



Apple iOSにおける ヒヤリ・ハット事象

Noriaki HAYASHI
Senior Researcher

Forward-looking Threat Research

日本スマートフォンセキュリティ協会（JSSEC）技術部会主催
「2013年のスマートフォンの脅威と2014年の脅威予測」カンファレンス
2013.11.28 (THU)

Introduction



林 憲明

Forward-looking **T**hreat **R**esearch

研究領域キーワード: スマートフォン、ソフトウェア無線
Internet of Things、車載機器、オンライン詐欺

大学卒業後、2002年トレンドマイクロ入社。国内専門のウイルス解析機関である「リージョナルトレンドラボ」を経て、2010年に新設されたグローバルの最先端脅威研究組織である「フォワードルッキングスレトリサーチ」へ異動。現在に至る。



技術部△ ネットワークWG
技術部△ アプリケーションWG



トレンドマイクロ株式会社
シニアリサーチャー

三つ巴の戦いが開幕



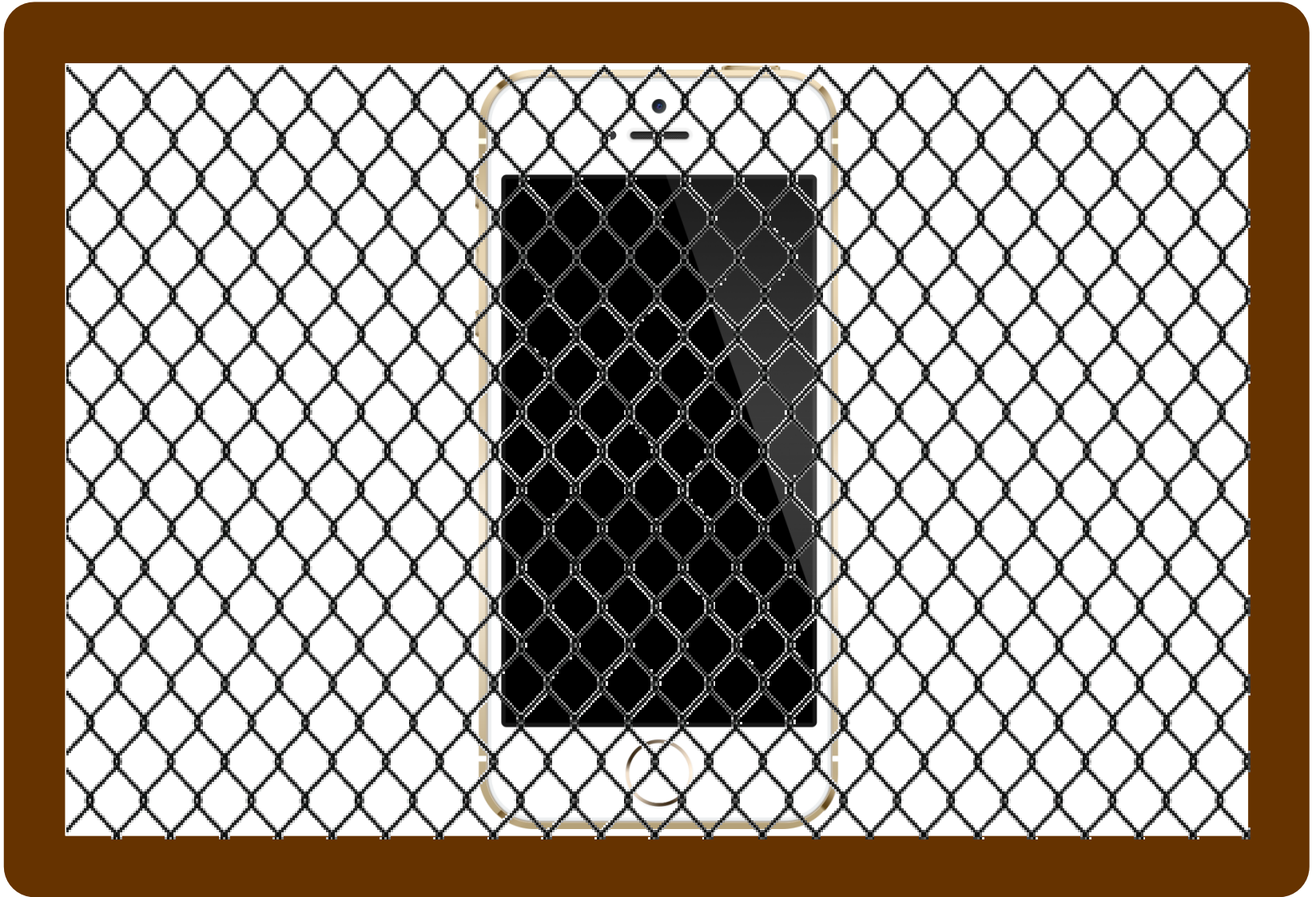
SoftBank



au

NTT
docomo

籠の中の鳥, App Storeの厳格審査



App Store におけるヒヤリ・ハット



App Store におけるヒヤリ・ハット

Happy Block

~Cute animals can make you happy~



2013年4月24日
App Storeで配布
期間限定で無料の
煽り広告入り

[ジャンル:アーケード - ゲーム, パズル]
実際は出会い系誘導

App Store におけるヒヤリ・ハット

Happy Block

~Cute animals can make you happy~



Happy Block ~Cute animals can make you happy~ [App]

Store Price Compatibility Publisher Status Unified App App Franchise
iOS Store Free iPhone, iPod touch Mamoru Saitou Removed from store N/A N/A

Rank History

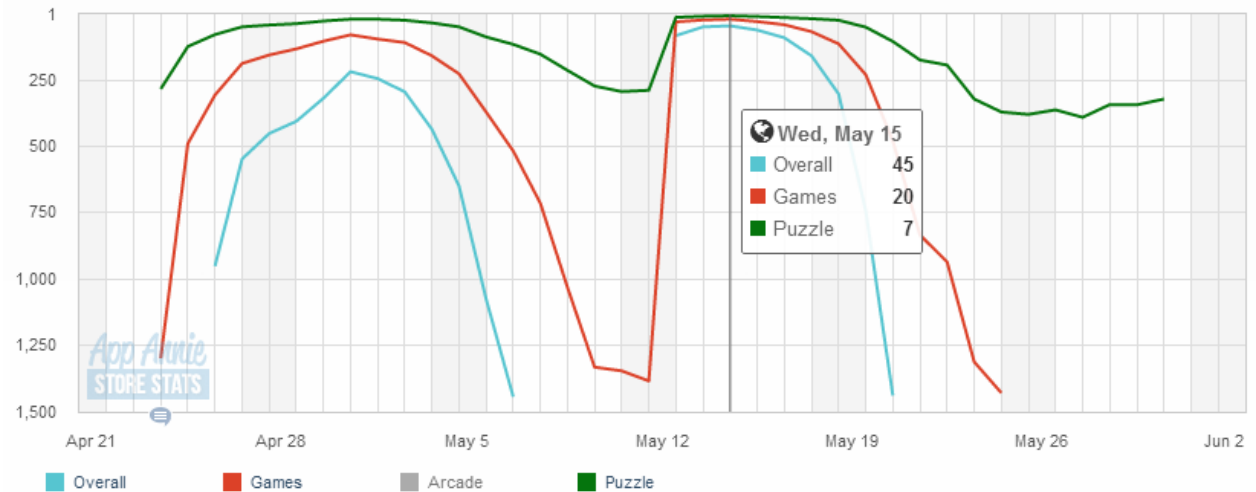
Japan - Apr 21, 2013 ~ Jun 3, 2013

Country: Japan Date Range: Apr 21, 2013 ~ Jun 3, 2013

Download Ranks

Scale

Day Hour



App Store におけるヒヤリ・ハット

プライバシー問題に注意

JavaScript によるヒヤリ・ハット



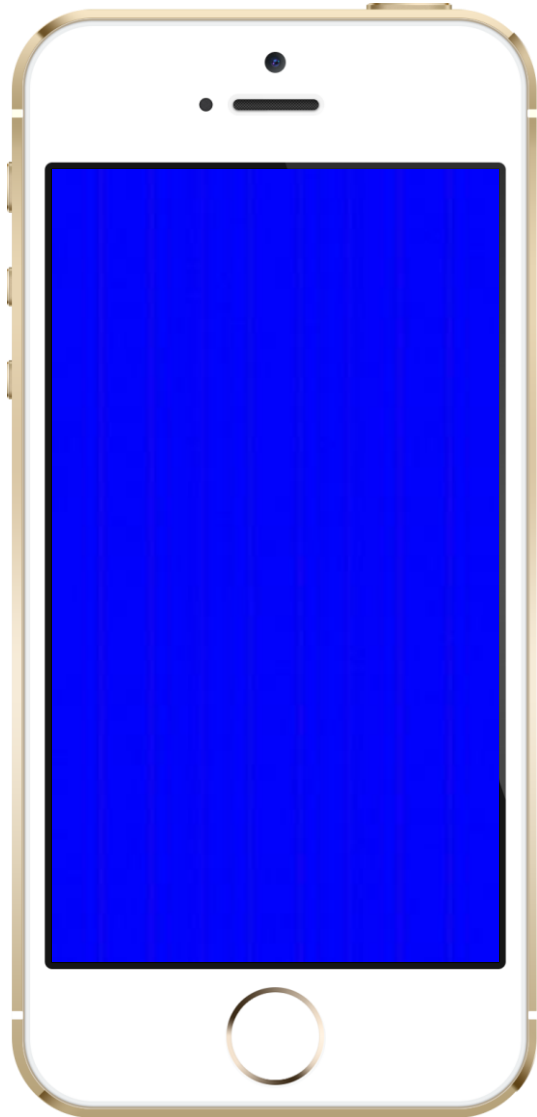
2013年3月7日頃～
Twitter で拡散ピーク

JavaScriptを使った
無限ループ：ブラクラ

ウイルス供用罪の
可能性？

非常に悪質な行為

BSOD!?!? によるヒヤリ・ハット



2013年11月6日頃～
Twitter で拡散ピーク

破損ファイルを使った
いたずら

内部処理の
エラー

破損ファイルで BSOD!?



MacOSXの標準
QuickTime
再生可能

ADDRESS	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
000C7C00	D9	13	04	FD	A8	85	F7	DA	AC	14	69	C6	2B	C2	59	F6	...
000C7C01	3F	49	52	5F	BC	68	FC	80	97	72	27	DC	56	23	ED	83	...
000C7C02	E8	35	C3	D5	09	77	80	3B	85	83	40	0C	20	60	0A	...	
000C7C03	00	74	08	00	01	22	06	01	10	0B	89	00	50	09	B1	09	...
000C7C04	04	48	42	11	10	54	22	32	08	ED	9F	55	CD	EF	8D	7E	...
000C7C05	7F	E7	33	7E	3C	89	EB	37	ED	C5	3C	7B	48	EF	DE	5C	...
000C7C06	FC	77	F9	07	FA	65	C1	22	B4	A3	62	2B	4A	4A	51	...	
000C7C07	A3	8E	11	27	48	C1	48	8C	12	83	90	42	44	0A	94	...	
000C7C08	E2	00	1A	0C	20	10	22	00	05	2A	01	00	00	08	0A	88	...
000C7C09	00	22	00	92	00	12	02	0E	11	02	6A	21	0A	CF	FF	...	
000C7C0A	FF	FF	FF	FF	B0	71	28	48	28	25	10	08	S2	A1	20	A8	...
000C7C0B	50	2E	15	08	88	C2	41	50	89	8E	75	6B	80	7C	EF	...	
000C7C0C	E3	BF	8F	5E	DC	F3	F1	77	EB	78	75	9E	79	D5	4D	63	...
000C7C0D	53	9E	B2	F8	E0	0F	00	3E	D0	DE	16	CC	EC	E8	17	...	
000C7C0E	7E	A3	57	25	FD	F5	A6	5F	F5	EF	FD	F6	29	8E	CF	D1	...
000C7C0F	DA	1F	F3	5C	2C	86	F7	BF	19	08	BF	92	1E	61	FD	...	
000C7C10	2C	6D	C5	00	00	00	00	00	00	00	00	00	00	00	00	00	...
000C7C11	00	80	00	00	00	29	70	02	44	81	70	5C	08	08	00	00	...
000C7C12	48	00	00	00	81	32	A2	10	90	45	A6	11	C8	1C	66	...	
000C7C13	EF	3F	3F	EF	FF	4F	8D	7E	7E	BF	5F	5A	D7	F5	...		
000C7C14	FE	73	08	FC	F2	FE	25	5F	1F	8E	3F	ED	7F	E4	F2	...	
000C7C15	1C	79	2E	F4	E3	2A	5A	32	A3	34	6C	D7	1B	46	9A	9D	...
000C7C16	02	E8	31	8F	DA	25	5A	6C	5C	A8	94	57	26	88	4E	F0	...
000C7C17	01	30	88	00	14	4A	0A	80	19	80	08	AC	00	89	22	40	...
000C7C18	04	00	A8	20	00	0B	14	03	80	00	00	2B	3A	6D	6F	6F	...
000C7C19	76	00	00	00	6C	8D	76	68	64	00	00	00	7C	25	FD	...	
000C7C1A	D8	7C	25	FD	D8	00	01	5F	90	00	1C	4A	30	00	01	00	...
000C7C1B	00	01	00	00	00	00	00	00	00	00	00	00	00	00	01	00	...
000C7C1C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	...
000C7C1D	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	...
000C7C1E	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	...
000C7C1F	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	...
000C7C20	6C	74	72	61	6B	00	00	00	5C	74	6B	68	64	00	00	00	...
000C7C21	0F	7C	25	FD	D8	7C	25	FD	D8	00	00	00	00	01	00	00	...
000C7C22	00	00	1C	4A	30	00	00	00	00	00	00	00	00	00	00	00	...
000C7C23	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00	...
000C7C24	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00	...
000C7C25	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	...
000C7C26	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	...
000C7C27	64	00	00	00	00	7C	25	FD	D8	7C	25	FD	D8	00	01	5F	...
000C7C28	90	00	1C	4A	30	00	00	00	00	00	00	00	2D	68	64	6C	...
000C7C29	72	00	00	00	00	6D	68	6C	72	76	69	64	65	00	00	00	...
000C7C2A	00	00	00	00	00	00	00	00	00	0C	56	69	64	65	6F	48	...
000C7C2B	61	6E	64	6C	65	72	00	00	0B	B3	6D	69	6E	68	00	00	...
000C7C2C	00	14	76	6D	68	64	00	00	00	01	00	00	00	00	00	00	...

破損ファイル

再生可能

ブラウザに関するヒヤリ・ハット

ブラウザ経由の 不正コード実行に注意

参考情報：Keen Team exploits Safari for mobile browser category

<http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/Keen-Team-exploits-Safari-for-mobile-browser-category/ba-p/6267341>

フィッシング詐欺にヒヤリ・ハット

最終確認時刻：

2013年11月27日 21:39

URL: [http://www.alt\[redacted\].c.fr/includes/js/Apple/MyAppleId.woa%20wadiirectToSignInlocalang%253Den_US.html](http://www.alt[redacted].c.fr/includes/js/Apple/MyAppleId.woa%20wadiirectToSignInlocalang%253Den_US.html)



URL: [http://www.alt\[redacted\].c.fr/includes/js/Apple/MyAppleId.woa%20wadiirectToSignInlocalang%3Den_](http://www.alt[redacted].c.fr/includes/js/Apple/MyAppleId.woa%20wadiirectToSignInlocalang%3Den_)

Detection ratio: 2 / 51

Analysis date: 2013-11-27 12:39:16 UTC (0 minutes ago)



フィッシング詐欺にヒヤリ・ハット

最終確認時刻：

2013年11月27日 21:39

URL: [http://www.alt\[redacted\].c.fr/includes/js/Apple/MyAppleId.woawadirectToSignInlocalang%253Den_US.html](http://www.alt[redacted].c.fr/includes/js/Apple/MyAppleId.woawadirectToSignInlocalang%253Den_US.html)

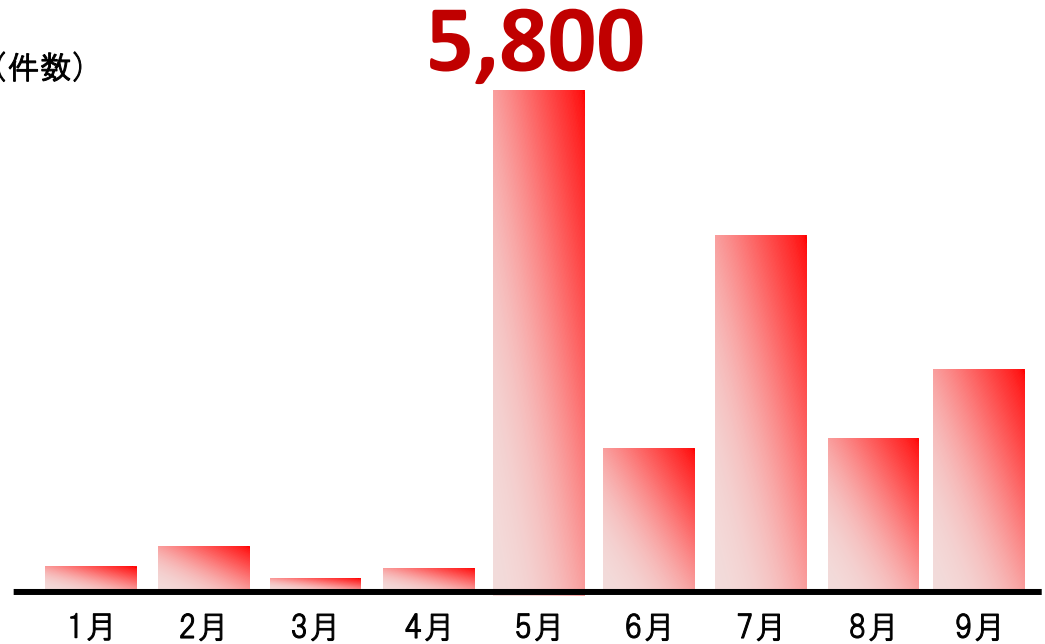


**AppleIDを狙った
フィッシング詐欺サイト
急増中**

フィッシング詐欺にヒヤリ・ハット



(件数)



2013年度 AppleID フィッシング件数

モバイル特有の
真偽判断の難しさ

フィッシング詐欺にヒヤリ・ハット

脆弱なパスワードの
使用に注意

Conclusion

- アプリのプライバシー問題に注意
 - ✓ アプリの利用許諾契約を読み飛ばさない
- ブラウザ経由の不正コード実行に注意
 - ✓ ソーシャルメディア内のリンクに要注意
- 脆弱なパスワードの使用に注意
 - ✓ PCと同等のパスワードポリシーを採用

むずかしいを、なくそう



Webレピュテーション
セキュアブラウザ
Smart Surfing
for iPhone and iPod
touch **無料**

5つまでのIDとパスワード
期間無制限で管理
PasswordManager 無料



Thank You!





TREND
MICRO™

講演者に対するお問い合わせは
noriaki_hayashi@trendmicro.co.jp

PasswordManager™ 無料版
5つまでのIDとパスワードを期間制限なし
にご利用いただけます。

<http://safe.trendmicro.jp/purchase/pm/trialthanks.aspx>

Smart Surfing for iPhone OS

<http://safe.trendmicro.jp/products/ssfi.aspx>

PasswordManager™



Smart Surfing
for iPhone OS



iOS で不正プログラムを確認か

<http://blog.trendmicro.co.jp/archives/5595>

Twitter上でブラクラURLを含む投稿の拡散を確認、iPhoneでも被害

<http://blog.trendmicro.co.jp/archives/6916>

iPhone を強制再起動させる動画ファイルの URL が Twitter などで拡散中

<http://blog.trendmicro.co.jp/archives/8114>