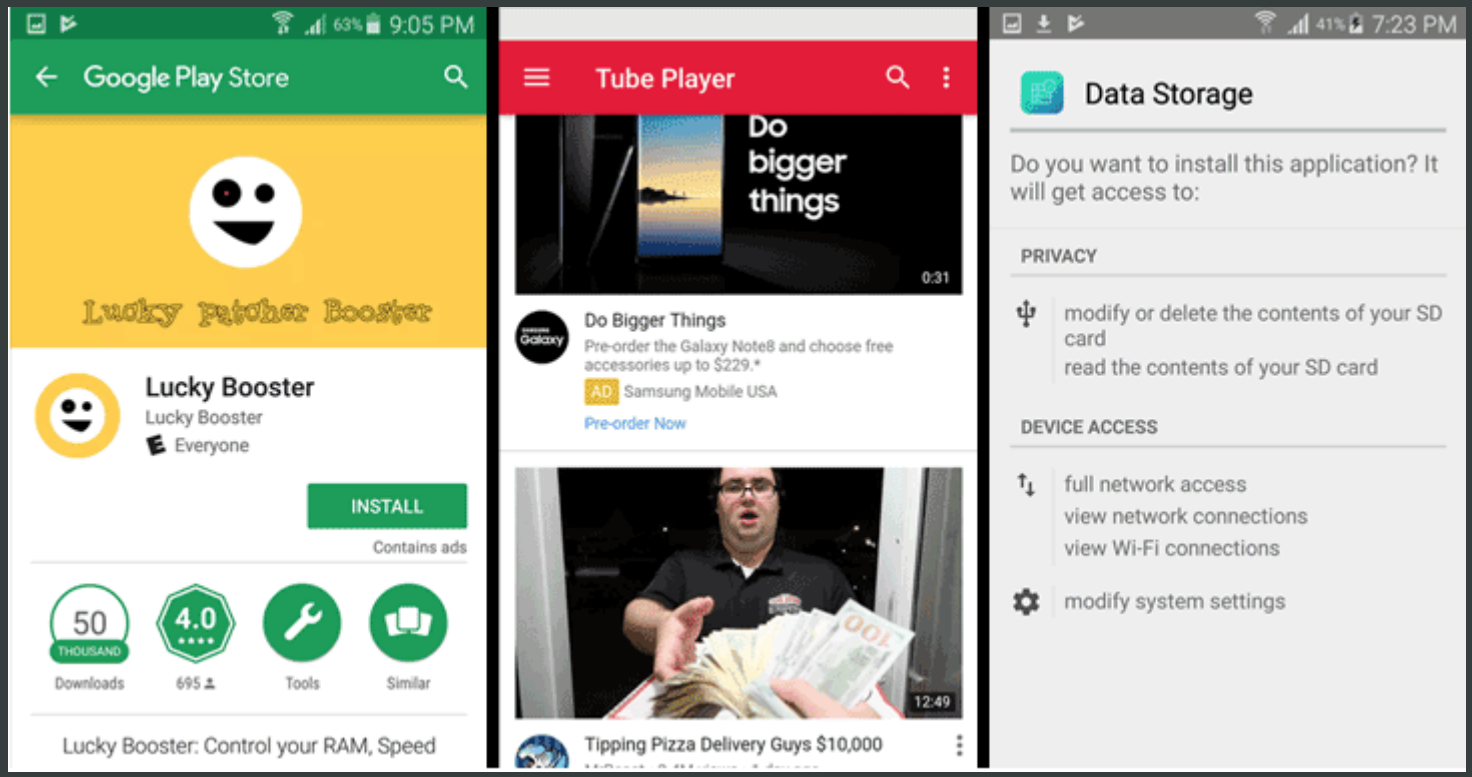
Security News Bytes

BY - APURV SINGH GAUTAM

WireX Android DDoS Botnet

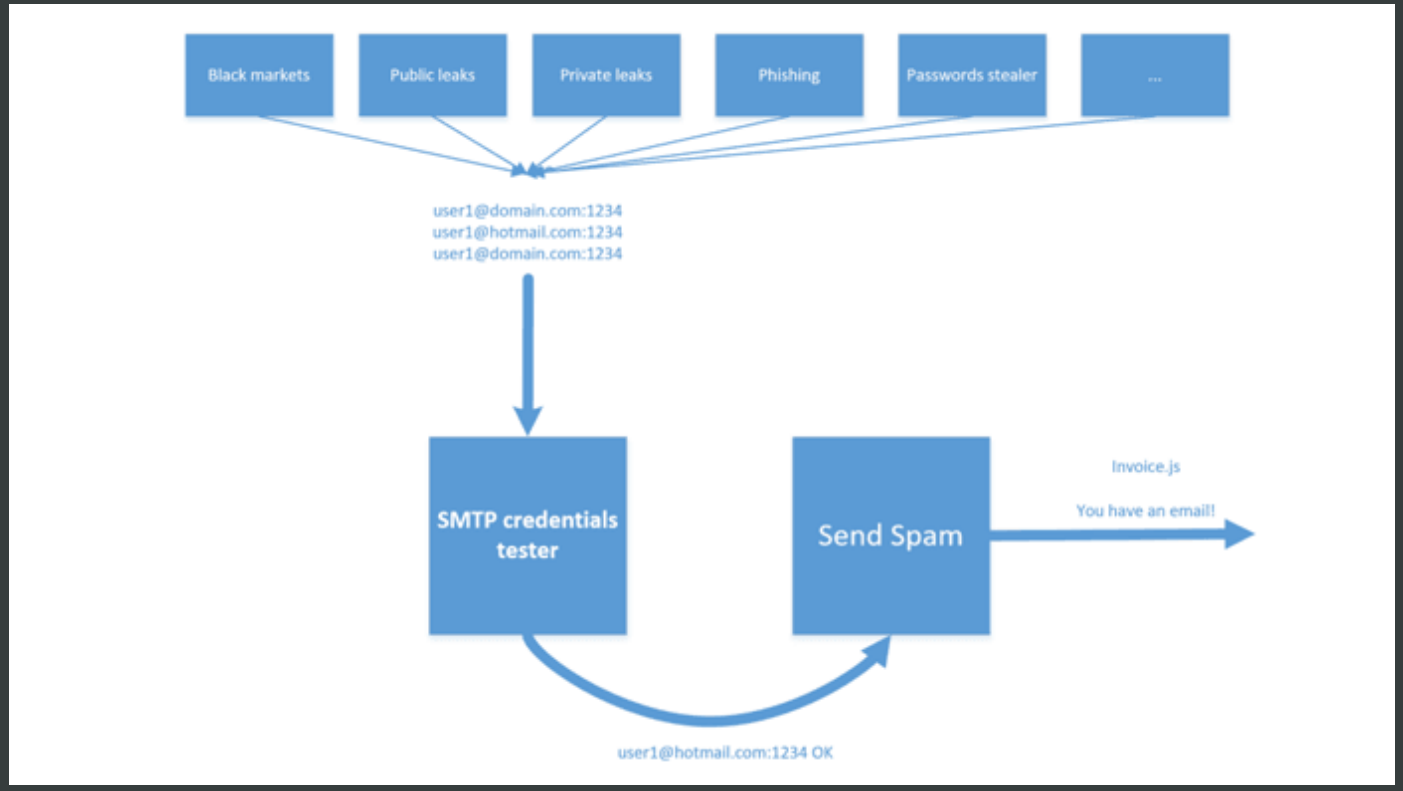
- Security Researchers have uncovered a new, widespread botnet
- WireX detected as “Android Clicker”, includes Android devices running one of the thousands malicious apps installed from Google Play store
- It is designed to conduct massive application layer DDoS attacks
- It has infected 120,000 Android smartphones by this month.
- Researchers noticed massive DDoS attacks (primarily HTTP GET requests) originated from more than 70,000 infected mobile devices from over 100 countries
- There are more than 300 malicious apps on Google Play which include the malicious WireX code.

- You can be protected if you have a newer version of Android that include Google Play's Protect feature, the company will automatically remove WireX apps from your device.
- Google removed around 500 Android apps utilising the rogur SDK that secretly distribute spywares to the users.



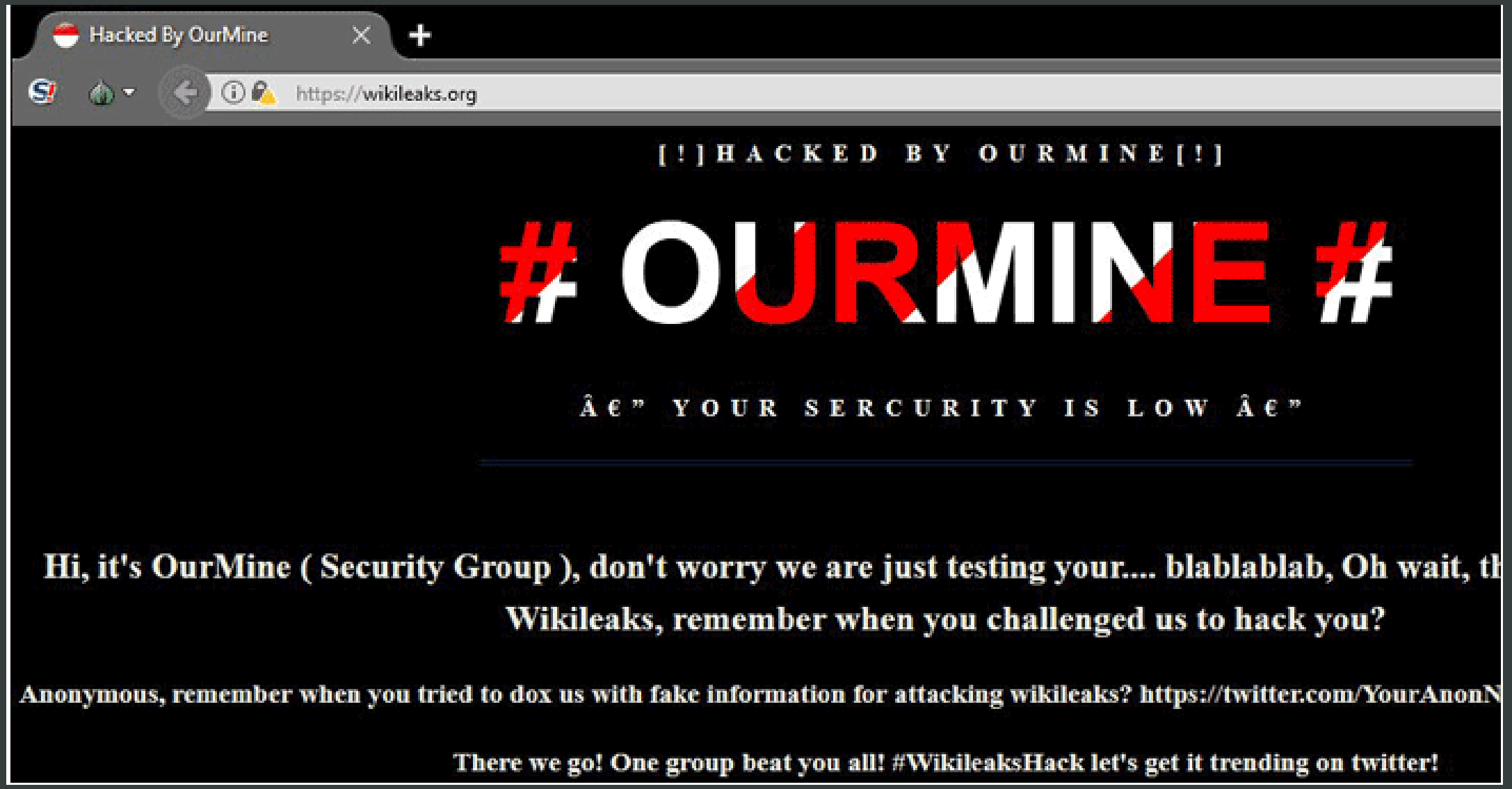
Email Address exposed from SpamBot Server

- 630 million email addresses used by a spambot to send large amounts of spam
- Hosted in Netherlands and stored without any access
- Used to send out spam and spread a banking trojan called Ursnif



Wikileaks Website Defaced by OurMine

- The notorious hacking group is known for breaching high-profile figures and companies' social accounts
- Including Facebook CEO Mark Zuckerberg, Twitter CEO Jack Dorsey, Google CEO Sundar Pichai, HBO, Game of Thrones, etc.
- There is no sign of WikiLeaks servers and website been compromised instead their website has been redirected to a hacker-controlled server using DNS poisoning attack.
- Soon WikiLeaks recovered their website.


Hacked By OurMine
https://wikileaks.org
[!]HACKED BY OURMINE[!]
OURMINE
Â€" YOUR SERCURITY IS LOW Â€"
Hi, it's OurMine (Security Group), don't worry we are just testing your.... blablablab, Oh wait, th
Wikileaks, remember when you challenged us to hack you?
Anonymous, remember when you tried to dox us with fake information for attacking wikileaks? https://twitter.com/YourAnonN
There we go! One group beat you all! #WikileaksHack let's get it trending on twitter!

Instagram Data Breach

- Hackers gained email addresses and phone numbers of many high-profile users.
- The flaw resides in Instagram’s application programming interface (API), which the service uses to communicate with other apps.
- The Instagram’s mobile API contains flaw specifically in the password reset option, which exposed mobile numbers and email addresses of the users in JSON response
- Instagram declined to name the high-profile users targeted in the breach
- The hacker name was unknown
- No account password were exposed

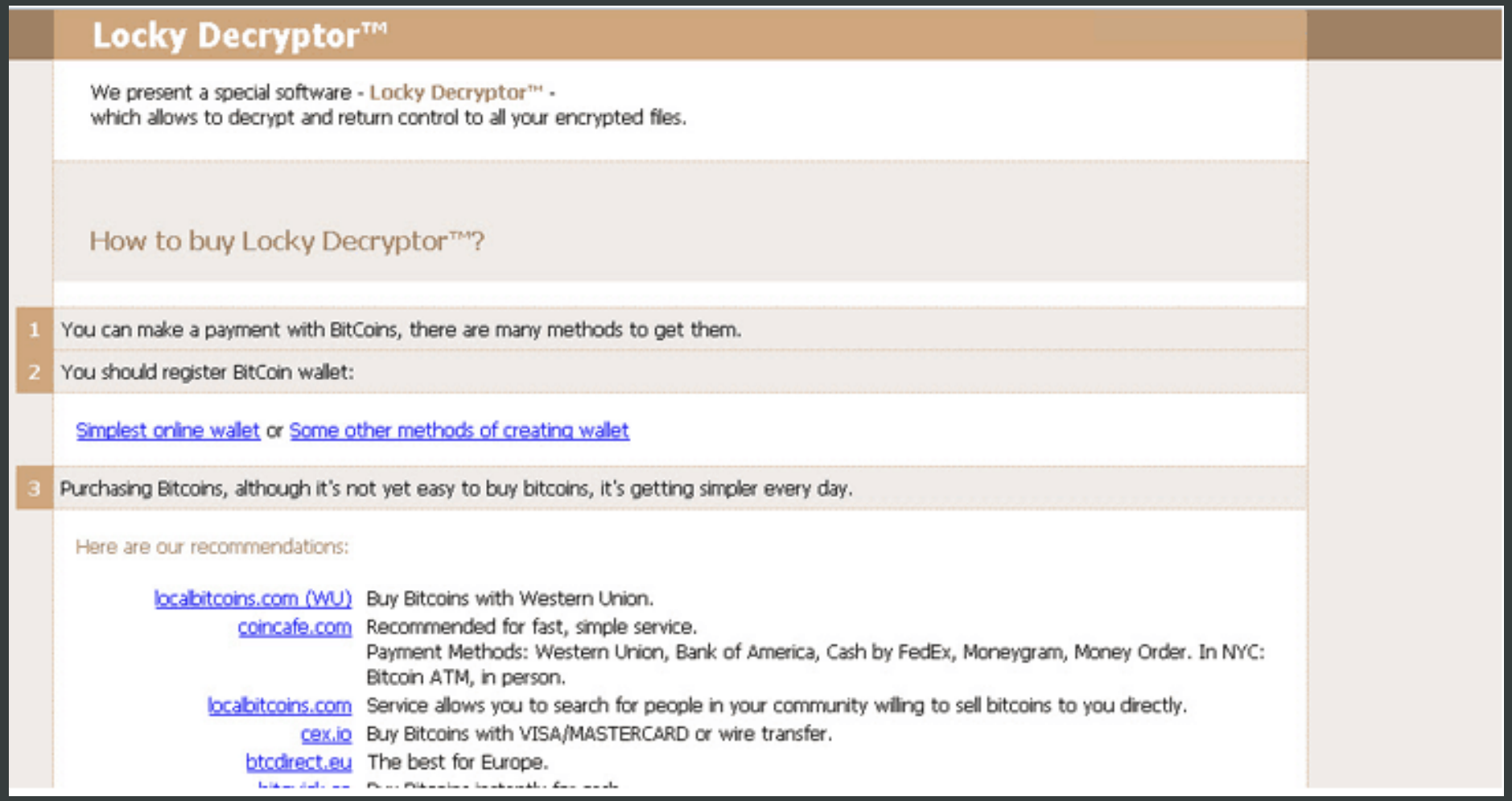
AngelFire CIA Malware

- Used by CIA to gain persistent remote access on Windows
- It does so by modifying its partition boot sector
- It modifies the partition boot sector to load and execute Wolfcreek every time the system boots up
- It contains a self loading driver that loads other drivers and user-made applications
- It also has a covert file system that attempts to install itself in non-partitioned space available on the targeted computer
- AngelFire needs administrative privileges on a target computer for successful installation
- It has variants in 32-bit version as well as 64-bit version

Locky Ransomare

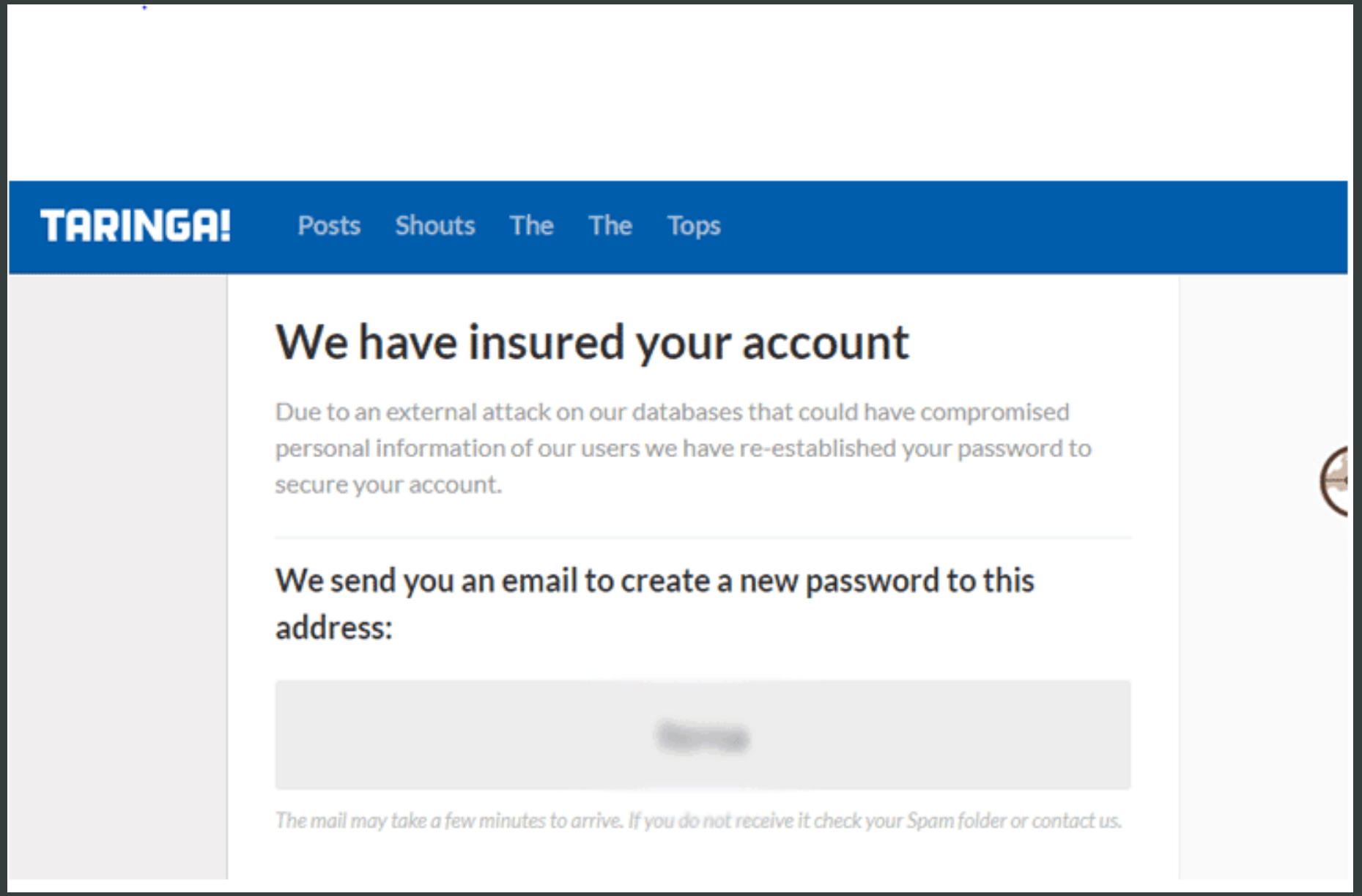
- Emails are being sent containing Locky ransomware
- Around 23 million messages have been sent in 24 hours
- The emails set out in the attack were extremely vague with subjects such as “please print”, “documents”, “images”, etc.
- The email comes with a zip attachment that contains a Visual Basic Script (VBS) file need inside a secondary ZIP file
- Once opened the VBS installs the ransomware and encrypts all the files
- The malware displays a ransomware message on the victim's desktop that instructs the victim to download and install Tor browser and visit the attacker's site for further instructions and payments

- The ransomware demands sum of 0.5 Bitcoin from victims to pay for a “Locky decryptor” in order to get their files back.



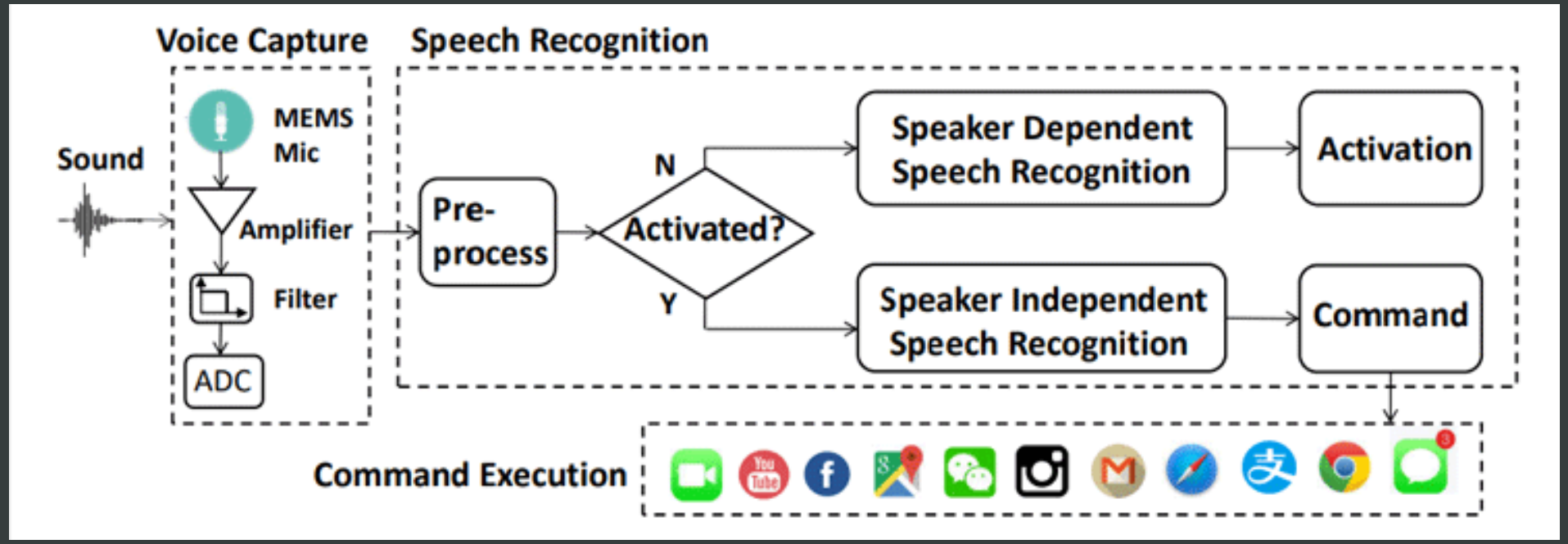
Tiranga Data Breach

- A popular social networking site geared towards Latin American users (just like Reddit)
- Users create and share thousands of posts every day on general topics like life hacks, tutorials, recipes, reviews and art
- According to LeakBase (breach notification service), 28,722,877 accounts which includes usernames, email addresses and hashed passwords for Tiranga was obtained by hackers
- Hashed passwords use an ageing algorithm called MD5 which is somewhat outdated so it will be easy for hackers to unhash it.


TARINGA!
Posts
Shouts
The
The
Tops
We have insured your account
Due to an external attack on our databases that could have compromised personal information of our users we have re-established your password to secure your account.
We send you an email to create a new password to this address:
The mail may take a few minutes to arrive. If you do not receive it check your Spam folder or contact us.

Dolphin Attack: Controlling Siri, Alexa and more

- Dolphin attack works by feeding the AI assistants commands in ultrasonic frequencies, which are too high for humans to hear but are perfectly audible to the microphones
- Cyber criminals can silently whisper commands to hijack Siri or Alexa and could force them to open malicious apps
- It can be used to visit malicious website, spying, injecting fake information and much more



Thank You