CERT-UA

Оновлено: 19.06.2023. Скориговано атрибуцію: UAC-0036 -> UAC-0102

Загальна інформація

Від учасника інформаційного обміну отримано електронний лист з темою "Помічена підозріла активність @UKR.NET" та додатком у вигляді PDF-файлу "Попередження про безпеку.pdf" надісланий, начебто, від імені технічної підтримки UKR.NET (електронна адреса відправника: "account.support.0@ukr.net").

Згаданий PDF-документ містить посилання на шахрайський вебресурс, що імітує вебсторінку поштового сервісу.

У випадку автентифікації на підробному вебсайті, логін та пароль користувача будуть надіслані зловмисникам, що створить передумови для отримання несанкціонованого доступу до електронної поштової скриньки користувача третіми особами.

CERT-UA вжито додаткових заходів з аналізу мережевої інфраструктури, що застосовується для здійснення аналогічних кібератак з 2021 року, в результаті чого виявлено, щонайменше, 118 пов'язаних доменних імен, що зареєстровані компанією "Internet Domain Service BS Corp." (@internet.bs, Багамські острови). Відповідні сервери, за даними Domaintools, розміщено в Нідерландах на технічному майданчику "Nice-IT" aka "@as49447.net" (номер автономної системи: 49447).

Описана активність відстежується за ідентифікатором UAC-0102.

Задля мінімізації вірогідності реалізації кіберзагроз у відношенні громадян України, ідентифіковані доменні імена додано до DNS RPZ зони, яка обслуговується CERT-UA, а також передано фахівцям CSIRT-NBU з метою внесення до DNS RPZ зони "шахрайство".

Закликаємо користувачів UKR.NET скористатися штатним функціоналом поштового сервісу та невідкладно вжити заходів з налаштування багатофакторної автентифікації.

Рекомендовано, починаючи з 01.01.2023, перевірити факти мережевої взаємодії з доменними іменами та IP-адресами, зазначеними в розділі "Індикатори кіберзагроз", принагідно звернувши увагу на наявність несанкціоновано налаштованих фільтрів пошти та сторонніх пристроїв/додатків, яким надо доступ до поштової скриньки.

Індикатори кіберзагроз

Мережеві:

```
hXXp://accounts.cm1-ukr[.]net/desktop/security/login/
hXXp://accounts.regs-ukr[.]net/desktop/security/login/
```

```
45[.]9.148.178  NL  @as49447.net
45[.]9.148.83   NL  @as49447.net
se-ukr[.]net    2023-05-28
sb-ukr[.]net    2023-05-28
regs-ukr[.]net  2023-05-28
om-ukr[.]net    2023-05-28
mst-ukr[.]net   2023-05-28
f3-ukr[.]net    2023-05-28
dat1-ukr[.]net  2023-05-28
8-ukr[.]net 2023-05-28
5-ukr[.]net 2023-05-28
4e-ukr[.]net    2023-05-28
v-ukr[.]net 2023-05-13
verify-ukr[.]net    2023-05-13
v1-ukr[.]net    2023-05-13
tc-ukr[.]net    2023-05-13
signup-ukr[.]net    2023-05-13
score-ukr[.]net 2023-05-13
p3-ukr[.]net    2023-05-13
k-ukr[.]net 2023-05-13
k1-ukr[.]net    2023-05-13
details-ukr[.]net   2023-05-13
cm1-ukr[.]net   2023-05-13
1-ukr[.]net 2023-05-13
0-ukr[.]net 2023-05-13
uf1-ukr[.]net   2023-05-04
mx3-ukr[.]net   2023-05-04
lvc-ukr[.]net   2023-05-04
bnt-ukr[.]net   2023-05-04
private-ukr[.]net   2023-04-29
msx-ukr[.]net   2023-04-29
edisk-ukr[.]net 2023-04-29
cck-ukr[.]net   2023-04-29
news-ukr[.]net  2023-03-23
password-ukr[.]net  2023-03-17
accounts-s-ukr[.]net    2023-02-24
kt-ukr[.]net    2023-02-23
a3-ukr[.]net    2023-02-19
uo-ukr[.]net    2023-02-18
bh-ukr[.]net    2023-02-18
lv-ukr[.]net    2023-02-14
kg-ukr[.]net    2023-02-06
dx-ukr[.]net    2023-02-06
kb-ukr[.]net    2023-02-04
tt-ukr[.]net    2023-02-03
o1-ukr[.]net    2023-02-02
hj-ukr[.]net    2023-02-02
```

```
uq-ukr[.]net    2023-01-30
serv1-ukr[.]net 2023-01-30
rew-ukr[.]net   2023-01-30
vv-ukr[.]net    2023-01-08
lc-ukr[.]net    2023-01-08
td-ukr[.]net    2023-01-04
mf-ukr[.]net    2023-01-04
reg-ukr[.]net   2022-12-30
el-ukr[.]net    2022-12-30
acc-ukr[.]net   2022-12-30
login-ukr[.]net 2022-12-10
confirm-ukr[.]net   2022-11-25
accounts-ukr[.]net  2022-10-16
support-ukr[.]net   2021-04-29
numsecukr[.]net 2019-04-11
(inactive)
crv-ukr[.]net   2023-05-04
bld-ukr[.]net   2023-05-04
virtual-ukr[.]net   2023-04-29
settingsukr[.]net   2023-04-29
session-ukr[.]net   2023-04-29
mxukr[.]net 2023-04-29
dubl-ukr[.]net  2023-04-29
cmx-ukr[.]net   2023-04-29
static-ukr[.]net    2023-04-08
stage-ukr[.]net 2023-04-08
safe-ukr[.]net  2023-04-08
s9-ukr[.]net    2023-04-08
reply-ukr[.]net 2023-04-08
prot-ukr[.]net  2023-04-08
pm-kv-ukr[.]net 2023-04-08
mta-ukr[.]net   2023-04-08
mod-ukr[.]net   2023-04-08
ksr1-ukr[.]net  2023-04-08
files-ukr[.]net 2023-04-08
client-ukr[.]net    2023-04-08
clients-ukr[.]net   2023-04-08
web-ukr[.]net   2023-04-02
step-ukr[.]net  2023-04-02
site-ukr[.]net  2023-04-02
settings-ukr[.]net  2023-04-02
pgh-ukr[.]net   2023-04-02
pas-ukr[.]net   2023-04-02
int-ukr[.]net   2023-04-02
inbox-ukr[.]net 2023-04-02
cca-ukr[.]net   2023-04-02
btx-ukr[.]net   2023-04-02
```

```
2fa-ukr[.]net    2023-04-02
vh-ukr[.]net     2023-03-24
out-ukr[.]net    2023-03-24
in-ukr[.]net     2023-03-24
cvi-ukr[.]net    2023-03-24
stv-ukr[.]net    2023-03-20
pge-ukr[.]net    2023-03-20
accounts---ukr[.]net     2023-03-20
changepassword-ukr[.]net     2023-03-17
accounts--ukr[.]net 2023-03-17
uc-ukr[.]net     2023-01-25
ub-ukr[.]net     2023-01-25
ck-ukr[.]net     2023-01-25
kv-ukr[.]net     2023-01-19
k1v-ukr[.]net    2023-01-19
vn-ukr[.]net     2023-01-13
ser-ukr[.]net    2023-01-13
p-ukr[.]net 2023-01-13
lt-ukr[.]net     2023-01-13
ml-ukr[.]net     2022-12-28
m1-ukr[.]net     2022-12-23
u1-ukr[.]net     2022-12-15
l-ukr[.]net 2022-12-15
mail-ukr[.]net   2022-12-13
conf-ukr[.]net   2022-12-13
account-ukr[.]net    2022-01-10
notify-ukr[.]net     2021-03-17
```

Графічні зображення

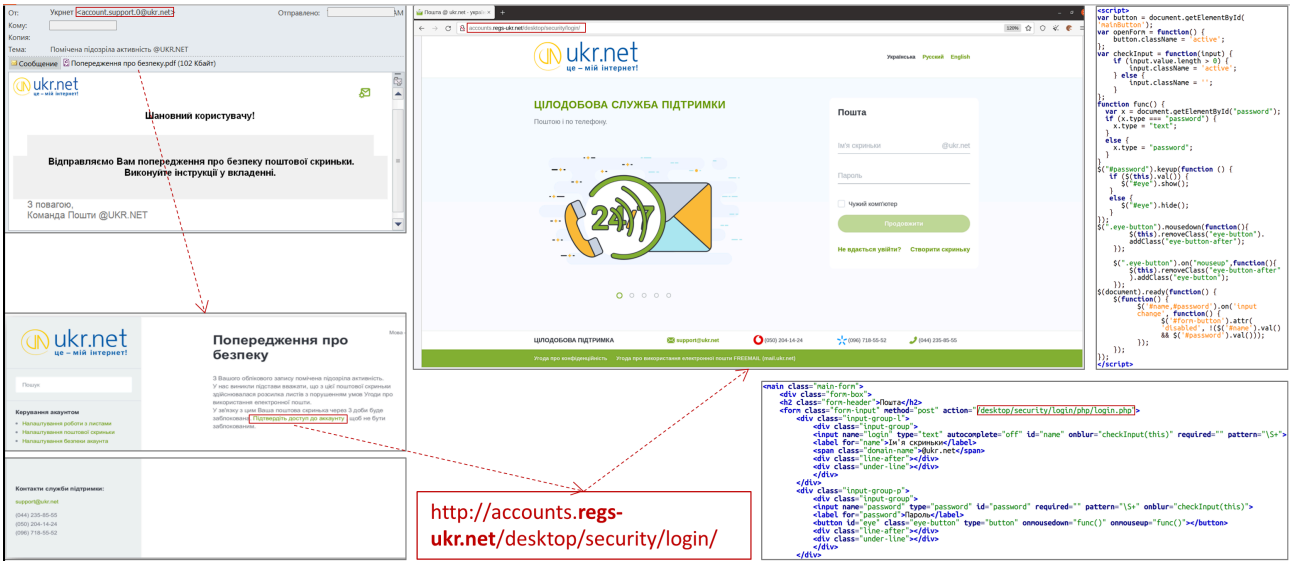

Рис. 1 Приклад фішингового листа та шахрайської вебсторінки

Source: https://cert.gov.ua/article/4928679