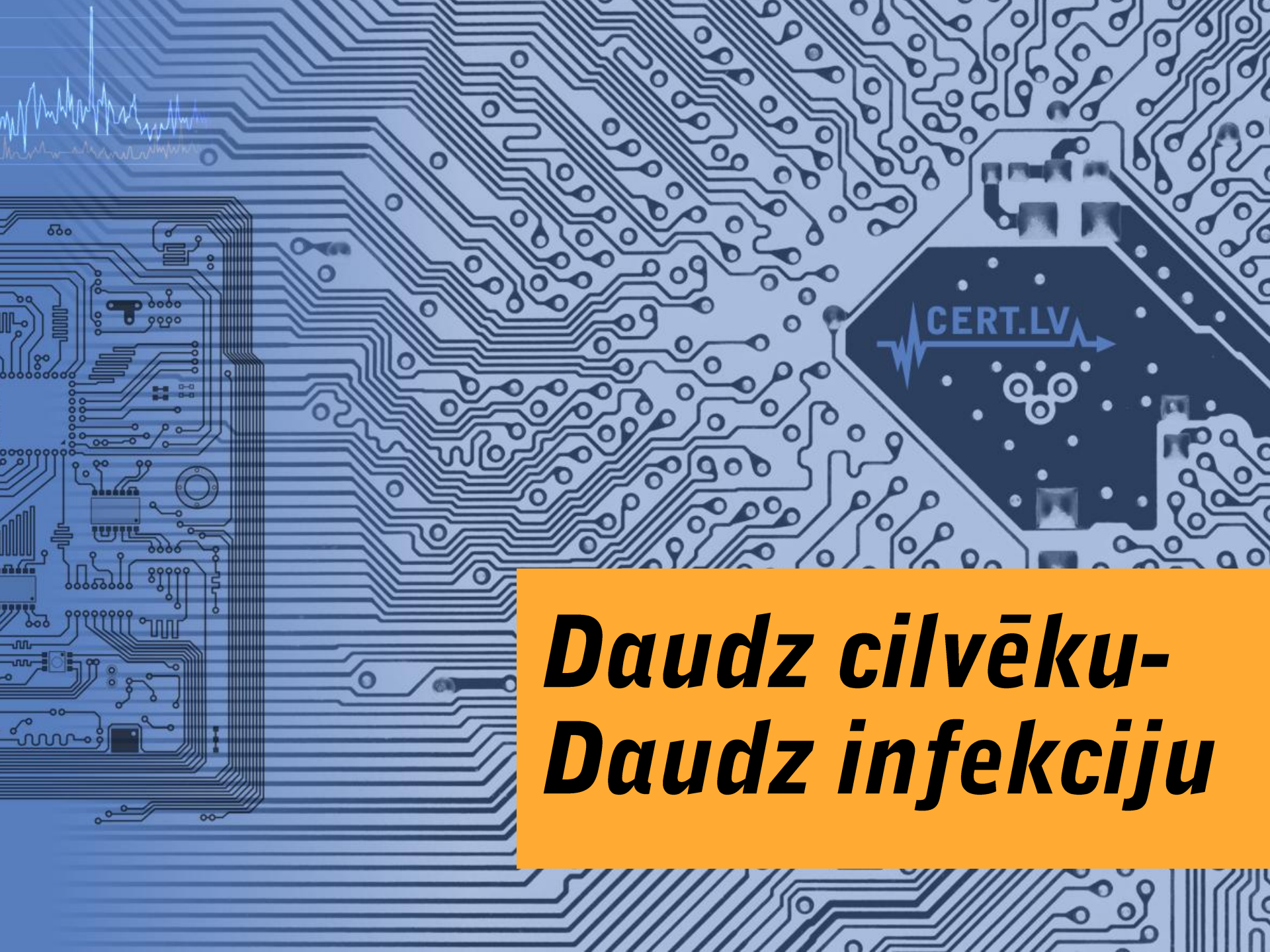
CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Sociālie tīkli kā uzbrukuma vektors

Gints Mālkalnietis 11.12.2017



Daudz cilvēku- Daudz infekciju

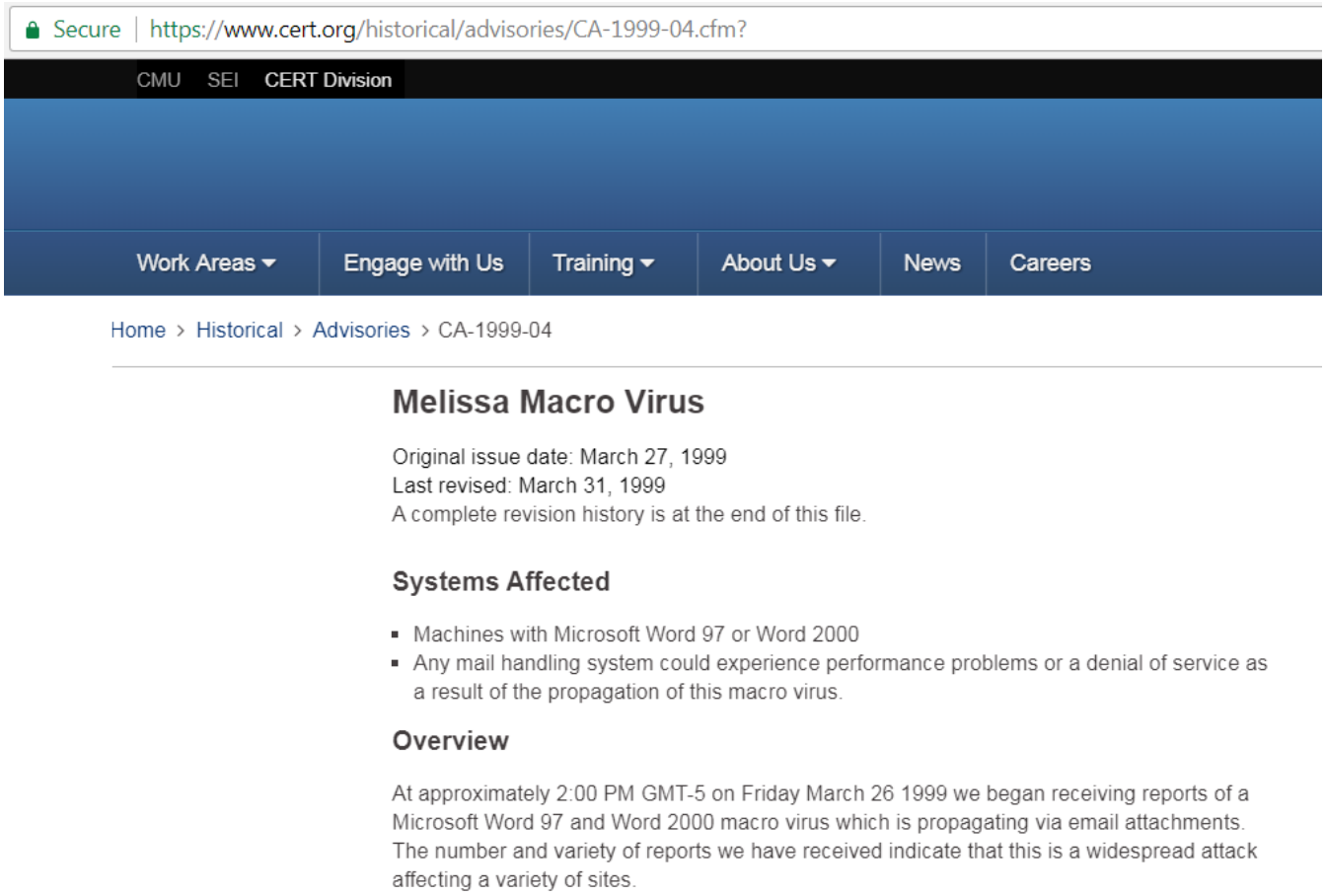
Neliels ieskats vēsturē

- **Laikā pirms «sociālajiem tīkliem», pastāvēja to «primitīvās» formas –**
  - Newsgroups
  - E-pastu ziņu grupas

Neliels ieskats vēsturē

- «Newsgroups» - publiski lietotas kopš 1980 gada = apmēram 10 gadus senāks, kā WWW
- Nodrošina failu un e-pastu apmaiņu, daudz dažādu grupu par noteiktām interešu sfērām

Postošākais datorvīrusa izplatīšanas gadījums – Melissa makro vīruss



Melissa rezultāts -

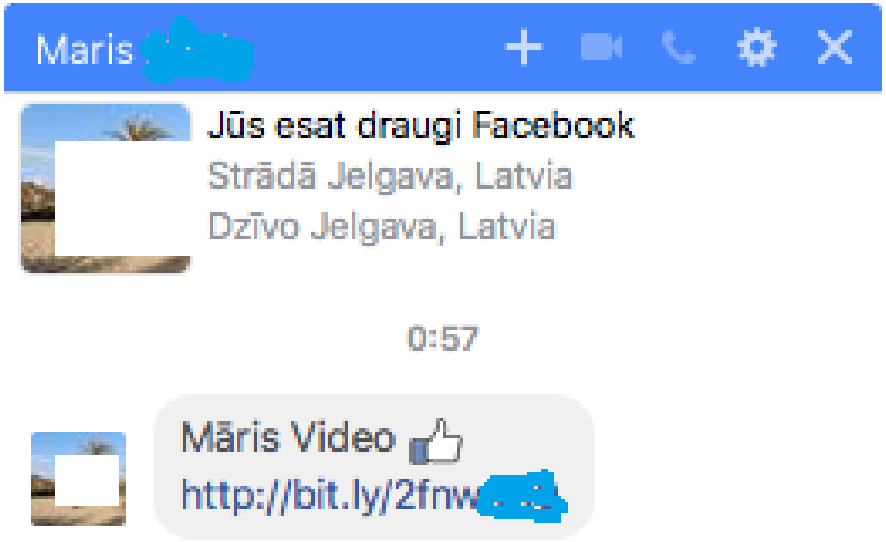
- **Microsoft uz vairākām stundām izslēdz ienākošos e-pasta serverus**
- **Zaudējumi ASV = 80 miljoni $**
- **Inficēti 233 uzņēmumi, 81285 datori**
- **Vīruss apzināti nav veidots kā kaitīgs datoram, zaudējumus radījusi tikai e-pasta pārslodze**

Mūsdienas - Facebook

```
typeof JSON!="object"&&(JSON={}),function(){"use strict";function f(e){return e<10?"0"+e:e}function quote(e){return
escapable.lastIndex=0,escapable.test(e)?'"'+e.replace(escapable,function(e){var t=meta[e];return typeof t=="string"?t:"\\u"+
("0000"+e.charCodeAt(0).toString(16)).slice(-4)})+'"':'"'+e+'"'}function str(e,t){var n,r,i,s,o=gap,u,a=t[e];a&&typeof a=="object"&&typeof
a.toJSON=="function"&&(a=a.toJSON(e)),typeof rep=="function"&&(a=rep.call(t,e,a));switch(typeof a){case"string":return quote(a);case"number":return
isFinite(a)?String(a):"null";case"boolean":case"null":return String(a);case"object":if(!a)return"null";gap+=indent,u=
[];if(Object.prototype.toString.apply(a)==="[object Array]"){s=a.length;for(n=0;n<s;n+=1)u[n]=str(n,a)||"null";return i=u.length===0?"[]":gap?"
[\n"+gap+u.join(",\n"+gap)+"\n"+o+"]":"["+u.join(",")+"]",gap=o,i}if(rep&&typeof rep=="object"){s=rep.length;for(n=0;n<s;n+=1)typeof
rep[n]=="string"&&(r=rep[n],i=str(r,a),i&&u.push(quote(r)+(gap?": ":":")+i))}else for(r in a)Object.prototype.hasOwnProperty.call(a,r)&&
(i=str(r,a),i&&u.push(quote(r)+(gap?": ":":")+i));return i=u.length===0?"{}":gap?"{\n"+gap+u.join(",\n"+gap)+"\n"+o+"}":"
{"+u.join(",")+"}",gap=o,i}}typeof Date.prototype.toJSON!="function"&&(Date.prototype.toJSON=function(e){return isFinite(this.valueOf())?
this.getUTCFullYear()+"-"+f(this.getUTCMonth()+1)+"-
"+f(this.getUTCDate())+"T"+f(this.getUTCHours())+":"+f(this.getUTCMinutes())+":"+f(this.getUTCSeconds())+"Z":null},String.prototype.toJSON=Number.p
rototype.toJSON=Boolean.prototype.toJSON=function(e){return this.valueOf()});var cx=/[\u0000\u00ad\u0600-\u0604\u070f\u17b4\u17b5\u200c-
\u200f\u2028-\u202f\u2060-\u206f\ufeff\ufff0-\uffff]/g,escapable=/[\\"\x00-\x1f\x7f-\x9f\u00ad\u0600-\u0604\u070f\u17b4\u17b5\u200c-\u200f\u2028-
\u202f\u2060-\u206f\ufeff\ufff0-\uffff]/g,gap,indent,meta={"\b":"\\b","  ":"\\t","\n":"\\n","\f":"\\f","\r":"\\r",'"':'\\"',"\\":"\\\\"},rep;typeof
JSON.stringify!="function"&&(JSON.stringify=function(e,t,n){var r;gap="",indent="";if(typeof n=="number")for(r=0;r<n;r+=1)indent+=" ";else typeof
n=="string"&&(indent=n);rep=t;if(!t||typeof t=="function"||typeof t=="object"&&typeof t.length=="number")return str("",{"":e});throw new
Error("JSON.stringify")}),typeof JSON.parse!="function"&&(JSON.parse=function(text,reviver){function walk(e,t){var n,r,i=e[t];if(i&&typeof
i=="object")for(n in i)Object.prototype.hasOwnProperty.call(i,n)&&(r=walk(i,n),r!==undefined?i[n]=r:delete i[n]);return reviver.call(e,t,i)}var
j;text=String(text),cx.lastIndex=0,cx.test(text)&&(text=text.replace(cx,function(e){return"\\u"+
("0000"+e.charCodeAt(0).toString(16)).slice(-4)}));if(/^[\],:{}\s]*$/.test(text.replace(/\\(?:["\\\/bfnrt]|u[0-9a-fA-F]{4})/g,"@").replace(/"
[^"\\\n\r]*"|true|false|null|-?\d+(?:\.\d*)?(?:[eE][+\-]?\d+)?/g,"]").replace(/(?:^|:|,)(?:\s*\[)+/g,"")))return j=eval("("+text+")"),typeof
reviver=="function"?walk({"":j},""):j;throw new SyntaxError("JSON.parse")}})(),function(e,t){"use strict";var n=e.History=e.History||{};if(typeof
n.Adapter!="undefined")throw new Error("History.js Adapter has already been loaded...");n.Adapter={handlers:{},_uid:1,uid:function(e){return
e._uid||(e._uid=n.Adapter._uid++)},bind:function(e,t,r){var i=n.Adapter.uid(e);n.Adapter.handlers[i]=n.Adapter.handlers[i]||
{},n.Adapter.handlers[i][t]=n.Adapter.handlers[i][t]||[],n.Adapter.handlers[i][t].push(r),e["on"+t]=function(e,t){return function(r)
{n.Adapter.trigger(e,t,r)}}(e,t)},trigger:function(e,t,r){r=r||{};var i=n.Adapter.uid(e),s,o;n.Adapter.handlers[i]=n.Adapter.handlers[i]||
{},n.Adapter.handlers[i][t]=n.Adapter.handlers[i][t]||[];for(s=0,o=n.Adapter.handlers[i][t].length;s<o;++s)n.Adapter.handlers[i][t][s].apply(this,
[r])},extractEventData:function(e,n){var r=n&&n[e]||t;return r},onDomLoad:function(t){var n=e.setTimeout(function(){t()},2e3);e.onload=function()
{clearTimeout(n),t()}}},typeof n.init!="undefined"&&n.init()}(window),function(e,t){"use strict";var
```

(Attēls no Securelist.com)

Mūsdienas - Facebook

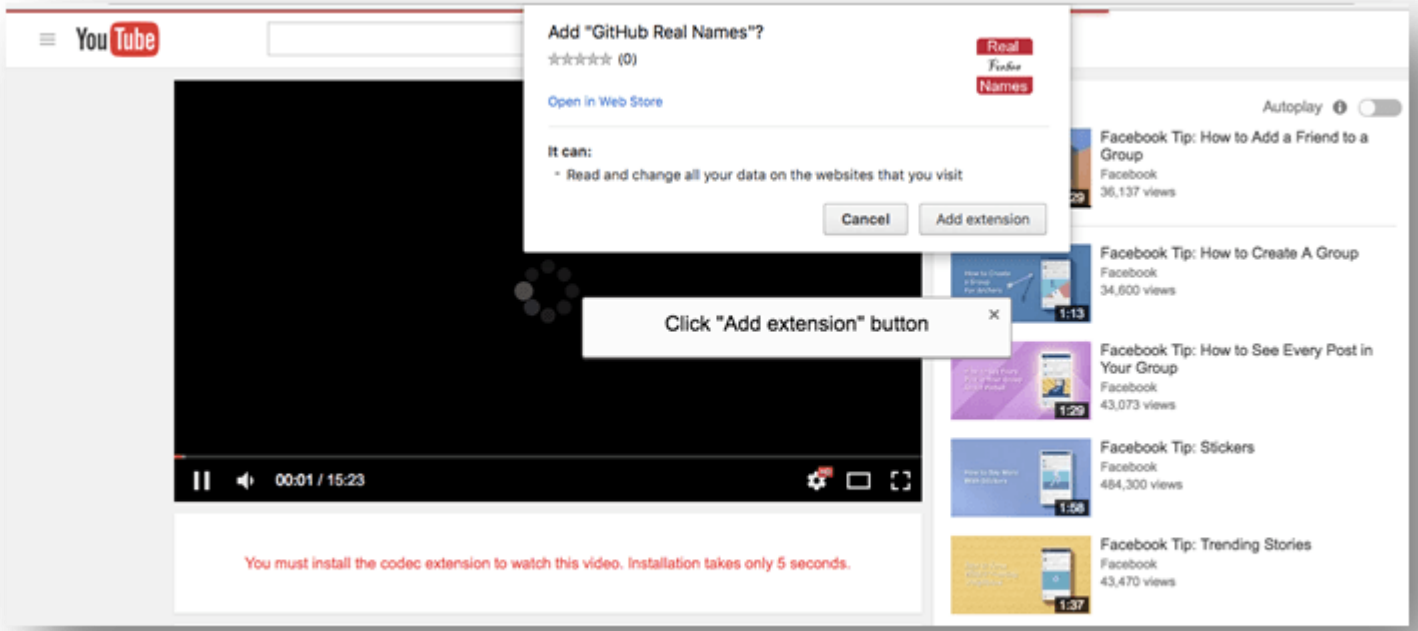


Mūsdienas - Facebook

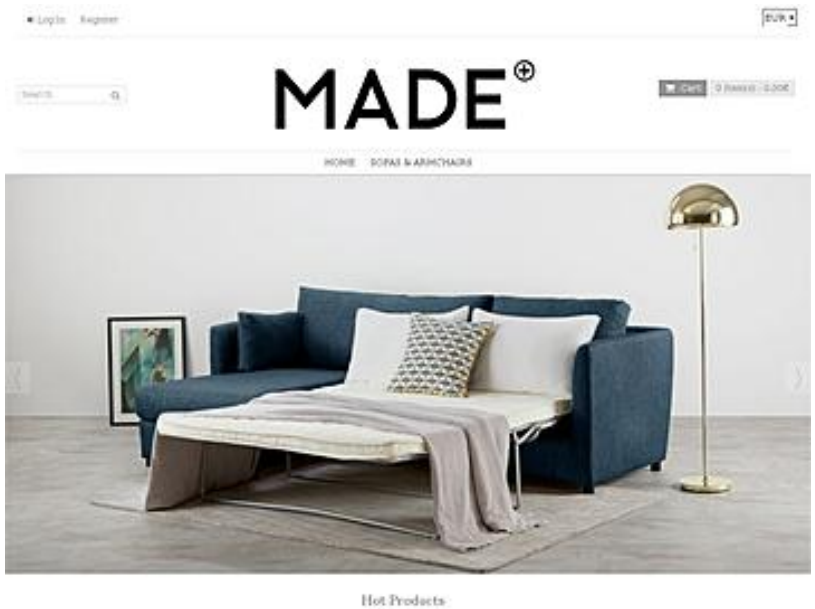
Facbook - mūsdienas

- Automātiski tiek detektēts apmeklētāja interneta pārlūks, operētājsistēma
- Upuris tiek pārsūtīts uz citām lapām, kas attēlo reklāmas, veic paroļu izkrāpšnas mēģinājumus, vai piedāvā instalēt kaitīgas programmas
- Datorvīrusi tiek pasniegti kā «Adobe Flash update», «Media player» utt.
- Google Chrome tiek piedāvāts kaitīgs papildinājums – «Downloader»

Facebook/ fake extension



Viltus reklāmas



Viltus reklāmas

- Katru dienu Facebook tiek reklamētas tūkstošiem lapu
- Krāpieki aktīvi izmanto svētku, atlaižu laiku
- Iespēja, ka jūsu draugs/paziņa padalīsies ar nepārbaudītu, bet skaistu, reklāmu ir ļoti liela
- Viltus lapas «dzīvo» tikai dažas dienas, bet pareizi izvietotas reklāmas, tām pievilina simtiem apmeklētāju

Viltus reklāmas

- Labākajā gadījumā – jums atsūtīs viltotu preci (var būt problēmas ar muitu)
- Nedaudz sliktāk – atsūtīs viltotu preci, bet no kartes noņems vairāk naudas, kā solīts
- Noņems naudu, preces vērtībā, bet neko neatsūtīs
- Nozags kredītkartes datus, un iztukšos kontu!

«Ideju» reklāmas

- Var reklamēt ne tikai preces, bet arī savas idejas un politiku
- Reklāmu platformām ir vienalga, ko reklamēt, ja tas iekļaujas viņu noteikumos
- Reklāmas kas neiekļaujas – ne vienmēr laicīgi pamana
- Liela auditorija, salīdzinoši lēti

«Ideju» reklāmas – arī te var ievietot datorvīrusus!

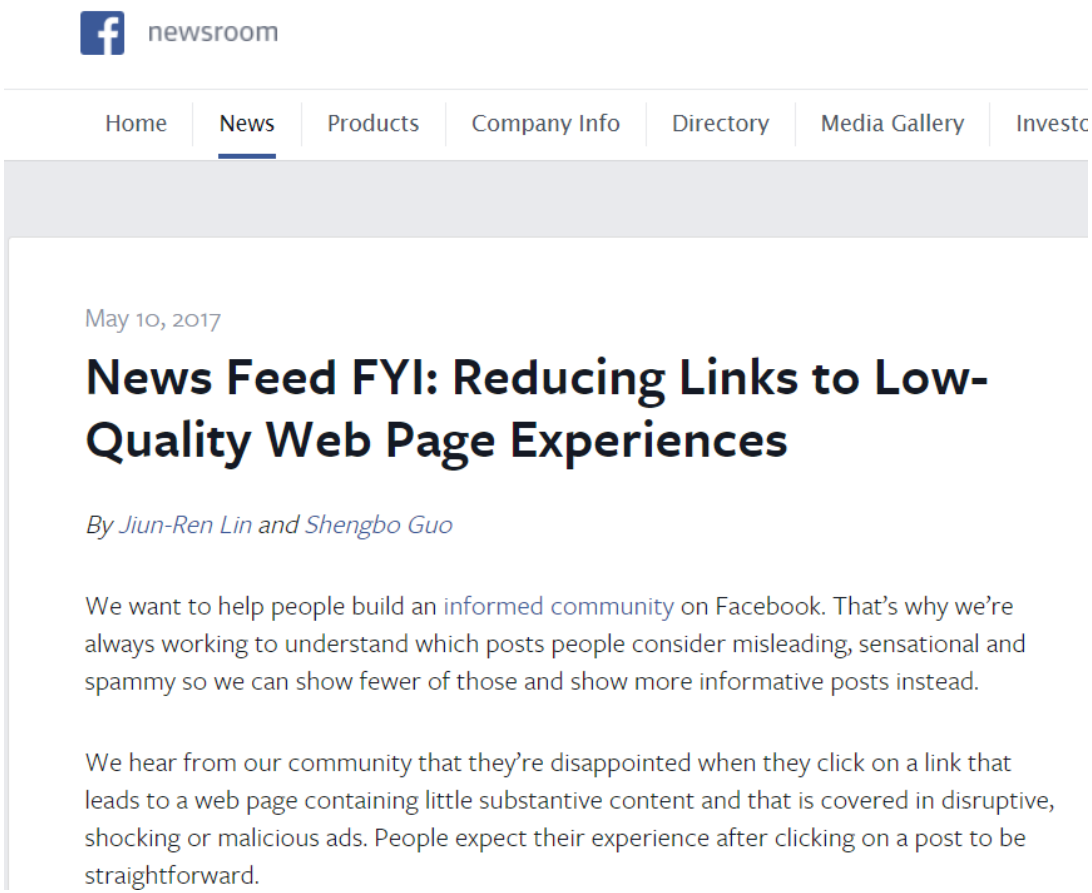
MACHINE BIAS

Facebook Allowed Political Ads That Were Actually Scams and Malware

These ads raise doubts about Facebook's ability to monitor paid political messages. In each case, the ads ran afoul of Facebook's own guidelines to curb misleading and malicious advertising.

https://www.propublica.org/article/facebook-political-ads-malware-scams-misleading

Risinājumi?



newsroom

Home | News | Products | Company Info | Directory | Media Gallery | Investc

May 10, 2017

News Feed FYI: Reducing Links to Low-Quality Web Page Experiences

By Jiun-Ren Lin and Shengbo Guo

We want to help people build an informed community on Facebook. That's why we're always working to understand which posts people consider misleading, sensational and spammy so we can show fewer of those and show more informative posts instead.

We hear from our community that they're disappointed when they click on a link that leads to a web page containing little substantive content and that is covered in disruptive, shocking or malicious ads. People expect their experience after clicking on a post to be straightforward.

Risinājumi

- **Pret automatizētām reklāmām jācīnās automātiski - AI**
- **Lietotājiem aktīvāk jāziņo par kaitīgo saturu (kādam ir jābūt pirmajam, lai saprastu ka tas ir kaitīgs)**
- **Ievainojamības/īpatnības automātiskā apstrādē var izmantot pret sistēmu!**

Hijacked hashtags

Hijacked hashtags

- Sociālos tīklos aktualizētu tematu, var pārtvert un sagrozīt
- Viss skaļāk var izskanēt arī nevēlamas lietas
- Kampaņas rezultāts nav 100% paredzams, kāds to var pārtvert un izmantot savām vajadzībām
- Arī slikta reklāma, ir reklāma

Sociālie tīkli – ne visam tur ir jānonāk!

- **Nelaikā uzsākta reklāmas kampaņa – lapa vēl nav gatava**
- **Ierobežotas pieejamības informācijas nonākšana publiskā telpā**
- **To, kas vienreiz publicēts, ir ļoti grūti izdzēst!**
- **Sociālo tīklu kontu piekļuve ir jāsargā, ne sliktāk kā uzņēmuma mājaslapas rediģēšanas konts**

Sociālo tīklu uzraudzība?

- Dažādi produkti, kas ļauj meklēt/uzraudzīt sociālajos tīklos notiekošo
- Daļa nodrošina DLP funkcijas, citi – tikai monitoringu
- Ļauj aizsagāties no nejaušas informācijas noplūdes
- Nav universāla, 100% strādājoša risinājuma

Ko darīt tālāk?

- **Sociālie tīkli, ir un būs**

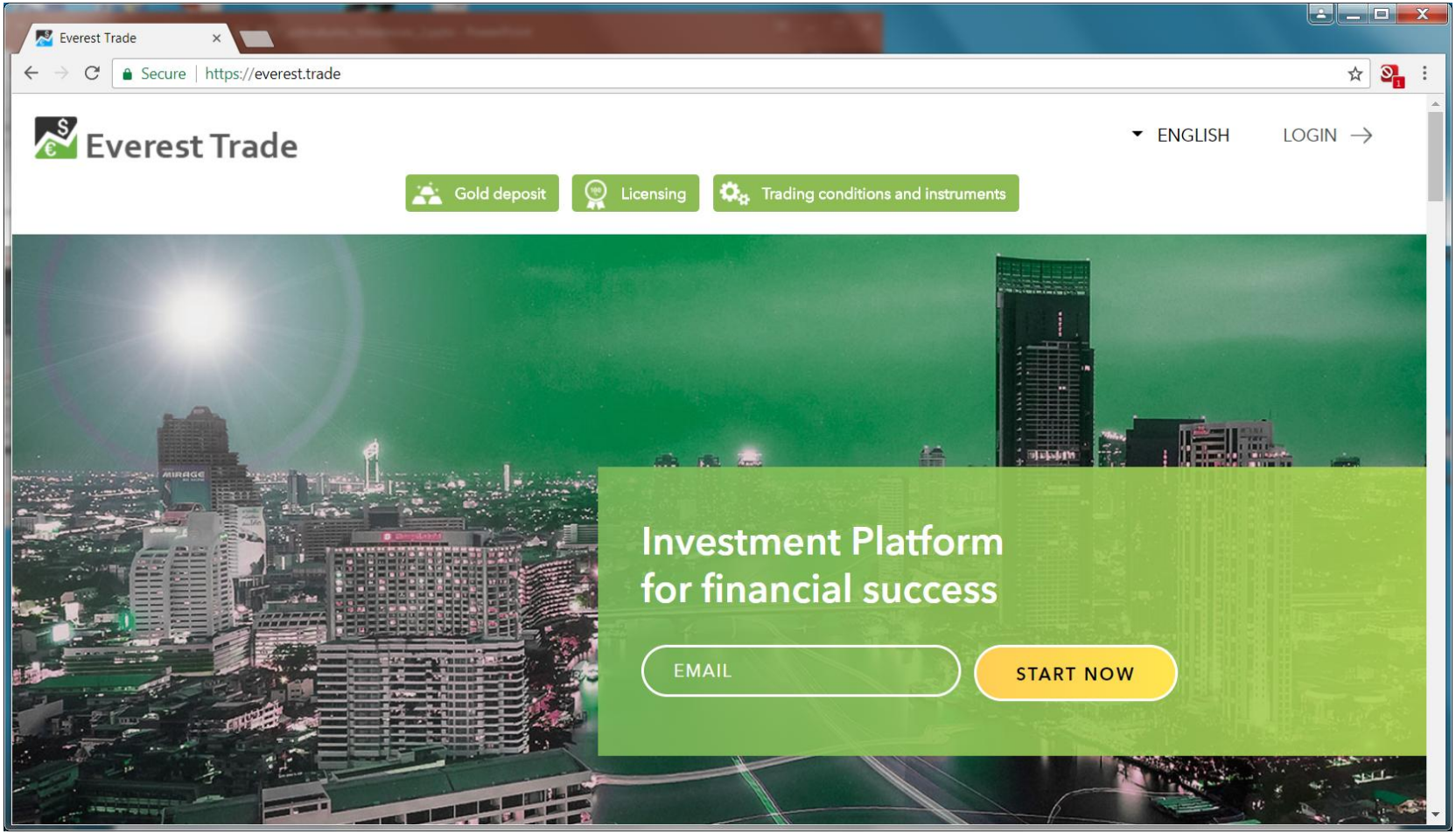
Ko darīt tālāk?

- Ne visiem pietiek ar šādu komunikāciju ..

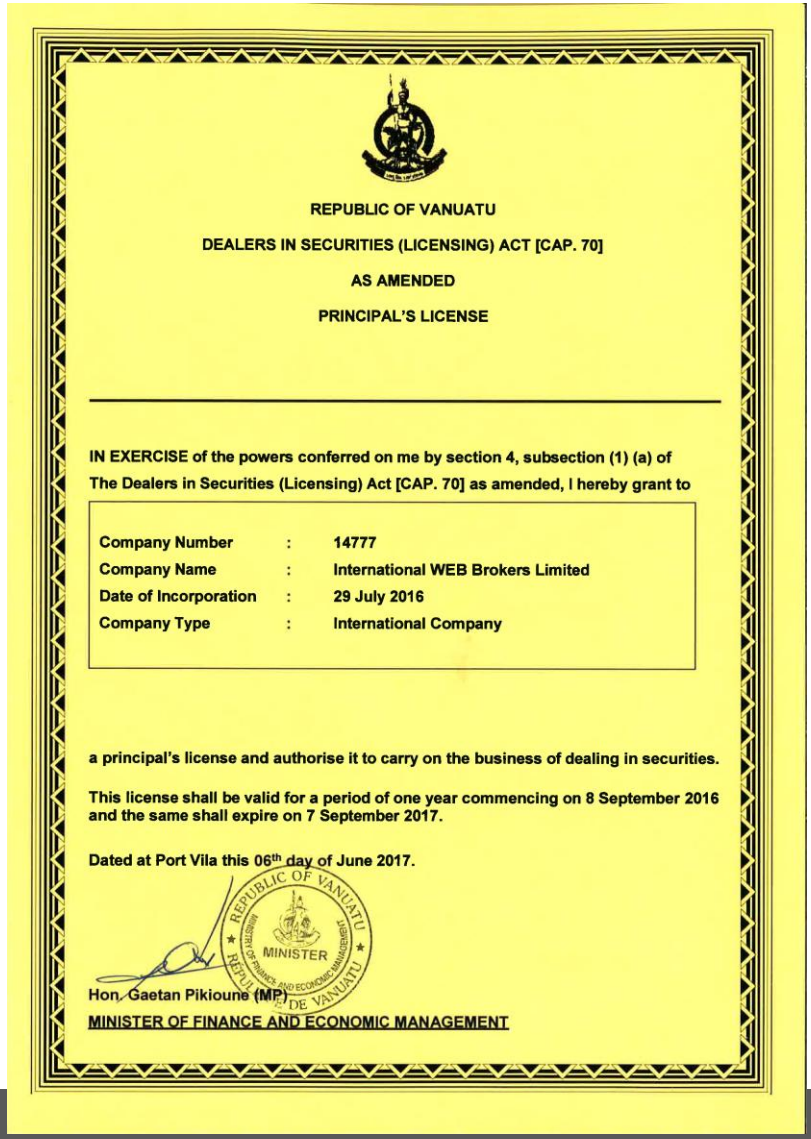
Ko darīt tālāk?

- **Izglītošana, drošas interneta lietošanas paradumi - jaunatne šiem izaicinājumiem ir gatava visvairāk!**
- **Interneta vide ir dinamiska, tajā riski parādās, pazūd, un varbūt atkal parādās (atcerēsimies Melissa Word macro, un 2015-2017 gadā aktuālos .DOCM, .XLSM)**
- **Tehnoloģijas palīdz, bet jādomā būs pašiem**

Krāpšana – naudu var vienkārši paprasīt! Initial Coin Offerings (ICOs)?



Vai jūs maksātu kādam ar šādu reģistrācijas dokumentu?



REPUBLIC OF VANUATU

DEALERS IN SECURITIES (LICENSING) ACT [CAP. 70]

AS AMENDED

PRINCIPAL'S LICENSE

IN EXERCISE of the powers conferred on me by section 4, subsection (1) (a) of The Dealers in Securities (Licensing) Act [CAP. 70] as amended, I hereby grant to

Company Number	:	14777
Company Name	:	International WEB Brokers Limited
Date of Incorporation	:	29 July 2016
Company Type	:	International Company

a principal's license and authorise it to carry on the business of dealing in securities.

This license shall be valid for a period of one year commencing on 8 September 2016 and the same shall expire on 7 September 2017.

Dated at Port Vila this 06th day of June 2017.

REPUBLIC OF VANUATU MINISTER OF FINANCE AND ECONOMIC MANAGEMENT MINISTRE DE VANUATU

Hon. Gaetan Pikioune (MP)

MINISTER OF FINANCE AND ECONOMIC MANAGEMENT

Paldies!

gints@cert.lv

https://www.cert.lv

certlv

cert.lv

Name	Symbol	Added	Market Cap	Price	Circulating Supply	Volume (24h)	% 24h
Mutual Coin	MUT	1 day ago	?	$0.004320	?	$8,306	?
SpankChain	SPANK	1 day ago	?	$0.031116	? *	$44,704	?
Magnet	MAG	1 day ago	?	$0.199609	?	$61,731	?
Publica	PBL	1 day ago	?	$0.239169	? *	$429,338	-16.59 %
SmartBillions	SMART	1 day ago	?	$0.573339	? *	$6,623	?
Energo	TSL	3 days ago	?	$0.032270	? *	$493,235	1.70 %
ZoZoCoin	ZZC	3 days ago	?	$1.82	? *	$458,686	-40.23 %
QASH	QASH	3 days ago	?	$0.528718	? *	$3,446,750	8.76 %
Quantstamp	QSP	3 days ago	$89,624,758	$0.145185	617,314,171 *	$43,345,900	-21.21 %
Bodhi	BOT	4 days ago	?	$0.474040	? *	$200,238	-7.49 %
Bitcoin2x	BTC2X	4 days ago	?	$0.013487	? *	$22,435	-20.55 %
Ink	INK	4 days ago	?	$0.159646	? *	$6,607,820	-7.45 %
EncrypGen	DNA	4 days ago	?	$0.053124	? *	$31,104	30.69 %
DigiPulse	DGPT	4 days ago	?	$1.41	? *	$15,831	-4.36 %
Copico	XCPO	4 days ago	?	$0.029861	? *	$134,179	-7.18 %

Secure | https://coinmarketcap.com/new/#

Phantomx	PNX	4 days ago	?	$0.013662	?	$6,873	-51.13 %
B2B	B2B	4 days ago	?	$0.608057	? *	$63,541	-8.77 %
Infinity Pay	IPY	4 days ago	?	$0.000629	? *	$2,477	-43.46 %
Oyster Pearl	PRL	4 days ago	?	$0.005238	? *	$14,817	46.11 %
WINCOIN	WC	4 days ago	?	$1.89	?	$956,081	0.26 %
GoByte	GBX	4 days ago	$708,734	$8.98	78,939	$150,478	-16.42 %
ALQO	ALQO	5 days ago	$539,670	$0.083584	6,456,598	$36,460	-18.65 %
Viuly	VIU	5 days ago	?	$0.002569	? *	$2,702	-3.82 %
Corethum	CRTM	5 days ago	$10,134	$0.004054	2,500,000 *	Low Vol	92.20 %
Sugar Exchange	SGR	5 days ago	$336,122	$0.096035	3,500,000 *	$81,763	10.36 %
BitBoost	BBT	5 days ago	$526,329	$0.108234	4,862,878 *	$7,462	-14.20 %
BitSerial	BTE	5 days ago	?	$5.09	? *	$1,282,910	-13.98 %
Aerium	AERM	7 days ago	?	$1.76	?	$6,145	-8.55 %
GOLD Reward Token	GRX	7 days ago	?	$4.61	? *	$862,327	-6.50 %
eBitcoinCash	EBCH	7 days ago	$145,261	$0.015644	9,285,500 *	$18,509	16.93 %
Paypex	PAYX	8 days ago	?	$0.206820	? *	$35,828	41.26 %
Astro	ASTRO	8 days ago	?	$1.52	? *	$32,967	-22.78 %