

***Target
Identification
Through Decoy
File Analysis***

Agenda

- Who am I
- Overview of Spear Phishing + Decoys
- How Decoy Documents Can Help Identify Targets of Exploit Files
- Automation and Future Work

/usr/bin/whoami

- Head of Unit 42 – Palo Alto Networks Threat Intelligence Team
 - Formerly Sr. Manager with Verisign's iDefense Threat Intelligence service.
 - Specialize in Cyber Crime and Espionage



CEO



CSO

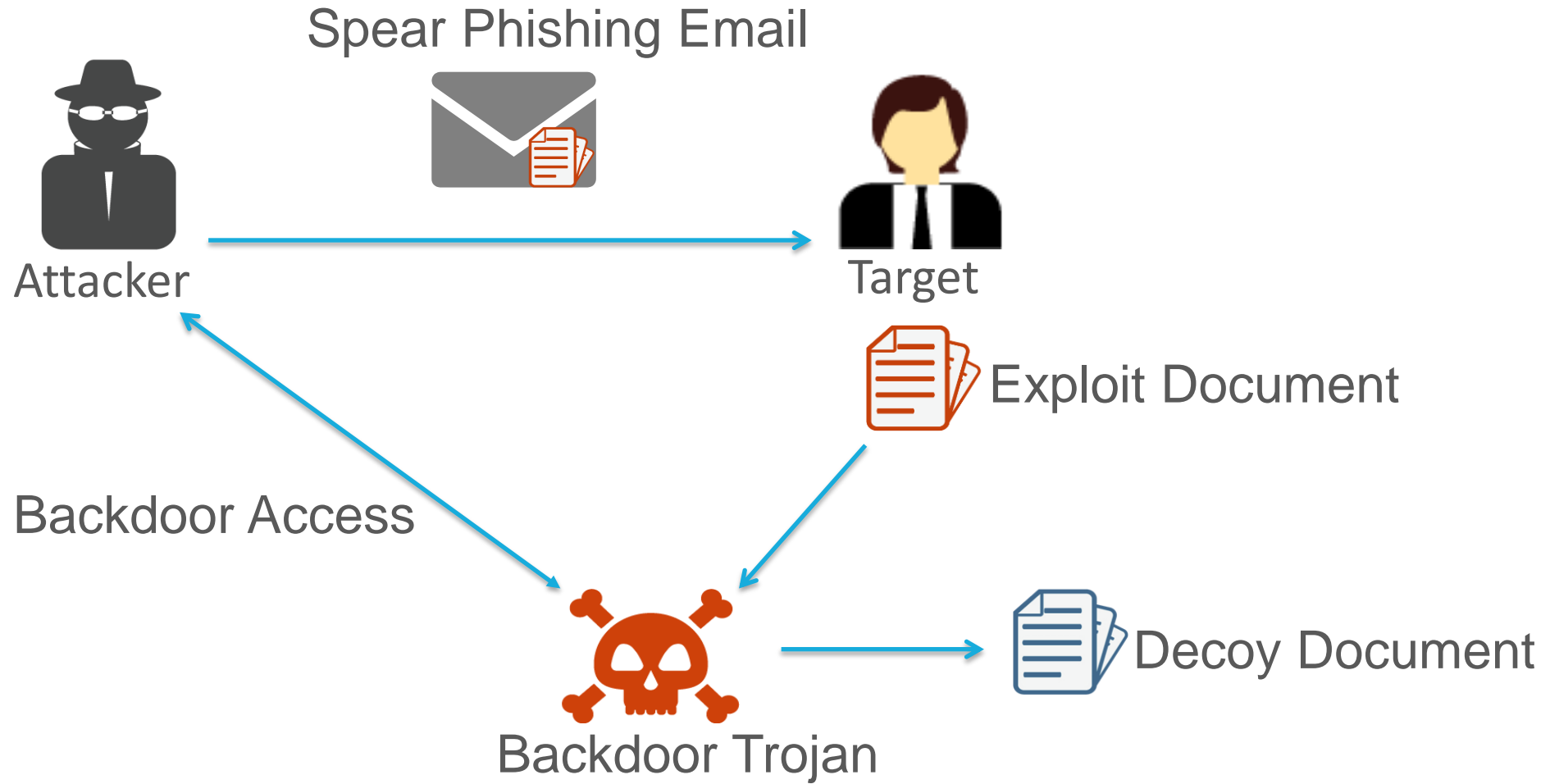




Mission: Analyze the data available to Palo Alto Networks to identify adversaries, their motivations, resources, and tactics to better understand the threats our customers face.



Spear Phishing + Decoy





Recycle Bin



Adobe Reader 9



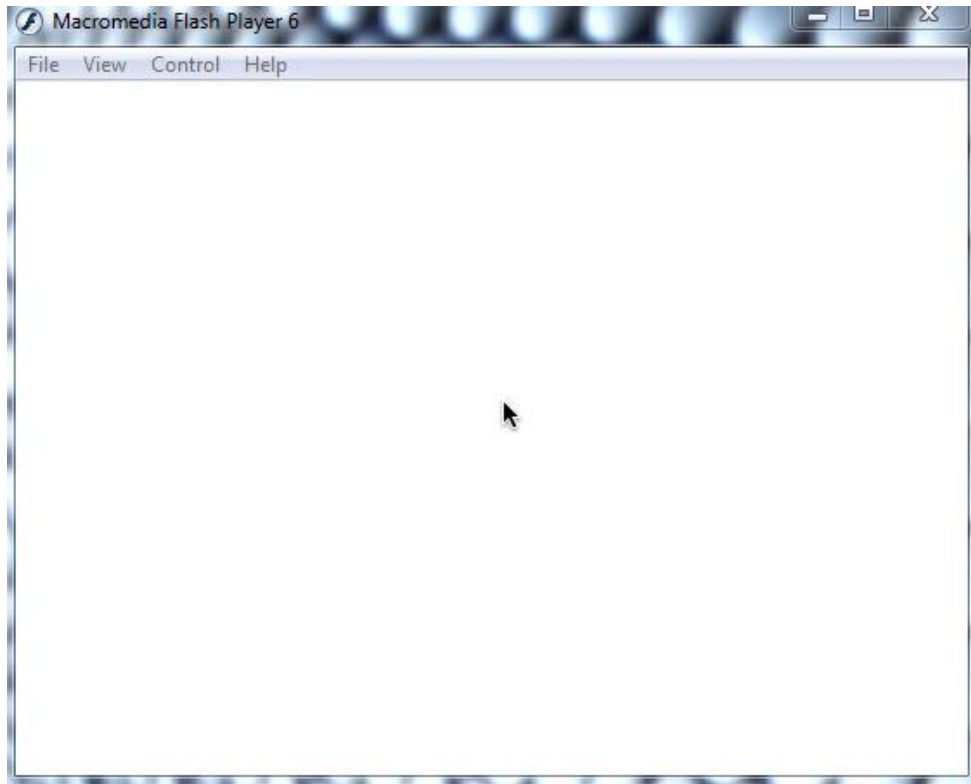
baefile



4:48 PM
9/8/2016

Decoy Examples

ต้น จิตภัสร์ กฤดากร
(Chitpas Tant Kridakon)



News in a Word Document

New computer virus causes havoc

A powerful new computer virus was today causing havoc with e-mail systems across the world.

Experts described the virus, called Goner, as one of the fastest-spreading they had yet seen and warned computer users to immediately delete it if they received it.

Alex Shipp, spokesman for anti-virus service MessageLabs, said: "It's spreading with tremendous speed and thousands of users in Britain have already been sent it.

"The virus mass mails itself out through e-mail and attempts to destroy anti-virus software on computers, which could prove extremely problematic for those unfortunate enough to receive it."

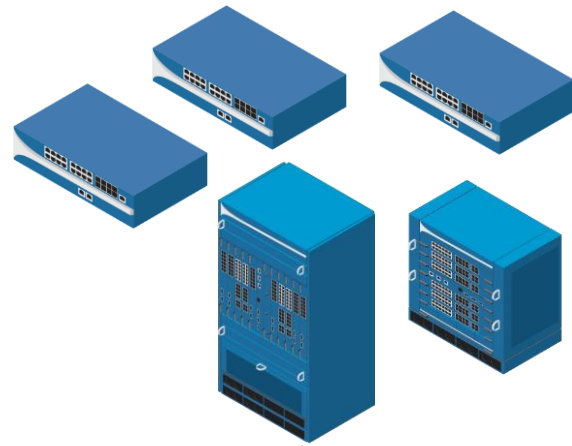
The infected e-mail has the word "Hi" as its subject and body text which reads "When I saw this screen saver, I immediately thought about you. I am in a harry (sic), I promise you will love it." Its attachment is labelled "gone.scr."

It was first detected this morning in the US but experts believe it was created in Europe.

The US, the UK and France are the worst hit of the 17 countries affected so far.

Mr Shipp said: "We had a handful of reports this morning but at mid-afternoon in the UK it went mad. We have had about 30,000 reports and the figure is rising."

Malware Sources + WildFire



Palo Alto Networks Firewalls



Malware Analysis
Verdict Determination



- Unknown Target
- Unknown Delivery Vehicle

Sharing
Partnerships

What Can Decoy Documents Tell us?

What language does the target read?

What topics are they interested in?

When would they have received the document?

What kind of access did the attacker need to get the document?

Decoy Documents to the Rescue : Language

6 Makanan Ini Bantu Sembuhkan Flu



Musim hujan identik dengan serangan flu. Penurunan daya tahan tubuh menyebabkan virus penyebab flu mudah menginfeksi tubuh. Meningkatkan daya tahan tubuh menjadi satu-satunya cara untuk menghalau serangan penyakit ini.

Vaksin ternyata bukan satu-satunya cara mencegah serangan flu. Menurut manajer konten kesehatan About.com, Rachel Berman RD, hidangan yang dikonsumsi sehari-hari ternyata juga bisa berperan menjadi benteng terhadap serangan penyakit yang umum diderita masyarakat dunia ini.

Berikut beberapa asupan yang direkomendasikan Berman sebagai pencegah serangan flu.

1. Biji labu ("pumpkin seed")

Biji labu kaya akan kandungan zinc, yang dapat membantu sel darah putih melawan virus dan penyakit. Berbagai olahan berbahan dasar biji labu bisa mencegah rasa bosan mengonsumsi hidangan satu ini.

Wishing You Merry Christmas

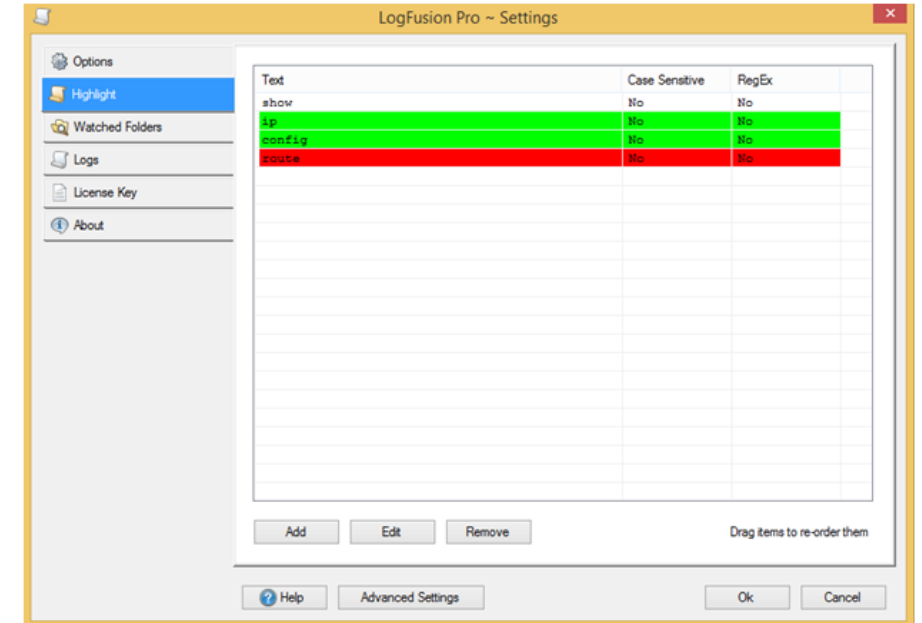


With loves and best wishes to you and your family!

Decoy Documents to the Rescue : Subject Matter

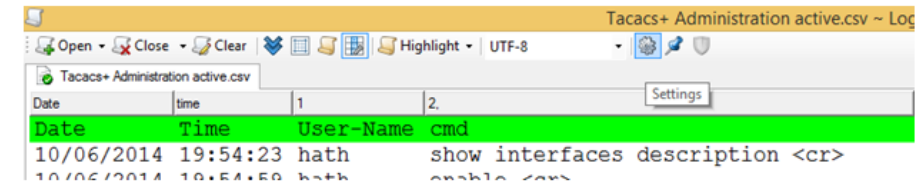


Các màu hiển thị theo thứ tự ưu tiên từ trên xuống dưới, màu nào đặt trên sẽ ưu tiên hiển thị. Thông thường thứ tự ưu tiên là: trắng > lục > đỏ. VD: với câu lệnh show ip route, sẽ hiển thị màu trắng




Lại chọn mục Highlight, tick vào lệnh config vừa tạo

5. Click vào Setting để thay đổi kích thước, font chữ hiển thị.



6. Cuối cùng, click vào Auto-Scroll to Bottom để luôn hiển thị thời gian thực.

Decoy Documents to the Rescue: Timing



GET ANSWERS TO YOUR TOUGHEST CYBERSECURITY CHALLENGES.

Secure your digital way of life today.

[REGISTER NOW](#)

Date : 3 November 2016
Time : 8:00am - 5:00pm
Venue : JW Marriott Hotel, Jakarta

[View Map](#)

Registration Center
Phone : 021-52962835
Fax : 021-52971899
SMS : 0813-8339-3500
Email: paloalto_event@mbicc.org

KEYNOTE AGENDA:

08:00 am Registration Opens
09:00 am Welcome by Emcee
09:05 am Welcome Address
09:15 am Turnaround and Transformation in Cybersecurity
09:45 am Security Breach: Investigation & Awareness
10:30 am Networking Break
10:45 am State of the Nation
11:15 am Panel: Customer Success Story
12:30 am Lunch

TRACK 1:		TRACK 2:	
1:30 pm	Sponsor Session	A Disruptive Endpoint Protection Ecosystems	Sponsor Session
2:00 pm	Migrating from Legacy Firewall	Secure The Cloud	Sponsor Session
2:30 pm	Sponsor Session	APT Prevention & Threat Intelligence	Sponsor Session
3:00 pm	APT Prevention & Threat Intelligence	Networking Break	
3:30 pm	Networking Break	Cyber Threat Intelligence Sharing	Sponsor Session
3:45 pm	Sponsor Session	Security in SDN	Sponsor Session
4:15 pm	Security in SDN	Defining a Modern Approach to Mobile Security with GlobalProtect	
4:45 pm	Sponsor Session		

INVITATION TO A SPECIAL SCREENING OF THE NORWEGIAN MOVIE "KON-TIKI"

In celebration of the 100th anniversary of the birth of the Norwegian explorer and adventurer Thor Heyerdahl, the Norwegian Embassy has the pleasure of inviting you and a guest to a special film evening featuring the 2012 Norwegian historical drama "Kon-Tiki". The film was nominated for the 2013 Oscars in the category "Best Foreign Film" and tells the story of Thor Heyerdahl and his 1947 Kon-Tiki expedition (see attached flyer). The screening will be preceded by a reception.

Venue: Cinémathèque, 22A Hai Ba Trung Street, Hoan Kiem, Hanoi

Date: 13 December, 2014

Time: Reception 19:00-20:00, Screening at 20:00

Seating is limited and based on a "first come, first served" basis. Reservations should be made by sending an email to officer.norwegian@yahoo.com.vn, no later than 12 December. In your e-mail, please advise if you will bring a guest.

If you are unable to attend, please forward this invitation to a colleague.



Decoy Documents to the Rescue : Decoy Source

India Bangladesh Relations: The Way Ahead

The reality of India-Bangladesh relations as it stands today is far removed from the idealism in bilateral relations which has been cherished since the Liberation War, especially in India. This book examines the irritants between the two countries and suggests a road map for improving relations.

The book covers the geography and history of Bangladesh as a backdrop. Thereafter, the strategic importance of Bangladesh to India, security perceptions of Bangladesh and a few economic aspects have been covered. A chronological review of Bangladesh's foreign policy towards India and her relations with other countries has been carried out in a separate chapter. This is followed by a detailed examination of the irritants between the two countries.

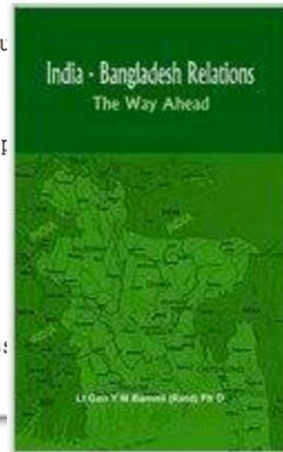
The views of a large cross-section of eminent personalities of both the countries have been included to substantiate the existing relations.

In the Final Chapter, 'The Way Ahead', the author has suggested an action plan for the future.

India Bangladesh Relations: The Way Ahead

by Lt Gen Y M Bammi (Retd) (Author)

Be the first to review this item



ISBN-13: 978-9380177212

ISBN-10: 9380177216

[Why is ISBN important?](#)

Have one to sell?

[Sell on Amazon](#)

[Add to List](#)

Hardcover

\$60.00

Other Sellers

from \$19.88

Buy new

Temporarily out of stock.

Order now and we'll deliver when available. [Details](#)

Ships from and sold by Amazon.com. Gift-wrap available.

FREE Shipping for Prime members once available

\$60.00

6 New from \$19.88

Qty: 1

[Add to Cart](#)

[Turn on 1-Click ordering](#)

Ship to:

Ryan Olson- Reston - 20190

More Buying Choices

6 New from \$19.88 | **1 Used from \$21.07**

7 used & new from \$19.88

[See All Buying Options](#)

The reality of India-Bangladesh relations as it stands today is far removed from the idealism in bilateral relations which has been cherished since the Liberation War, especially in India. This book examines the irritants between the two countries and suggests a road map for improving relations. The book covers the geography and history of Bangladesh as a backdrop. Thereafter, the strategic importance of Bangladesh to India, security perceptions of Bangladesh and a few economic aspects have been covered. A chronological review of Bangladesh's foreign policy

[Read more](#)

[Report incorrect product information](#)

Decoy Documents to the Rescue : Decoy Source

A screenshot of the Microsoft Excel application interface. The window title is "c19d3242d43c71f03f... Search Sheet". The ribbon includes Home, Insert, Page Layout, Formulas, Data, Review, and View. The Home tab is active, showing options for Paste, Font, Alignment, Number, Conditional Formatting, Format as Table, Cell Styles, Cells, and Editing. The active cell is H23. The spreadsheet contains several tables of redacted data. One table has columns: NAMES, DESIGNATION, BIRTH DATE, and CELL NUMBER. Other sections are labeled "COMMAND GROUP", "CENTRAL STAFF", and "KEY PERSONNEL - as of 23 June 2014".

DIRECTORY

As of 03 December 2013

RANK/NAME	NICKNAME/ NICKNAME OF WIFE	DESIGNATION	MILITARY LINE
COMMAND			
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
COORDINATING STAFF			
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
PERSONAL STAFF			
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
SPECIAL STAFF			
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Decoy Documents to the Rescue : Organization Specific

OUTGOING DISPATCH

CALL SIGN	SERIAL NR	PRECEDENCE	DATE/TIME	X'MITTING INSTRN
	017	PRIORITY	130930H SEPT 13	H/C
FM:			DRFTD BY:	
TO:			APPRVD BY:	
INFO:			RLSD BY:	

GNRC

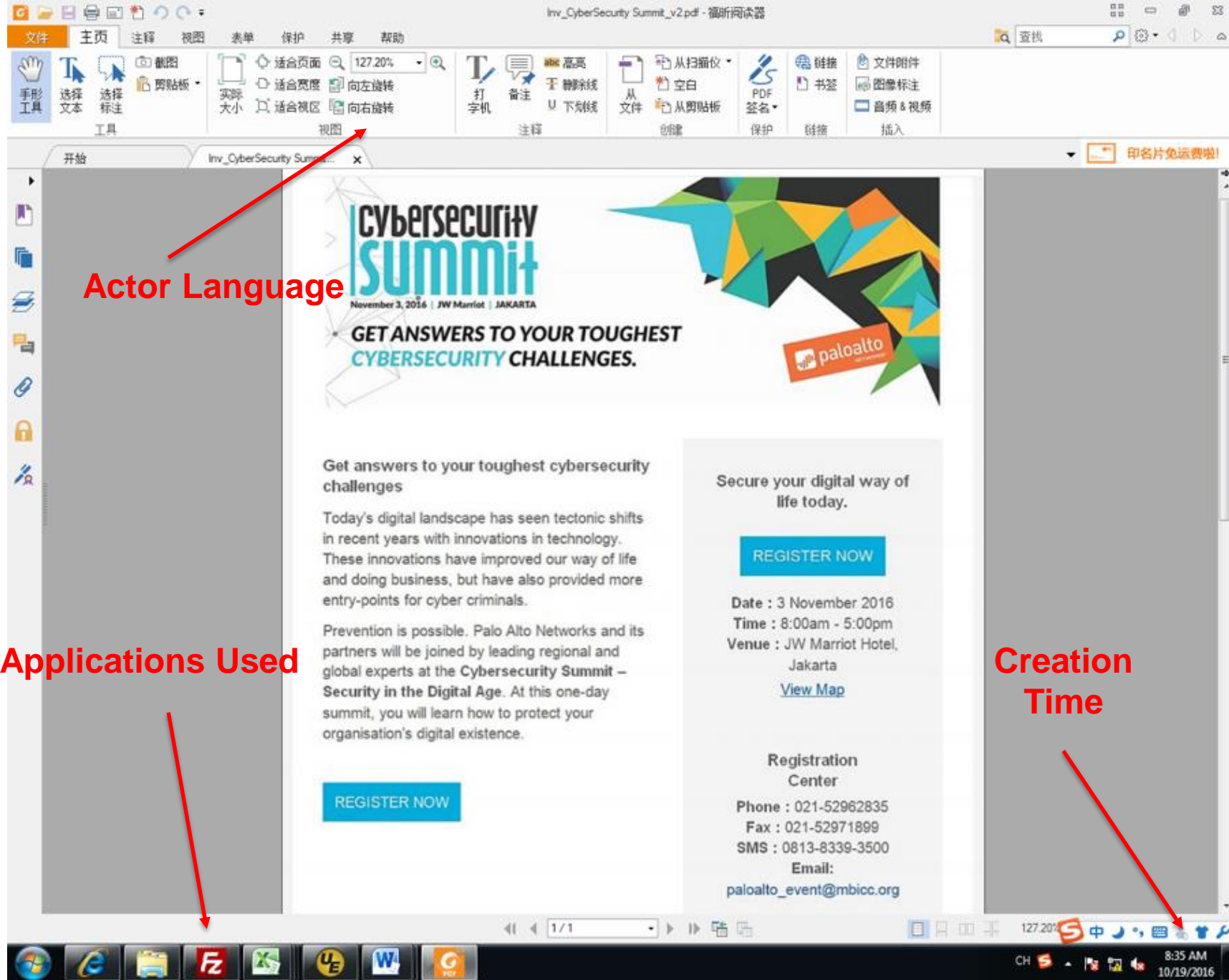
BT... CONFID X CITE DISPATCH REQUISITION

1. RQST AVAIL ONE (1) EA MOUTHPIECE OF LOUD HAILER TO BE USED BY THIS UNIT
2. AS PER INSPECTION CONDTD BY CMM THE MOUTHPIECE OF LOUD HAILER OF THIS UNIT IS ALREADY DETERIORATED AND NEEDS IMMEDIATE REPLACEMENT TO MAINTAIN THE INTERNAL COMMUNICATION OF THIS UNIT
3. IF AVAIL CMM RQST SEND TO THAT WILL BE PROCEEDING IN NFNL AOR TO CONDUCT REPAIR X THIS UNIT IS CURRENTLY MOORED P/S TO M/V
4. RQST ADV

BT...

TOD/ _____

Actor Mistakes



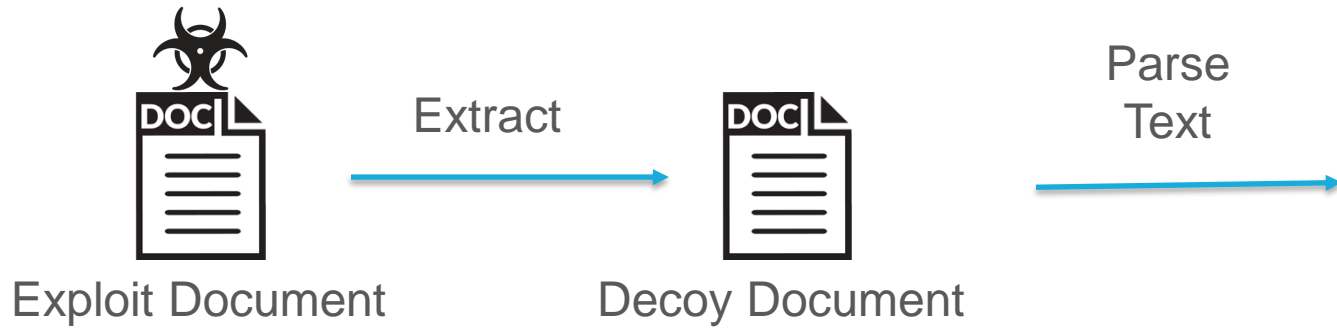
Actor Language

Applications Used

Creation Time



Automation and Future Work



India Bangladesh Relations: The Way Ahead\x0D\x0DThe reality of India-Bangladesh relations as it stands today is far removed from the idealism in bilateral relations which has been cherished since the Liberation War, especially in India. This book examines the irritants between the two countries and suggests a road map for improving relations.\x0D\x0DThe book covers the geography and history of Bangladesh as a backdrop. Thereafter, the strategic importance of Bangladesh to India, security perceptions of Bangladesh and a few economic aspects have been covered. A chronological review of Bangladesh\x92s foreign policy towards India and her relations with other countries has been carried out in a separate chapter. This is followed by a detailed examination of the irritants between the two countries.\x0D\x0D The views of a large cross-section of eminent personalities of both the countries have been included to substantiate the existing relations.\x0D\x0D In the Final Chapter, \x91The Way Ahead\x92, the author has suggested an action plan for the future.\x0D\x0D\x0D\x0D Russ Fowler\x0DCanada\x0D\x03\x0D\x0D\x04\x0D\x0D\x03\x0D\x0D\x04\x0D\x0D\x0D

Identify Themes
And Group Documents



Generate
Word-cloud

More like this...



Contact info:

rolson@paloaltonetworks.com

Blog:

researchcenter.paloaltonetworks.com/unit42

