this makes detecting the criminals a never-ending game of cat and mouse. It is often found that malware authors proactively monitor the detection rates of their product, allowing them to stay one step ahead of AV vendors by making improvements to their code to avoid detection. In some cases, authors can make small changes in their code to keep their malware as dangerous to the end user as it was the day they released it.

This appears to be the case the case with the Locky ransomware. This old malware didn’t need to have anything new, as the authors behind Locky just had to tweak the only part of the process that can never be fixed - the end user. The most recent change for Locky came as one of the most popular ways to spread malware: spear phishing emails.

In this blog post, a VBS file archived via zip is dissected showing the techniques used by threat actors to avoid detection.

Our Technical Teardown

The original command-and-control server (C2) at the time of this writing is down, so I will be using INetSim to simulate the C2. INetSim is a Linux tool used to emulate common Internet services such as HTTP, HTTPS, DNS, and many others. Implemented on a REMnux virtual machine in our lab environment, INetSim will serve as a fake DNS server. This allows for the VBS script to connect to its C2 at atesbocegianaokulu [dot] com/y872ff2f. Once the DNS request is made, INetSim will act as the C2 and serve the malicious payload.

The attack happens in two stages: The first stage is the spear phishing email that has a zip archive attached, pictured in Figure 1.a. Inside the archive is a VBS file with the same name as the archive, pictured in the Figure 1.b.

Figure 1.a - Phishing Email

Figure 1.b - Zip File and VBS File

When the victim decompresses the archive, and clicks on the file, the VBS script starts to run. The script tries to connect to the C2 and download the ransomware payload as seen in the Figure 2.a and Figure 2.b:

Figure 2.a - VBS script code:the code has two different C2s separated with a dash and the name of the payload. If the VBS script can’t download the payload from the first C2 it tries to download it from the second one.

Figure 2.b - VBS Script Code New Name

The word “Enterprise” in Figure 2.b is used to avoid the malicious code detection by static analysis in an attempt to make the end user think that it is a valid component of some sort of enterprise utility. At the same time, it uses the string to split the malicious instructions, the real instructions are:

Microsoft.XMLHTTP Adodb.streaM shell.Application Wscript.shell Process Get Temp Type Open Write ResponseBody Savetofile \GINPcFUJR.exe http: //

In Figure 3, the VBS script can be seen connecting to the C2 and downloading the payload.

Figure 3 - PCAP vbs Script

The script saves the second stage payload in the AppData/Local/Temp folder with a different name, then runs the malware as seen in Figure 4 and Figure 5.

Figure 4 -Temp Folder

Figure 5 - Stage 2 of the Malware is Running

The attack ends after encryption with the ransom message, seen below in Figure 6, then deletes itself.

Figure 6 - Ransomware Window

Now all files on the system are encrypted with Diablo6, which we already know as Locky ransomware. Figure 6.a shows the affected files, post-encryption, with the new Diablo6 file type.

Figure 6.a - DIABLO6 Encryption

The Locky Diablo6 Ransomware will target the following file types:

.sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbackup, .backup, .backupdb, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpqge, .kdb, .db0, .dba, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b, .p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .psd, .dbf, .mdf, .wb*2, .rtf,* .wpd, .dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm*, .pptx, .ppt,* .xlk*, .xlsb*, .xlsm, *.xlsx*, *.xls,* .wps, .docm, .docx, .doc, .odb, .odc, .odm, *.odp*, .ods, *.odt*.

The domain dbr663dnbssfrodison[dot]net was recently created on August 1st, 2017 using the registrant email: jenniemarc(at)mail.com. A reverse Whois Lookup on that account shows that 333 domains were registered by this email starting in 2016 and as recently as October 2017. Some of those domains are known to be serving other families of ransomware which can be seen in the appendix. We can use this registrant and these domains to proactively detect and prevent the download of the Locky payload.

How to Stop Locky and Attacks Like It

Phishing emails can be tricky, as they're specifically designed to trick the end user into initiating an action that they believe to be legitimate. Whether it's opening a malicious email attachment or entering credentials to a fake Gmail or Yahoo login page, mitigating social engineering attacks can be achieved with user education. Below are some simple actions to take to help prevent these types of attacks:

1. Never open email if you don't know the sender.
2. Never open a document if you don't know where it came from.
3. Backup your personal information constantly.

If you use our endpoint protection product, CylancePROTECT®, you are already protected from this attack.

This is one form of many different attack patterns that we are seeing. The threat can be distributed via HTML attachments disguised as invoices, Word documents embedded with malicious macro code or Visual Basic scripts (VBS), malicious URLs in spam emails, VBS, JS files archived via RAR, ZIP or 7ZIP, and DDE Office Documents.

Indicators of Compromise (IoCs)

9fe8323e5e88383283551e86bfe82518bbf68c00ae8e955fa91c738400a2d6d5
05234bcb6b5276cc39da03969be99dff7398217729dc896ef04db2fb58dd1cca
F689391B0527FBF40D425E1FFB1FAFD5C84FA68AF790E8CC4093BCC81708C11B

Atesbocegianaokulu [dot] com
dbr663dnbssfrodison [dot] net
213.142.130.106

y872ff2f.exe
GlNPcFUJR.exe

APPENDIX

Domain Name: foolerpolwer(dot)info
Creation Date: 8/4/2017
Payload: JS Locky Downloader
Hash256: 175054f99fad729d18bfc5314a162ca418f13a41e7325afe33b214c9d94aea72

Domain Name: tertrodefordown(dot)info
Creation Date: 9/21/2017
Payload: VBS Locky Downloader
Hash256: 25b6e194d57c0e2abd27c68da2815e869f089151d5581a33f8ca9e8a0b9b2de3

Domain Name: sdfsdgfsdfsdfsd(dot)info
Creation Date: 9/1/2017
Payload: Trojan Banker
Hash256: 3136fd5a06ad5b1cdc48ade31fe5fdce6c050e514f028db18230d31801592995

Domain Name: droohsdronfhystgfh(dot)info
Creation Date: 8/17/2017
Payload: Ransom Locky
Hash256: 3d653771933422f9a081ea122865da76edde83cdeb41b8b8e377833e75e21aca

Domain Name: soundgoodhj(dot)info
Creation Date: 8/6/2017
Payload: Ransom Gryphon
Hash256: 5e306f5a6aebc5c13ff92dc7de73f0618207deb925c1e4c66c25730f64caeac9

Domain Name: hg777hdorotosskot(dot)info
Creation Date: 4/12/2017
Payload: Ransom Locky
Hash256: 61897573ac9e221c42a7a1fe9d1468b6fd10911df8ffd9485deaa158505896aa

Domain Name: rateventrithathen(dot)info
Creation Date: 9/20/2017
Payload: Ransom Locky
Hash256: 6687de88bb2798f6e0e8c96fca699a59f0ecc9baecda006887c70962e76d381b

Domain Name: toplooneytopwe(dot)info
Creation Date: 6/18/2016
Payload: JS Locky Downloader
Hash256: 99e299930cf68c9c76f4a2bec7489c496e3a8f9e9c6b3e45794d6484b8151412

Domain Name: porticutoof(dot)info
Creation Date: 12/8/2016
Payload: JS Locky Downloader
Hash256: 9adb8658dd1827fbdb36d864e804f8dd5804c5ca0739affd91c4168066c4b048

Domain Name: grandfatherisgood(dot)biz
Creation Date: 9/12/2017
Payload: Trojan
Hash256: a41523a75206b6eabeacd06a33abc681e7969a396f69b3b93a802ef162aa2d6b

Domain Name: petrovichmargonovbratva(dot)biz
Creation Date: 8/4/2017
Payload: Trojan Banker
Hash256: a4a0dcb422530fc0e79adeac90583125c70b6a3ffe13d315d882bb10c7711ffb

Domain Name: unhanorarse(dot)info
Creation Date: 9/20/2017
Payload: Ransom Locky
Hash256: c35f705df9e475305c0984b05991d444450809c35dd1d96106bb8e7128b9082f

Domain Name: lollyonn(dot)info
Creation Date: 12/9/2016
Payload: JS Locky Downloader
Hash256: c8118a8efd5d201792cf1c3abeeda249036000205fab144fdbdc7fdf20aa77d7

Domain Name: ciickdomka(dot)info
Creation Date: 10/6/2017
Payload: Ransom Locky
Hash256: df255af635a2dde04c031db95862f11e1bf44fe5cfc10d3b20bd4678ed818567

Domain Name: jacklosko(dot)info
Creation Date: 10/5/2017
Payload: Ransom Locky
Hash256: eead04036eccb12ea4e27c38047bbad6899ada4cc1e9e9154c5ac1dfdedd38cc

Domain Name: tolopkedoper(dot)info
Creation Date: 10/3/2017
Payload: Ransom Locky
Hash256: f196a81eab51eadbcf3c5171c3c23ce35a7320a8434676ac9265dda2c0aec229

Domain Name: mokazylokh(dot)info
Creation Date: 10/8/2017
Payload: Trojan
Hash256: f317cd282eabf150e660619a686ac9c2af11ac59d103abaea2756c221d33af45

Domain Name: trmbobodortyuoiyrt(dot)org
Creation Date: 8/7/2017
Payload: Ransom Locky
Hash256: f689391b0527fbf40d425e1ffb1fafd5c84fa68af790e8cc4093bcc81708c11b

Domain Name: moroplinghaptan(dot)info
Creation Date: 9/20/2017
Payload: JS Locky Downloader
Hash256: fde84a9e721c55675452ed2d2f12f224e19a0a24116d3a47efe1633b1c6b404c

DOMAIN NAME	**CREATION DATE**
carderverifiedstore(dot)biz	10/16/2017
cvvshopvalid(dot)info	10/16/2017
dollsgoals(dot)info	10/16/2017
onlinestoretrack2(dot)biz	10/16/2017
shopcvvvalid(dot)biz	10/16/2017
shoptrack2online(dot)info	10/16/2017
sutranjdf(dot)info	10/13/2017

netflixpersonnal-billing(dot)info	10/9/2017
netflixsupport-verification(dot)info	10/2/2017
netflixupdate(dot)info	9/22/2017
35sdc2(dot)biz	9/20/2017
bw2g3sg(dot)biz	9/20/2017
dkkdjslla(dot)info	9/13/2017
kamadexa(dot)info	9/13/2017
intesasanpaoloverifica(dot)info	9/3/2017
ingdirectonline(dot)info	8/29/2017
o2bonusbandwidthpromo(dot)info	8/6/2017
opencloudstorage(dot)info	8/2/2017
gdrroonttolsdart(dot)info	7/31/2017
trombositting(dot)org	7/31/2017
zasxqwedcvfr(dot)info	7/19/2017
projectconceive(dot)info	7/18/2017
koolakolasq(dot)info	7/14/2017
nortonfja(dot)info	7/12/2017
pp-transaktion-de(dot)info	7/7/2017
pp-transaktion(dot)info	7/7/2017
sweetbalancereuro(dot)top	7/7/2017
transaktion-de(dot)info	7/7/2017
transaktion-pp(dot)info	7/7/2017
transaktion(dot)info	7/7/2017
castrolopezf(dot)top	7/5/2017
ccollergla(dot)top	7/5/2017
cesarjeg(dot)top	7/5/2017

cmoahyrdla(dot)top	7/5/2017
coolmanianade(dot)top	7/5/2017
daaloodac(dot)top	6/27/2017
dastonond(dot)top	6/27/2017
dbvopeoo(dot)top	6/27/2017
dndsmoidsa(dot)top	6/27/2017
doamebnsa(dot)top	6/27/2017
rammonteredot(dot)info	6/27/2017
taripoinov(dot)top	6/22/2017
beturuitem(dot)top	6/21/2017
clippodoops(dot)top	6/21/2017
coolfamerl(dot)top	6/21/2017
julesmitthxrfusion(dot)top	6/21/2017
memaleicas(dot)top	6/21/2017
yateheenth(dot)top	6/21/2017
caloploerd(dot)top	6/20/2017
cloplodanx(dot)top	6/20/2017
comocsmad(dot)top	6/20/2017
bing-msn(dot)top	6/16/2017
chatwork(dot)org	6/16/2017
securesparkasse(dot)info	6/16/2017
amozion(dot)top	6/15/2017
checkio2uha(dot)top	6/15/2017
sparkassensicherheit(dot)top	6/15/2017
sparsecure(dot)info	6/15/2017
banggonefl(dot)top	6/14/2017

bobydokeq(dot)top	6/14/2017
bodeaskopq(dot)top	6/14/2017
bommbewakq(dot)top	6/14/2017
bzmomfasej(dot)top	6/14/2017
information-sicherheit-deutschland(dot)top	6/13/2017
kundenservice-sicherheit-deutschland(dot)top	6/13/2017
samaywondererer(dot)top	6/13/2017
support-kundenservice-sicherheit(dot)top	6/13/2017
support-sicherheit-deutschland(dot)top	6/13/2017
andrwnolas(dot)top	6/10/2017
trominguatedrop(dot)org	6/10/2017
aboomnsaoq(dot)top	6/8/2017
alopoaqux(dot)top	6/8/2017
angorzmq(dot)top	6/8/2017
anonoduz(dot)top	6/8/2017
friecedara(dot)top	6/8/2017
hncidhweh(dot)top	6/8/2017
sicherere-sparkasse(dot)info	6/5/2017
sparkassen-hilfe(dot)info	6/5/2017
sparkassen-support(dot)info	6/5/2017
validatiion(dot)info	6/1/2017
7tausd(dot)info	5/31/2017
asdg68a(dot)info	5/31/2017
atufd5a(dot)info	5/31/2017
bilinom(dot)info	5/31/2017
data-service-de(dot)info	5/31/2017

friecedara(dot)org	5/31/2017
irveneloni(dot)info	5/31/2017
jyatdha5(dot)info	5/31/2017
nyminalowe(dot)info	5/31/2017
pp-data-service-de(dot)info	5/31/2017
sparkasse-onlinebanking(dot)info	5/31/2017
sparkasseonline(dot)info	5/31/2017
xciahessea(dot)info	5/31/2017
deinesparkasse(dot)info	5/30/2017
e67tfgc4uybfbnfmd(dot)org	5/30/2017
hv7verjdhfbvdd44f(dot)info	5/30/2017
soonnydfokkhekildfr(dot)info	5/30/2017
fly-search(dot)top	5/27/2017
flysearch(dot)top	5/27/2017
travel-pro(dot)top	5/27/2017
youtoolgrabeertorse(dot)org	5/24/2017
donaifryac(dot)top	5/23/2017
goodcoolac(dot)top	5/23/2017
sopoqaira(dot)top	5/23/2017
y887drossetorling(dot)info	5/23/2017
yonaopqsd(dot)top	5/23/2017
zopoaheika(dot)top	5/23/2017
aboulthous(dot)top	5/22/2017
reterbawax(dot)top	5/22/2017
zelispecto(dot)top	5/20/2017
orderid(dot)info	5/18/2017

justgoogkaz(dot)top	5/17/2017
kinkplusvb(dot)top	5/17/2017
oldloverfg(dot)top	5/17/2017
pichdollard(dot)top	5/17/2017
realpolyfv(dot)top	5/17/2017
mernederu(dot)top	5/16/2017
valiidation(dot)top	5/16/2017
veriificatiion(dot)info	5/16/2017
betsransfercomunications(dot)org	5/14/2017
bublegoom(dot)top	5/14/2017
maximusstafastoriesticks(dot)info	5/14/2017
sdfsdfsdf22aaa(dot)biz	5/14/2017
vallidity(dot)info	5/14/2017
verifiy(dot)info	5/14/2017
veriify(dot)top	5/14/2017
herrossoidffr6644qa(dot)top	5/13/2017
astracama(dot)top	5/11/2017
chinawokia(dot)top	5/11/2017
momendfakol(dot)top	5/11/2017
qipokacool(dot)top	5/11/2017
sjffonrvcik45bd(dot)info	5/11/2017
viperfoxca(dot)top	5/11/2017
cewjnjkewlwefjn(dot)top	5/5/2017
skihaz(dot)org	5/5/2017
wscfgfr23azfg(dot)top	5/5/2017
bilinom(dot)top	5/3/2017

gangvooloq(dot)top	5/3/2017
inatinmeg(dot)top	5/3/2017
ionernment(dot)top	5/3/2017
johnalmcx(dot)top	5/3/2017
mopooland(dot)top	5/3/2017
samaybktfacjxiqxrt(dot)top	5/3/2017
samaytfacjxiozqzxt(dot)top	5/3/2017
shonmitab(dot)top	5/3/2017
sousedopac(dot)top	5/3/2017
teds04(dot)top	5/3/2017
teff23(dot)top	5/3/2017
terr44(dot)top	5/3/2017
weekdkla(dot)top	5/3/2017
newdoagear(dot)top	5/1/2017
newfornz(dot)top	5/1/2017
seahomevb(dot)top	5/1/2017
horsezangd(dot)top	4/28/2017
kingzoneg(dot)top	4/28/2017
4rebaopfgrewe(dot)top	4/26/2017
batypli3werty(dot)top	4/26/2017
reytxdgyeaaa4(dot)top	4/26/2017
castropoolx(dot)info	4/13/2017
fkksjobnn43(dot)org	4/12/2017
parking-service(dot)us	4/12/2017
chinasolz(dot)top	4/10/2017
doomnooaxc(dot)top	4/10/2017

funmasterg(dot)top	4/10/2017
kancoolk(dot)top	4/10/2017
sunajobc(dot)top	4/10/2017
bloomexit(dot)info	4/9/2017
fortflutter(dot)info	4/9/2017
zipzipzipzob(dot)top	4/9/2017
mhforum(dot)biz	4/8/2017
astrasunxc(dot)top	4/6/2017
faprilzexuetemidrrter(dot)wang	4/6/2017
kapelfoorh(dot)top	4/6/2017
lopo99(dot)top	4/6/2017
nobelopoenz(dot)top	4/6/2017
sore32(dot)top	4/6/2017
sudo32(dot)top	4/6/2017
vedsa43(dot)top	4/6/2017
cole87(dot)top	4/5/2017
douh887(dot)top	4/5/2017
faprilzexuetequwxtw(dot)top	4/5/2017
fop94(dot)top	4/5/2017
fpp07(dot)top	4/5/2017
gormanovsarbentol(dot)xyz	4/5/2017
lopo00(dot)top	4/5/2017
mene004(dot)top	4/5/2017
poprtgedfjijogsrrgefdofwewogosvoasowarufoqwedqfwerioeqiwwqfwe(dot)top	4/5/2017
xcff43g(dot)top	4/5/2017
airventilgood(dot)top	4/3/2017

mop22(dot)top	4/3/2017
nie92p(dot)top	4/3/2017
s234op(dot)top	4/3/2017
ubc188(dot)top	4/3/2017
ineragons(dot)info	4/2/2017
microsoft-update-server82148(dot)top	4/2/2017
bkasioqpz(dot)top	3/31/2017
gerbnopesa(dot)top	3/31/2017
nowsunnygk(dot)top	3/31/2017
opennewsnz(dot)top	3/31/2017
sunfloridjk(dot)top	3/31/2017
obamaloshara(dot)top	3/27/2017
chromehakc(dot)top	3/26/2017
fffgooaldq(dot)top	3/26/2017
ffjoleedas(dot)top	3/26/2017
hoopcinezc(dot)top	3/26/2017
newsectorbs(dot)top	3/26/2017
testoviydom2(dot)wang	3/26/2017
watherfka(dot)top	3/26/2017
chromebewfk(dot)top	3/24/2017
chromefastl(dot)top	3/24/2017
naiikkledc(dot)top	3/22/2017
voperforseanx(dot)top	3/22/2017
dboosajqn(dot)top	3/21/2017
fooplodanx(dot)top	3/21/2017
gooolgeremf(dot)top	3/21/2017

treetopztrxxdertyu(dot)top	3/21/2017
truemityunituistep(dot)top	3/21/2017
bobdomjda(dot)top	3/20/2017
yunityreyrehol(dot)top	3/20/2017
infosavetop(dot)top	3/17/2017
sonicfopase(dot)top	3/17/2017
gijilemependel(dot)top	3/16/2017
newfjoledc(dot)top	3/16/2017
nngolodasz(dot)top	3/16/2017
fkauueeepla(dot)top	3/14/2017
fploosate(dot)top	3/14/2017
lobsterscrewallt(dot)top	3/14/2017
djlooedpoa(dot)top	3/11/2017
toytyaclucomunit(dot)top	3/10/2017
dpooldoopla(dot)top	3/9/2017
marchjobkax(dot)top	3/8/2017
sxyseywerty(dot)top	3/7/2017
domain121111331(dot)top	3/6/2017
domaina12wsss(dot)top	3/3/2017
foolalexas(dot)top	3/3/2017
tregretryfaltervipo(dot)top	3/3/2017
pentsshoperqunity(dot)top	3/2/2017
rolerxunitywsto(dot)top	3/2/2017
nondopled(dot)top	3/1/2017
hoolpofaw(dot)top	2/27/2017
govementruystd(dot)top	2/23/2017

adroeneqerty(dot)top	2/17/2017
sumnitdomains(dot)top	2/16/2017
polaerunity(dot)top	2/15/2017
basopoew(dot)top	2/14/2017
fopeioaas(dot)top	2/11/2017
zoerpoled(dot)top	2/10/2017
dqpowera(dot)top	2/9/2017
vanrityunity(dot)top	2/9/2017
unityiestgen(dot)top	2/4/2017
footarepu(dot)top	1/26/2017
folueopa(dot)top	1/24/2017
panntyplenty(dot)top	1/24/2017
pennysgoods(dot)top	1/24/2017
sallykandymandy(dot)top	1/23/2017
toagoores(dot)top	1/23/2017
transponitieswan(dot)top	1/21/2017
sutraponef(dot)top	1/20/2017
aloepolera(dot)top	1/16/2017
treetopzxxtredtyu(dot)wang	1/16/2017
dogtosamdnc(dot)top	1/13/2017
fooperight(dot)top	1/13/2017
sicherheit-deutschland-kundenservice(dot)top	1/12/2017
kledwdjvfklopcopdcjsdfdqlkweqwljrquriepewewqrufjcladqpiomzzds(dot)top	1/11/2017
senchar(dot)biz	1/11/2017
travelsserts(dot)wang	1/7/2017
weiter-zur-bank(dot)top	1/7/2017

bogidoggy(dot)top	1/6/2017
networksinform(dot)top	1/6/2017
security-amerilcanexpress(dot)online	1/5/2017
823ad893992(dot)top	1/2/2017
828347d8923(dot)top	1/2/2017
xoejyyhoncfdvdgzxe(dot)top	1/2/2017
roverstop(dot)top	12/27/2016
igoodsnd(dot)wang	12/22/2016
igoodsst(dot)top	12/22/2016
verifizierung23857392(dot)biz	12/22/2016
dealkolld(dot)top	12/21/2016
weiter-zur-bank(dot)biz	12/21/2016
weiterleitung-zur-bank(dot)biz	12/21/2016
au-netbank(dot)top	12/20/2016
errorfola(dot)top	12/20/2016
newgiftnd(dot)wang	12/20/2016
newgiftst(dot)top	12/20/2016
dbftnty456ffff(dot)top	12/16/2016
salesnd(dot)top	12/16/2016
jobbelopa(dot)top	12/15/2016
zombiedoomq(dot)top	12/15/2016
dondokier(dot)top	12/13/2016
stickersdes(dot)org	12/13/2016
copiesnd(dot)top	12/12/2016
nnapoakea(dot)top	12/12/2016
qopahighk(dot)top	12/12/2016

fraujenod(dot)top	12/9/2016
aloesantanewd(dot)top	12/7/2016
testidoalkas(dot)top	12/7/2016
wrkoolegedd(dot)top	12/7/2016
youtoof(dot)info	12/7/2016
httphqs(dot)top	12/1/2016
httsps(dot)top	11/30/2016
postbodaw(dot)top	11/24/2016
uepolicae(dot)top	11/24/2016
baaslorelab(dot)wang	11/22/2016
gooholtan(dot)wang	11/22/2016
trentil(dot)top	11/18/2016
doc4tolllcp(dot)top	7/6/2016
1topfllrt(dot)top	7/4/2016
aeropoer(dot)top	6/30/2016
easy-money20000(dot)top	6/29/2016
hookup4444(dot)top	6/29/2016
megadating333(dot)top	6/29/2016
atonement(dot)top	6/24/2016
bareknuckle(dot)top	6/24/2016
guillotine(dot)top	6/24/2016

The BlackBerry Cylance Threat Research Team

About The BlackBerry Cylance Threat Research Team

The BlackBerry Cylance Threat Research team examines malware and suspected malware to better identify its abilities, function and attack vectors. Threat Research is on the frontline of information security and often deeply examines malicious software, which puts us in a unique position to discuss never-seen-before threats.