

# Attacks and Defenses in the Cyber Landscape

Who are the cyber attackers?



# Who are the cyber attackers?

- Nation State
- Cyber Criminal Groups
- Script Kiddies

# Who are the cyber attackers?

- Nation States
- Cyber Criminals
- Script Kiddies

## CYBERSECURITY

[TECH](#) | [MOBILE](#) | [SOCIAL MEDIA](#) | [ENTERPRISE](#) | [CYBERSECURITY](#) | [TECH GUIDE](#)

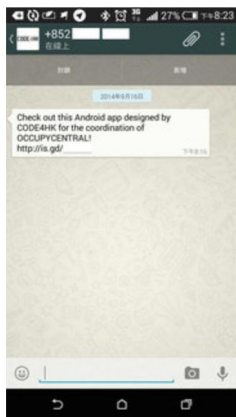
### **In India-Pakistan conflict, there's a long-simmering online war, and some very good hackers on both sides**

- A longstanding conflict between India and Pakistan escalated Wednesday when the countries said they carried out airstrikes against one another.
- Experts have long warned about a two-decade long cyber rivalry that has also continually escalated into the present day.
- India and Pakistan have carried out increasing cyberattacks against one another.
- The conflict has also been plagued by the rapid spread of inflammatory rumors on Facebook and messaging services, some of which have escalated into real hands-on fighting.

## TECHNOLOGY

# Protesters in Hong Kong Are Targets of Scrutiny Through Their Phones

By PAUL MOZUR OCT. 1, 2014



An example of a phishing message delivered to Whatsapp users in Hong Kong.

HONG KONG — As tens of thousands of protesters in Hong Kong continued to shut down the city’s main arteries on Wednesday in a call for democracy, a quieter struggle was playing out to monitor the demonstrations online.

The most recent salvo came to light on Tuesday, when Lacocon Mobile Security said that it had tracked the spread of a fake mobile application aimed at eavesdropping on protesters’ communications. In what is known as a phishing attack, smartphone users in Hong Kong have been receiving a link on WhatsApp to download the software, along with a note: “Check out this Android app designed by Code4HK for the coordination of OCCUPY CENTRAL!”

hands-on fighting.

## RELATED COVERAGE



## MACHINE LEARNING

Mobile Malware: Small Numbers, but Growing OCT. 1, 2014

## SINOSPHERE BLOG

Message for Beijing Hidden in a Hong Kong Street Poem OCT. 1, 2014



Hong Kong Government’s Strategy on Protesters: Wait Them Out OCT. 1, 2014



## SINOSPHERE BLOG

To Beat China Censorship, Hong Kong Protesters Flock to Off-Grid Messaging App SEPT. 29, 2014

W

Inbox  
https://inbox.google.com

The New York Times

SUBSCRIBE N

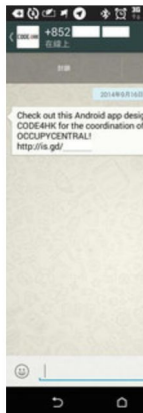
867 views | Feb 26, 2019, 12:10pm

TECHNOLOGY

*Proteste*

By PAUL MOZUR

# Cybercrime & Hackers 'More Devastating' To SMB's Than Fire, Flood & Transit Strike Combined



**Roger Aitken** Contributor ⓘ

Markets

An example of a phishing message delivered to Whatsapp users in Hong Kong.

Android app designed by Code4HK for the coordination of OCCUPY CENTRAL!"



SINOSPHERE BLOG

To Beat China Censorship, Hong Kong Protesters Flock to Off-Grid Messaging App

SEPT. 29, 2014

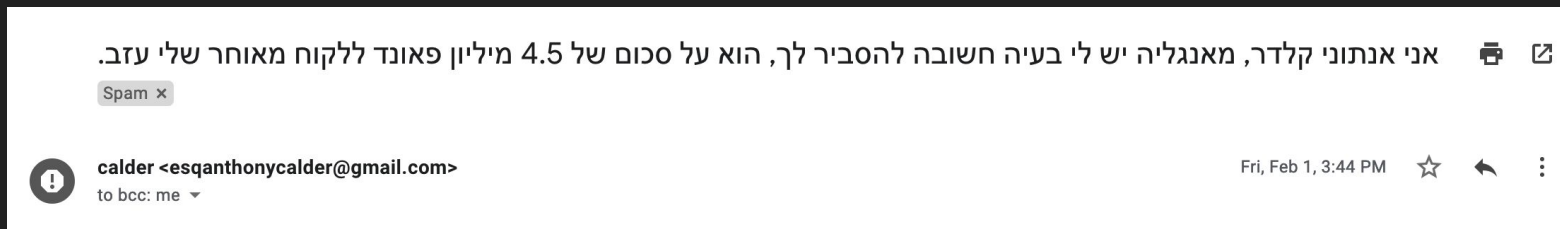
hands-on fighting.

# Cyber Attacks - The Basics

- Social Engineering
- Exploits

# Cyber Attacks - The Basics

- Social Engineering
- Exploits





# Cyber Attack

- Social Engineering
- Exploits

לי עזב.

Spam x



calder <e...>  
to bcc: me

Applications Places System | Fri Oct 22, 9:44 AM | ran

81-86-54-21.dsl.pipex.com/www.bankhapaolim.co.il

Gmail Google Reader ynet Facebook אינטרנט ישראל URL Decoder/Enc... Other Bookmarks

### מגוון הטבות ייחודיות חדי חודש

למידע נוסף

### חדש מבנק הפועלים: הלוואה רב ערוצית - מכל מקום ובכל זמן

למידע נוסף

### שירות מטיח בטרמינל: מזמינים מטיח לפני הטיסה ואוספים אותו בשדה התעופה.

למידע נוסף

### אפליקציית הארגון הסולרי מהיום, ה- iPhone שלכם מחליף את הארגון!

להורדה חינם AppStore-מ

### מעוניין לפתוח חשבון בבנק הפועלים? פתח חשבון עכשיו

### פועלים באינטרנט בשוק ההון

מט"ח	תל אביב	חול
3.610 21.10.10 דולר יציג	1.24%	1272.25 25 א"
5.064 21.10.10 איח יציג	1.05%	1172.9 100 א"
3.5% רביית פריים	1.08%	231.5 15 טק-ט

נכון ל: 16:26 21.10.10

תל אביב 25 אביב 100 לפורטל הפיננסי

### עוד באתר

מפת אתר  
תעריפון הבנק  
מחשבוני  
Newsletter  
RSS  
מילון מונחים  
תנאי גישה

### הבנק ופעילותו

אודות הבנק  
אחריות חברתית  
פועלים בקהילה  
דרושים

### עוד בפועלים

משכנתא  
פועלים אקספרס  
פעילים  
ישראלט

### מוצרים ושירותים

יתרון מובהק  
פיקדונות  
תוכניות חיסכון  
אמות פריקט בבניה  
הלוואות

### לקוחות

בנקאות פרטית  
סטודנטים  
חיילים  
צעירים  
דן חסן

### ערוצי שירות


סקיפים  
אינטרנט  
טלון  
סלולרי  
אי"פון  
שירות עצמי  
פועלים במייל

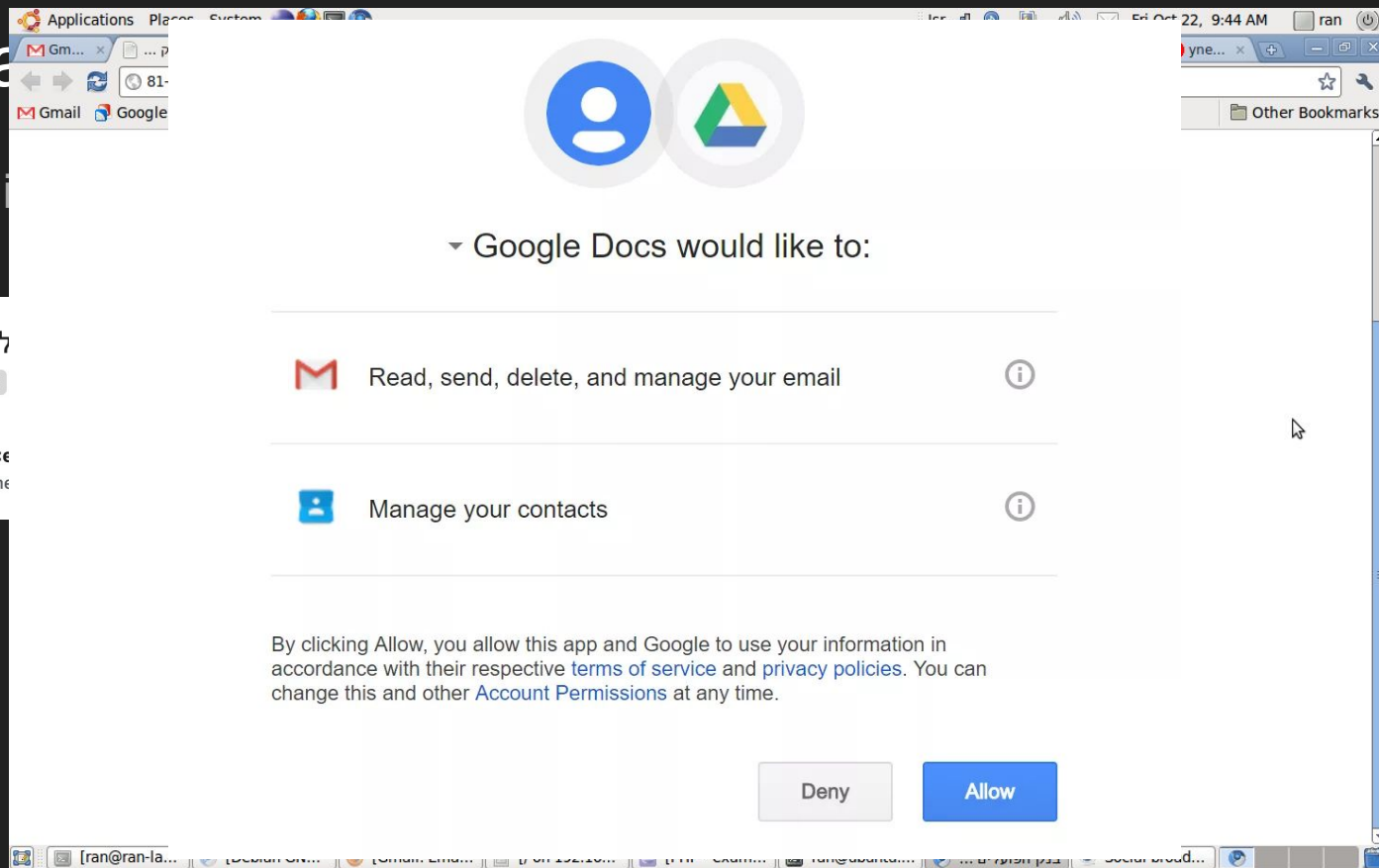
[ran@ran-la...] [Debian GN...] [Gmail: Ema...] [/ on 192.16...] [PHP - exam...] ran@ubuntu... בנק הפועלים ... Social broad...

# Cyber Attack





- Social Engineering
- Exploits

לי עזב.  
Spam x

 calder <e...>  
to bcc: me



The screenshot shows a browser window with a Google account permission dialog box. At the top, there are two circular icons: a blue person icon and the Google Docs logo. Below them, the text reads "Google Docs would like to:". There are two permission items listed:

-  Read, send, delete, and manage your email 
-  Manage your contacts 

At the bottom, there is a paragraph of text: "By clicking Allow, you allow this app and Google to use your information in accordance with their respective [terms of service](#) and [privacy policies](#). You can change this and other [Account Permissions](#) at any time." Below this text are two buttons: a grey "Deny" button and a blue "Allow" button.

# Cyber Attacks - The Basics

- Social Engineering
- Exploits
  - Clickless
  - With social engineering

# Cyber Attacks - The Basics

- Social Engineering
- Exploits
  - Clickless
  - With social engineering

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

## HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

# Cyber Attacks - The Basics

- Social Engineering
- Exploits
  - Clickless
  - With social engineering

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

UK bank falls victim to SS7 attacks, allowing cybercriminals to drain accounts and reminding us why SMS two-factor authentication sucks

26



Jason Hahn

Feb 3, 2019



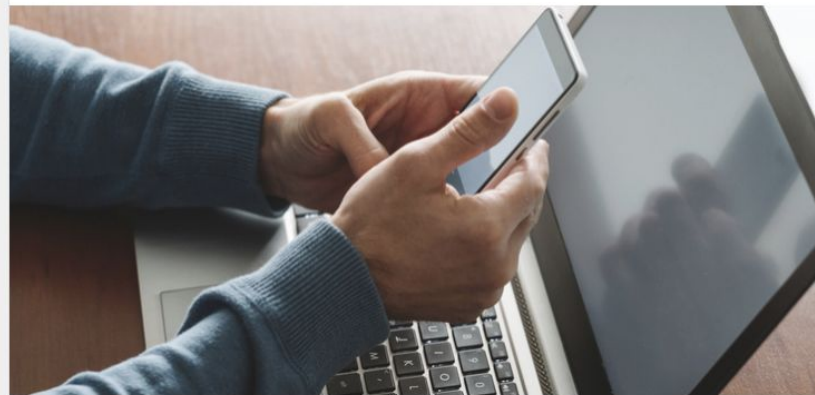
f 147



92

Total Shares 239

NEWS



I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

# Cyber Attacks - What do They Want?

- Money
- Data
- Resources

# Ransomware

- Financial Impact (2017)
  - Paid ransom - \$25M
  - Indirect damage - \$5 Billion



# Target Breach - Overview

- Discovered in December 2013
  - Target announced that it had been breached by attackers
- 70M customers PII's were stolen
- 40M credit cards were stolen





Load [Mozilla Firefox](#) [Google Chrome](#) [Opera](#)

Country	Dump type	Dump mark	Debit/Credit
<input type="text" value="All"/>	<input type="text" value="All"/>	<input type="text" value="All"/>	<input type="text" value="All"/>
Bins	Bank & State & City	Base and other	Additional
2,376282	<input type="text" value="All"/>	<input type="text" value="All"/>	<input type="checkbox"/> Expired 12/13 <input type="checkbox"/> Track1 <input type="text" value="Exp. date (1312)"/> <input type="text" value="Last 4 Digits"/> <input type="text" value="Select code"/>

Find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - [REDACTED] [500k of fresh dumps](#)

Bin	Card	Debit/Credit	Mark	Expired	Track 1	Code	Country	Bank	Base	Price	Cart
551686	MASTERCARD	DEBIT	STANDARD	11/14	Yes	101	United States, MI, GRAND RAPIDS, 49512	CHEMICAL BANK	Tortuga-6	26.6\$	<input type="button" value="+"/> +
414709	VISA	CREDIT	SIGNATURE	02/16	Yes	101	United States, PA, HARRISBURG, 17111	CAPITAL ONE BANK (USA) N.A. <i>Dump or cc of this particular bank (BIN) cannot be replaced or refunded.</i>	Tortuga-6	39.2\$	<input type="button" value="+"/> +
512107	MASTERCARD	CREDIT	GOLD	02/16	Yes	101	United States, AZ, MESA, 85206	CITIBANK N.A. <i>Dump or cc of this particular bank (BIN) cannot be replaced or refunded.</i>	Tortuga-6	44.8\$	<input type="button" value="+"/> +

# Monetization

- Credit card data was sold in the underground market
- Range in price from \$26.60 to \$44.80 to each card number
- Hackers sold between 1-3 millions cards, profiting around \$53M dollars

# Aftermath

- Direct financial damages to reported by Target are \$252 million
- In March, 2014, Target's CIO, Beth Jacob, resigned
- In May, 2014, Gregg Steinhafel, Target's CEO resigned
- In the fourth quarter of 2013, Target's profits dropped 46% compared with the year before
- Estimated dollar cost to credit unions and community banks for reissuing 21.8 million cards stolen in the Target breach is 100\$ million

# Botnets



**CNN BUSINESS** Markets Tech Media Success Perspectives Video 🔍 ☰

## Massive cyberattack turned ordinary devices into weapons

by Samuel Burke @CNNTech

🕒 October 22, 2016: 10:37 AM ET

[👍 Recommend 0](#) [✉](#) [f](#) [🐦](#) [in](#) [⋮](#)

This image is a screenshot of the top portion of a CNN Business news article. The header features the CNN Business logo on the left, followed by navigation links for Markets, Tech, Media, Success, Perspectives, and Video. On the right side of the header, there are icons for search and a menu. The main headline is "Massive cyberattack turned ordinary devices into weapons" in a large, black, sans-serif font. Below the headline, the author's name "by Samuel Burke" and Twitter handle "@CNNTech" are displayed. A timestamp "October 22, 2016: 10:37 AM ET" is shown on the left. On the right, there is a "Recommend 0" button and a row of social media sharing icons for email, Facebook, Twitter, LinkedIn, and a more options menu.

# Smartphones - Why Are They Interesting?

- Sensors
- Data
  - Contain personal information
  - Have access to organizational data
  - Bring Your Own Device (BYOD)

# מייסדי NSO רוכשים את השליטה בחברה לפי שווי של 800 מיליון דולר

שלו חוליו ועמרי לביא, בשיתוף הקרן האירופית נובלפינה, רוכשים את השליטה בחברת הסייבר הישראלית מקרן פרנסיסקו פרטנרס. חוליו ולביא צפויים להשקיע במהלך כ-100 מיליון דולר



הגר רבט, כלכליסט פורסם: 14:55 , 14.02.19

מייסדי קבוצת NSO, בשיתוף נובלפינה - קרן פרייבט אקוויטי אירופית, רוכשים את החברה מידי קרן פרנסיסקו פרטנרס בעלת השליטה. עפ"י הערכות העסקה תתבצע לפי שווי של 800 מיליון דולר.

- [למ"ס: צניחה במכירת דירות חדשות ב-2018](#)
- [נפרדים מהסופר ג'מבו: איירבוס תפסיק לייצר את מטוס ה-A380](#)
- [פרסומת להלוואה: בנק ישראל קנס את ישראלכרט ב-675 אלף שקל](#)

What can we do?



What can we do?







# What are the damages?

- 38% of the businesses breached estimated costs between \$1M to \$5M+
  - Downtime
  - Records
  - Fines
  - Notification

## Types of Headache

**Migraine**



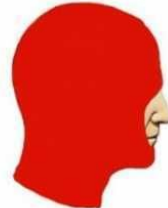
**Hypertension**



**Stress**



**Insurance**



Thanks!