ALVEREAD
TECHNOLOGY FOCUS

Az OSINT lehetőségei a fake news és scam tartalmak vizsgálatában II. rész

„*Operation Alice*" – a kripto-fraud hálózat felderítése

SECURITY TESTING LABORATORY
MAKING THE WORLD SAFER

Tartalom

Bevezető

A tanulmány első része a Csányi Sándor, Soros György, Mészáros Lőrinc, illetve Karácsony Gergely nevével is visszaélő, csaló kriptovaluta kereskedési rendszer, a Bitcoin Loophole nemzetközi és hazai vonatkozású kampányát vette górcső alá.

A Bitcoin Loophole egy, a Bitcoin kereskedelmére épülő átverés/csalás (*scam*), amely 2018-ban vált ismertebbé, és amelyre már több fraud-monitoring és csalás elleni szervezet is felhívta a figyelmet. A Bitcoin Loophole magát irreálisan magas hozamokat ígérő, mesterséges intelligenciával támogatott kereskedési rendszernek állítja be, a valóságban azonban arra szolgál, hogy a befektetők pénzét kicsalja.

A vizsgált kampány 2020. augusztus 10-én vált, ismertté, amikor több hazai médium is felhívta a figyelmet, hogy egy, a 24.hu internetes újság arculatával megjelenő oldal Csányi Sándor nevével visszaélve próbálja meg kicsalni az extra nyereségre vágyók pénzét. A korábbi elemzés bemutatta, miként épül fel a Bitcoin Loophole köré épült hálózat és hogyan navigálja a látogatókat többszöri átirányításon keresztül a kampány landing oldalára.

A Facebook reklámokkal támogatott Bitcoin Loophole kampányok működése

A tanulmányban megjegyzésre került, hogy a *bitcoinloophole.bestoffers.com* központi oldal vizsgálatakor olyan információk kerültek felszínre, amelyek messzebbre vezetnek, és egy következő anyagban kerülnek az adatok bemutatásra.

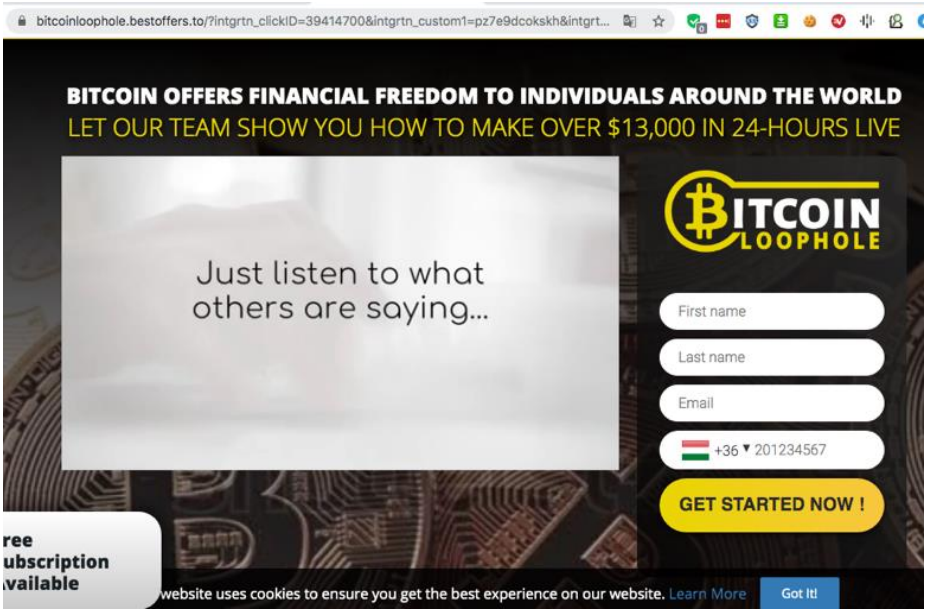
Jelen tanulmány célja tehát bemutatni a *bitcoinloophole.bestoffers.com* központi oldalhoz kapcsolódó összetett, többszáz oldalból álló, partnerprogram (*affiliate*) rendszerben működő kripto-fraud vagy kripto-scam hálózatot.

A hálózat felderítése

A korábban bemutatott Bitcoin Loophole kampány csak egy, a különféle kriptovalutás csalások közül. Akár sokszáz vagy többezer hasonló, a kriptovaluták népszerűségét kihasználó csalás létezhet, amelyek felderítéséhez rengeteg erőforrásra lenne szükség.

A csalók láthatóan fejlett, jól működő rendszereket használnak, amelyek összehangoltan és automatizáltan működnek. Feltételezhető, hogy egy (vagy több) partnerprogram-jellegű hálózat áll a Bitcoin Loophole (és a hasonló kampányok) mögött, ahol a „partnerprogram" résztvevői a működtető infrastruktúráját (sablonok, templatek, átirányítók és központi oldal) használják. A partnereknek csak az álhírtartalmak gyártása (amelyhez a sablonrendszer rendelkezésre áll), illetve a reklámok kihelyezése a feladatuk, amelyért cserébe részesülnek például a *bitcoinloophole.bestoffers.to* oldalra vezetett látogatóktól kicsalt összegekből.

A *bitcoinloophole.bestoffers.to* oldalon begyűjtött személyes adatokkal kapcsolatban feltételezhető, hogy azokat további csalási kísérletekhez használják fel. Az ilyen jellegű információk meglehetősen értékesek, főleg akkor, ha láthatóan egy „fogékony" áldozat adatairól van szó. Ugyanis, ha egyszer becsapható volt az óvatlan vagy kevésbé biztonságtudatos alany, akkor a későbbiekben is jó lehetőséget láthatnak benne a csalásra szakosodott bűnözők. Mert bár a károsultak valószínűleg nem fognak többé kriptovalutába vagy kereskedési platformokba fektetni, más csalásra még nyitottak lehetnek, illetve a begyűjtött adatok további csalásokhoz is felhasználhatók..



bitcoinloophole.bestoffers.com – az adatgyűjtő és regisztrációs oldal

A központi oldal vizsgálata

Mivel a korábbi vizsgálatok rávilágítottak arra, hogy a *bitcoinloophole.bestoffers.to* oldal a kampány központi, elszámolásért és adatgyűjtésért felelős rendszere, ezért ellenőrzésre került a weblap forráskódja.

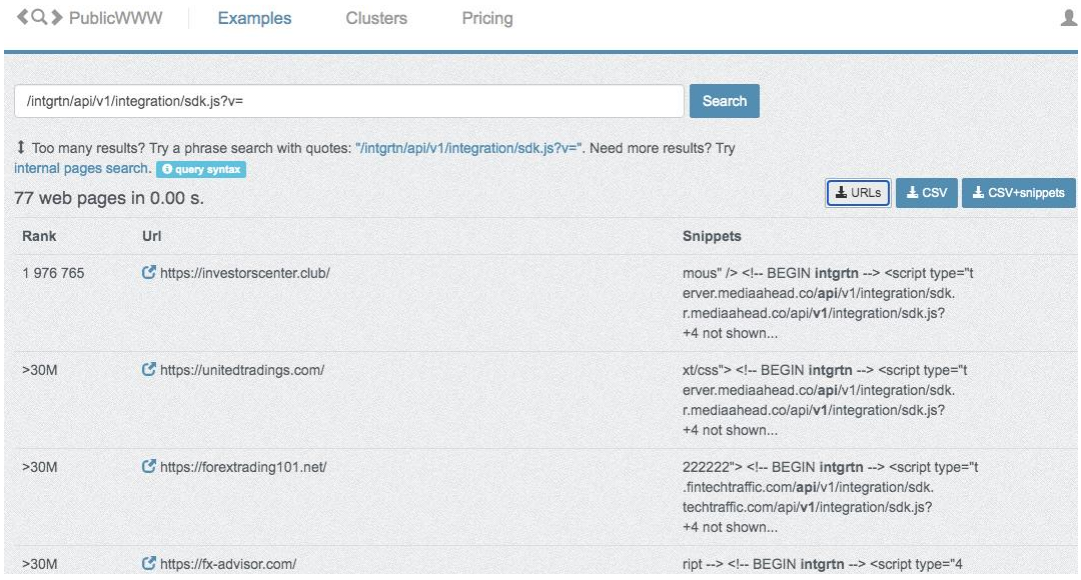
A forráskódban megtalálható volt egy script elem hivatkozás, amely alapján feltételezhető, hogy egy API rendszer működik a felület mögött, amely valamilyen automatizált funkciókat biztosít a rendszer számára.


```
<script>
    window.intgrtnInit = function () {
        var path = "/";
        if (window.location.pathname.split("/")[1] && window.location.pathname.split("/") > 2
            path = "/" + window.location.pathname.split("/")[1] + "/";
        }
        window.intgrtn.setOptions({
            server: {
                endpoint: "/intgrtn",
                ignoreProjectEndpoint: true
            },
            cookies: {
                path: path
            },
                    });
            };

    (function (d) {
        if (window.intgrtn) {
            return;
        }
        var s = d.createElement("script");
        var date = new Date();
        s.src = "/intgrtn/api/v1/integration/sdk.js?v=" + date.getFullYear().toString() + dat
date.getHours().toString() + Math.round(date.getMinutes() / 10).toString();
        d.getElementsByTagName("head")[0].appendChild(s);
    }(document));
</script>
```

„/intgrtn/api/v1/integration/sdk.js?v=" – feltételezett API működés az oldal mögött

A *PublicWWW* kódkereső alkalmazás arra is választ adott, hogy más weblapok is használják-e ezt a kódrészletet. A kódkereső legalább 77 olyan további oldalt azonosított, amelyben ugyanez a kódrészlet szerepel, tehát ezek az oldalak ugyanazt a scriptet (és API interfészt) használják a működésükhöz.

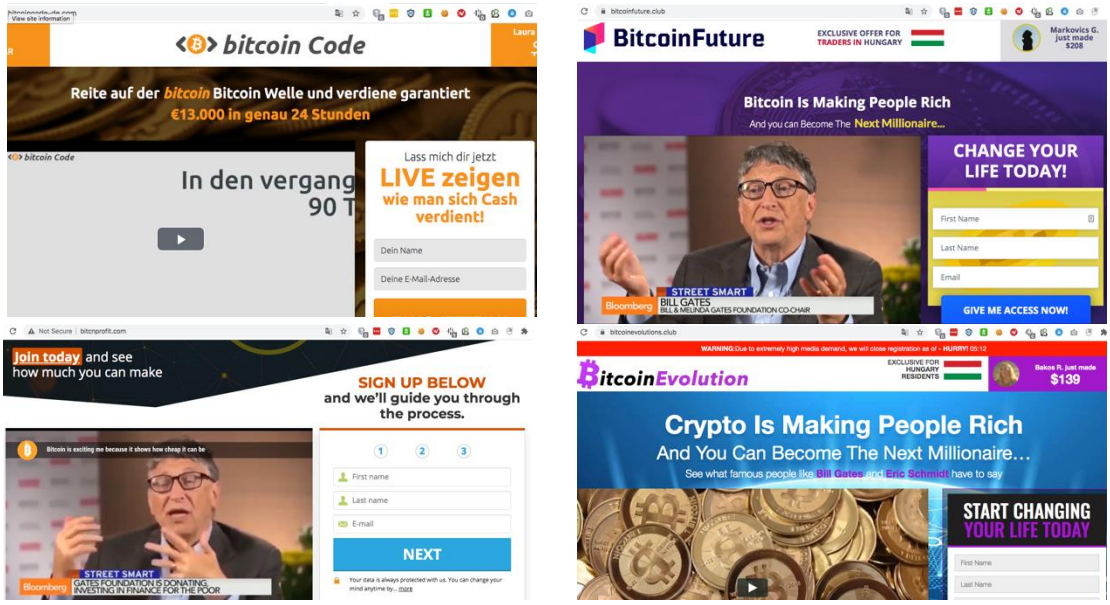


PublicWWW kódkereső találatai, 77 oldal használja ugyanezt a kódot

URL	URL
https://investorscenter.club/	https://unitedtradings.com/
https://forextrading101.net/	https://fx-advisor.com/
https://fx-advisors.com/	http://secretinvestorsociety.com/
http://guardianangelapp.net/	https://adformula.co/
https://crowdprofits.net/	http://thebtcode.com/
https://ethcodes.com/	https://thebitcoinscodes.com/lp3.php
https://infinityappclub.com/	http://fxrevengezone.com/
https://qprofitsystm.com/	https://greentreeprofits.com/
http://srstrendrider.net/	https://fxdelta.net/
https://bestbitcoinsystem.com/	https://bitcoingroup.club/
https://ice9.club/	https://1kdailyprofits.co/
https://bitcoincode-de.com/	https://bitcoinfuture.club/
https://bitcoincode-it.com/	https://bitcoincode-es.com/
https://algotradesignals.net/	http://ozziforexreviews.com/
https://tradecannabisstock.com/	https://cryptogeniusexpert.com/
https://thewealthmatrixpro.com/	https://iproinvestor.org/
https://bitcoin-blueprint.org/	https://adflippers365.com/
https://easytradeapp.co/	https://teslerapp2.net/
https://immediateedge.club/	https://bannerbanc.com/
https://btcodeclub.com/	https://www.bitcoinrevolutionofficial.com/
http://mrclinic.net/	https://pattern-trader.club/
http://bestcoinapp.com/	https://thecryptogps.club/
https://tesler2app.club/	https://1gprofit.club/
https://thecryptotraders.club/	https://fxrobotixapp.com/
http://hairisk.com/	http://getyourhaironline.com/
http://freeteethquote.com/	http://b4nhair.com/
https://cryptoengine.club/	http://topfinanzberater.com/
https://cryptocashfortunes.club/	https://immediateedgeapps.club/
https://qprofitsystem.club/	http://bitcoincashgrab.net/
https://xsystemtrading.com/	http://bitcnprofit.com/
http://thecallowaycryptosystem.com/	https://copygeorgesoros.com/
https://bitcoinholom.club/	https://wealthmatrixpro.club/
https://cryptoboomofficial.com/	https://bitcoinevolutions.club/
https://cryptohoppers.club/	https://bitc-billionaire.com/bitcoinbillionaire/de/
https://bitc-profit.com/bitcoin-profit/	https://bitcoinrejoin.club/
https://bitcoinmillionairepros.club/	https://bankingonblockchain.club/
https://www.24traderprofx.news/	https://btcprofitclub.app/
https://bitcodes.club/	https://immediateedgesapp.club/
https://bitcoinsunriseapp.com/	

A kódrészlet alapján azonosított 77 weboldal listája

Az oldalak jellemzően kereskedéssel, illetve kriptovalutákkal kapcsolatosak és megtalálhatók közöttük a korábbi tanulmányból megismert, és a Bitcoin Loophole-hoz hasonló Bitcoin Code, EtherCode, Bitcoin Systems, Bitcoin Evolution kripto-fraud vagy kripto-scam alkalmazások is.

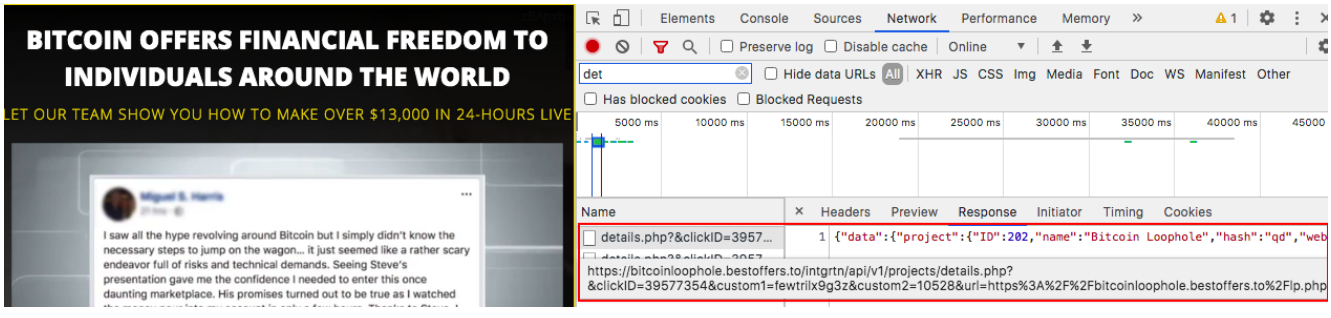


Bitcoin Code, Bitcoin Future, Bitcoin Profit, Bitcoin Evolution weboldalak

A weblapok között egyéb kriptovaluta „kereskedési" rendszerek is megtalálhatók. Mindben közös, hogy a Bitcoin Loophole-hoz hasonlóan kirívóan magas hozamokat ígérnek, amelyet mesterséges intelligenciával támogatott, automata kereskedési rendszer fog biztosítani a befektető számára.

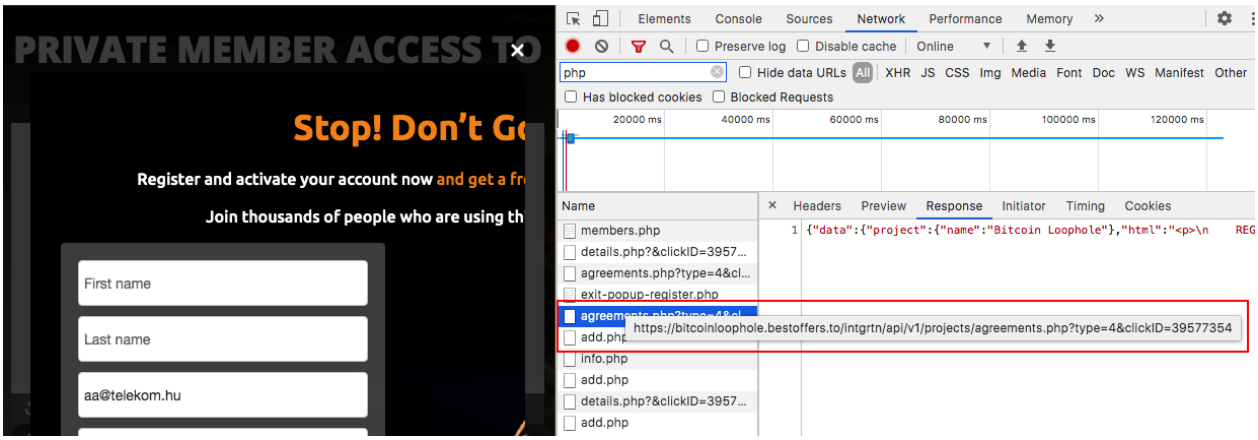
Az API interfész vizsgálata

A *bitcoinloophole.bestoffers.to* oldal működésének vizsgálata során a hálózati forgalom ellenőrzése megerősítette, hogy betöltődéskor valóban egy API kommunikáció történik. Az oldal adatokat kér a szerveren tárolt, az „*intgrtn/api/v1/projects/details.php*" címen elérhető API interfésztől.



„intgrtn/api/v1/projects/details.php" – API hívás URL paraméterekkel

Látható, hogy az API híváshoz több URL paraméter is átadásra kerül, illetve, hogy a tartalom betöltődésekor további API kommunikáció is történik.



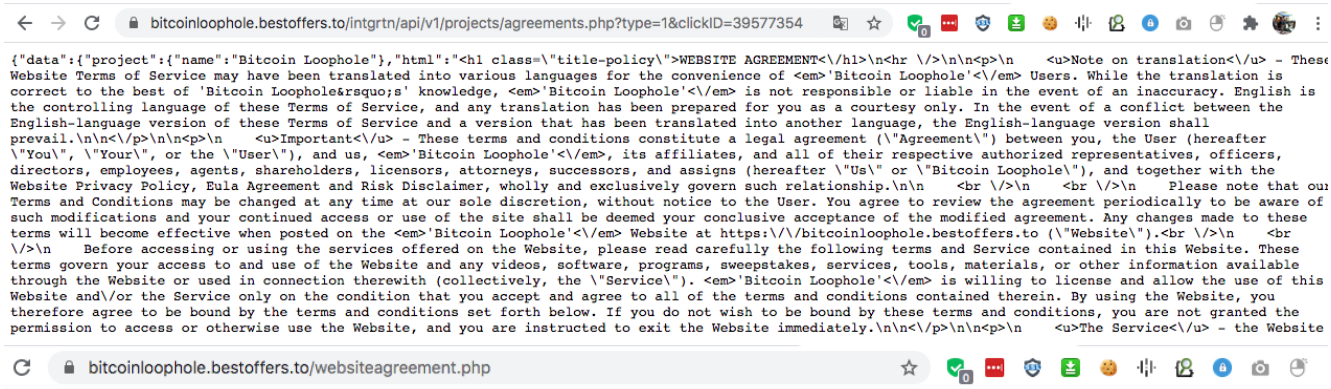
„intgrtn/api/v1/projects/agreements.php?type=4&clickID=39577354" kommunikáció

Az API hívásokat ellenőrizve megállapítható volt, hogy az oldal betöltődésekor olyan tartalmakat jelenít meg, amelyeket az API interfész válaszai töltenek be az oldalba.

https://bitcoinloophole.bestoffers.to/intgrtn/api/v1/projects/agreements.php?type=4&clickID=39577354 API hívás

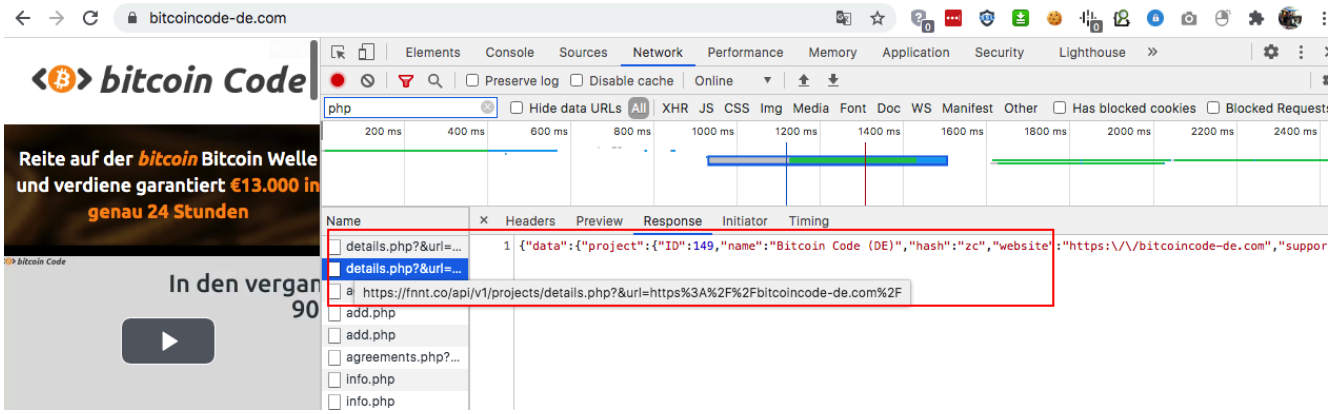
agreements.php?type=4&clickID=39577354 API hívás válaszának megjelenése az oldalon

A „*type=*" változó azonosítja, hogy éppen mely *agreement* tartalmat kell megjeleníteni. Például a 4-es azonosító a RISK DISCLAIMER tartalmat jeleni meg, a *type=1* paraméter a WEBSITE AGREEMENT tartalmát tölti be.

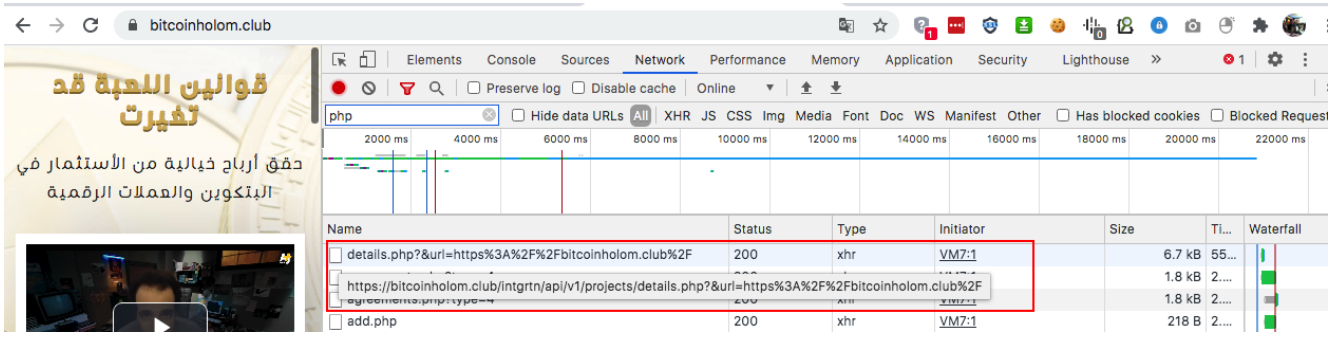


Az API hívás type=1 paraméterrel a WEBSITE AGREEMENT tartalmat tölti be az oldalba

A PublicWWW kódkereső segítségével korábban azonosított 77 weboldalt megvizsgálva nyilvánvalóvá vált, hogy mindegyikük ugyanezt az API interfészt használja. Egyes oldalak esetében az API interfész a vizsgált oldalon volt elérhető, más esetekben egy másik szerverről került meghívásra. Ez feltételezi, hogy a helyi API interfész is csatlakozhat egy központi adatbázishoz, mivel mindegyik API interfész mögött ugyanazok az adatok voltak megtalálhatók. (A külső API interfészek más-más címen és IP-vel voltak elérhetők).

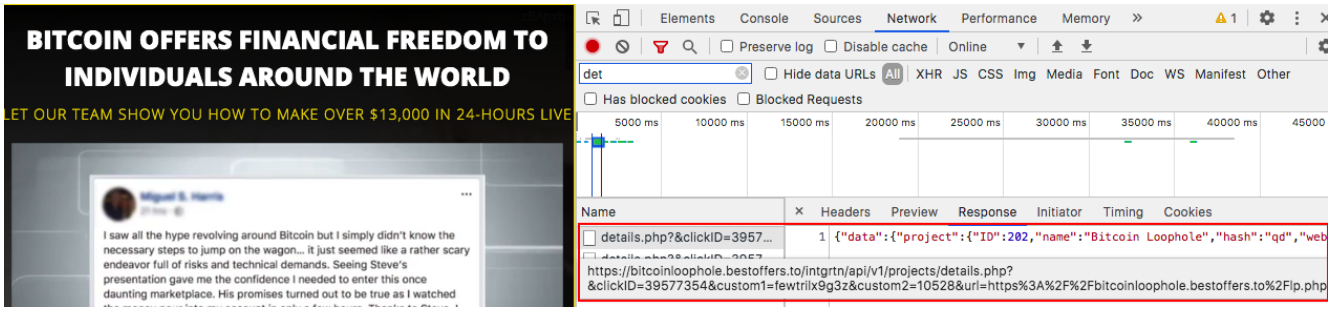


A BitcoinCode esetében az API egy másik szerverről kerül meghívásra

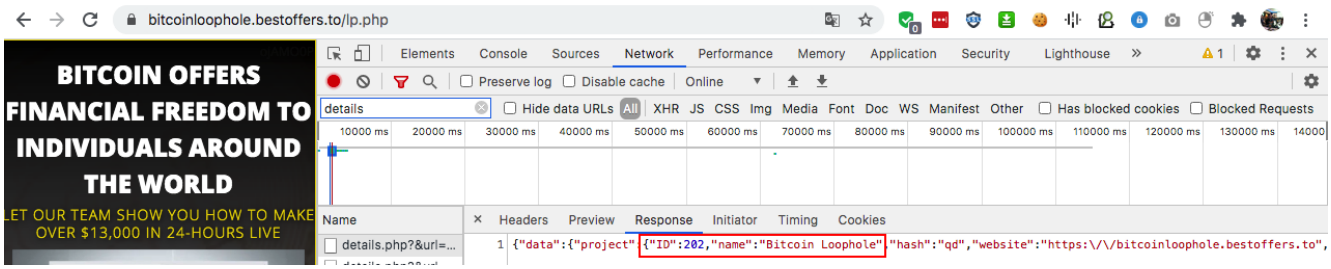


A Bitcoinholom esetében az API ugyanazon a szerveren található

A *bitcoinloophole.bestoffers.to* oldalon található API interfész *details.php* állományának meghívását vizsgálva láthatóvá vált, hogy arra olyan JSON válasz érkezik, amelyben megtalálható az oldal azonosítója (*project ID*), a projekt vagy oldal neve, webcíme, illetve egyéb tartalmi elemei és azonosítói.



„intgrtn/api/v1/projects/details.php?clickID=39577354" – API hívás URL paraméterekkel



A project ID 202 a Bitcoin Loophole azonosítója

Mivel a project ID 202 a Bitcoin Loophole-t azonosítja, feltételezhető volt, hogy több projektet, azaz több, hasonló tartalmat is kiszolgál az API. A clickID paraméter értékeinek változtatásával ez bizonyítást nyert: attól függően, hogy milyen érték került a *clickID* változó után megadásra, más-más hasonló, kripto-fraud oldalakat lehetett a lekérdezéssel azonosítani.

A clickID értékének változtatásával többszáz hasonló kripto-fraud oldal volt azonosítható

Mivel az API erre lehetőséget biztosított, ezért egy automatikus eszközzel a *clickID* értékét 300001 és 42 millió között léptetve lehetőség volt letölteni az API interfészből azokat a projekteket és oldalakat, amelyek ezt az API-t használják[1].

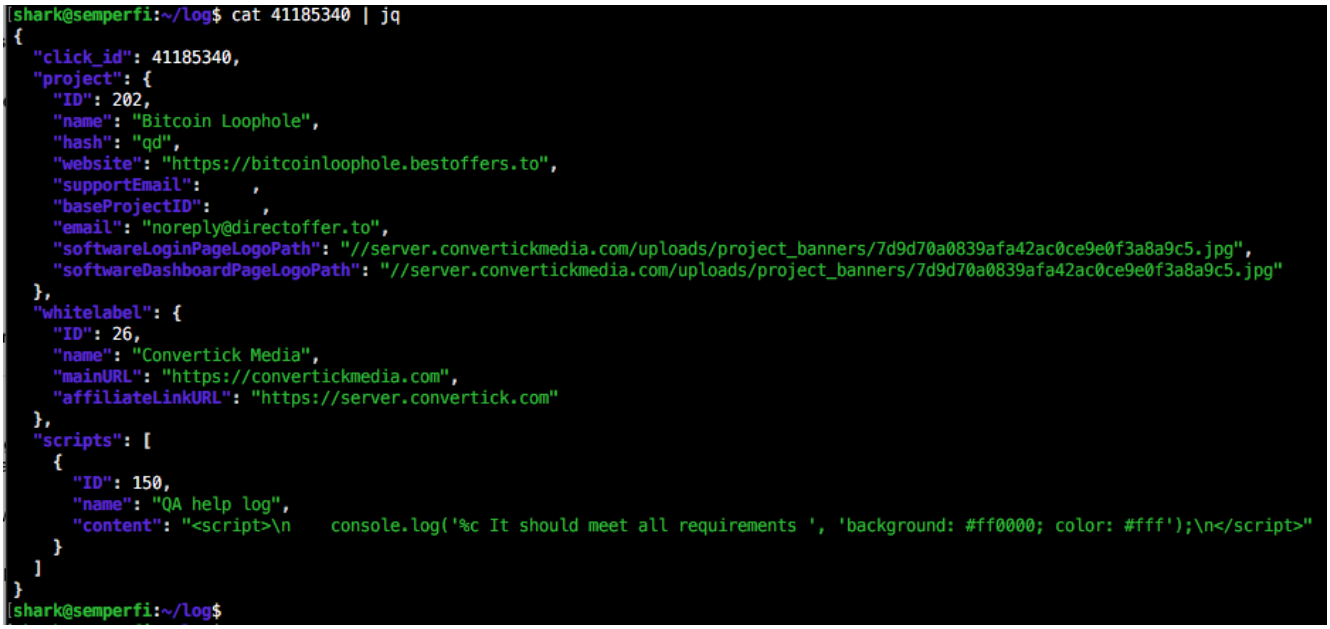
A vizsgálathoz egy olyan szerver és alkalmazás lett felépítve, amely 10 publikus IP címmel rendelkezett, illetve minden egyes HTTP/HTTPS kérést másik IP címen keresztül küldött ki. Ezzel sikerült elkerülni a *rate limit* túllépést és elérni, hogy a szerver vagy az API ne blokkolja az egy IP címről érkező konkurens kapcsolatokat.

A vizsgálathoz csaknem 42 millió API hívást kellett volna elküldeni, amely még a 10 IP cím esetében is kitiltással járhatott volna (nem beszélve az idő és erőforrás felhasználásról, vagy túlterhelésről), ezért előbb manuális vizsgálatnak lettek alávetve a clickID értékek. A kézi ellenőrzés feltárta, hogy egy-egy projekthez akár többszáz clickID is tartozhat, azaz ugyanaz a projektadat jelenik meg többszáz clickID esetében is. Meghatározásra került, hogy releváns tartalom csak clickID=300001-től jelenik meg, illetve, hogy elegendő lehet 100-as lépésekkel növelni az alkalmazásban a clickID értékét. (Így belátható időn belül végig szkennelhető volt az API, bár a 100-as ugrásokkal elképzelhető, hogy egyes projektek kimaradtak).

A kézi módszer arra is rávilágított, hogy kb. clickID=42000000 értékig szerepel releváns tartalom az API adatbázisában. (Ez a vizsgálat idején csak részlegesen volt igaz, naponta ellenőrzésre került, hogy meddig érhető el az API-n keresztül releváns tartalom, és minden nap többezer clickID-vel bővült a mögöttes adatbázis).

Az automatikus eszköz legyűjtötte az API hívások válaszait, de nem minden mező került azonban elmentésre, mivel túl sok helyre lett volna szükség az adatok tárolásához. A fontosabb és mentendő mezők kiválasztása a kézi vizsgálatok alapján történt meg, és csak olyan API válasz került elmentésre, melyben szerepelt releváns adat és olyan Project ID érték, amely még nem került tárolásra.

[1] *Az üzemeltetők - alighanem a vizsgálat adatforgalmát észlelve - később letiltották ezt a lehetőséget.*



ClickID: 41185340, Projekt ID: 202 - Bitcoin Loophole és a fontosabb adatmezők

ClickID:41090960, Project ID:928 – Bitcoin Evolution és a fontosabb adatmezők

A feltételezés az volt, hogy ha 300001-től léptetésre kerül a ClickID értéke, akkor a visszakapott válaszokból az automatikus eszköz segítségével a teljes hálózat (amely ezt az API-t, illetve mögöttes adatbázis használja) feltérképezhetővé válik és minden olyan oldal azonosítható lesz, amely ennek a részét képezi.A felderítés eredménye egy olyan adatbázis lett, amely tartalmazza a hálózathoz tartozó összes oldal nevét, URL címét, banner kiszolgáló szerverét, Google és egyéb tracking kódját.

Az adatok feldolgozásával megállapítást nyert, hogy a vizsgálat idején az egyedi Project ID alapján több mint 600 oldal kapcsolódott az API-n keresztül a hálózathoz.

Bitcoin Billionaire ES	https://lp.themarketsinsider.com/cm/futurewealth/
Bitcoin Blueprint	https://bitcoin-blueprint.greatoffers.to
	https://bitcoin-blueprint.org
	https://bitcoinblueprint.club
	https://bitcoinblueprints.net
	https://safeoffer.co/bitcoinblueprint
	https://specialvipoffer.com/bitcoinblueprint
Bitcoin Boom	https://get-profits-now.com/bitcoinboom
Bitcoin Booster	https://get-profits-now.com/bitcoinbooster
Bitcoin Cash Grab	https://bitcoincashgrab.co
	https://bitcoincashgrab.com
Bitcoin Circuit	https://chiefoffers.net/bitcoincircuit/
	https://ecryptodaily.co/bitcoincircuit
	https://get-profits-now.com/bitcoin-circuit/
	https://lp.themarketsinsider.com/fx6/bitcoin-circuit/
Bitcoin Code	https://asuccesshub.com/bitcoincode
	https://bitcoin-code.greatoffers.to
	https://bitcoincodeworld.com
	https://btc-code.bestoffers.to
	https://chiefoffers.net/bitcoincode
	https://get-profits-now.com/bitcoincode
	https://realvipdeal.com/bitcoincode
	https://specialinvite.co/bitcoincode
	https://specialvipoffer.com/bitcoincode
	https://thebitcoinscodes.com
	https://vipoffer.net/bitcoincode
Bitcoin Code (DE)	https://bitcoincode-de.com
Bitcoin Code (ES)	https://bitcoincode-es.com
Bitcoin Code (IT)	https://bitcoincode-it.com
Bitcoin Code 2	https://btccode.greatoffers.to
Bitcoin Code ES	https://lp.themarketsinsider.com/cm/bitcoin-code/
Bitcoin Code FR	https://bitcoin-code-fr.bestoffers.to
Bitcoin Code RU	https://bitcoin-code-ru.bestoffers.to

Több mint 600 azonosított oldal és URL, oldalnév szerint csoportosítva

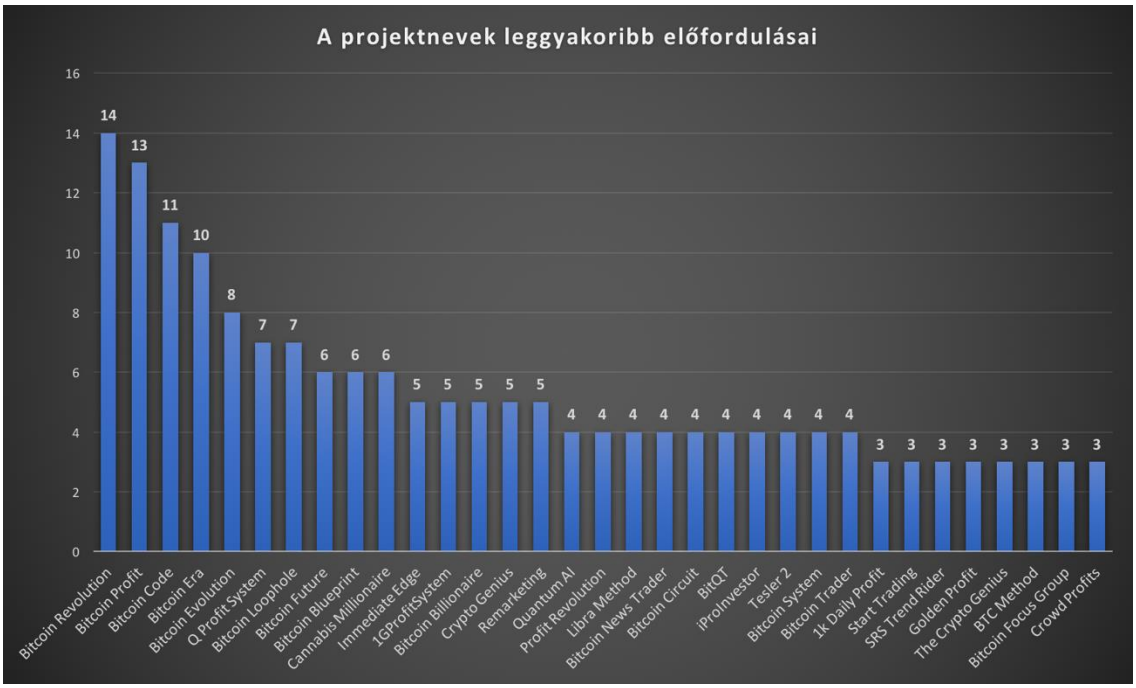
Bár a Project ID azonosítók egyediek, azonban a projekt nevek és URL címek akár ismétlődhetnek is, illetve egy-egy projektnévhez akár több URL cím is tartozhat. Ennek oka lehet, hogy egy projekt esetleg több módon is elszámolásra kerülhet, vagy bár az URL ugyanaz, de más script paraméterekkel töltődik be az oldal (például nyelvi változók).

```
-4837301|1219|Convertick - Bitcoin Method|Ft|https://roiverticals.co/|None|None
-34837301|1219|Convertick - Bitcoin Method|Ft|https://roiverticals.co/|None|None
<script type='text/javascript'>
var appId = 'xxxxxxx-xxxx-xxxxx-xxxxx-xxxxx'; //get your App-ID and replace
var data = {};
(new URL(window.location.href)) //example how to send all the URL parameters
.searchParams.forEach((el, k) => {
var key = k.replace(/\[.*]/, '');
if (data[key]) {
if (Array.isArray(data[key])) {
data[key].push(el);
} else {
data[key] = [data[key], el];
}
} else {
data[key] = el;
}
});
var webPush = WebPush(appId, data); //send data to push77
document.addEventListener('webpush-sw-registered', event => {
webPush.handleSubscribeUser();
});
</script>
```

```
+38970401|1220|Algo - Immediate Edge Bot|Gt|https://roiverticals.co|None|None
+38970401|1220|Algo - Immediate Edge Bot|Gt|https://roiverticals.co|None|None
<script type='text/javascript'>
var appId = 'xxxxxxx-xxxx-xxxxx-xxxxx-xxxxx'; //get your App-ID and replace
var data = {};
(new URL(window.location.href)) //example how to send all the URL parameters
.searchParams.forEach((el, k) => {
var key = k.replace(/\[.*]/, '');
if (data[key]) {
if (Array.isArray(data[key])) {
data[key].push(el);
} else {
data[key] = [data[key], el];
}
} else {
data[key] = el;
}
});
var webPush = WebPush(appId, data); //send data to push77
document.addEventListener('webpush-sw-registered', event => {
webPush.handleSubscribeUser();
});
</script>
```

ProjectID 1219 és 1220 a projektek nevében térnek el egymástól

Ha csak az egyedi oldalcímeket nézzük, összesen 635 egyedi URL cím volt azonosítható.



A leggyakoribb projektnevek

A Bitcoin Revolution, Bitcoin Profit és a Bitcoin Code a három leggyakrabban előforduló kripto-fraud projektnév az adatbázisban. Megjelennek azonban más, pl. „*Bitcoin Code (DE)*" vagy „*Bitcoin Profit 763*" alakokban is, így a valóságban ezek a projektek nagyobb számban vannak jelen az API adatbázisában.

Project name	URL
Bitcoin Code	https://asuccesshub.com/bitcoincode
	https://bitcoin-code.greatoffers.to
	https://bitcoincodeworld.com
	https://btc-code.bestoffers.to
	https://chiefoffers.net/bitcoincode
	https://get-profits-now.com/bitcoincode
	https://realvipdeal.com/bitcoincode
	https://specialinvite.co/bitcoincode
	https://specialvipoffer.com/bitcoincode
	https://thebitcoinscodes.com
	https://vipoffer.net/bitcoincode
Bitcoin Code (DE)	https://bitcoincode-de.com
Bitcoin Code (ES)	https://bitcoincode-es.com
Bitcoin Code (IT)	https://bitcoincode-it.com
Bitcoin Code 2	https://btccode.greatoffers.to
Bitcoin Code ES	https://lp.themarketsinsider.com/cm/bitcoin-code/
Bitcoin Code FR	https://bitcoin-code-fr.bestoffers.to
Bitcoin Code RU	https://bitcoin-code-ru.bestoffers.to

Bitcoin Era	https://24profits.com/bitcoinera
	https://asuccesshub.com/bitcoinera
	https://bitcoinera.bestoffers.to
	https://bitcoinzera.club
	https://chiefoffers.net/bitcoinera
	https://ecryptodaily.co/bitcoinera
	https://financenonstop.shop/bitcoinera
	https://get-profits-now.com/bitcoinera
	https://likino.top/bitcoinera
	https://lp.fxvc.eu/fx7/bitcoin-era-fx/
	https://lp.themarketsinsider.com/cm4/bitcoin-era-2/
	https://top-offers.vip/bitcoinera
Bitcoin Profit	http://btcprofitclub.app/
	https://asuccesshub.com/bitcoinprofit
	https://bitcnprofit.com
	https://bitcoin-profit.bestoffers.to
	https://bitcoinprofit.greatoffers.to
	https://caschcoin.com/bitcoinprofit
	https://chiefoffers.net/bitcoinprofit
	https://get-profits-now.com/bitcoin-profit
	https://lp.fxvc.eu/fx8/bitcoin-profit-2
	https://lp.themarketsinsider.com/lp/bitcoin-profit/
	https://realvipdeal.com/bitcoin-profit
	https://specialinvite.co/bitcoinprofit
	https://specialvipoffer.com/bitcoinprofit
	https://vipoffer.net/bitcoin-profit
Bitcoin Profit (PL)	https://profitbitcoin.net
Bitcoin Profit (TH)763 (secondary)	https://btcprofit.ecotrack.top/en/btcprofit/
Bitcoin Profit /Compass 811	https://www.profitspros.com/?aid=w2FUDBu5Ts
Bitcoin Profit 2	https://lp.themarketsinsider.com/cm5/bitcoin-profit-3/
Bitcoin Profit 763	https://btcprofit.ecotrack.top/
Bitcoin Revolution	https://24profits.com/bitcoinrevolution
	https://asuccesshub.com/bitcoinrevolution
	https://bitcoin-revolution.bestoffers.to
	https://bitcoinrevolution.greatoffers.to
	https://bitcoinrevolutionofficial.com
	https://chiefoffers.net/bitcoinrevolution
	https://ecryptodaily.co/bitcoinrevolution
	https://get-profits-now.com/bitcoin-revolution
	https://mdz1.club/bitcoinrevolution
	https://realvipdeal.com/bitcoinrevolution

	https://safe-offers.net/bitcoinrevolution
	https://specialinvite.co/bitcoinrevolution
	https://specialvipoffer.com/bitcoinrevolution
	https://vipoffer.net/bitcoinrevolution
Bitcoin Revolution ES	https://lp.fxvc.eu/fx15/bitcoin-revolution-es/
Bitcoin Revolution RU	https://safe-offers.net/bitcoinrevolutionru
BitcoinCode CPL	https://bit-code.info
Convertick - Bitcoin Profit	https://tracklik.com
Converting Team - Bitcoin Profit w our prelander	https://getmoneyvibes.com/
Profit Bitcoins - IT	https://profitbitcoins.club
Trafficon - Bitcoin Revolution w prelander	http://worlds-greatest-news.com/news/student-earns
Trafficon - Global - Bitcoin Code w mom Prelander	https://roiverticals.co/vol_click

Projektvariációk és URL-ek, amelyek a Bitcoin szót tartalmazzák

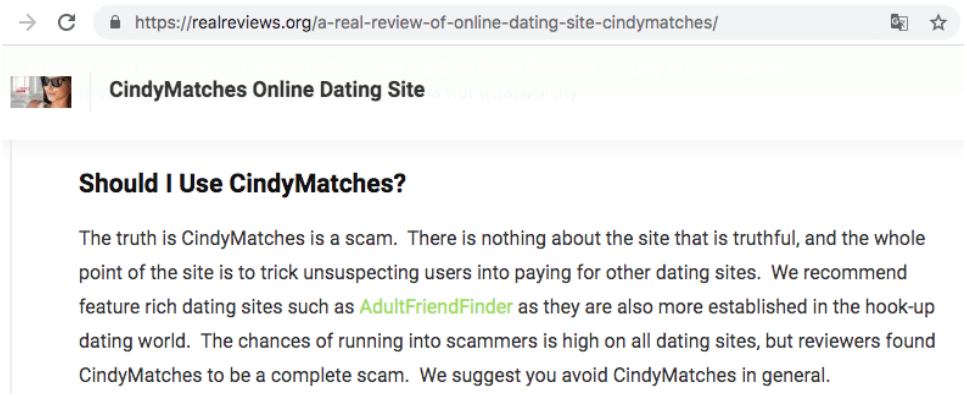
Érdekesség, hogy az API nem csupán a kripto-fraud vagy kripto-scam tartalmakat, hanem erotikus és társkereső oldalakat is kiszolgál. Az alábbi weblapok is az API interfészt használják központi tartalomvezérlésre, illetve elszámolásra.

Project name	URL
Bonga Cams (Desktop) - 1.2 $ to 2.7 $	https://www.bongacams.com
Bonga Cams (Mobile) - 0.6$ to 1.8$	https://www.bongacams.com
VR FuckDolls (All Devices) - 18$ to 42$	https://bit.ly/2J4otlu
StudGame - Adult/Gay (All Devices) - 18$ to 42$	https://bit.ly/30alvBO
Real Adult Sex Game (All Devices) - 18$ to 42$	https://bit.ly/2Jq3mcv
Matchsniper US/UK/AU/NZ/CA (Desktop/Mobile) - 2.5 $	https://prnt.sc/pqt5dy
LookADate US/UK/AU/NZ/CA (Desktop/Mobile) - 2.5 $	https://prnt.sc/pra4ty
DateHiker US/UK/AU/NZ/CA (Desktop/Mobile) - 5 $	https://prnt.sc/ptvopf
Meetem.club US/UK/AU/NZ/CA (Desktop/Mobile) - 2.5 $	https://prnt.sc/pvz5s4
DateHiker US/UK/AU/NZ/CA (Desktop/Mobile) - 2.5 $	https://prnt.sc/ptvopf
Date-Search (Desktop/Mobile) US/AU/CA/NZ/ZA - 5 $	https://prnt.sc/qirqs8
AshleyMadison US/CA (Adult/All-Devices) 3.5 $ [Prelander 1]	https://prnt.sc/qxsa9w
AshleyMadison US/CA (Mainstream/All-Devices) 3.5 $ [Prelander 1]	https://prnt.sc/tifz1a
ThatRussianGirl (All-Devices) US/UK/CA/AU/NZ/IE/ZA - 2.5 $	https://thatrussiangirl.com
CindyMatches US/UK/CA/AU/NZ/IE/ZA (All-Devices) - 3 $	https://cindymatches.com/
EmmasMadchen DE/AT/CH (All-Devices) - 3 $	https://emmamadchen.de/
IndigoMatches (All-Devices) US/UK/CA/AU/NZ/IE/ZA - 2.5 $	https://prnt.sc/qtw2ad
MilfTicket (All-Devices) US/UK/CA/NZ/AU/ZA - 3.2 $	https://prnt.sc/raskph
[TOP] VenusMatches (All-Devices) US/CA/AU/UK/NZ/IE/ZA - 2 $	https://venusmatches.com/
MeetLocals US/AU/NZ/UK/CA (All-Devices) - 3 $	http://we-meet-locals.com/
OneNightMilf US/UK/CA/NZ/AU (All-Devices) - 3 $	https://onenightmilf.com/t4/
[HOT] Jucydate US/GB/AU/NZ/CA/ZA (All-Devices) - 1 $	https://jucydate.com/

MapMyMilf US/UK/AU/NZ/CA (All-Devices) - 2 $	https://mapmymilf.com/profiles
KissRussianGirls (Desktop & Mobile) - 4 $	https://www.kissrussiangirls.com/qa/register03.php
MILFSense [EMAIL] (All-Devices) - 2.5 $	https://prnt.sc/suvdrj
[Dirk] DateAsianWoman (Desktop/Tablet) 6 $	https://www.dateasianwoman.com/
[Dirk] MeetUkrainianGirl (Desktop/Tablet) - 6 $	https://prnt.sc/sydnwb
[TOP]EroticMadness US/UK/CA/AU/NZ/IE/ZA (Desktop/Mobile) - 3$	https://eroticmadness.com/
MyCuteGirlFriends US/UK/CA/AU/NZ/IE/ZA (Desktop/Mobile) - 3$	https://mycutegirlfriends.com/
***In-House* Virtual Sex Match Lander 1 (All-Devices) - 30 $**	https://prnt.sc/twqcfw
AdultDates (All-Devices) - 3 $	https://www.adultdates.com/
LiveYourWetDream (All-Devices) US/GB/AU/NZ/CA/ZA - 2.5 $	https://liveyourwetdream.com/landing
[TOP] JoinTheDating (All-Devices) US/AU/GB/CA/NZ - 2$	https://jointhedating.com/

„Társkereső" oldalak, amelyek ugyanezt az API-t használják

A „randi" oldalaktól eltekintve az API-t használó partneri hálózat címeinek többsége (536 egyedi URL) különféle kripto-fraud vagy kripto-scam csalásokhoz kapcsolódik, bár kérdéses, hogy a „randi" oldalak milyen célzattal működnek.



Az API adatbázisában szereplő CindyMatches oldal feltehetőleg scam

Az API-n keresztül letöltött adatok ellenőrzése rávilágított arra, hogy több oldal már nem működik, azonban az URL-ek jelentős része jelenleg is üzemel. A vizsgálat alatt is jelentek meg újabb projektek, látható volt, hogy a hálózat folyamatosan növekszik.

Összefoglalás

A vizsgálat során 644 egyedi projektet és hozzájuk kapcsolódóan 634 egyedi URL címet azonosítottunk, amelyek jelentős része (536) különféle kripto-fraud vagy kripto-scam csaláshoz kapcsolódik.

A korábbi tanulmánnyal összhangban jelen vizsgálat eredményei is arra engednek következtetni, hogy ezek az oldalak egy kiterjedt *affiliate* partneri hálózat API interfészét és mögöttes adatbázisát használják. A csalók láthatóan fejlett, jól működő rendszereket vesznek igénybe, amelyek összehangoltan és automatizáltan működnek.

A Bitcoin Loophole, Bitcoin Era, Bitcoin Revolution és társaik a korábbi tanulmányban ismertetett módon: álhírekkel, Facebook reklámokkal és Google hirdetésekkel csalják adatgyűjtő oldalukra a gyanútlan, és biztonságtudatossági szempontból felkészületlenebb látogatókat, hogy hihetetlen hozamok ígéretével befektetésre bírják őket, azaz kicsalják a pénzüket.

Felmerül a kérdés, hogyan lehet védekezni az álhírekkel ötvözött és csalási szándékkal létrehozott oldalakkal szemben?

Jelenleg nem létezik olyan technológia, amely képes lenne az ilyen tartalmakat kiszűrni. Ha csak az álhíreket vizsgáljuk, megjelentek már a mesterséges intelligencia felhasználására tett törekvések, azonban az ilyen megoldások gyerekcipőben járnak, a közeljövőben még nem fognak biztos megoldást jelenteni.

A hír- és tényellenőrző szolgáltatások (*fact checker*) jelenleg az emberi erőforrásokra támaszkodnak, de korántsem tökéletesek. Nehezen zárják ki azokat az emberi tényezőket, amelyekkel a mesterséges intelligenciáknak nem kell megküzdenie (például a tényszerűséget erodáló érzelmeket és szubjektivitást).

A legműködőképesebb megoldásnak a felhasználók (internet használók) biztonságtudatosságának fejlesztése látszik. Az értő olvasás mellett a felhasználónak tisztában kell lennie a rá leselkedő veszélyekkel, és át kell látnia a „fantasztikusan jó ajánlatok" manipulatív kommunikációján. Ha valami túl jó üzletnek tűnik, az általában gyanús, mert csodák (legalábbis az üzleti életben) nincsenek. A felhasználói biztonságtudatosság mellett az üzleti realitásérzéknek is működnie kell.

A Bitcoin Loophole és a hasonló, hihetetlen hozamokat kínáló befektetések ígérete gyanút kell, hogy ébresszen és a felhasználónak fel kell tennie magának a kérdést: *Nem túl szép ez ahhoz, hogy igaz legyen?* Ha a kétely ráveszi a felhasználót, hogy utána nézzen a „kihagyhatatlan ajánlatnak" (például egyszerű rákereséssel vagy akár OSINT módszerek alkalmazásával), sokkal nehezebb dolga lesz a csalóknak és sokkal kevesebb áldozata lesz a tevékenységüknek.