Bitdefender

A Bitdefender antivírus termékeket gyártó cég percenként több mint 400 új fenyegetést fedez fel, és naponta mintegy 40 milliárd fenyegetettségi lekérdezést validál. A cég az elmúlt évek során innovációkat vezetett be a rosszindulatú szoftverek elleni védelem, az IoT biztonság, a viselkedéselemzés és a mesterséges intelligencia területén.

A kutatás-fejlesztési képességeit folyamatosan kihasználva, a tapasztalt és fellelt új fenyegetések segítenek abban, hogy termékeiket rendszeresen olyan új képeségekkel ruházzák fel, amelynek köszönhetően a legújabb támadások ellen is sikerrel veszik fel a versenyt.

Kutatóik a jelenlegi geopolitikai helyzet kapcsán kialakult nemzetközi kiberháborút is kiemelt figyelemmel kísérik, és napi rendszerességgel készítenek friss kiberbiztonsági riportokat. Ezek alapján a Bitdefender az alábbi orosz – ukrán háború vonatkozásában kialakult csalásokra hívja fel a figyelmet, amelyek jelenléte most is megfigyelhető a kibertérben.

Bár a közelmúltbeli kibertámadások már nem kifejezetten csak az ukrán infrastruktúrát, vagy a civil lakosságot célozták, a folyamatban lévő háború által generált globális feszültség valószínűleg célzottabb támadásokban fog megnyilvánulni, amelyek elrettenthetik a sürgősségi segélyszolgálatok és a humanitárius segítségnyújtási erőfeszítéseket az országban. Ezen csalások célja továbbra is a destabilizáció, illetve az új elemként megjelenő pénz-és adatszerzés.

1) Ukrán katonákhoz és családtagjaikhoz kötődő adathalászat

A fehérorosz állam által támogatott hackerek új adathalász kampányt indítottak, mellyel az ukrán katonákat, azok családjait és ismerőseit célozzák meg. A kampány az ukrán-orosz konfliktus információs műveleteinek része és az érintettek privát "i.ua" és "meta.ua" fiókjait célozzák. Miután a fiókot feltörték, a támadók az IMAP protokoll segítségével hozzáférnek az összes üzenethez. Ezt követően a támadók az áldozat címjegyzékében tárolt

elérhetőségi adatokat használják arra, hogy az adathalász üzeneteket más célpontokhoz is eljuttassák.

Az e-mailekben azt állítják, hogy a címzettnek meg kell erősítenie adatait, abból a célból, hogy igazolja az illető, hogy ő nem spambot, különben két napon belül lezárják a postafiókját.

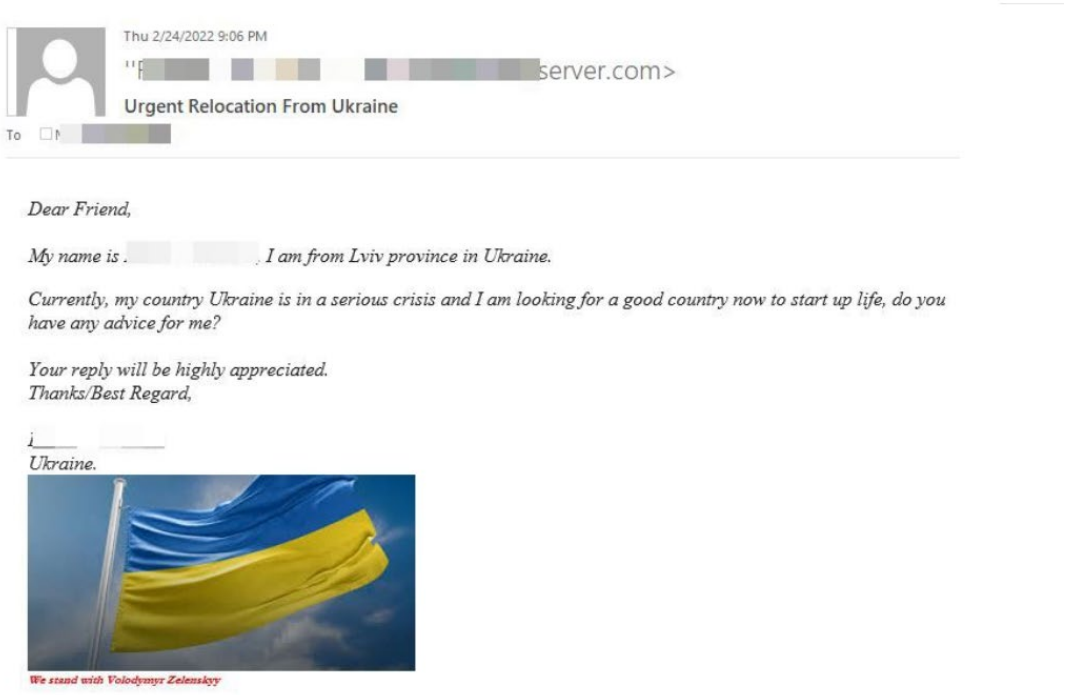
> *"Dear user! Your contact information or not you are a spam bot. Please, click the link below and verify your contact information. Otherwise, your account will be irretrievably deleted. Thank you for your understanding. Regards, I.UA Team"*

Az ukrán kormány a tevékenységet egy UNC1151 néven nyomon követhető fenyegettségi szereplőnek tulajdonította, ami egy minszki székhelyű csoport, és a Fehérorosz Köztársaság védelmi minisztériumához kapcsolható. A teljes képhez hozzátartozik, hogy ezt a kampányt már Fehéroroszországban is megfigyelték és detektálták. A hackercsoport feltehetően legalább 2016 óta aktív. 2021 novemberében azt írták róluk, hogy számos kormányzati és civil szervezetet vettek már célba, főként Ukrajnában, Litvániában, Lettországban, Lengyelországban és Németországban. Mindezek mellett a célpontok között fehérorosz disszidensek, médiaszervezetek és újságírók is szerepeltek. Idén is felmerült már a nevük, ugyanis januárban az ukrán kormányzati weboldalakat ért defacemant (honlaprongálás) támadásokat is ők követhették el.

2) Az ukrán menekülteknek segítőket célzó adathalász támadások

Valószínűleg egy államilag támogatott fenyegetettségi szereplők által koordinált spear-phishing kampány célpontjai az ukrajnai menekülteknek logisztikai támogatást nyújtó európai kormányzati alkalmazottak voltak. A támadók az ukrán fegyveres szolgálatok tagjainak
valószínűleg kompromittált e-mail fiókjait használják az adathalász üzenetek továbbítására.
Az adathalász-támadások kizárólag európai kormányzati szerveket céloztak, és hozzátették, hogy egyelőre nem tudják a támadásokat egy konkrét, államilag támogatott hackercsoportnak tulajdonítani. Az e-mail egy rosszindulatú makró csatolmányt tartalmazott, amely egy rosszindulatú szoftver letöltésére tett kísérletet.

Az üzenetet látszólag egy Ukrajnában élő személy küldi azzal a tárggyal, hogy „Urgent Relocation from Ukraine” / "Sürgős áttelepülés Ukrajnából". A levélben pszichológiai manipulációt alkalmazva tanácsot vagy segítséget kérnek a csalók. Az első levél nem tartalmaz pénzutalásra vagy adatmegosztásra vonatkozó kérést, erre az esetlegesen kialakult levelezés során később kerülhet sor.



A Bitdefender telemetriái szerint a csaló e-mailek 91%-át holland IP-címekről küldték. A terjesztés szempontjából 61% Dél-Koreába, 10% Írországba, 6% az Egyesült Államokba, 5-5% Dániába és Svédországba, valamint korlátozott számban az Egyesült Királyságba, Németországba, Japánba és Indiába irányult.

3) Adománygyűjtő csalások

A nagyobb globális események és válságok általában rosszindulatú spamkampányokat indítanak el, amelyek az emberi érzelmeket és az emberek segítő szándékát, vagy éppen bizonytalanságát használják ki. Így volt ez a COVID-19 kitörésekor is, és így van ez a jelenlegi geopolitikai krízis során is.

Az adománygyűjtő csalás abból áll, hogy az emberek törvényes adománygyűjtőknek adják ki magukat, és pénzt kérnek a rászorulók

megsegítésére. A kampány jellemzően a közösségi média oldalakon (leginkább Twitteren és Facebookon) és e-mail-ben terjed. De ezek mellett előfordulhat, hogy a csalók telefonon keresik meg leendő áldozatjelöltjeiket.

Az ilyen jellegű csalásokat viszonylag nehéz kiszűrni: a Bitdefender és a biztributor azt javasolja, hogy a felhasználók tegyenek fel maguknak néhány kérdést, mielőtt bármekkora összeget is átutalnak, vagy bármilyen személyes, pénzügyi adatokat adnak meg.

- Megbízható-e az a személy vagy szervezet, akinek pénzt adsz?
- Ismerem-e őket, hallottam-e már róluk korábban?
- Van róluk más egyéb információ az interneten?
- Milyen véleménnyel vannak róluk mások, megbízhatónak tartják őket?
- Nyitottak a párbeszédre, vagy egyoldalú a kommunikációjuk?
- Transzparensen működnek-e?
- Kérnek tőlünk pénzügyi adatokat?
- Felajánlottak valamilyen ajándékutalványt a jótékonyságért cserébe?
- Én találtam meg őket, vagy ők kerestek meg engem?

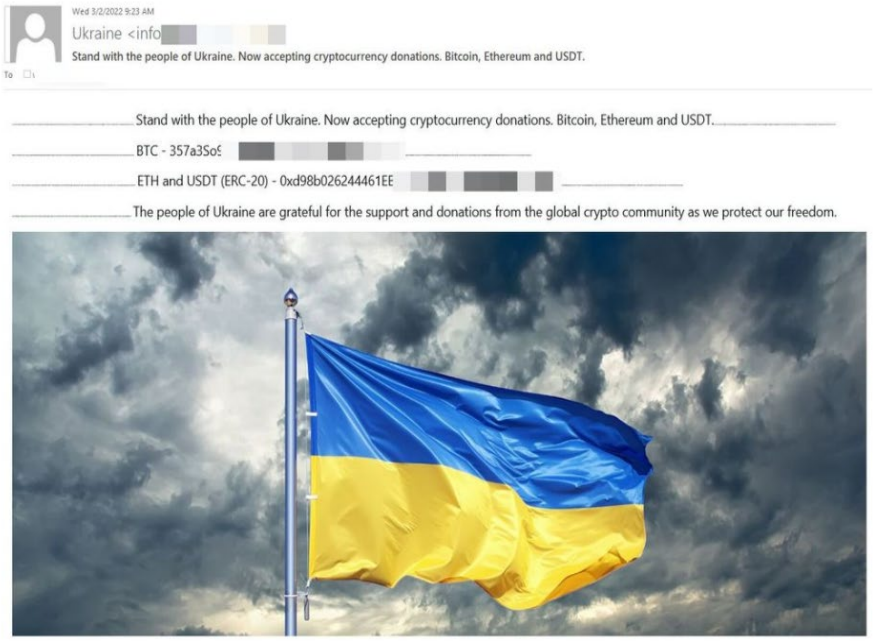
4) Kriptovalutás adományozós csalások

Ukrajna, a jelenlegi krízis kapcsán, kriptovalutában is fogadja a humanitárius és jótékonysági felajánlásokat, amelynek köszönhetően ez idáig több mint 50 millió dollár értékű kriptovalutát sikerült összegyűjteni Ukrajna megsegítésére. Azonban van ennek egy árnyoldala is: ennek hatására a kiberbűnözők is akcióba lendültek.

A Bitdefender több

- „Help Ukraine” / „Segítse Ukrajnát!”
- „Stand with the people of Ukraine” / Állj ki az ukrán nép mellett”
- „Urgent! Help Children in Ukraine” / „Sürgős! Segítsen az ukrán gyerekeknek”
- „Donate to Ukraine” / „Adományozzon Ukrajnának”

tárgyú csaló e-mailt, adathalász oldalt és egyéb fórumot azonosított, amelyekkel a segítőkész felhasználók jóhiszeműségét kihasználva igyekeznek pénzt szerezni a csalók. A hamis segítségkérő és adománygyűjtő mozgalom során a támadók olyan, jellemzően Bitcoin és Ethereum kriptovaluta adománygyűjtést hirdetnek, amely semmilyen kapcsolatban nem áll az ukrán kormányzattal és annak adománygyűjtő tevékenységével. Hogy hihetőbbé tegyék a gyűjtés valódiságát, számos meggyőzésre alkalmas eszközt alkalmaznak, például a npr[.]org, az ENSZ Humanitárius Ügyeket Koordinációs Hivatala (OCHA), az UNICEF, esetleg az Act for Peace nemzetközi vagy az Ukraine Crisis Relief Fund nevű ukrán humanitárius szervezet nevében küldenek ki e-maileket az áldozatoknak, és fórumbejegyzéseket tesznek közzé a hamis mozgalomról.



Tue 3/1/2022 6:18 PM

HELP UKRAINE <[redacted].ua>

HELP UKRAINE stop the war!

To [redacted]

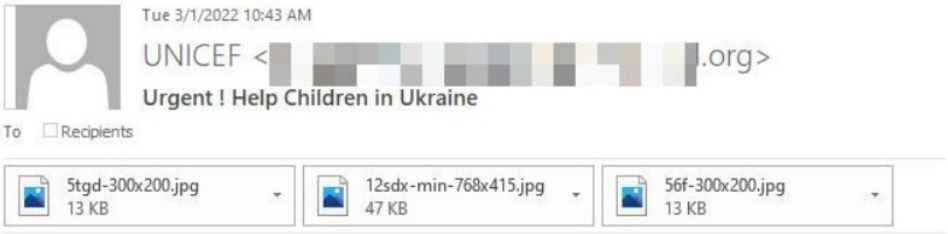
Army of Ukraine need your support ! Please help us defend our freedom and independence!
Thank you for everyone !
The National Bank of Ukraine has decided to open a special fundraising account to support the Armed Forces of Ukraine.
Here is original source : https://bank.gov.ua/en/news/all/natsionalniy-bank-vidkriv-spetsrahunok-dlya-zboru-koshtiv-na-potrebi-armiyi
PLEASE, DO NOT IGNORE THIS MESSAGE !

Stand with the people of Ukraine.
Now accepting cryptocurrency donations. Bitcoin, Ethereum and USDT.

BTC - bc1qv729ckc4[redacted]

ETH and USDT (ERC-20) - 0x0dcf682C[redacted]

We very sorry for a such spam ! But people of Ukraine need your support !
Thank you for everyone !
Here is original source : https://bank.gov.ua/en/news/all/natsionalniy-bank-vidkriv-spetsrahunok-dlya-zboru-koshtiv-na-potrebi-armiyi
Please, do not blacklist this domain !



Tue 3/1/2022 10:43 AM

UNICEF <[redacted].org>

Urgent ! Help Children in Ukraine

To Recipients

5tgd-300x200.jpg 13 KB | 12sdx-min-768x415.jpg 47 KB | 56f-300x200.jpg 13 KB

Hello

In times of crisis, we turn to others for help or step up to assist.

Millions of civilians are caught in the middle of an escalating military conflict and humanitarian crisis, and casualties are rising.

Your donation to this fund will support Ukrainians in need, with a focus on the most vulnerable, including children.

We receive this through BTC OR ETH since all banks are closed.

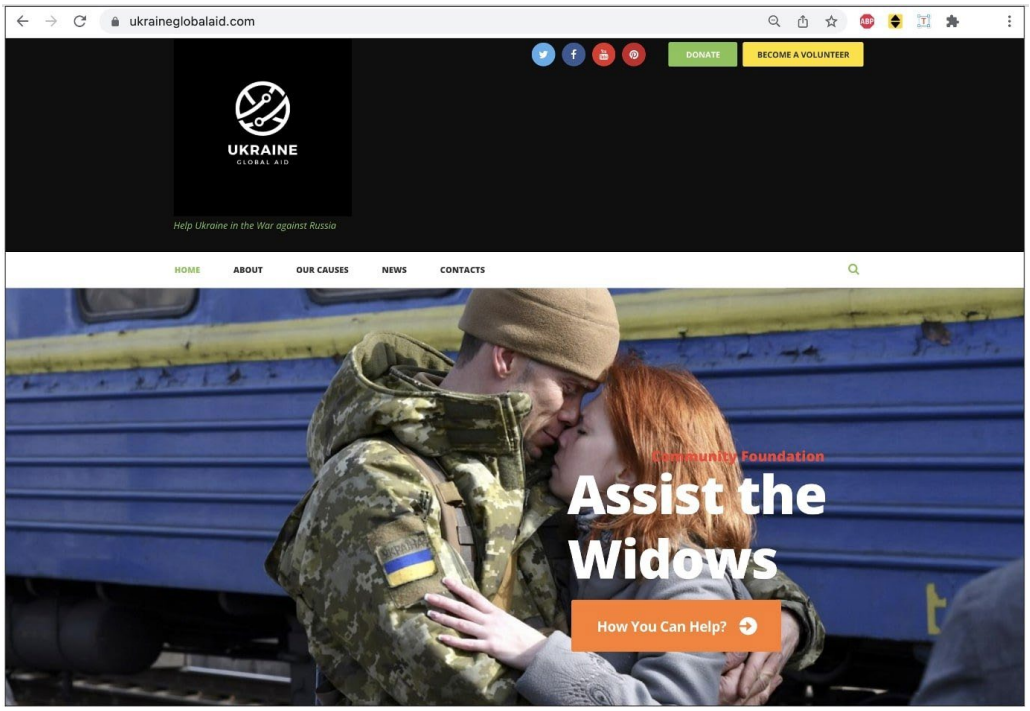
All Supporters (5265)

Save Children
$436,792
Donated of 500,000 goal

BITCOIN ID = 3Q437aYNYuT[redacted]

ETH ID = 0xa666e53BdF65b1[redacted]

Mindezek mellett azonosításra került néhány adománygyűjtő .org domain is, amelyeket csalási szándékkal hoztak létre, továbbá felfedezték az UkraineGlobalAid[.]com weboldalt is, ami első ránézésre valódinak tűnhet, alaposabban megvizsgálva azonban jól észrevehetők a gyanús jelek és a hibás hivatkozások.

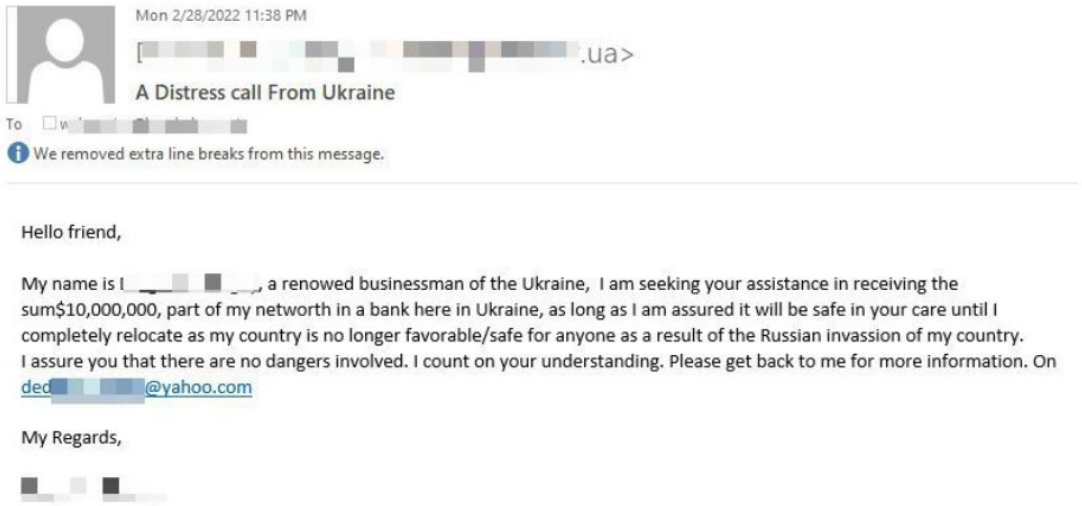


Mivel ezek a csalási módszerek a jelen körülményekre támaszkodva igyekeznek kihasználni az emberek jóhiszeműségét, a gyanútlan felhasználók könnyen áldozattá válhatnak. Azáltal, hogy az ukrán kormány kriptovalutában is fogadja az adományokat, sajnos fennáll az esélye az ilyen jellegű csalásoknak.

A csaló e-mailek 25%-a az Egyesült Királyságba, 14%-a az Egyesült Államokba, 10%-a Dél-Koreába, 8%-a Japánba, 7%-a Németországba, 4%-a Romániába, valamint 2-2%-a Görögországba, Finnországba, Olaszországba és Magyarországra érkezett.

5) Nigériai herceg-típusú csalások

A Bitdefender spamszűrői a régebbi, ún. nigériai herceg-átverés „ukrán változatát" is észrevették. A csalás során egy neves ukrán üzletember nevében küldenek e-mailt, amelyben 10 millió dollár átutalásához kérik a címzettek segítségét. Kiemelik, hogy erre csak addig van szükség, amíg biztonságos helyre nem tud költözni a levél feladója.



Mon 2/28/2022 11:38 PM

[redacted].ua>

A Distress call From Ukraine

To [redacted]

We removed extra line breaks from this message.

Hello friend,

My name is [redacted], a renowed businessman of the Ukraine, I am seeking your assistance in receiving the sum$10,000,000, part of my networth in a bank here in Ukraine, as long as I am assured it will be safe in your care until I completely relocate as my country is no longer favorable/safe for anyone as a result of the Russian invasion of my country. I assure you that there are no dangers involved. I count on your understanding. Please get back to me for more information. On [redacted]@yahoo.com

My Regards,

[redacted]

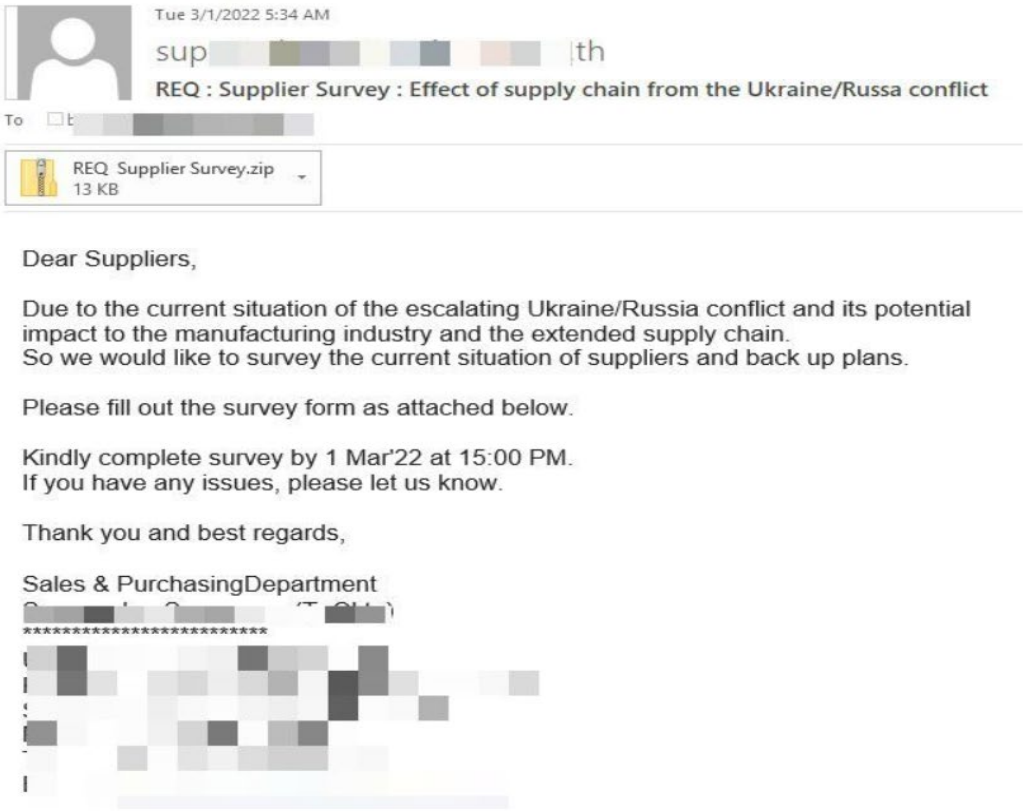
A csalók, akik e különleges átverés mögött állnak, botswanai (83%), németországi (10%) és franciaországi (5%) IP-címekről küldenek e-maileket. Fő célközönségük a németországi (42%), törökországi (16%), amerikai (16%), írországi (8%) és lengyel (3%) felhasználók.

Sajnos azok a felhasználók, akik válaszolnak erre az e-mailre, kapcsolatba kerülnek a csalókkal, akik a kialakult konverzáció során személyes és pénzügyi adatokat fognak kérni, abból a célból, hogy az illető segítsen a pénz kiutalásában az országból. Bár az e-mail konkrétan nem ígér a címzetteknek anyagi jutalmat a segítségükért, a csalók egyik eszköze mégis az, hogy a további levelezés során valamilyen jutalékot ígér a segítőnek. Az átverés az egészben ott van, hogy a csaló valamilyen adminisztrációs vagy tranzakciós díjakat kér az áldozattól, arra hivatkozva, hogy ezen összeg nélkül nem lehet a nagyobb tétel átutalását megkezdeni.

6) Agent Tesla és Remcos nevű kártevők

Március 1. óta a Bitdefender két olyan adathalászkampányt követett nyomon, amelyek két jól ismert távoli hozzáférésű trójai vírussal - Agent Tesla és Remcos - próbálják megfertőzni a címzetteket.

Kampány 1:
Az első rosszindulatú spam-kampány a feldolgozóiparban működő szervezeteket célozza meg egy .zip formátumú "REQ Supplier Survey" elnevezésű csatolmányon keresztül. A támadók az e-mailben arra kérik a címzetteket, hogy töltsenek ki egy felmérést az ukrajnai háborúra reagáló biztonsági terveikről.


Tue 3/1/2022 5:34 AM

sup[redacted]th

REQ : Supplier Survey : Effect of supply chain from the Ukraine/Russa conflict

To [redacted]

REQ_Supplier Survey.zip
13 KB

Dear Suppliers,

Due to the current situation of the escalating Ukraine/Russia conflict and its potential impact to the manufacturing industry and the extended supply chain.
So we would like to survey the current situation of suppliers and back up plans.

Please fill out the survey form as attached below.

Kindly complete survey by 1 Mar'22 at 15:00 PM.
If you have any issues, please let us know.

Thank you and best regards,

Sales & PurchasingDepartment
[redacted]
****
[redacted]

A rosszindulatú kód letöltése és telepítése közvetlenül az áldozat gépén található Discord-hivatkozásról történik. Érdekes azonban, hogy a rosszindulatú fájllal való interakció során a Chrome egy tiszta verziója is letöltődik a felhasználók eszközére - valószínűleg a felhasználók elterelésére tett kísérletről van szó.

Az Agent Tesla egy hírhedt MaaS (Malware-as-a-service) RAT (Remote Access Trojan - távoli hozzáférésű trójai) és adatlopó kártevő, amely a közelmúlt pandémiás időszaka során népszerű volt a kiberbűnözők körében, és számos e-mail alapú támadást hajtottak végre a segítségével. Az elkövetők az Agent Tesla-t arra használják, hogy érzékeny információkat (többek között hitelesítő adatokat, billentyűleütéseket és vágólapadatokat szerezzenek a célpontoktól.

A Bitdefender elemzése szerint a támadások látszólag holland (86%) és magyar (3%) IP-címekről indultak. A rosszindulatú e-mailek világszerte eljutottak a címzettekhez, többek között Dél-Koreába (23%), Németországba (10%), az Egyesült Királyságba (10%), az Egyesült Államokba (8%), a Cseh Köztársaságba (14%), Írországba (5%), Magyarországra (5%), Svédországba (3%) és Ausztráliába (2%).

2. kampány:
A második rosszindulatú spamkampány során a támadók egy dél-koreai székhelyű, diagnosztikai eszközökre szakosodott egészségügyi vállalatnak adják ki magukat, hogy egy Excel csatolmányon keresztül (SUCT220002.xlsx) fertőzzék meg az áldozatok eszközeit a Remcos nevű RAT-ot.

Az üzenet az Ukrajnában zajló konfliktusra hivatkozik („Ukraine war” / „Ukrán háború” tárggyal), és a támadók azután érdeklődnek az e-mailben, hogy a címzettek kívánják-e valamelyik megrendelésüket felfüggeszteni, amíg a szállítások és a járatok újraindulnak. A kibertámadók főként rosszindulatú dokumentumokon vagy archívumokon keresztül telepítik a Remcos nevű kártevőt, abból a célból, hogy teljes ellenőrzést szerezzenek áldozataik rendszerei felett. Ha a bűnözők bejutottak a rendszerbe, akkor akár rögzíthetik a billentyűleütéseket, képernyőképeket, hitelesítő adatokat vagy más érzékeny információkat is, amiket közvetlenül a szervereikre exportálhatnak.

A rosszindulatú e-mailek 89 százaléka német IP-címekről, 19 százaléka pedig az Egyesült Államokból származik. A támadók az írországi (32%), indiai (17%), amerikai (7%), brit (4%), németországi (4%), vietnami (4%), oroszországi (2%), dél-afrikai (2%) és ausztrál (2%) címzettekre összpontosítanak.

7) Az Európai Bizottság nevében elkövetett adathalászat

Az elmúlt héten egy olyan adathalász kampány bontakozott ki a kibertérben, amely az Európai Bizottság (továbbiakban EB) nevével él vissza. A bűnözők az EB nevében egy „Situation at the EU borders" / „Helyzet az EU ukrajnai határainál" tárgyú e-mailt küldenek a felhasználóknak, amely levél tartalmaz egy-egy káros hivatkozást és fájlcsatolmányt is. A hivatkozások .exe és .zip fájlok letöltését elindító linkre mutatnak, a mellékelt jellemzően egy .docx fájlt tartalmaz.

A Bitdefender kutatói az elmúlt két hét során azt a trendet figyelték meg, hogy a támadók nagyon gyorsan reagáltak Ukrajna és más szervezetek törvényes közleményeire azáltal, hogy utánozták és lemásolták az üzenetek formátumát. Jelenleg arra lehet számítani, hogy az adathalász- és malware-kampányok sokfélesége, valamint a naponta küldött üzenetek mennyisége folyamatosan növekedni fog, és a támadók ennek megfelelően – és ehhez - igazítják majd a pszichológiai manipuláción alapuló módszereiket.

A Bitdefender és hazai képviselőjeként a biztributor azt javasolja a felhasználóknak, hogy:

- ezekben a nehéz időkben a felhasználók legyenek különösen éberek és fokozottan gyanakvóak, biztonságtudatosak;
- fogadják fenntartással az idegen eredetű megkereséseket, főleg, ha valamilyen Ukrajnához köthető elem szerepel a tárgy mezőben;
- soha ne kattintsanak olyan e-mailekben vagy üzenetekben található linkekre, mellékletekre, csatolmányokra, amelyek sürgős adományozásra kérik;
- ne reagáljanak impulzívan az azonnali cselekvésre felszólító üzenetekre;
- kizárólag hivatalos és megbízható jótékonysági szervezeteken, nonprofit szervezeteken és adománygyűjtőkön keresztül adományozzanak;
- rendszeresen ellenőrizzék pénzügyi számláikat, hogy a gyanús tevékenységeket vagy jogosulatlan terheléseket minél hamarabb kiderüljenek;
- ne vegyenek részt hamis információk terjesztésében és legyen egyértelmű jel egy-egy olyan üzenet, felhívás, ami arra ösztönöz, hogy a leírtak minél hamarabb kerüljenek megosztásra;
- állítsanak be egyedi jelszavakat, minden online fiókhoz mást;
- használjanak megfelelő vírusvédelmi szoftvert, amelyet tartsanak naprakészen.

A modern biztonsági megoldások megakadályozzák a rosszindulatú linkek elérését, a telepítés előtt blokkolják a rosszindulatú szoftvereket, és értesítik a felhasználókat, ha rosszindulatú tartalmakat kapnak.

A vállalatok számára kihívást jelent olyan közös szabályrendszer kiadása, amely minden infrastruktúrára azonos módon vonatkozik. Van azonban néhány olyan intézkedés, amelyet az adott cég IT biztonsági szakemberei azonnal alkalmazhatnak:

- ellenőrizzék a belső rendszereket és a vállalat által kiadott eszközöket, majd győződjenek meg arról, hogy a legújabb biztonsági frissítések telepítésre kerültek;
- tartsák naprakészen a zero-day sérülékenységeket tartalmazó listájukat, hiszen a kritikus sebezhetőségeket mindig hatásos fegyverként vethetik be a támadók;
- tartsanak rendszeresen IT biztonsági tudatosító képzéseket, előadásokat a munkavállalók számára;
- győződjenek meg arról, hogy minden alkalmazott tisztában van a cég biztonsági szabályaival (pl. VPN használata, a munkaeszköz kizárólag munkavégzésre való használata stb.)
- végezzék el a hálózati infrastruktúra gyors auditját azért, hogy megbizonyosodjanak arról, hogy nincsenek felesleges nyitott portok;
- korlátozzák a távoli asztali kapcsolatok használatát (hacsak nem feltétlenül szükséges).

Minden olyan magyar cégnek és intézménynek, amelyik orosz technológiáját a kialakult helyzetben európaira cserélné, a Bitdefender ingyen vagy igen jelentős árengedménnyel biztosít alternatívát.