COBALT DICKENS Goes Back to School…Again

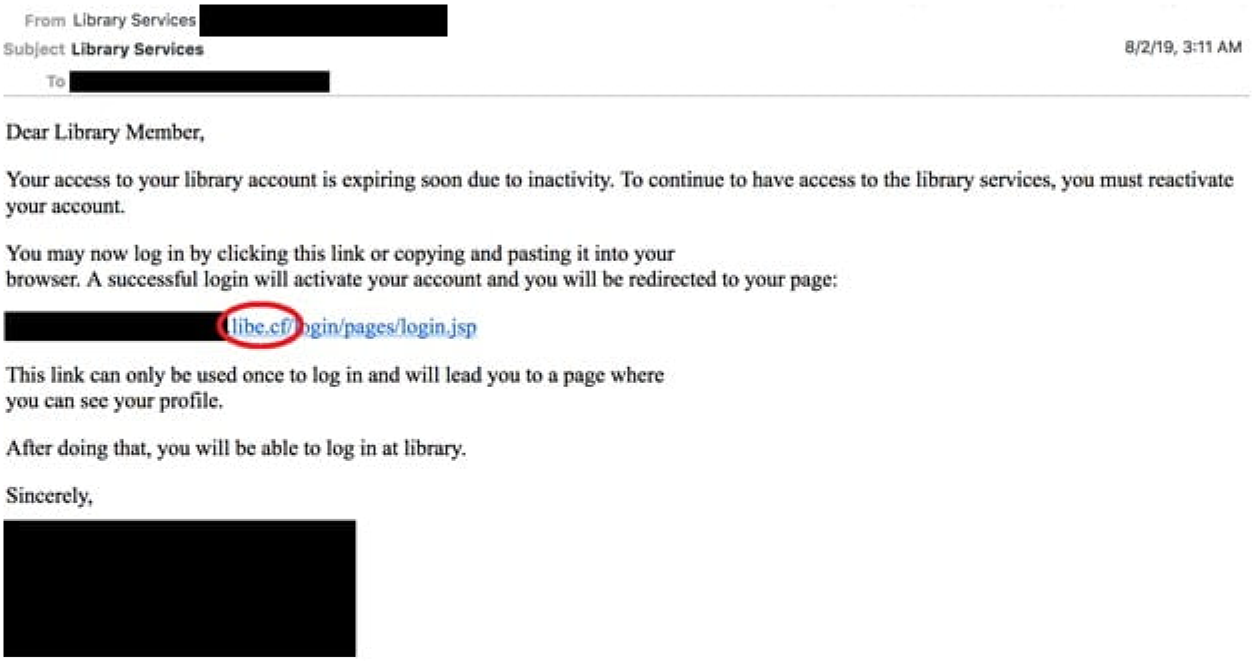
secureworks.com/blog/cobalt-dickens-goes-back-to-school-again

Counter Threat Unit Research Team

The COBALT DICKENS threat group persists despite law enforcement actions and public disclosures, conducting another global campaign targeting universities. Wednesday, September 11, 2019 *By: Counter Threat Unit Research Team*

In March 2018, the U.S. Department of Justice indicted the Mabna Institute and nine Iranian associates for compromising hundreds of universities to steal intellectual property and benefit financially. Secureworks® Counter Threat Unit™ (CTU) researchers assigned the *name COBALT DICKENS to this likely Iranian government-directed threat group. Despite this indictment and other disclosures of COBALT DICKENS campaigns, the threat group (also known as Silent Librarian) shows no signs of stopping its activity as of this publication. CTU™ researchers have observed the threat actors using free online services as part of their operations, including free certificates, domains, and publicly available tools.*

In July and August 2019, CTU researchers discovered a new large global phishing operation launched by COBALT DICKENS. This operation is similar to the threat group's August 2018 campaign, using compromised university resources to send library-themed phishing emails. The messages contain links to spoofed login pages for resources associated with the targeted universities. Unlike previous campaigns that contained shortened links to obscure the attackers' infrastructure, these messages contain the spoofed URL (see Figure 1).



From Library Services [redacted]
Subject Library Services
8/2/19, 3:11 AM
To [redacted]

Dear Library Member,

Your access to your library account is expiring soon due to inactivity. To continue to have access to the library services, you must reactivate your account.

You may now log in by clicking this link or copying and pasting it into your
browser. A successful login will activate your account and you will be redirected to your page:

[redacted]libe.cf/login/pages/login.jsp

This link can only be used once to log in and will lead you to a page where
you can see your profile.

After doing that, you will be able to log in at library.

Sincerely,

[redacted]

Figure 1. Phishing message containing a link to a COBALT DICKENS domain (circled in red). (Source: Secureworks)

Recipients who click this link are directed to a web page that looks identical or similar to the spoofed library resource. After the victims enter their credentials, their web browsers are redirected to the next.php file, where the credentials are stored locally in the pass.txt file. The victim's browser is then sent to the legitimate site being spoofed (see Figure 2).

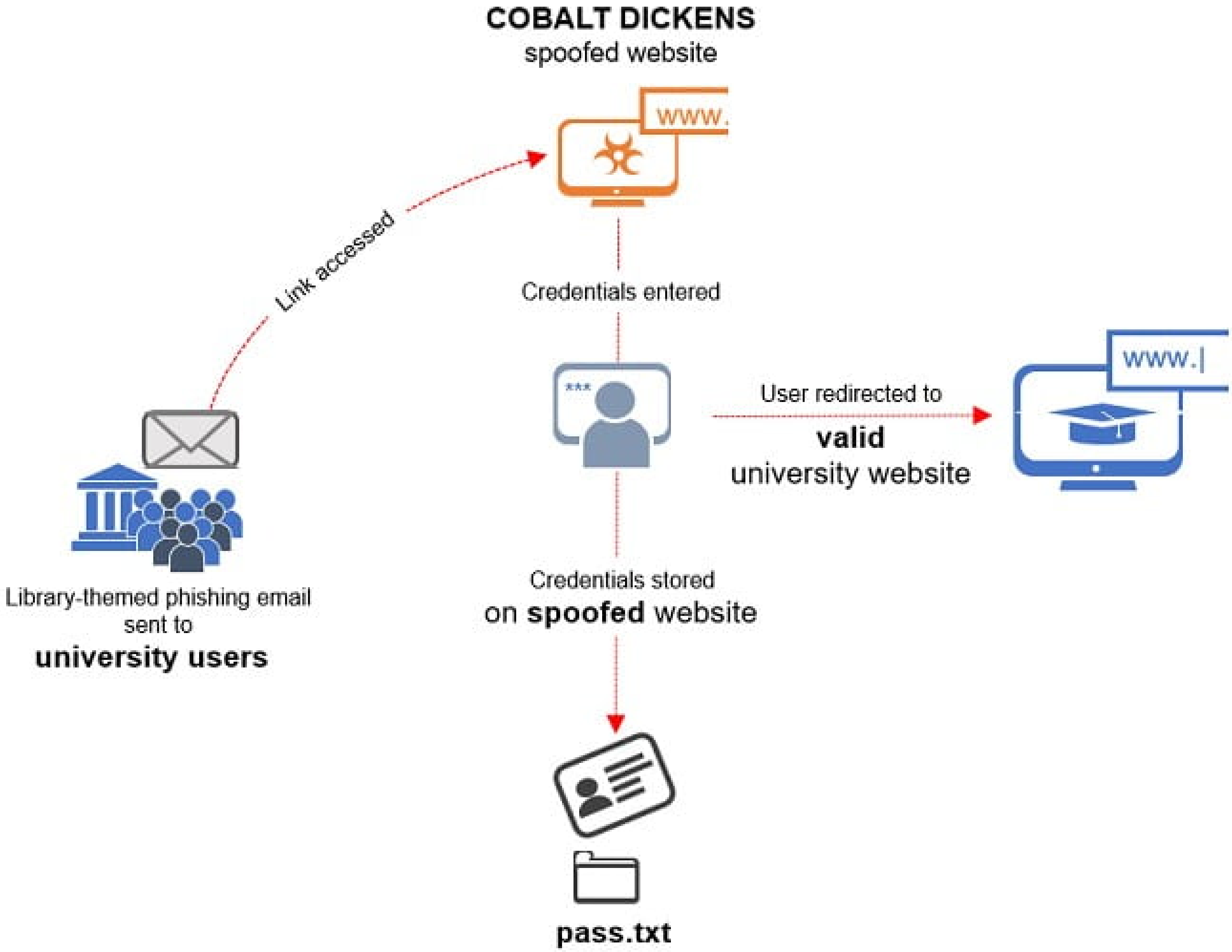


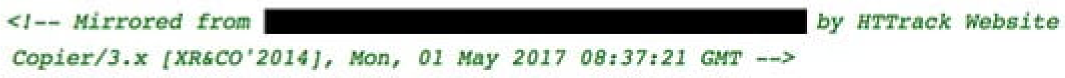
Figure 2. Lifecycle of a COBALT DICKENS credential-harvesting phishing operation. (Source: Secureworks)

For this campaign, the threat actors registered at least 20 new domains targeting over 60 universities in Australia, the United States, the United Kingdom, Canada, Hong Kong, and Switzerland. These domains were registered using the Freenom domain provider, which administers the following free top-level domains (TLDs) unless the domain is considered "special":

- .ml
- .ga
- .cf
- .gq
- .tk

Many of these domains use valid SSL certificates, likely to make the spoofed pages appear authentic. The overwhelming majority of the certificates observed in 2019 were issued by Let's Encrypt, a nonprofit organization that programmatically issues free certificates. However, past campaigns used certificates issued by the Comodo certificate authority.

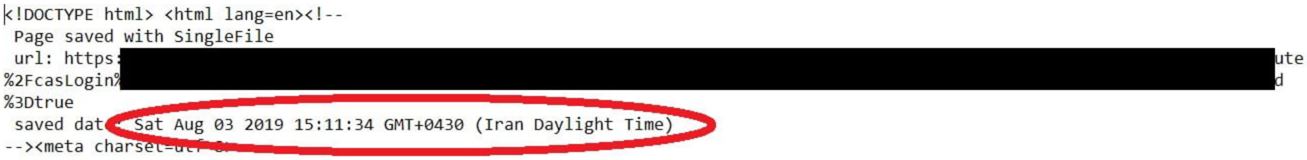
COBALT DICKENS uses publicly available tools, including the SingleFile plugin available on GitHub and the free HTTrack Website Copier standalone application, to copy the login pages of targeted university resources. Metadata in a spoofed login page created on August 1 suggests that COBALT DICKENS sometimes uses older copied versions of target websites. A comment left in the source code indicates it was originally copied on May 1, 2017 (see Figure 3). However, the university was targeted by numerous COBALT DICKENS operations, including the August 2018 and August 2019 campaigns.



```
<!-- Mirrored from [redacted] by HTTrack Website
 Copier/3.x [XR&CO'2014], Mon, 01 May 2017 08:37:21 GMT -->
```

Figure 3. A comment in the source code of a spoofed page created by COBALT DICKENS. (Source: Secureworks)

Metadata in other spoofed web pages supports the assessment that the threat actors are of Iranian origin. Specifically, a page copied on August 3 reveals an Iranian-related timestamp (see Figure 4).



```
<!DOCTYPE html> <html lang=en><!--
 Page saved with SingleFile
 url: https:[redacted]ute
%2FcasLogin%[redacted]d
%3Dtrue
 saved date: Sat Aug 03 2019 15:11:34 GMT+0430 (Iran Daylight Time)
--><meta charset=utf-8>
```

Figure 4. Metadata in COBALT DICKENS spoofed web page indicating that an Iran-based threat actor may have copied the legitimate website. (Source: Secureworks)

As of this publication, CTU researchers observed COBALT DICKENS targeting at least 380 universities in over 30 countries. Many universities have been targeted multiple times. The threat actors have not changed their operations despite law enforcement activity, multiple public disclosures, and takedown activity.

Some educational institutions have implemented multi-factor authentication (MFA) to specifically address this threat. While implementing additional security controls like MFA could seem burdensome in environments that value user flexibility and innovation, single-password accounts are insecure. CTU researchers recommend that all organizations protect Internet-facing resources with MFA to mitigate credential-focused threats.

To provide broader awareness of the threat group's campaigns and curtail its activities, CTU researchers listed all known domains associated with COBALT DICKENS operations in Table 1. Several domains used prior to the indictment remain in use as of this publication. CTU researchers recommend that organizations use available controls to review and restrict access to these domains. They may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context

mlibo.ml	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
blibo.ga	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
azll.cf	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
azlll.cf	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
lzll.cf	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
jlll.cf	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
elll.cf	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
lllib.cf	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
tsll.cf	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
ulll.tk	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
tlll.cf	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
libt.ga	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
libk.ga	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
libf.ga	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
libe.ga	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
liba.gq	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
libver.ml	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations

ntll.tk	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
ills.cf	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
vtll.cf	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
clll.tk	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
stll.tk	Domain name	Hosting phishing website used by COBALT DICKENS for August/July 2019 operations
llii.xyz	Domain name	Hosting phishing website used by COBALT DICKENS
lill.pro	Domain name	Hosting phishing website used by COBALT DICKENS
eduv.icu	Domain name	Hosting phishing website used by COBALT DICKENS
univ.red	Domain name	Hosting phishing website used by COBALT DICKENS
unir.cf	Domain name	Hosting phishing website used by COBALT DICKENS
unir.gq	Domain name	Hosting phishing website used by COBALT DICKENS
unisv.xyz	Domain name	Hosting phishing website used by COBALT DICKENS
unir.ml	Domain name	Hosting phishing website used by COBALT DICKENS
unin.icu	Domain name	Hosting phishing website used by COBALT DICKENS
unie.ml	Domain name	Hosting phishing website used by COBALT DICKENS
unip.gq	Domain name	Hosting phishing website used by COBALT DICKENS
unie.ga	Domain name	Hosting phishing website used by COBALT DICKENS

unip.cf	Domain name	Hosting phishing website used by COBALT DICKENS
nimc.ga	Domain name	Hosting phishing website used by COBALT DICKENS
nimc.ml	Domain name	Hosting phishing website used by COBALT DICKENS
savantaz.cf	Domain name	Hosting phishing website used by COBALT DICKENS
unie.gq	Domain name	Hosting phishing website used by COBALT DICKENS
unip.ga	Domain name	Hosting phishing website used by COBALT DICKENS
unip.ml	Domain name	Hosting phishing website used by COBALT DICKENS
unir.ga	Domain name	Hosting phishing website used by COBALT DICKENS
untc.me	Domain name	Hosting phishing website used by COBALT DICKENS
jhbn.me	Domain name	Hosting phishing website used by COBALT DICKENS
unts.me	Domain name	Hosting phishing website used by COBALT DICKENS
uncr.me	Domain name	Hosting phishing website used by COBALT DICKENS
lib-service.com	Domain name	Hosting phishing website used by COBALT DICKENS
unvc.me	Domain name	Hosting phishing website used by COBALT DICKENS
untf.me	Domain name	Hosting phishing website used by COBALT DICKENS
nimc.cf	Domain name	Hosting phishing website used by COBALT DICKENS
anvc.me	Domain name	Hosting phishing website used by COBALT DICKENS

ebookfafa.com	Domain name	Hosting phishing website used by COBALT DICKENS
nicn.gq	Domain name	Hosting phishing website used by COBALT DICKENS
untc.ir	Domain name	Hosting phishing website used by COBALT DICKENS
librarylog.in	Domain name	Hosting phishing website used by COBALT DICKENS
llli.nl	Domain name	Hosting phishing website used by COBALT DICKENS
lllf.nl	Domain name	Hosting phishing website used by COBALT DICKENS
libg.tk	Domain name	Hosting phishing website used by COBALT DICKENS
ttil.nl	Domain name	Hosting phishing website used by COBALT DICKENS
llil.nl	Domain name	Hosting phishing website used by COBALT DICKENS
lliv.nl	Domain name	Hosting phishing website used by COBALT DICKENS
llit.site	Domain name	Hosting phishing website used by COBALT DICKENS
flil.cf	Domain name	Hosting phishing website used by COBALT DICKENS
e-library.me	Domain name	Hosting phishing website used by COBALT DICKENS
cill.ml	Domain name	Hosting phishing website used by COBALT DICKENS
fill.cf	Domain name	Hosting phishing website used by COBALT DICKENS
libm.ga	Domain name	Hosting phishing website used by COBALT DICKENS
eill.cf	Domain name	Hosting phishing website used by COBALT DICKENS

llib.cf	Domain name	Hosting phishing website used by COBALT DICKENS
eill.ga	Domain name	Hosting phishing website used by COBALT DICKENS
nuec.cf	Domain name	Hosting phishing website used by COBALT DICKENS
illl.cf	Domain name	Hosting phishing website used by COBALT DICKENS
cnen.cf	Domain name	Hosting phishing website used by COBALT DICKENS
aill.nl	Domain name	Hosting phishing website used by COBALT DICKENS
eill.nl	Domain name	Hosting phishing website used by COBALT DICKENS
mlib.cf	Domain name	Hosting phishing website used by COBALT DICKENS
ulll.cf	Domain name	Hosting phishing website used by COBALT DICKENS
nlll.cf	Domain name	Hosting phishing website used by COBALT DICKENS
clll.nl	Domain name	Hosting phishing website used by COBALT DICKENS
llii.cf	Domain name	Hosting phishing website used by COBALT DICKENS
etll.cf	Domain name	Hosting phishing website used by COBALT DICKENS
1edu.in	Domain name	Hosting phishing website used by COBALT DICKENS
aill.cf	Domain name	Hosting phishing website used by COBALT DICKENS
atna.cf	Domain name	Hosting phishing website used by COBALT DICKENS
atti.cf	Domain name	Hosting phishing website used by COBALT DICKENS

aztt.tk	Domain name	Hosting phishing website used by COBALT DICKENS
cave.gq	Domain name	Hosting phishing website used by COBALT DICKENS
ccli.cf	Domain name	Hosting phishing website used by COBALT DICKENS
cnma.cf	Domain name	Hosting phishing website used by COBALT DICKENS
cntt.cf	Domain name	Hosting phishing website used by COBALT DICKENS
crll.tk	Domain name	Hosting phishing website used by COBALT DICKENS
csll.cf	Domain name	Hosting phishing website used by COBALT DICKENS
ctll.tk	Domain name	Hosting phishing website used by COBALT DICKENS
cvnc.ga	Domain name	Hosting phishing website used by COBALT DICKENS
cvve.cf	Domain name	Hosting phishing website used by COBALT DICKENS
czll.tk	Domain name	Hosting phishing website used by COBALT DICKENS
cztt.tk	Domain name	Hosting phishing website used by COBALT DICKENS
euca.cf	Domain name	Hosting phishing website used by COBALT DICKENS
euce.in	Domain name	Hosting phishing website used by COBALT DICKENS
ezll.tk	Domain name	Hosting phishing website used by COBALT DICKENS
ezplog.in	Domain name	Hosting phishing website used by COBALT DICKENS
ezproxy.tk	Domain name	Hosting phishing website used by COBALT DICKENS

eztt.tk	Domain name	Hosting phishing website used by COBALT DICKENS
flll.cf	Domain name	Hosting phishing website used by COBALT DICKENS
iell.tk	Domain name	Hosting phishing website used by COBALT DICKENS
iull.tk	Domain name	Hosting phishing website used by COBALT DICKENS
izll.tk	Domain name	Hosting phishing website used by COBALT DICKENS
lett.cf	Domain name	Hosting phishing website used by COBALT DICKENS
lib1.bid	Domain name	Hosting phishing website used by COBALT DICKENS
lib1.pw	Domain name	Hosting phishing website used by COBALT DICKENS
libb.ga	Domain name	Hosting phishing website used by COBALT DICKENS
libe.ml	Domain name	Hosting phishing website used by COBALT DICKENS
libg.cf	Domain name	Hosting phishing website used by COBALT DICKENS
libg.ga	Domain name	Hosting phishing website used by COBALT DICKENS
libg.gq	Domain name	Hosting phishing website used by COBALT DICKENS
libloan.xyz	Domain name	Hosting phishing website used by COBALT DICKENS
libnicinfo.xyz	Domain name	Hosting phishing website used by COBALT DICKENS
libraryme.ir	Domain name	Hosting phishing website used by COBALT DICKENS
libt.ml	Domain name	Hosting phishing website used by COBALT DICKENS

libu.gq	Domain name	Hosting phishing website used by COBALT DICKENS
lill.gq	Domain name	Hosting phishing website used by COBALT DICKENS
llbt.tk	Domain name	Hosting phishing website used by COBALT DICKENS
llib.ga	Domain name	Hosting phishing website used by COBALT DICKENS
llic.cf	Domain name	Hosting phishing website used by COBALT DICKENS
llic.tk	Domain name	Hosting phishing website used by COBALT DICKENS
llil.cf	Domain name	Hosting phishing website used by COBALT DICKENS
llit.cf	Domain name	Hosting phishing website used by COBALT DICKENS
lliv.tk	Domain name	Hosting phishing website used by COBALT DICKENS
llse.cf	Domain name	Hosting phishing website used by COBALT DICKENS
ncll.tk	Domain name	Hosting phishing website used by COBALT DICKENS
ncnc.cf	Domain name	Hosting phishing website used by COBALT DICKENS
nctt.tk	Domain name	Hosting phishing website used by COBALT DICKENS
necr.ga	Domain name	Hosting phishing website used by COBALT DICKENS
nika.ga	Domain name	Hosting phishing website used by COBALT DICKENS
nsae.ml	Domain name	Hosting phishing website used by COBALT DICKENS
nuec.ml	Domain name	Hosting phishing website used by COBALT DICKENS

rill.cf	Domain name	Hosting phishing website used by COBALT DICKENS
rnva.cf	Domain name	Hosting phishing website used by COBALT DICKENS
rtll.tk	Domain name	Hosting phishing website used by COBALT DICKENS
sctt.cf	Domain name	Hosting phishing website used by COBALT DICKENS
shibboleth.link	Domain name	Hosting phishing website used by COBALT DICKENS
sitl.tk	Domain name	Hosting phishing website used by COBALT DICKENS
slli.cf	Domain name	Hosting phishing website used by COBALT DICKENS
till.cf	Domain name	Hosting phishing website used by COBALT DICKENS
titt.cf	Domain name	Hosting phishing website used by COBALT DICKENS
uill.cf	Domain name	Hosting phishing website used by COBALT DICKENS
uitt.tk	Domain name	Hosting phishing website used by COBALT DICKENS
ulibe.ml	Domain name	Hosting phishing website used by COBALT DICKENS
ulibr.ga	Domain name	Hosting phishing website used by COBALT DICKENS
umlib.ml	Domain name	Hosting phishing website used by COBALT DICKENS
umll.tk	Domain name	Hosting phishing website used by COBALT DICKENS
uni-lb.com	Domain name	Hosting phishing website used by COBALT DICKENS
unll.tk	Domain name	Hosting phishing website used by COBALT DICKENS

utll.tk	Domain name	Hosting phishing website used by COBALT DICKENS
vsre.cf	Domain name	Hosting phishing website used by COBALT DICKENS
web2lib.info	Domain name	Hosting phishing website used by COBALT DICKENS
xill.tk	Domain name	Hosting phishing website used by COBALT DICKENS
zedviros.ir	Domain name	Hosting phishing website used by COBALT DICKENS
zill.cf	Domain name	Hosting phishing website used by COBALT DICKENS

Table 1. Indicators associated with COBALT DICKENS operations.