INTHEWILD

The Current State of Cybercrime

Berk Veral, Sr Product Marketing Manager
RSA, The Security Division of EMC

RSA

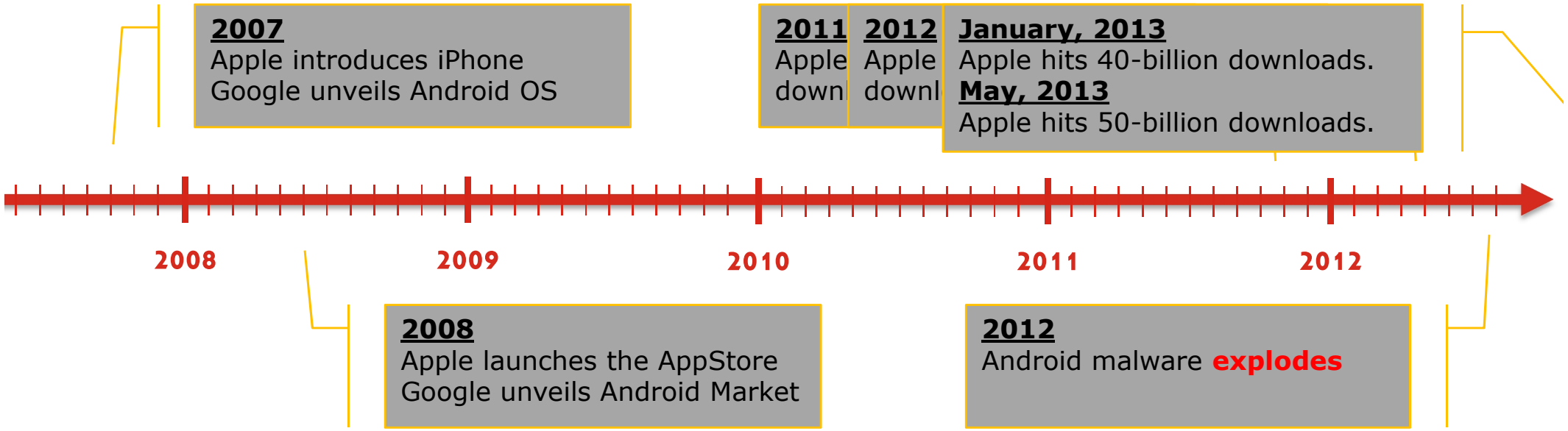
EMC²

© Copyright 2013 EMC Corporation. All rights reserved.

As the world

goes mobile cyber crime will follow

© Copyright 2013 EMC Corporation. All rights reserved.



1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

71% of organizations

allow employees to use their own mobile devices for company business

Source: GI mSecurity Survey Report, Goode Intelligence

1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

2,000,000,000

estimated number of worldwide active smartphone devices by end of 2013

Source: Deloitte

1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

68.8% Android

18.8% Apple iOS

4.5% RIM

5.8% Others

Market share of top 4 providers

1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

79% Android

19% Symbian

2% Others

Malware targeting OS

© Copyright 2013 EMC Corporation. All rights reserved.

350,000 malicious Android apps in ‘12

Jumped from 1,000 in 2011

Source: TrendMicro TrendLabs

© Copyright 2013 EMC Corporation. All rights reserved.

1,000,000 malicious Android apps in ‘13

Estimated

Source: TrendMicro TrendLabs

1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

86% all Android malware

repackaged versions of legitimate apps with malicious payloads

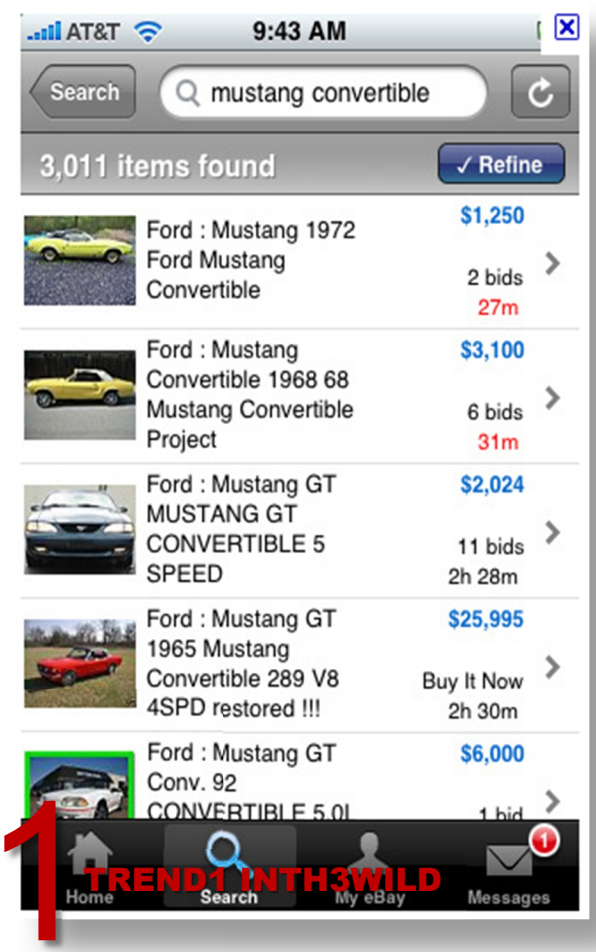
Source: Android Malware Genome Project
Department of Computer Science, North Carolina State University

1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

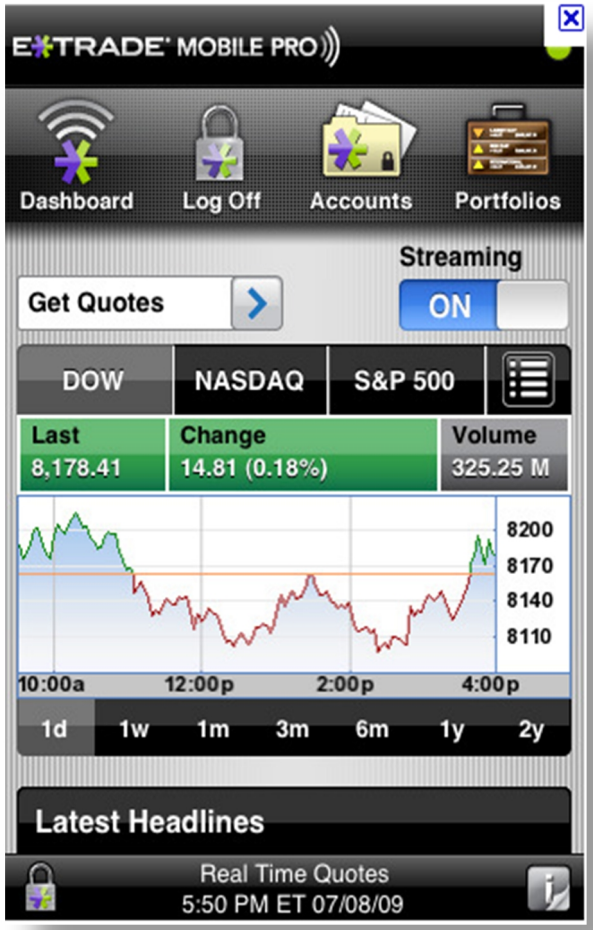
Mobile Services

eCommerce



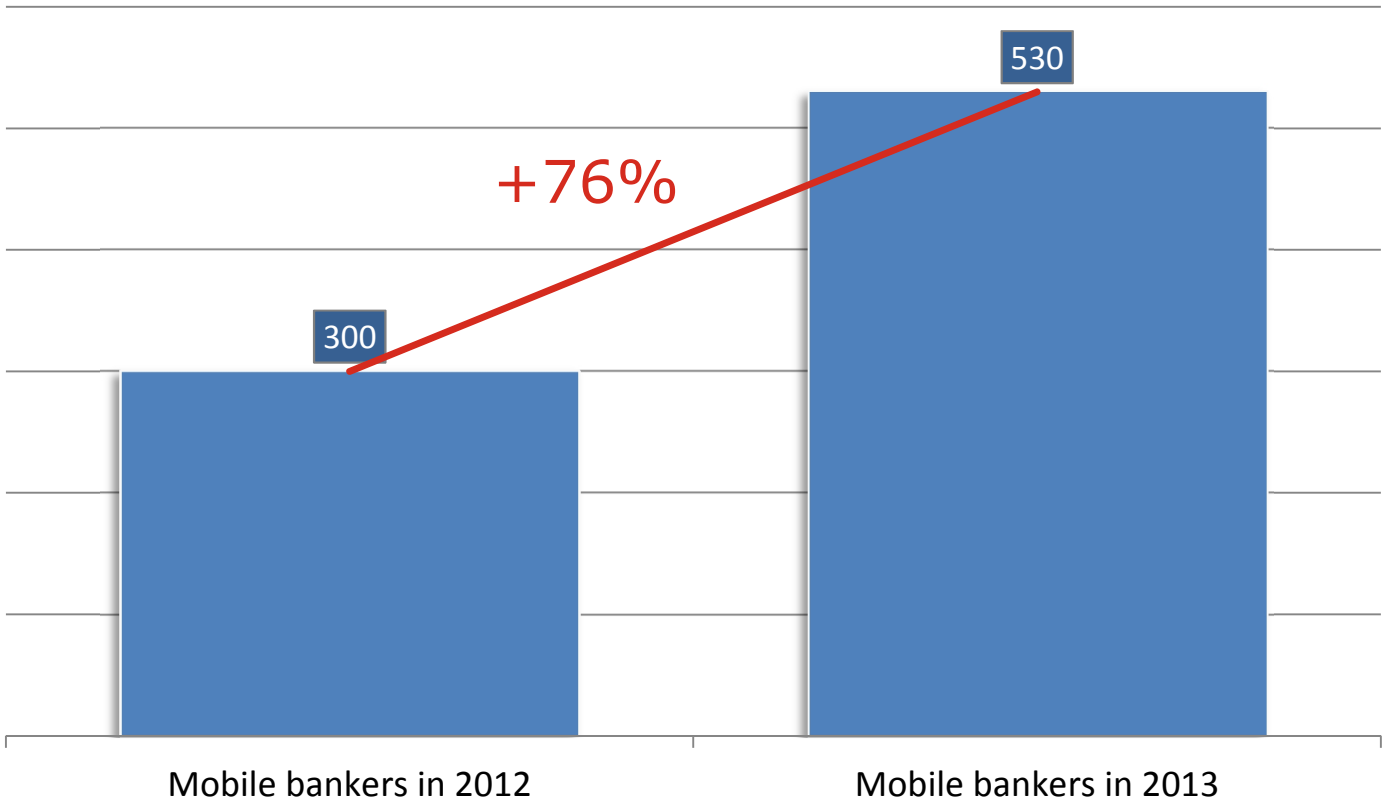
Online Banking

Online Trading



© Copyright 2013 EMC Corporation. All rights reserved.

Personal Finances



1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

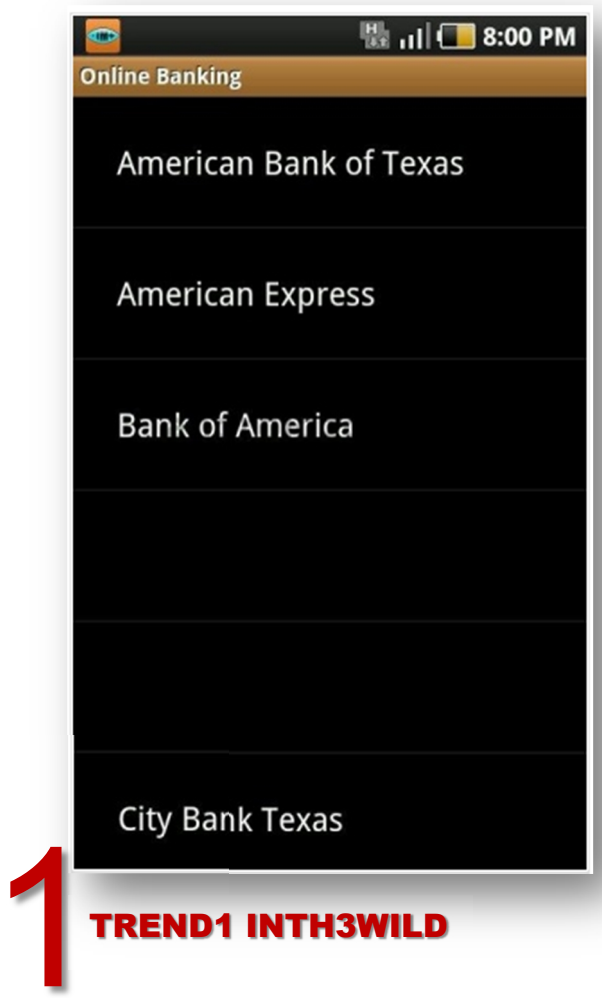
Malicious apps are posing as legitimate apps

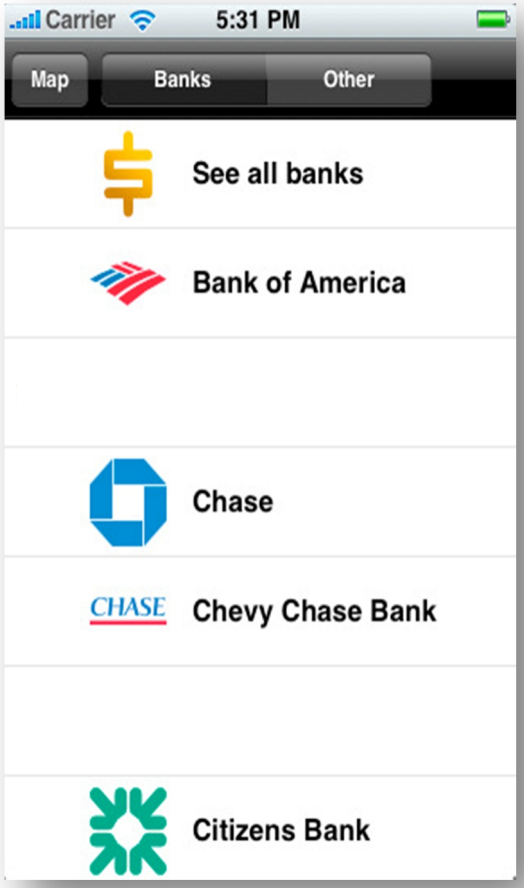
For Malware Distribution
For Phishing Scams

1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

Redirectors, ATMs and Portals





1 TREND1 INTH3WILD

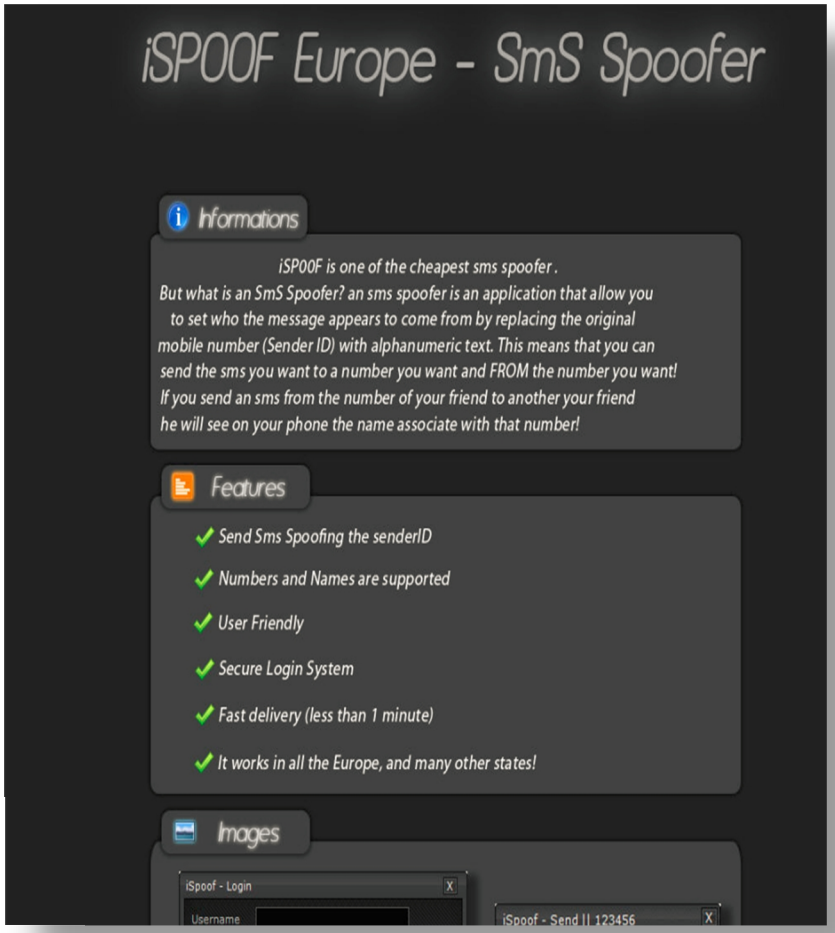
© Copyright 2013 EMC Corporation. All rights reserved.

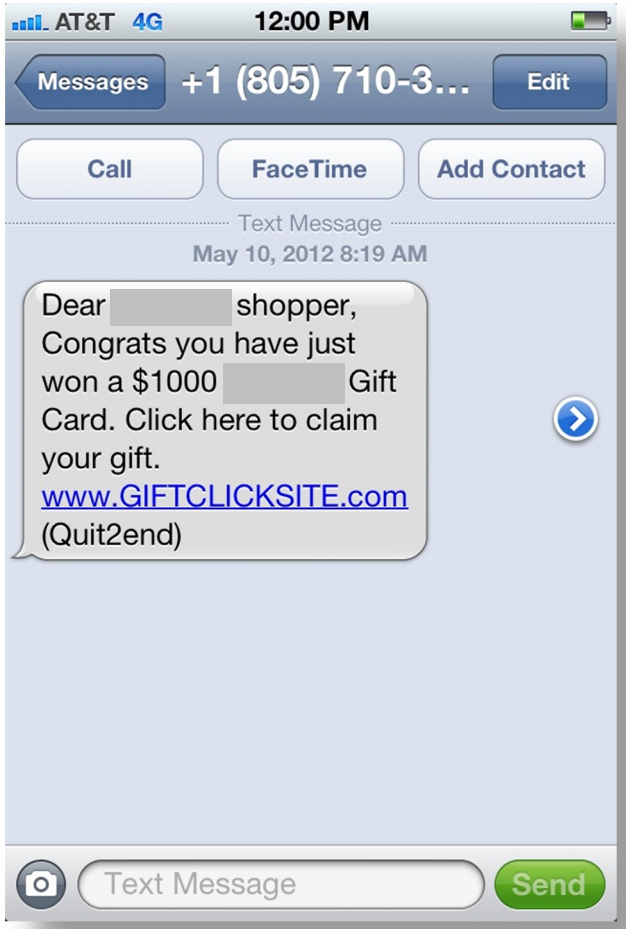
Games

1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

Phishing, SMiShing





1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

Mobil Malware & HTML Injection

Web Inject 1

As a result of unauthorized access to customers' personal information transmitted over the networks of mobile operators, [Redacted-RSA] bank in cooperation with the company's Premium Mobile Security suite, is now offering a program to strengthen the security of your personal information to complete payment transactions and other activities with your bank account. More than 15 million customers of banks and financial institutions around the world already use this system to protect their mobile access.

To encode and protect information transmitted to your mobile phone, install the free software linked below.

Please choose the operating system that runs on your mobile phone:

☐ **Android (Samsung, HTC,...)**

☐ **iOS (iPhone)**

☐ **BlackBerry**

☐ **Symbian (Nokia)**

☐ **Other**

Current mobile phone number:

1 **TREND1 INTH3WILD**

© Copyright 2013 EMC Corporation. All rights reserved.

Citadel

Web Inject 2

An SMS text message with a link to download the Android Premium Security Suite has been sent to the phone number indicated.

Please follow the link in the message and start the application installation process.

If you have not received the message, enter the following address into the address bar of your mobile browser:

hxxp://[Redacted – RSA].net/androidversion2.apk

Upon the program's initial run, please enter the activation code appearing on the screen.

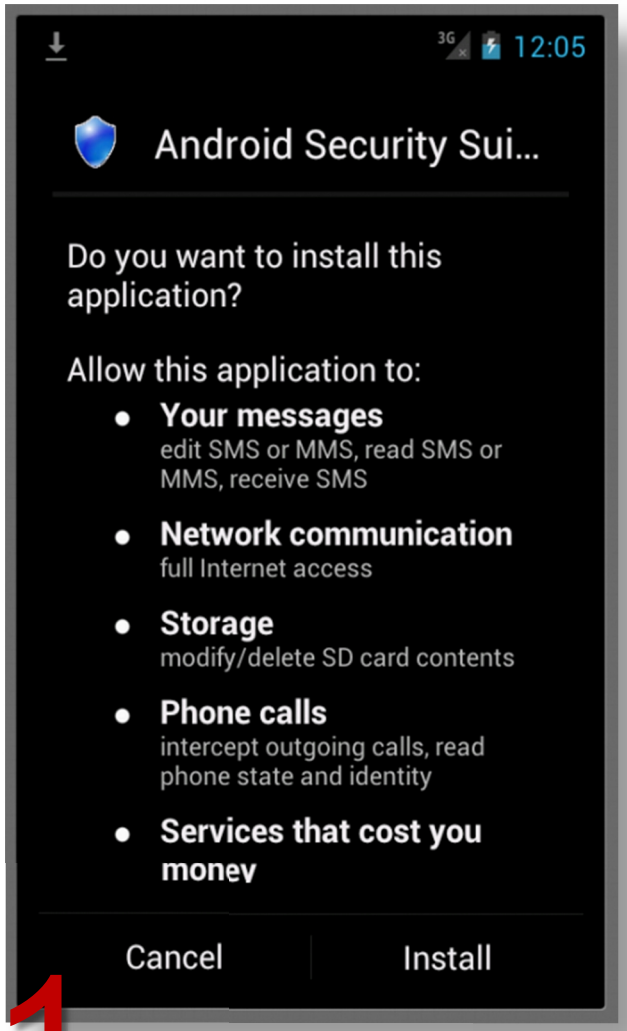
Activation Code: [ ]

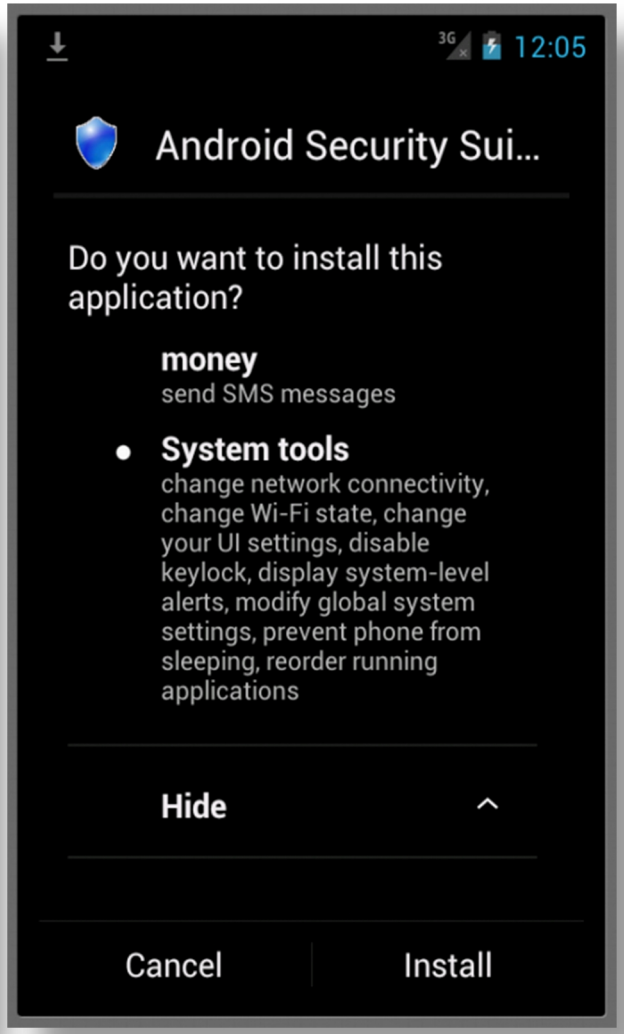
Digital Signature: [ ]

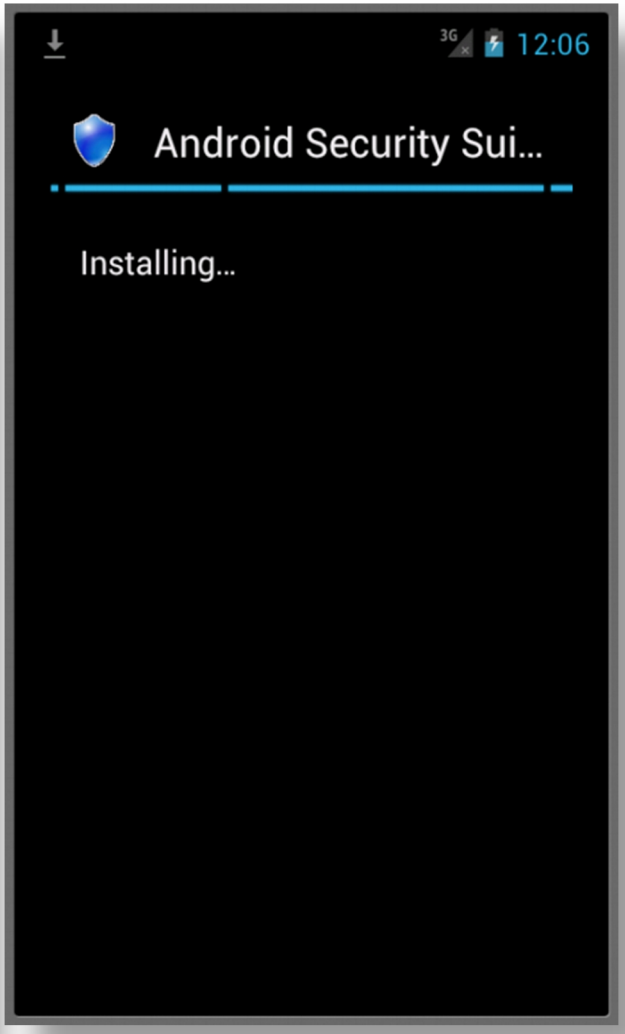
1 **TREND1 INTH3WILD**

© Copyright 2013 EMC Corporation. All rights reserved.

Citadel



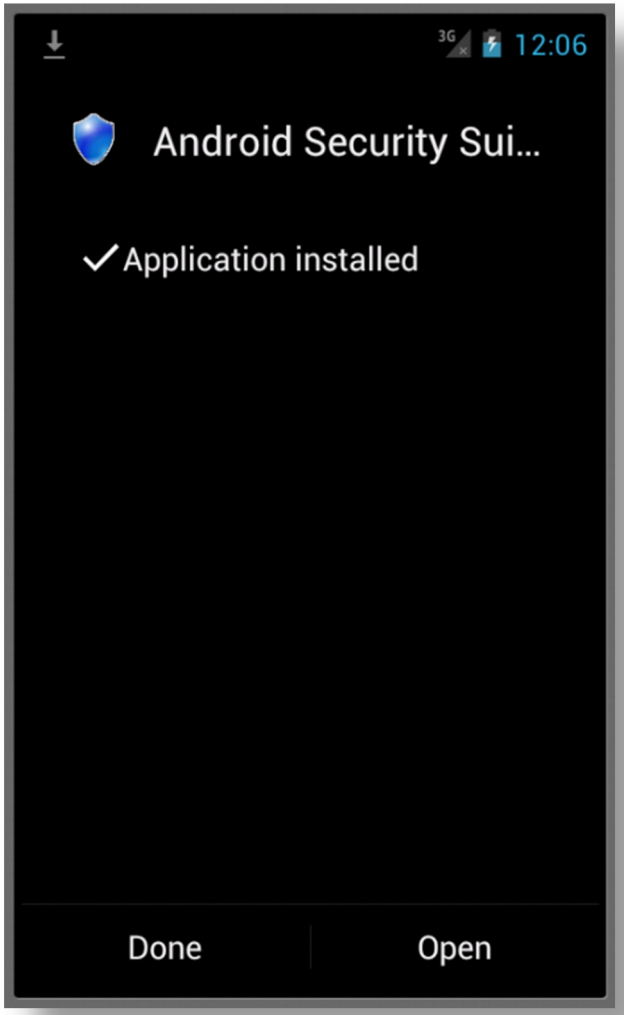




1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

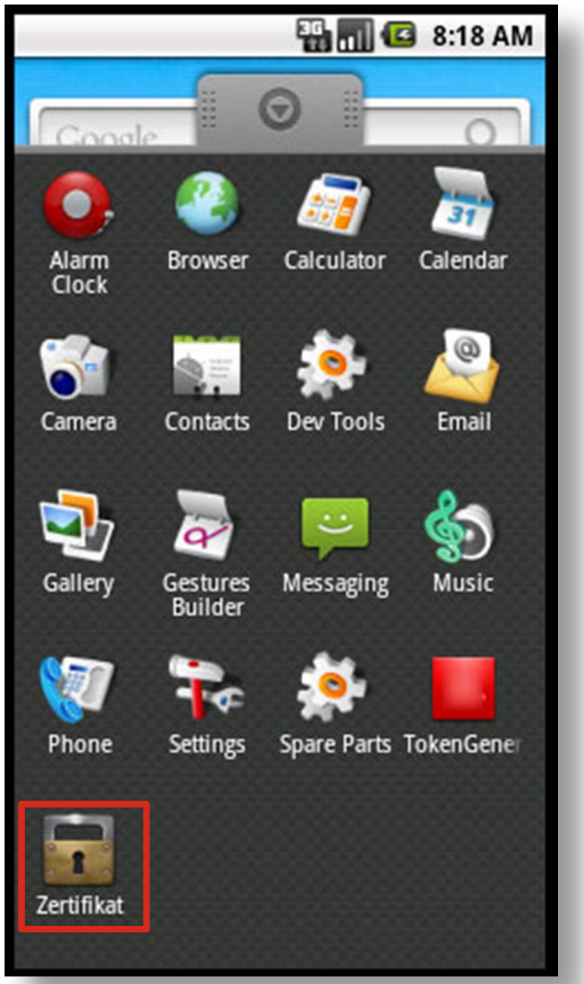
Citadel



1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

ZitMO



1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

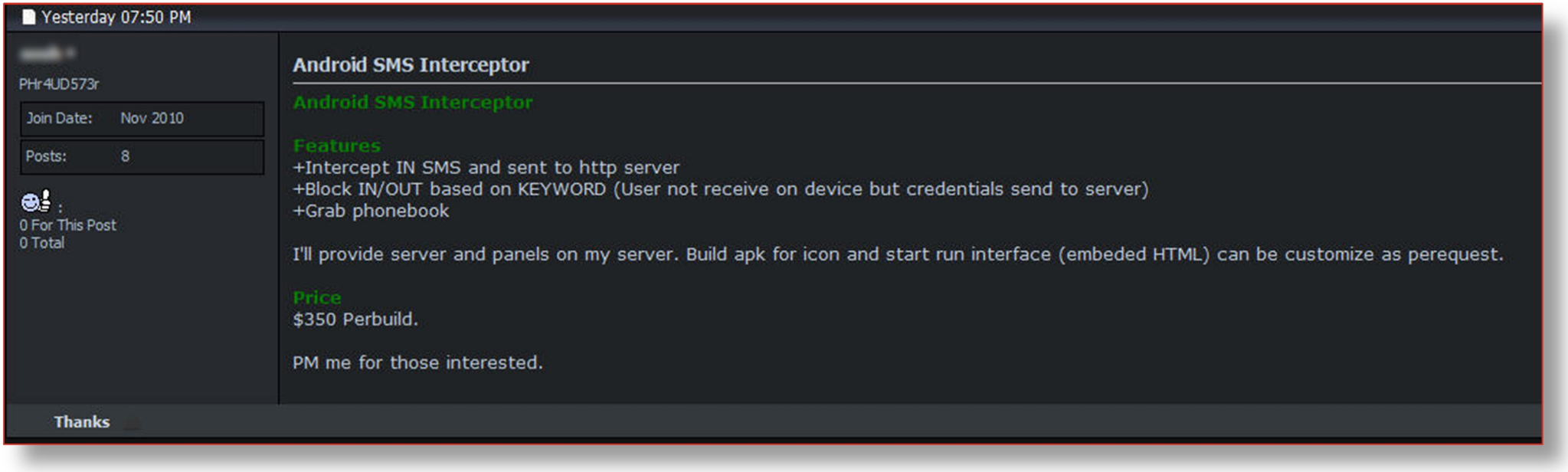
ZitMO

```
[Broadcast receivers]
---------------------
      com.security.service.receiver.SmsReceiver          Action: android.provider.Telephony.SMS_RECEIVED

      com.security.service.receiver.ActionReceiver       Action: android.intent.action.USER_PRESENT

      com.security.service.receiver.RebootReceiver       Action: android.intent.action.ACTION_SHUTDOWN

[Started services]
------------------
[Enforced permissions]
----------------------

[Permissions bypassed]
----------------------

[Information leakage]
---------------------

[Sent SMS]
----------
      [6.35391616821]              Number: +[redacted]
                                   Message: INOK
```

1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

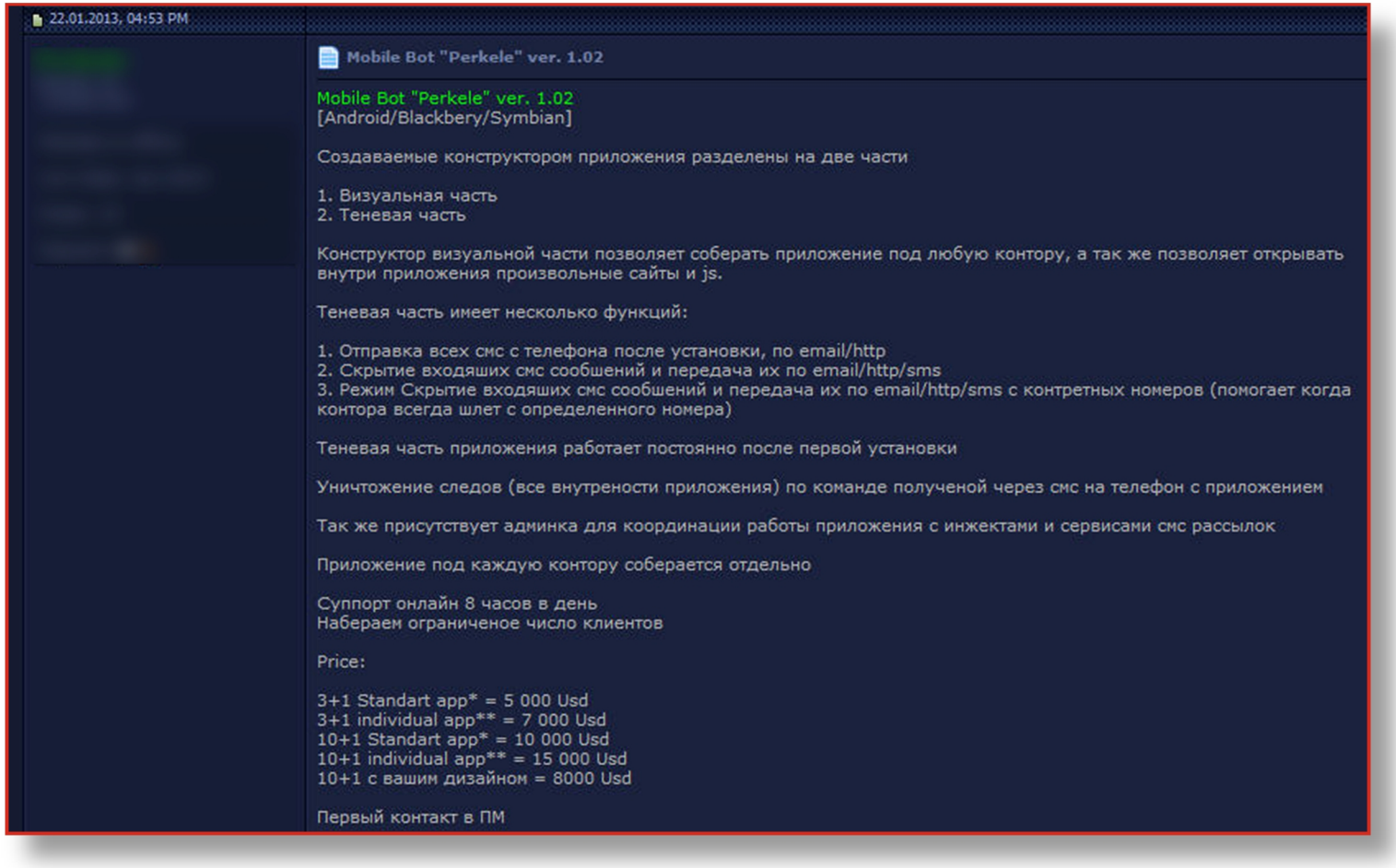
SMS Sniffers



1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

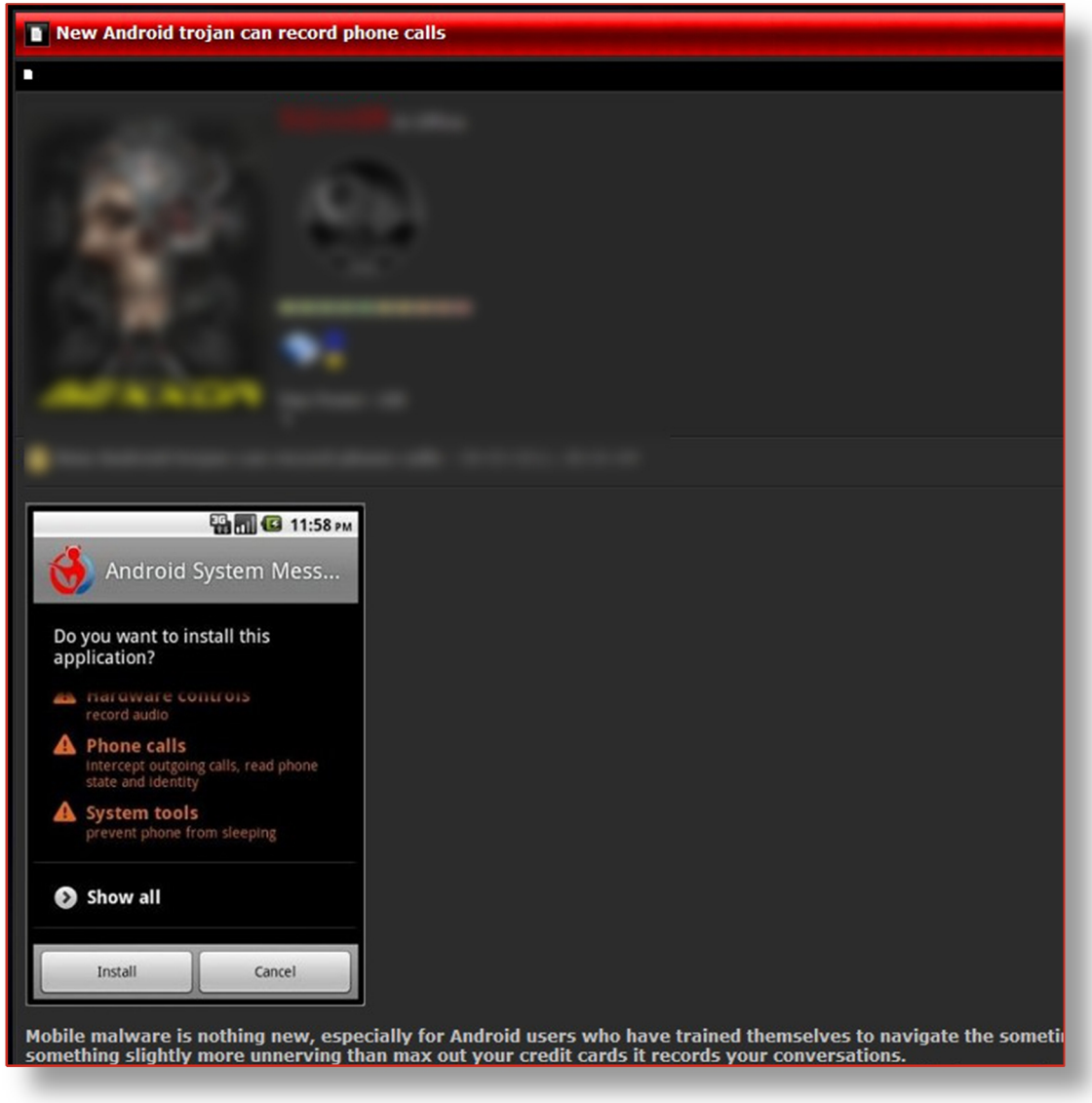
Perkele



1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

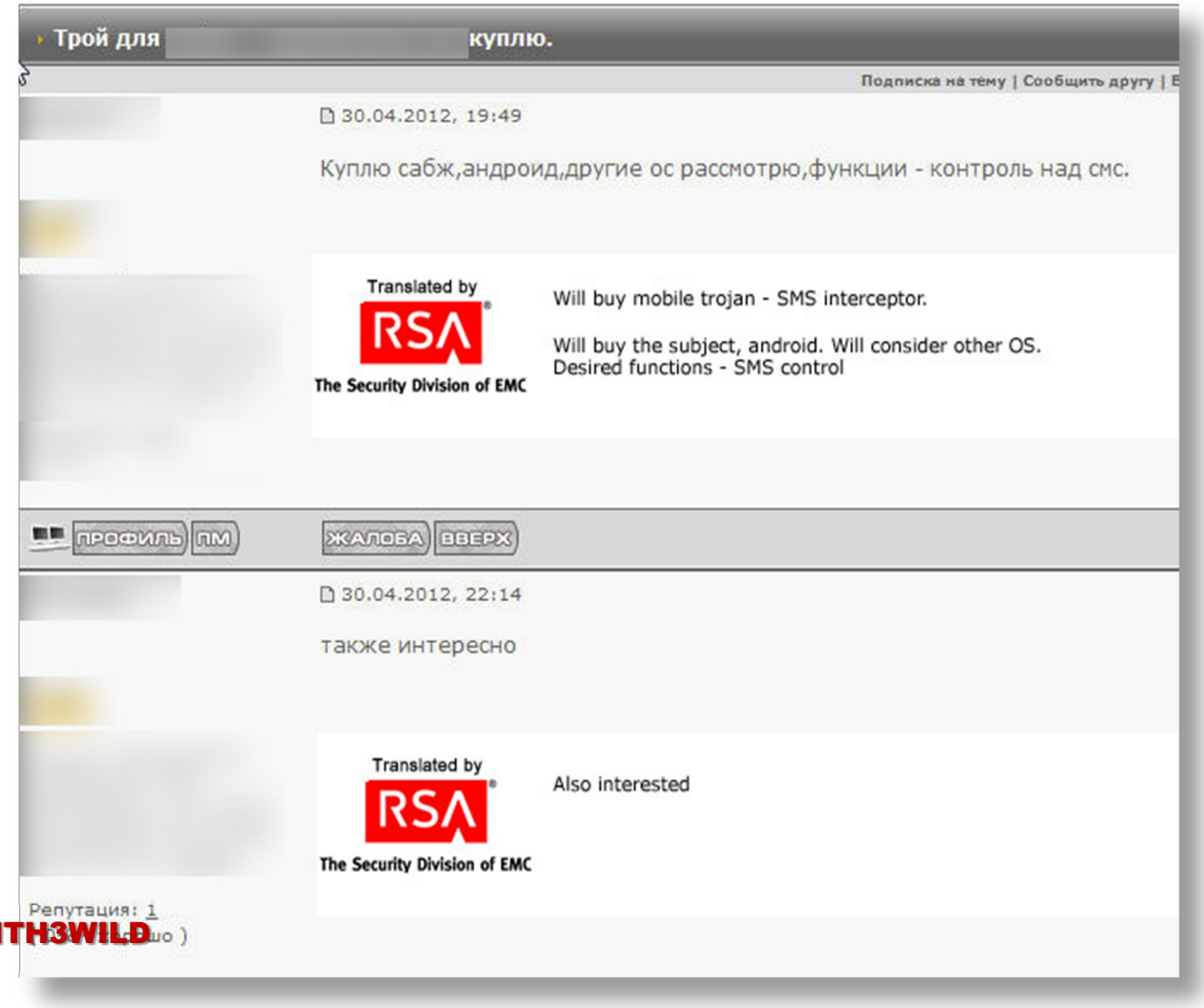
Voice



1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

SMS Interceptor Demand

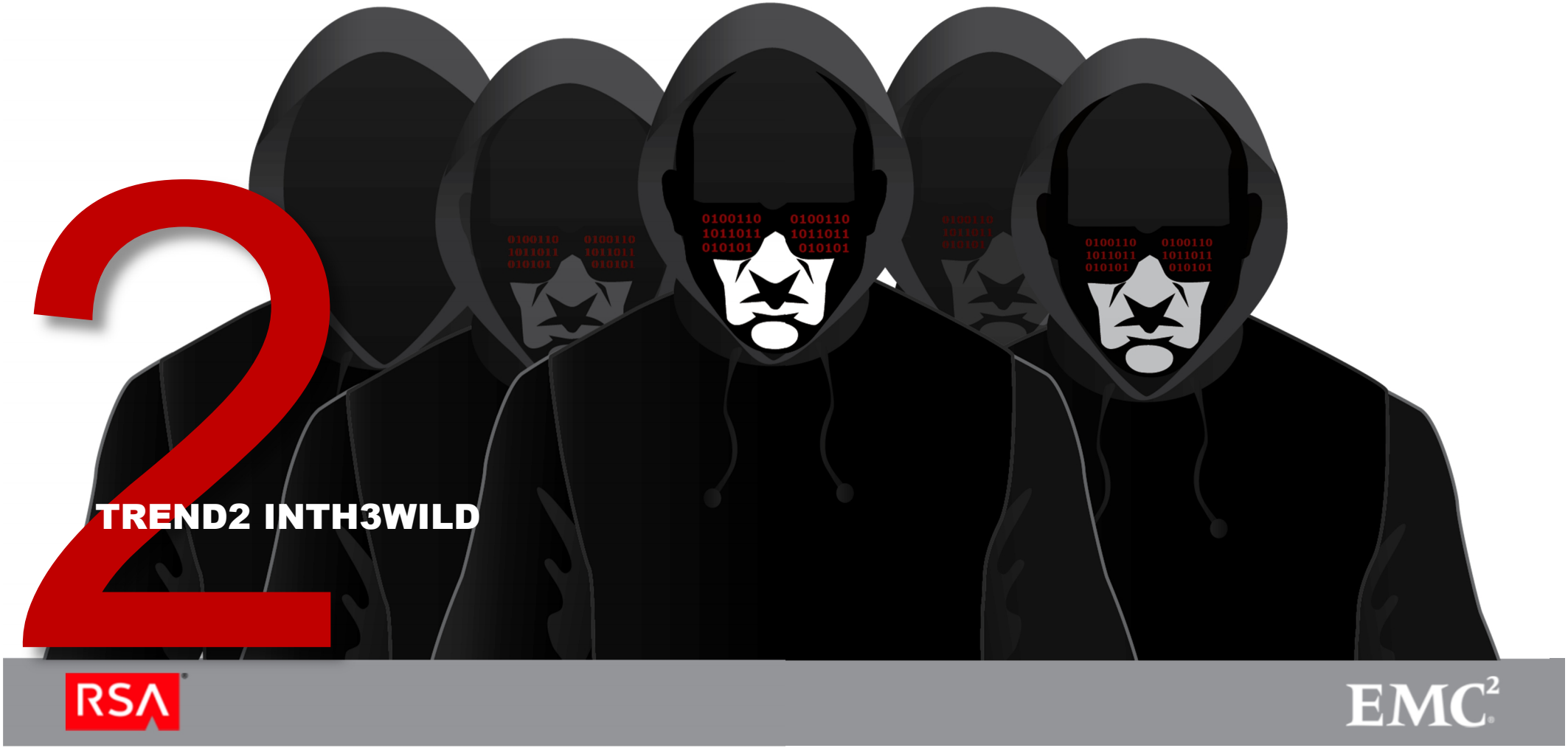


1 TREND1 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

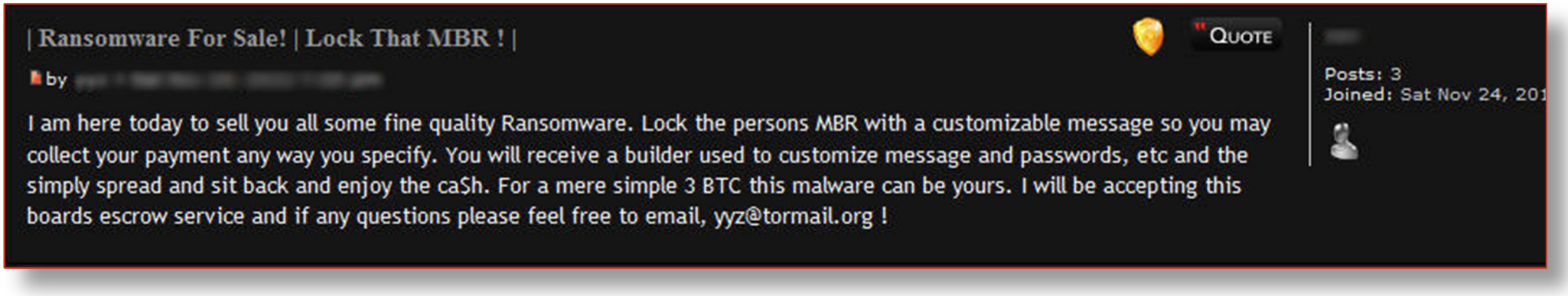
World wide

Trojans are going deeper underground



© Copyright 2013 EMC Corporation. All rights reserved.

Ransomware


| Ransomware For Sale! | Lock That MBR ! |

by

QUOTE

Posts: 3
Joined: Sat Nov 24, 201

I am here today to sell you all some fine quality Ransomware. Lock the persons MBR with a customizable message so you may collect your payment any way you specify. You will receive a builder used to customize message and passwords, etc and the simply spread and sit back and enjoy the ca$h. For a mere simple 3 BTC this malware can be yours. I will be accepting this boards escrow service and if any questions please feel free to email, yyz@tormail.org !

2 TREND2 INTH3WILD

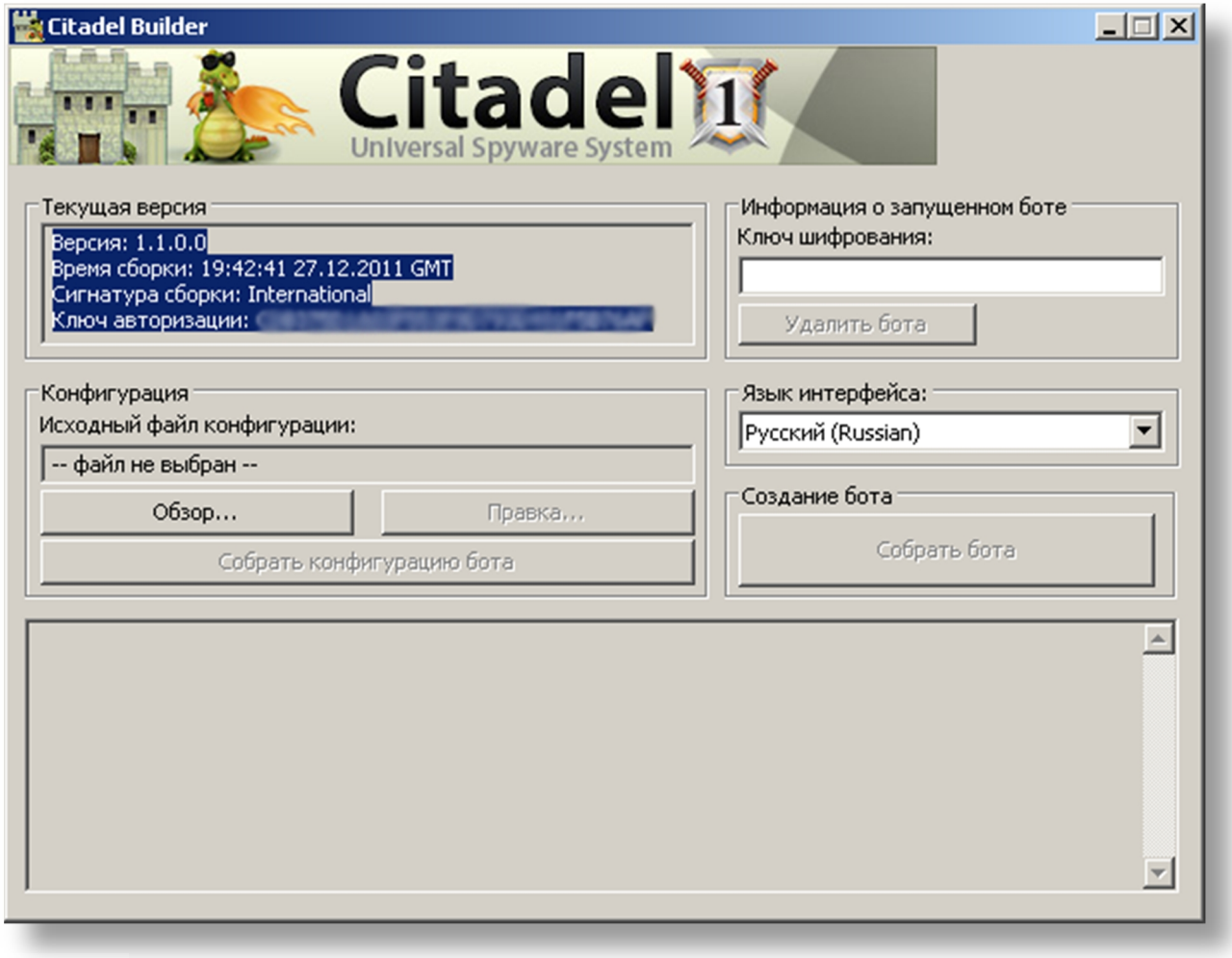
© Copyright 2013 EMC Corporation. All rights reserved.

Ransomware

2 TREND2 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

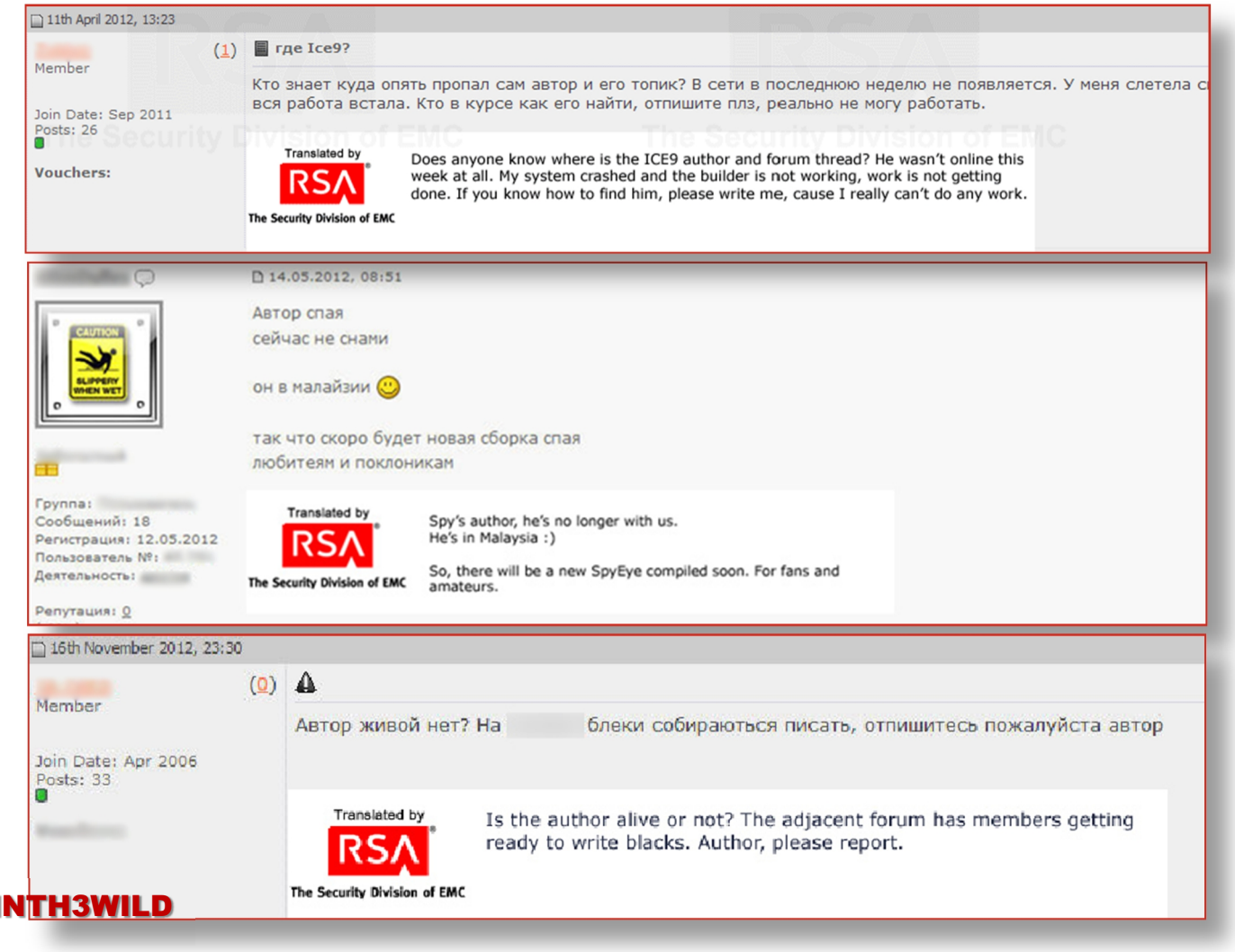
Trojans: Citadel



2 TREND2 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

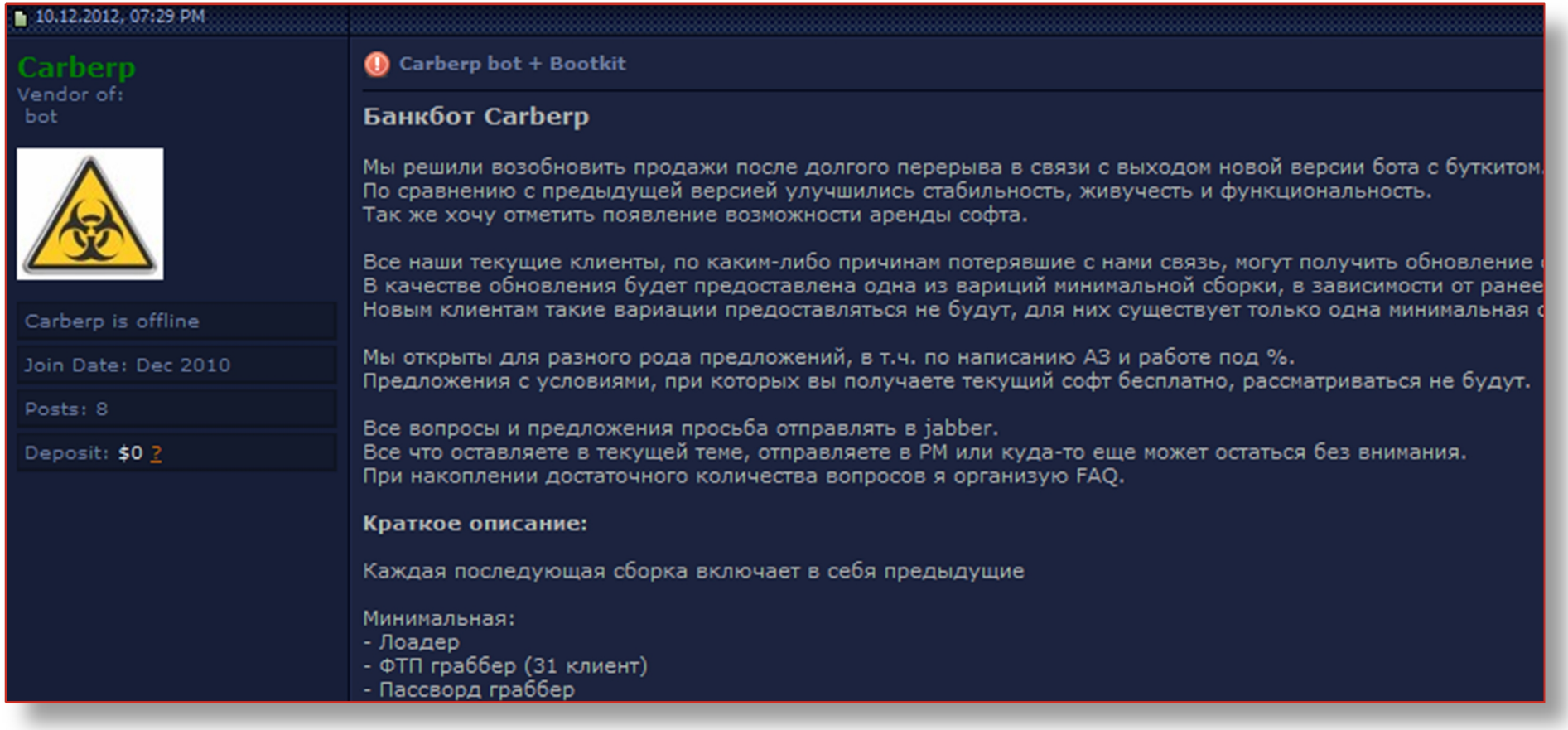
Trojans: Developers



2 TREND2 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

Trojans: Carberp



2 TREND2 INTH3WILD

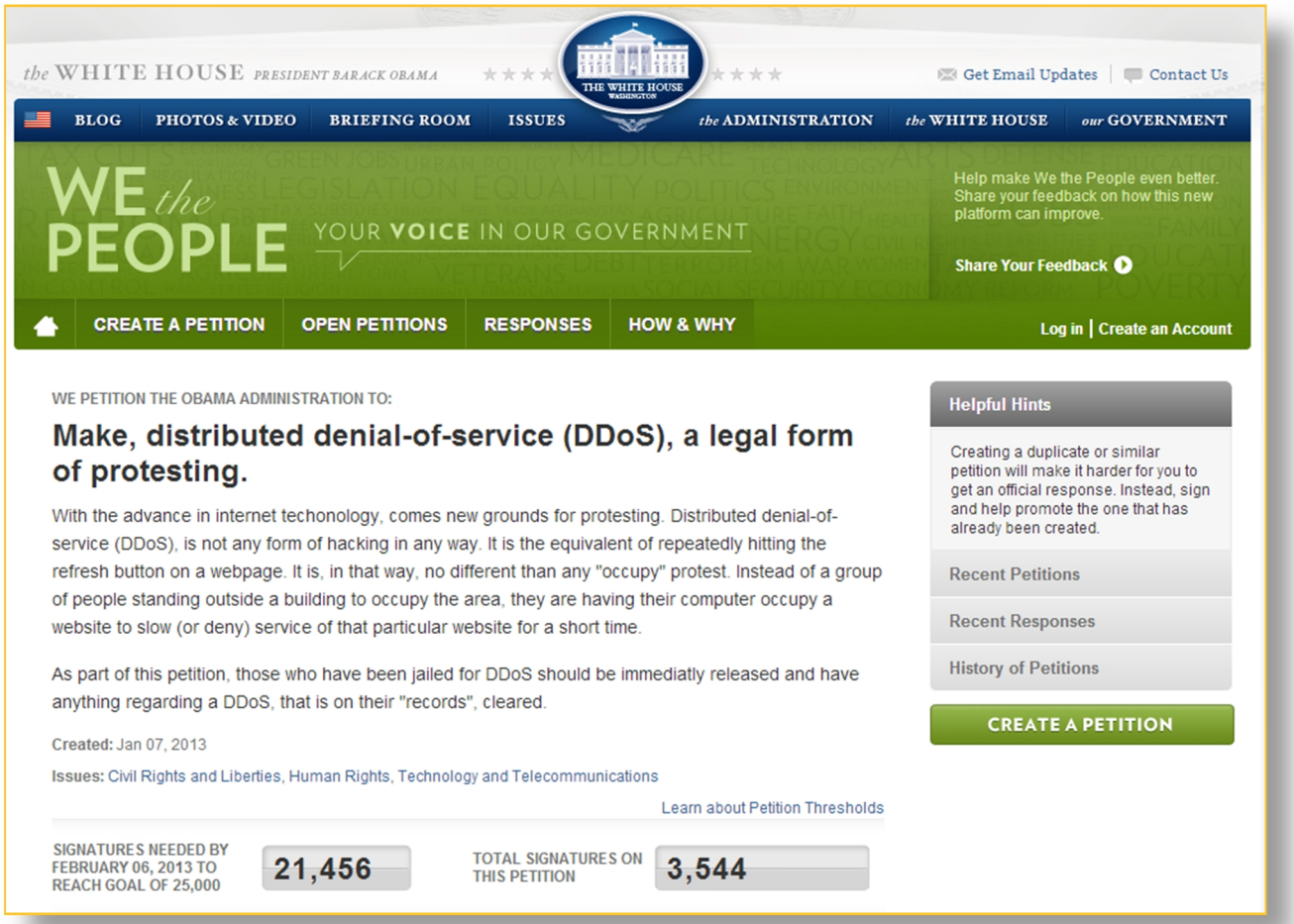
© Copyright 2013 EMC Corporation. All rights reserved.

Hacktivism

and the ever targeted enterprise

© Copyright 2013 EMC Corporation. All rights reserved.

Anonymous



3 TREND3 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

Op Ababil

Thursday, April 18, 2013

The Citizens Bank and Ameriprise Financial And M&T Bank have been targeted of Cyber Attacks

6:20 PM | Posted by hilfol fozoul |

Tweet 1

The Izz ad-Din al-Qassam has targeted the citizens Bank and M&T Bank and Ameriprise Financial in its series of attacks in the latest days at the 7th week of the third phase and disrupted the Online Banking services of these banks for hours. The cyber attacks to the banks and financial institutions according to Qassam group will be continued until to removing the insulting film from the internet.

The only way for stopping the attacks, is to removing the insulting film from the internet.

3 TREND3 INTH3WILD

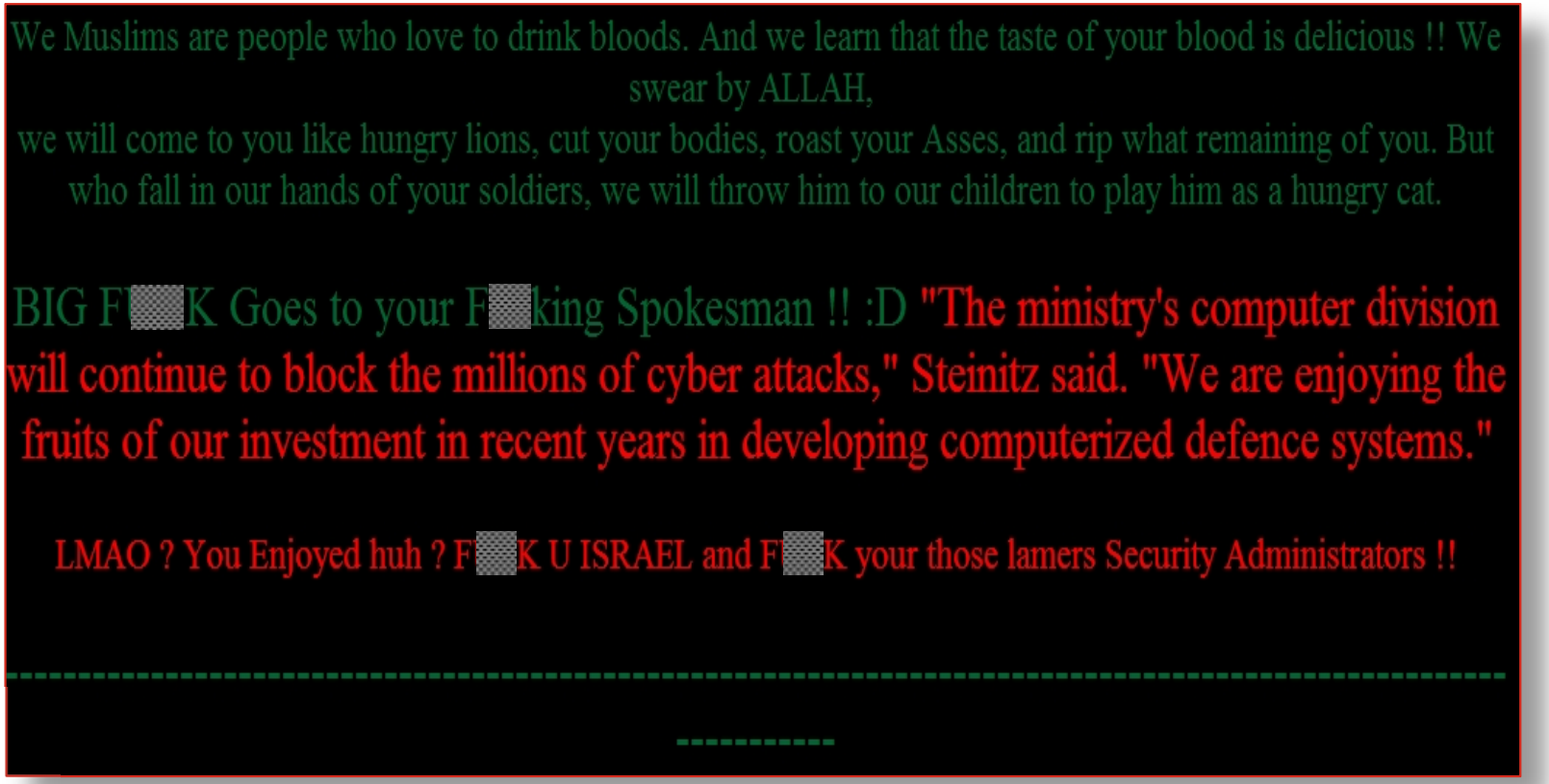
© Copyright 2013 EMC Corporation. All rights reserved.

Op Ababil

3 TREND3 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

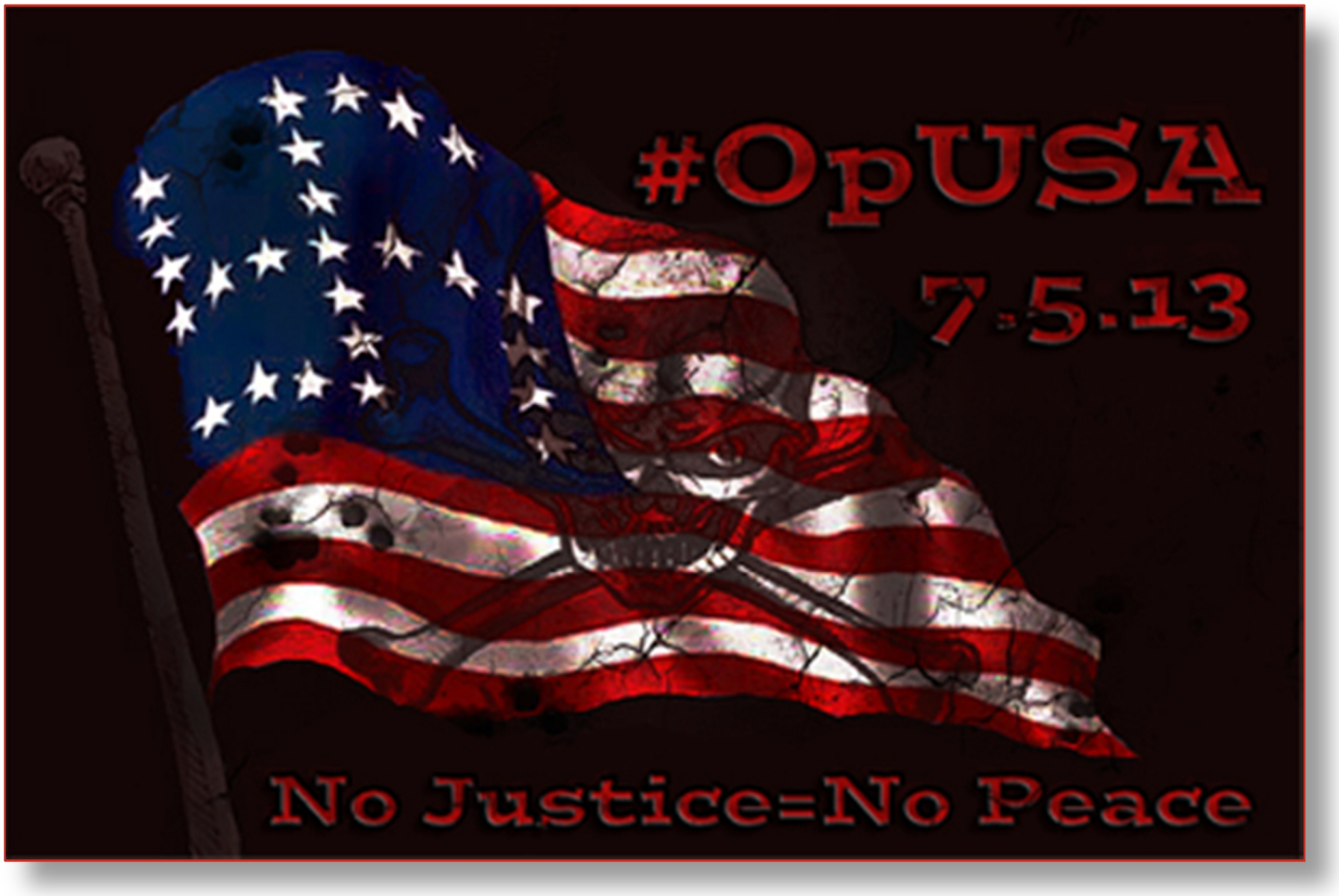
OpIsrael



3 TREND3 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

OpUSA



3 TREND3 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

Account takeover

and increasing use of manual assisted cyber attacks

4

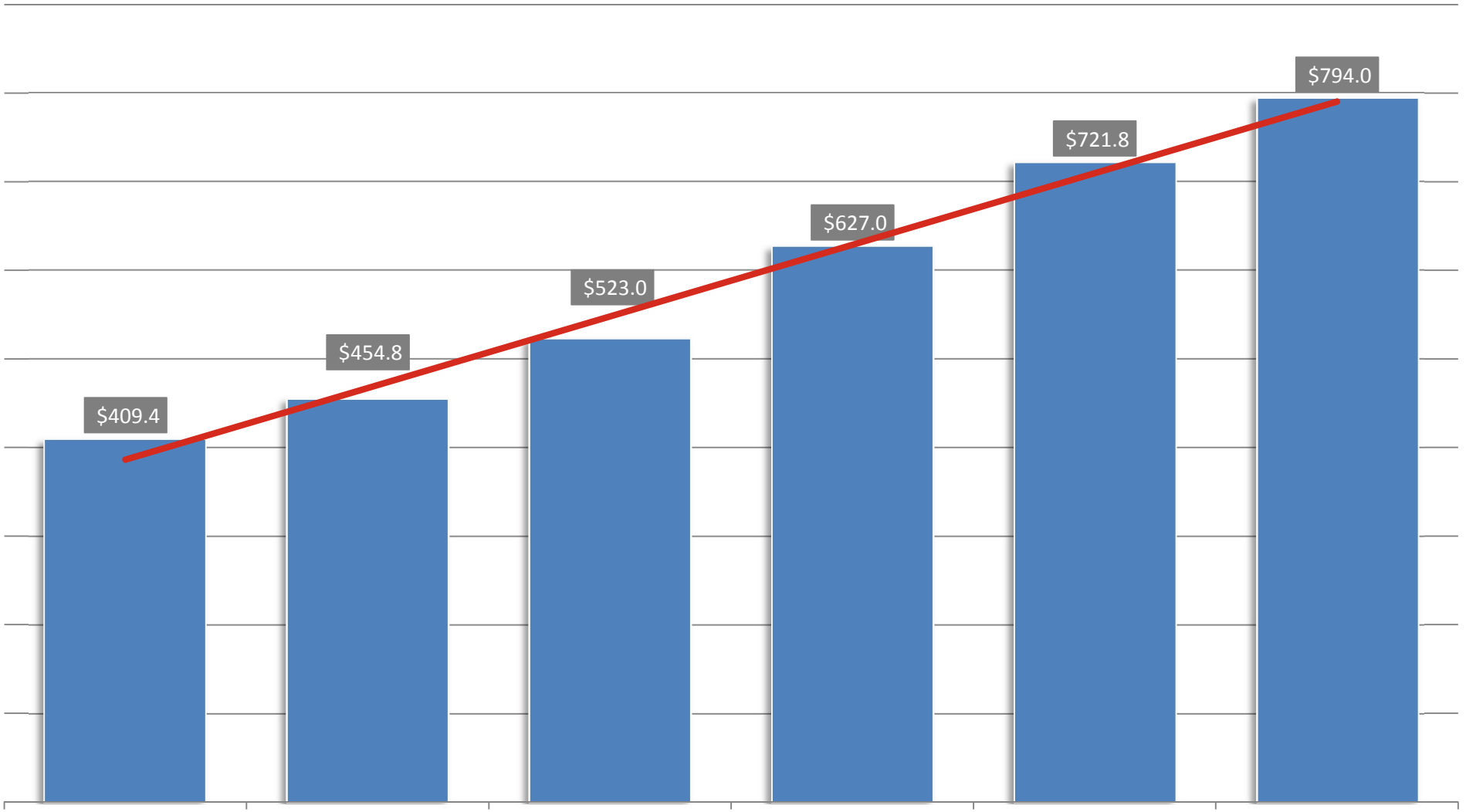
TREND4 INTH3WILD

RSA

EMC²

© Copyright 2013 EMC Corporation. All rights reserved.

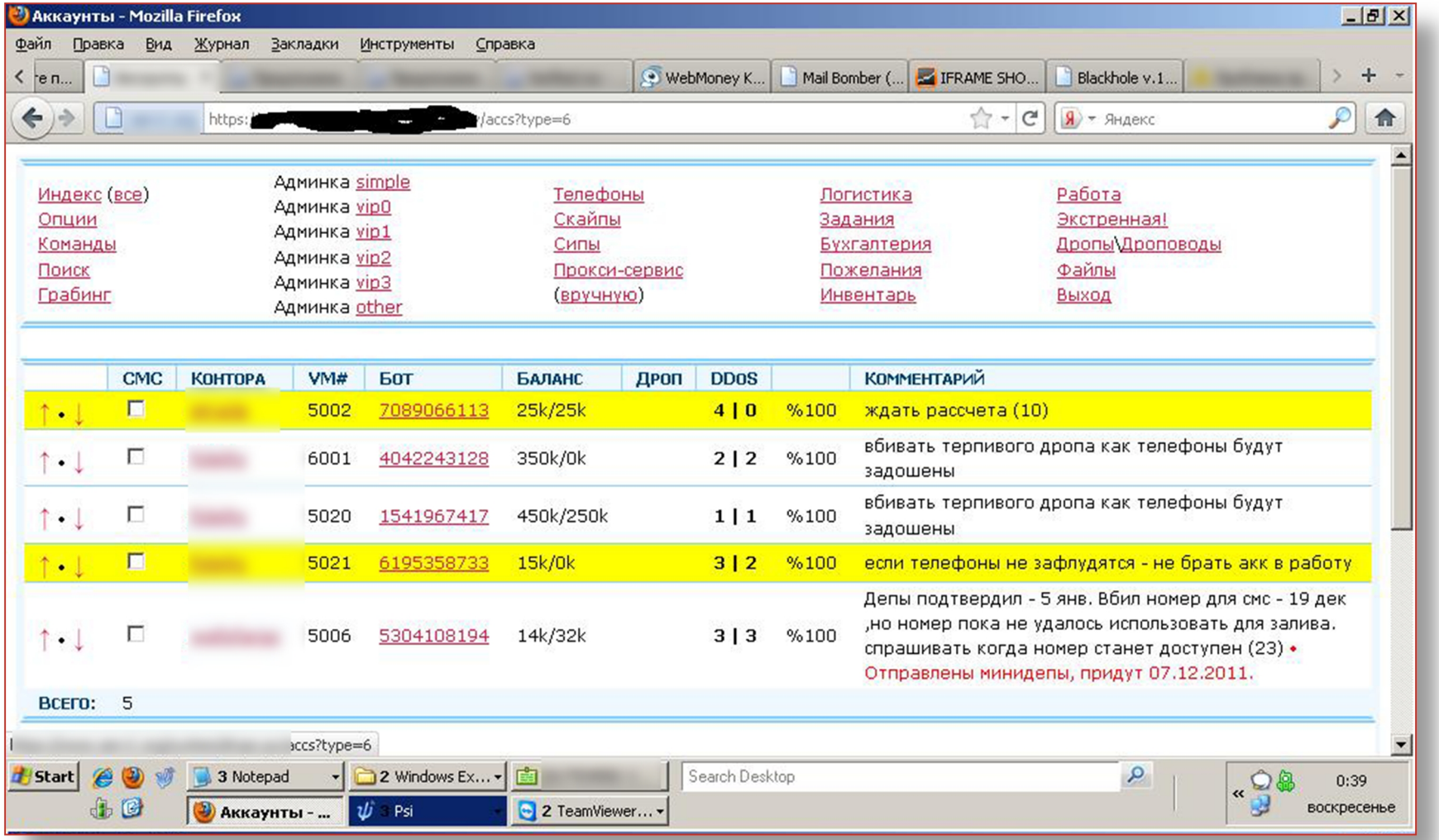
Corporate Account Takeover Losses (global, mil $)



4 TREND4 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

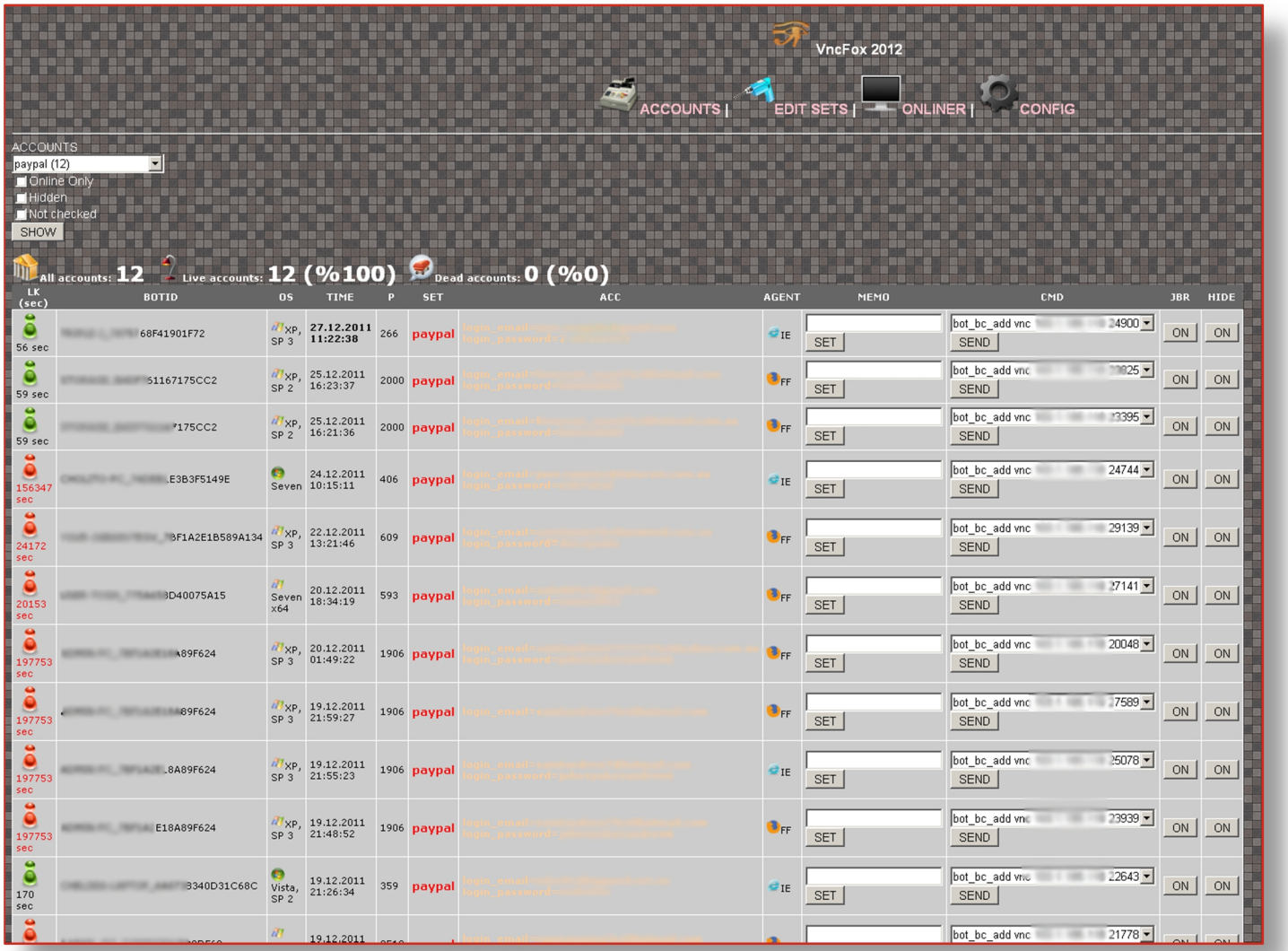
Project Blitzkrieg



4 TREND4 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

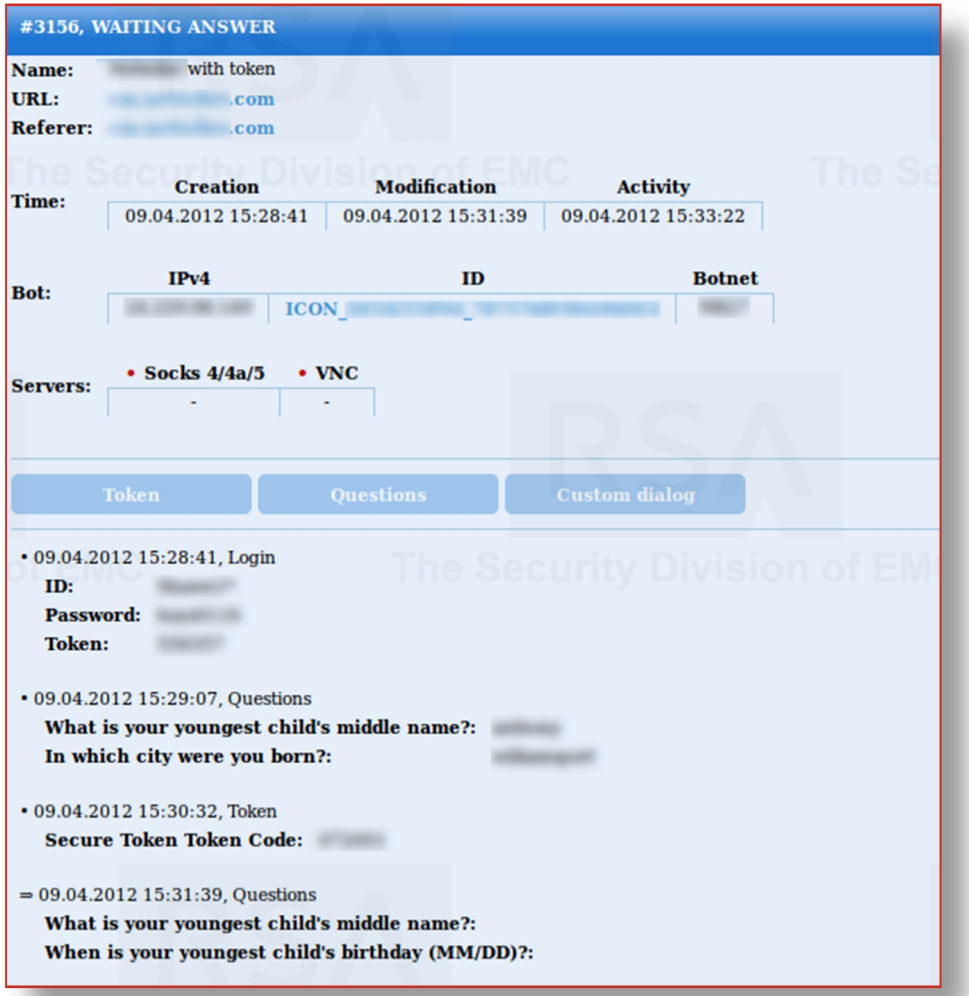
Citadel VNC Panel



4 TREND4 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

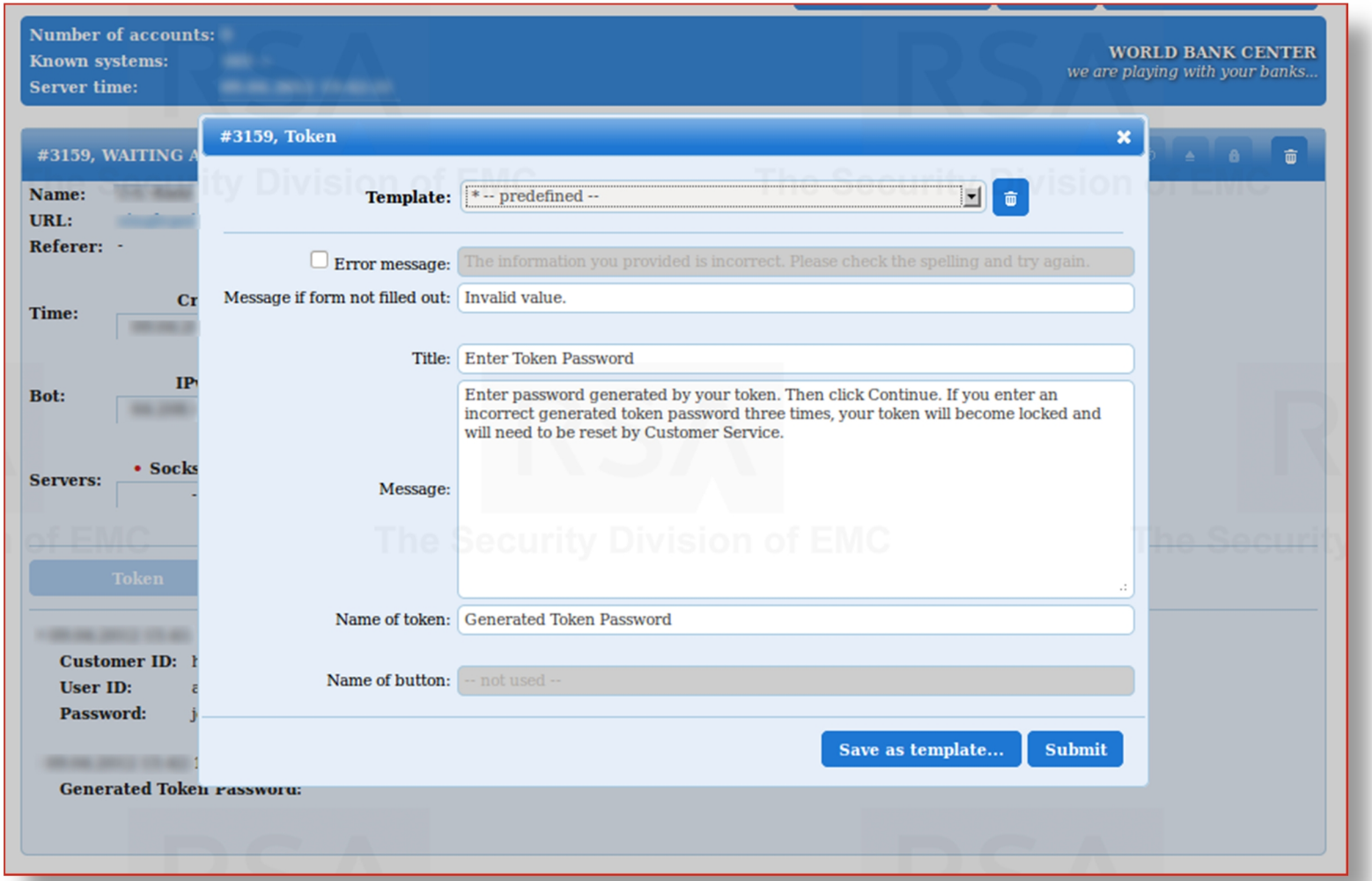
Zeus Plugin



4 TREND4 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

Zeus Plugin Token Screen



4 TREND4 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

Cybercriminals

will leverage big data principles to increase effectiveness of attacks

© Copyright 2013 EMC Corporation. All rights reserved.

Exploit Kits

5 TREND5 INTH3WILD

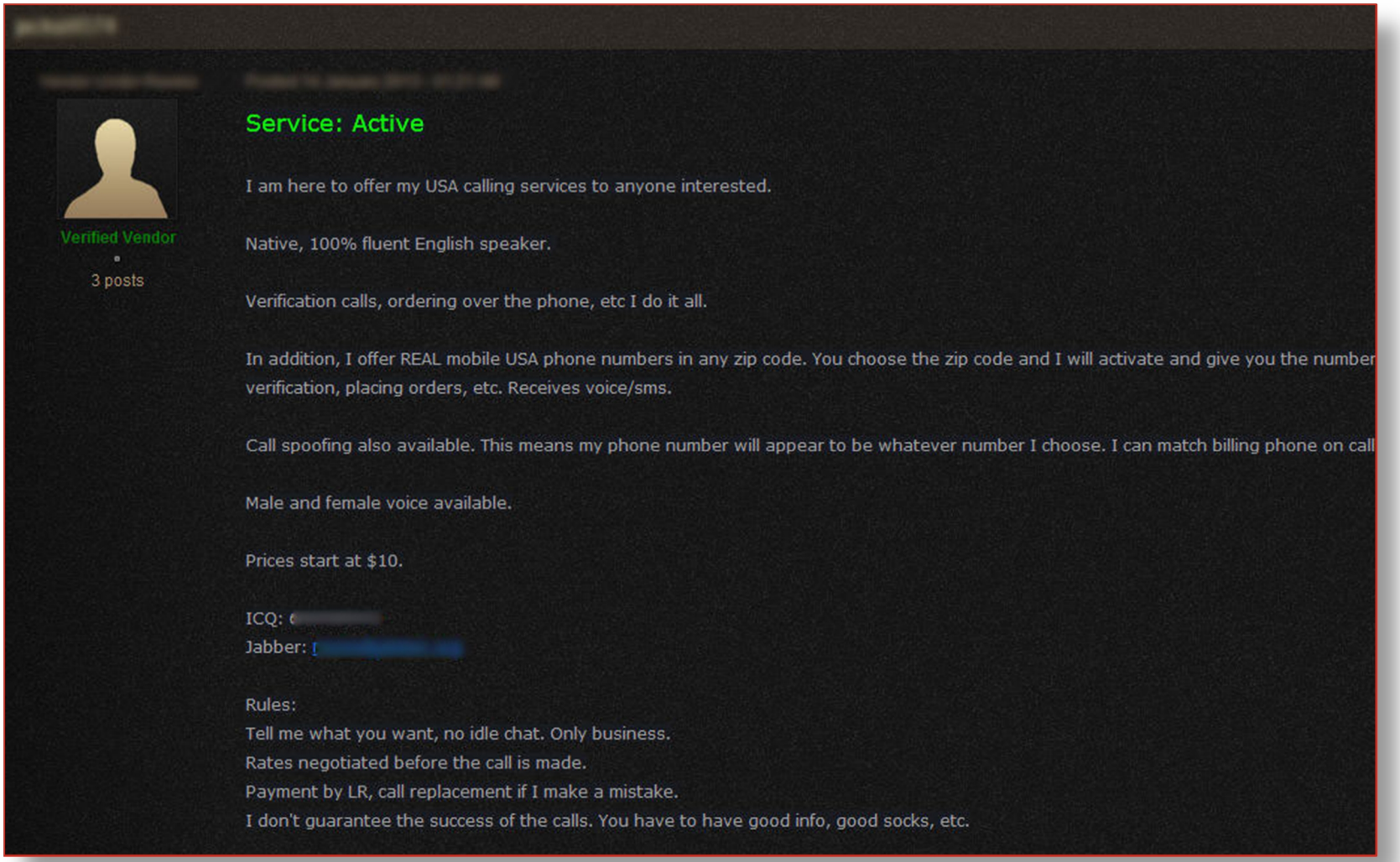
© Copyright 2013 EMC Corporation. All rights reserved.

Botnet Infrastructure

5 TREND5 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

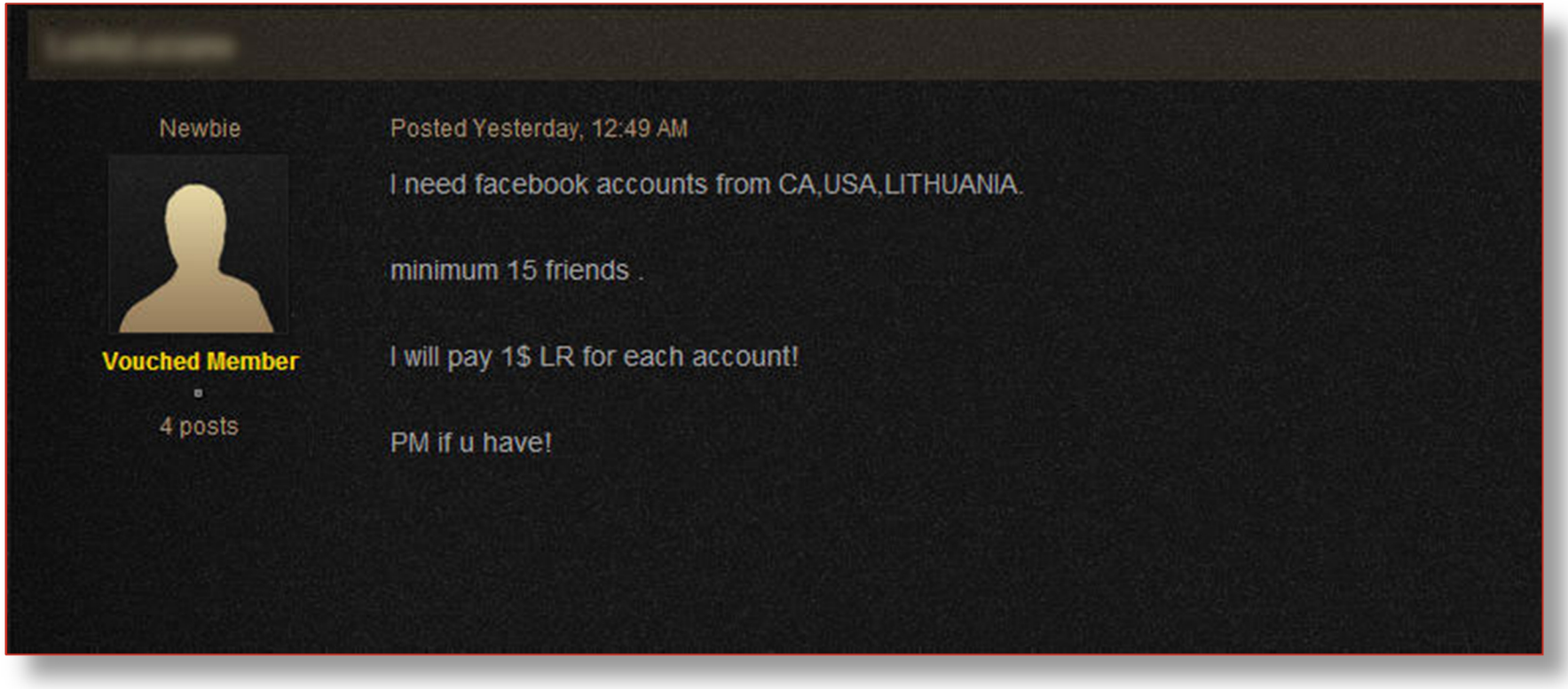
Call Center Service



5 TREND5 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

Facebook Accounts



5 TREND5 INTH3WILD

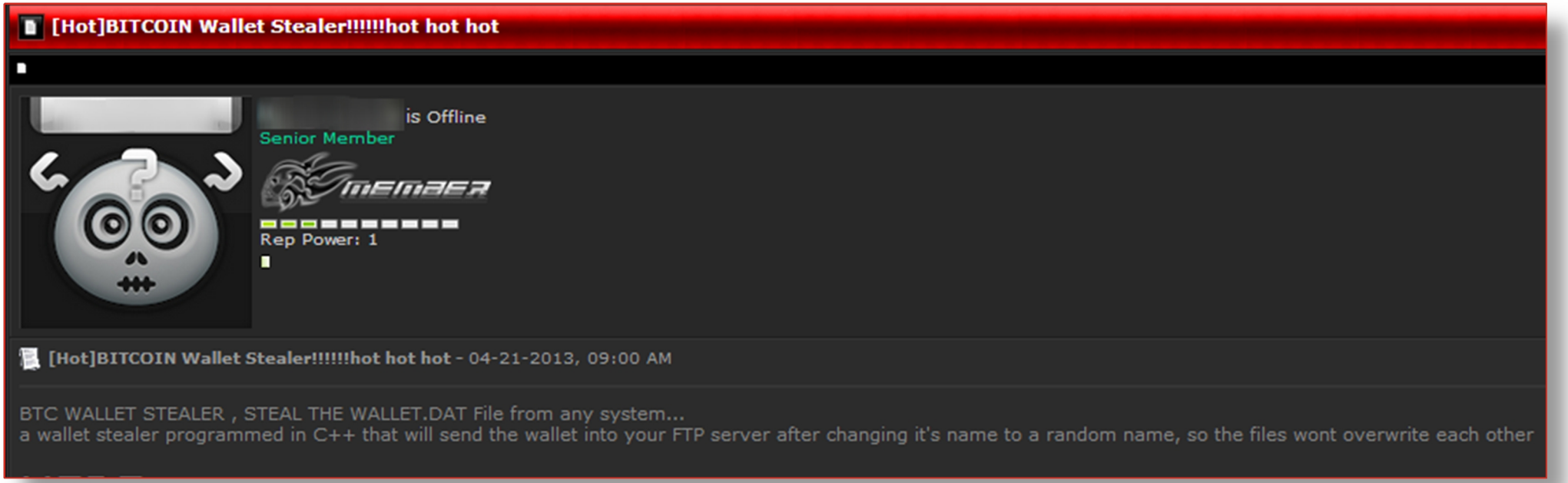
© Copyright 2013 EMC Corporation. All rights reserved.

Facebook Ads

5 TREND5 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

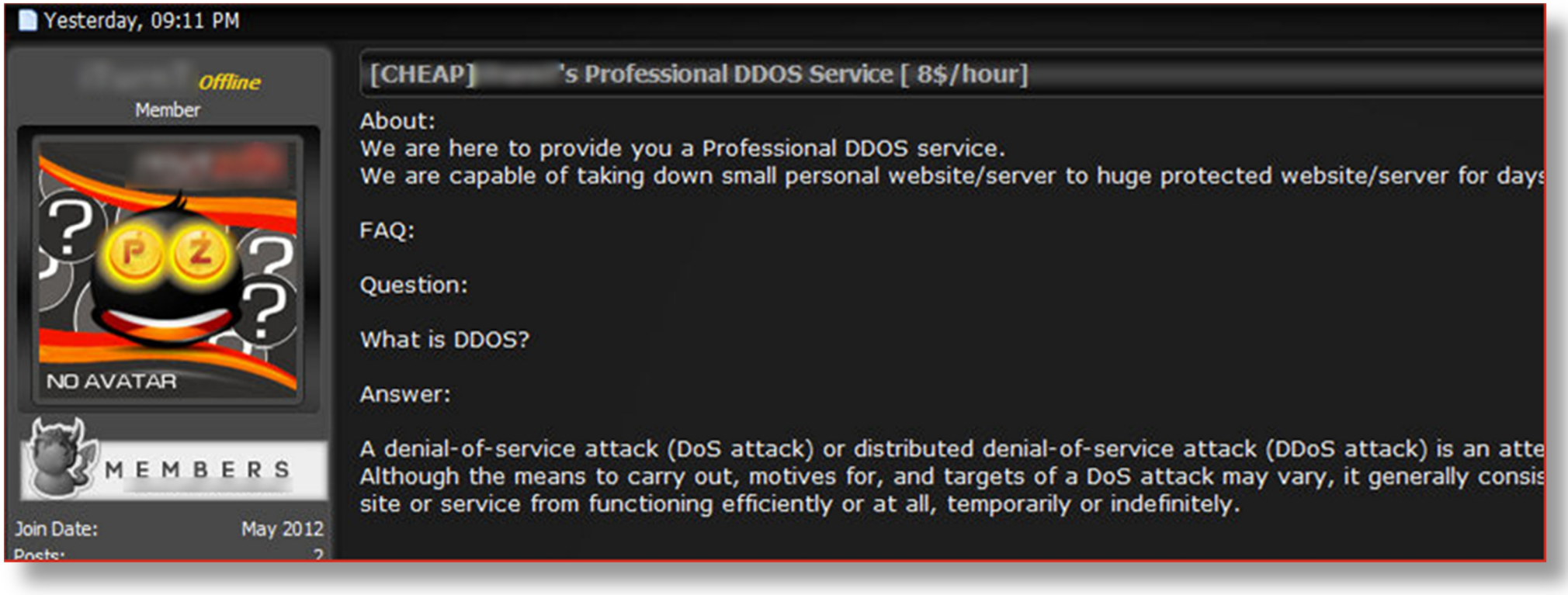
Bitcoin Stealer



5 TREND5 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

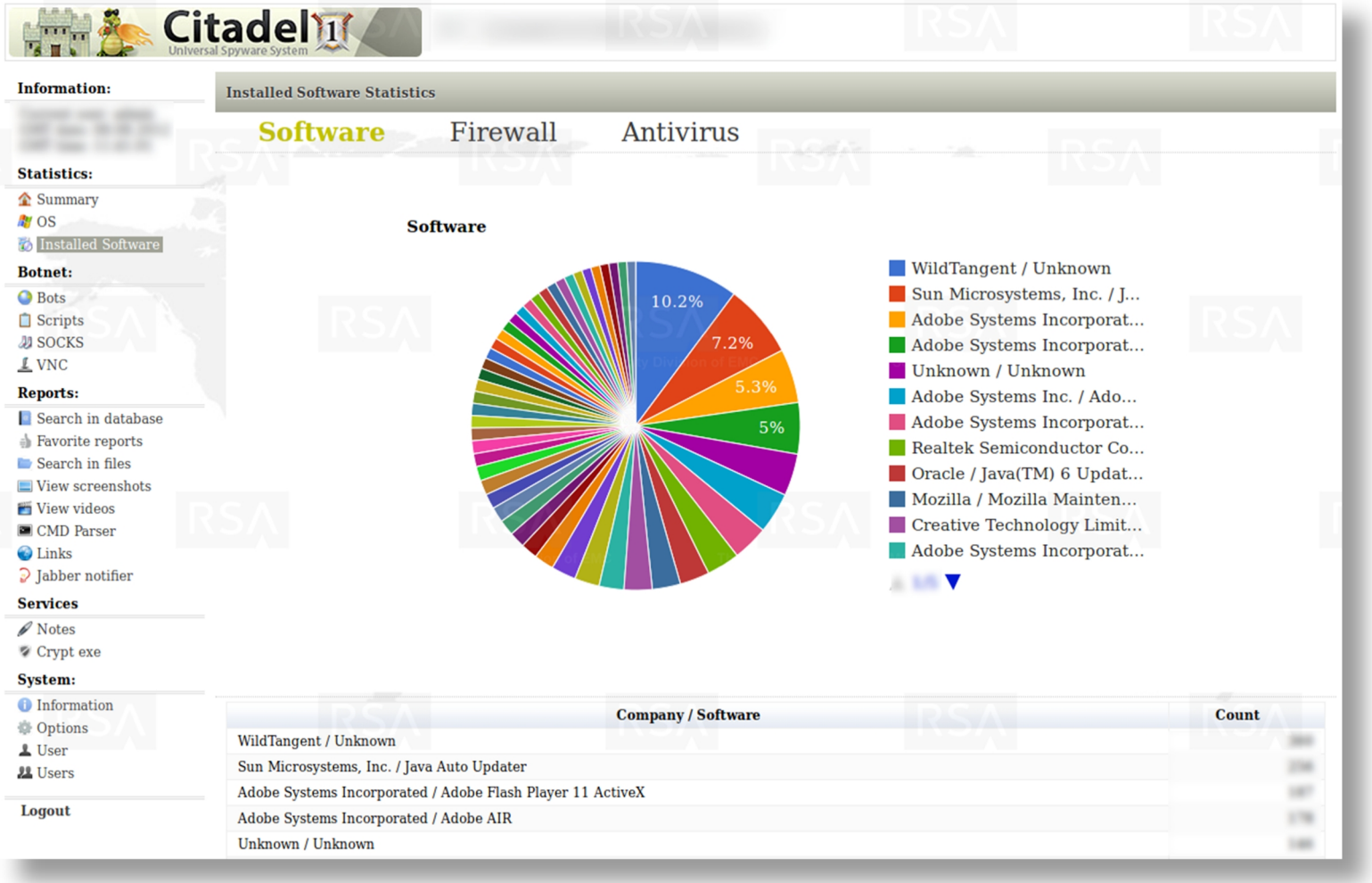
DDoS Attacks



5 TREND5 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

Big Data Analytics



5 TREND5 INTH3WILD

© Copyright 2013 EMC Corporation. All rights reserved.

Questions

© Copyright 2013 EMC Corporation. All rights reserved.