RSACONFERENCE2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Data Encryption For Virtualized Enterprise

SESSION ID: DSP-T07B

Misha Nossik

CTO, VP R&D
AFORE Solutions
@mnossik

AFORE
SECURE THE CLOUD. TRUST THE CLOUD.

The Horror

Adobe's source code was parked on hackers' unprotected server

Kirk   Oct 11, 2013 6:21 AM

...italize on other people's mistakes. But they make their own as well.

...: A massive breach of Adobe Systems' network was discovered after the source

...rous products, including the Web application development platform ColdFusion,

...n a hacker's unprotected Web server open to the Internet.

...d customer credit card records, was

...nvestigating a breach when Alex

...independently found what turned out

SECURITY // ATTACKS & BREACHES

NEWS
4/26/2012
11:23 AM

VMware Breached, More Hypervisor Source Code To Come

Mathew J. Schwartz
News

Hacker Hardcore Charlie reveals stolen VMware source code and documents from Asian defense contractors, promises more disclosures in May.

Is your hypervisor safe?

Inform...

Home   News & Co...

STRATEGIC CIO

RSA SecurID Breach Cost $66 Million

EMC details second quarter 2011 cost to replace tokens, monitor customers, and handle fallout from RSA's SecurID breach.

Virtualisation | Applications | Operating Systems | Ne...

Chinese 'Comment Crew' hackers emptied QinetiQ of top-secret military data

US firm complacent about serious breaches, Bloomberg alleges

By John E Dunn | Techworld | Published: 12:11, 02 May 2013

In Security:
News
Reviews
Features
How-tos
Slideshows

One of the US's critical military and espionage contractors QinetiQ North America (QNA) was successfully pillaged for huge amounts of top-secret know-how by the infamous Chinese 'Comment Crew' or PLA 61398 hacking group in a campaign stretching over years, Bloomberg has reported.
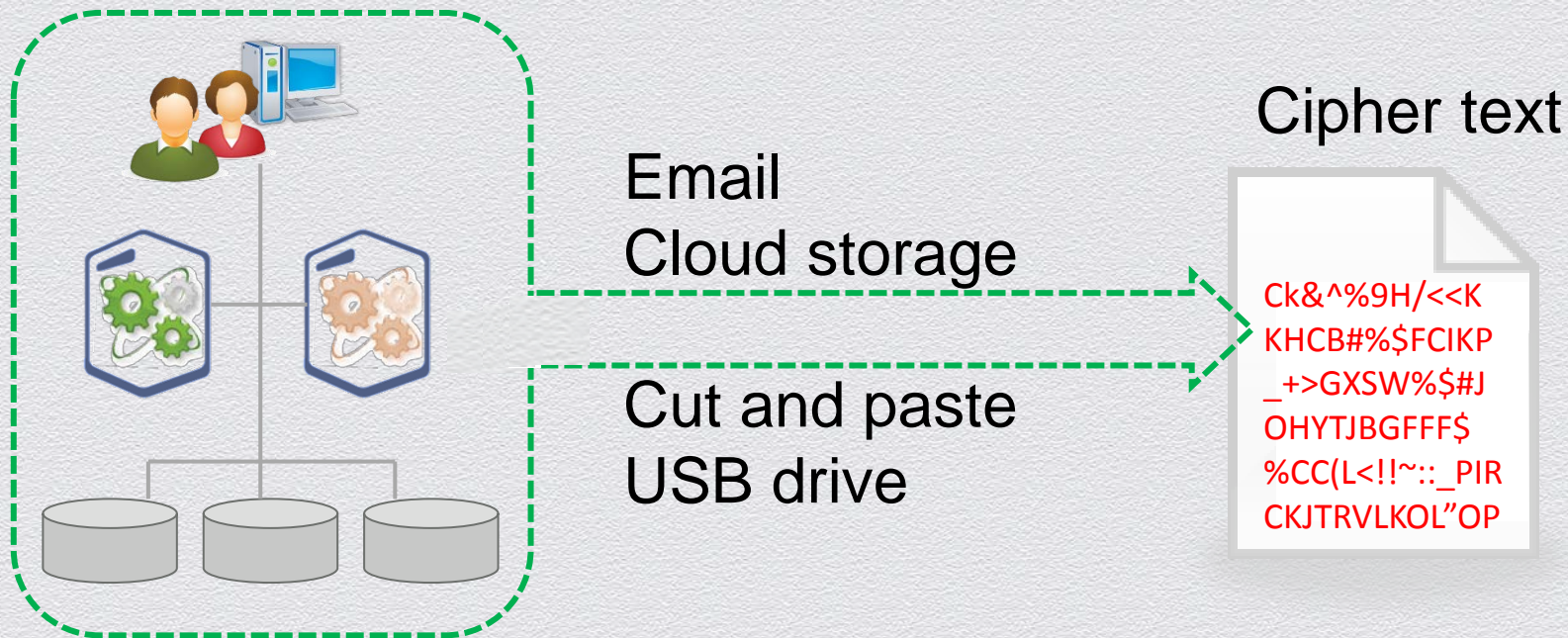
Reports and accusations of Chinese hacking are now ten-a-penny but what has been reconstructed by Bloomberg's journalists after talking to investigators tells a story that will be as embarrassing as it is depressing for both QNA and the US defence establishment.

The hacking was so extensive that external consultants ended up more or less working permanently inside the firm to root out malicious software and compromises on an ongoing basis.

AFORE

SECURE THE CLOUD. TRUST THE CLOUD.

#RSAC

RSACONFERENCE2014

What To Do

#RSAC

RSACONFERENCE2014

Encryption Defined Perimeter

Email
Cloud storage

Cut and paste
USB drive

Cipher text

Ck&^%9H/<<K
KHCB#%$FCIKP
_+>GXSW%$#J
OHYTJBGFFF$
%CC(L<!!~::_PIR
CKJTRVLKOL"OP

#RSAC

RSACONFERENCE2014

Group-Policy–Defined Trust

Authorized User + **Validated OS** + **Certified App** = **Data Decrypted**

Secure App Container

Certified App

Entire Application Stack "Security Zone"

Key Manager

Security Zone

App | Web Server | App Server | DB Server

Sec Admin

AFORE

SECURE THE CLOUD. TRUST THE CLOUD.

#RSAC

RSACONFERENCE2014

What Is Easier?

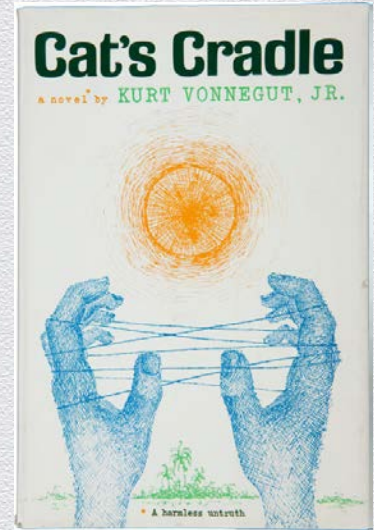**or**

AFORE
SECURE THE CLOUD. TRUST THE CLOUD.

#RSAC
RSACONFERENCE2014
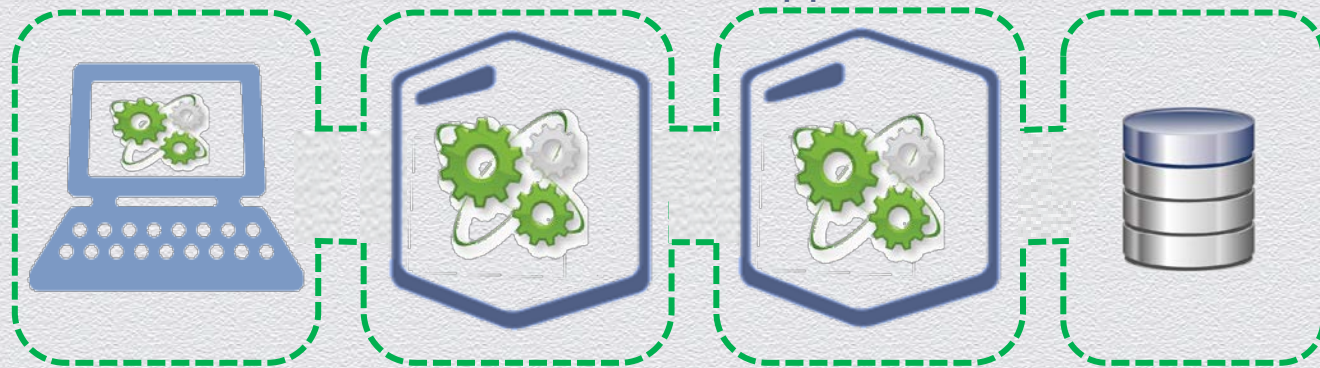
Caution: It Is Contagious

Conclusions

- Encryption is the key element of software-defined perimeter

- Data need to be encrypted at all times until needed for legitimate use

- Sec admin makes security decisions, transparent to users

- In a multi-tiered world of enterprise apps encrypted perimeter extends to all tiers

AFORE

SECURE THE CLOUD. TRUST THE CLOUD.

#RSAC

RSACONFERENCE2014