IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

APT. Evolución de las tácticas. Situación de España en el panorama europeo

CENTRO CRIPTOLÓGICO NACIONAL

ESCUELA DE CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y EVALUACIÓN

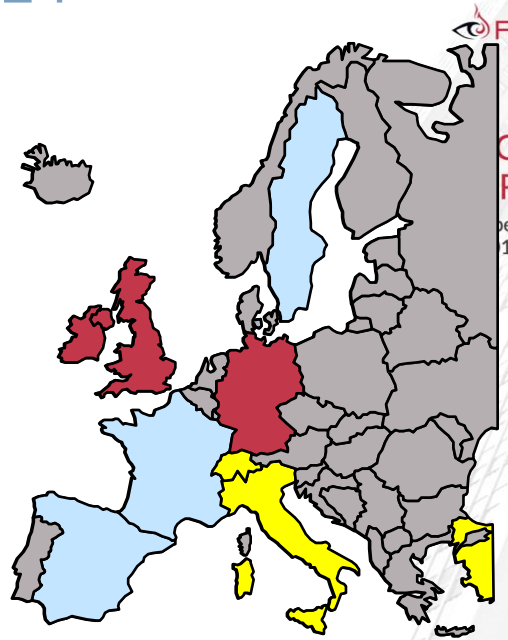
- Álvaro García
- FireEye
- alvaro.garcia@fireeye.com

ÍNDICE

2014

APT Detection

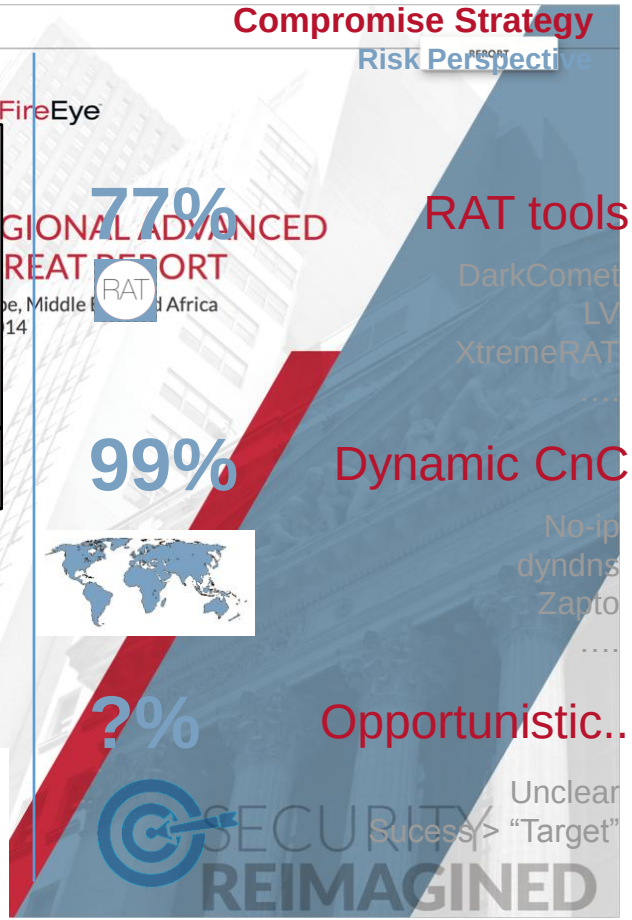
Country Analysis



1. United Kingdom (17%)
2. Germany (12%)
3. Saudi Arabia (10%)
4. Turkey (9%)
5. Switzerland (8%)
6. Italy (6%)
7. Qatar (5%)
8. France (4%)
9. Sweden (4%)
10. Spain (3%)

Compromise Strategy

Risk Perspective



Therefore…

Malware map mimics economic and politics map..

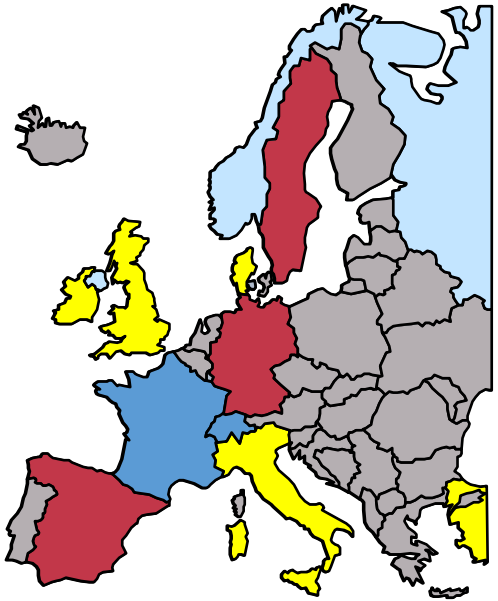
Conventional malware remains effective..

Attackers increased in number but not in skills..

FireEye
SECURITY REIMAGINED

2015

APT Detection
Country Analysis



1. Israel (11%)
2. Saudi Arabia (11%)
3. Spain (10%)
4. Germany (10%)
6. Italy (9%)
7. Denmark (6%)
8. Turkey (6%)
9. Norway (5%)

Compromise Strategy
Risk Perspective

200% Unique attacks

LV/NJRat
Dridex
Modified RAT tools
....

60% "New-old" techniques

Dridex
APT.NS01
....

5% "Unseen" techniques..

GitHub

WitchCoven
APT29
....

Therefore…

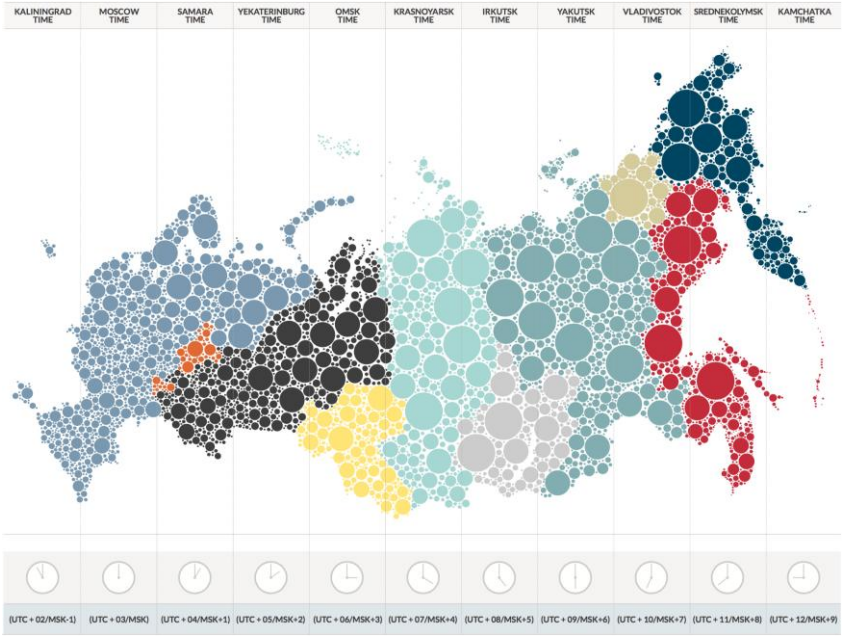
Attacks increased x2. Spain is main player..

Again malware map mimics economic and politics map..

Attackers evolve on procedures and tactics..

FireEye SECURITY REIMAGINED

Intel Case Study I: July 2015 – APT 29 - HAMMERTOSS



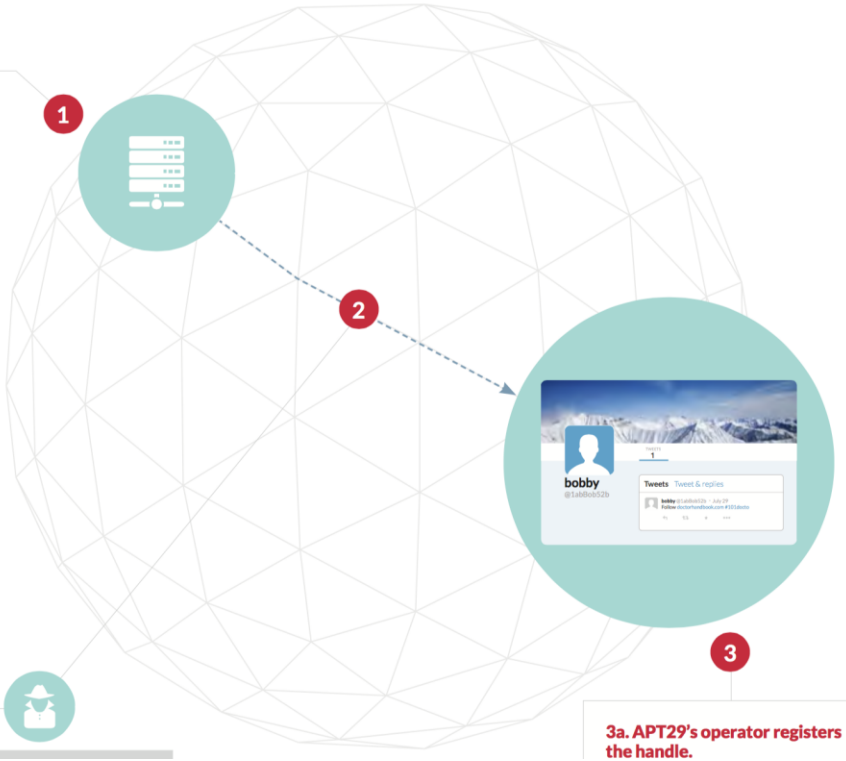
- We track their activities in early 2015.
- Unique mix of “already seen” techniques
- Dynamic CnC by tweeter post.
- Steganography on valid images
- PowerShell scripting to Cloud storage.

STAGE 1:

The Communication Process Begins with Twitter

1. HAMMERTOSS contains an algorithm that generates Twitter handles telling the malware to visit a specific Twitter handle on a specific day.

A Twitter handle is a user ID associated with Twitter's website. For instance, FireEye's Twitter handle, @FireEye, has a URL: https://www.twitter.com/fireeye. The HAMMERTOSS algorithm uses a basename, like "Bob," and appends and prepends three CRC32 values based on the current date. An example, may be 1abBob52b, which would have the URL: hxxps://www.twitter.com/1abBob52b.



3a. APT29's operator registers the handle.

STAGE 2:

Tweeting a URL, Minimum File Size of an Image, and Part of an Encryption Key

If APT29's operator has registered that particular day's handle, he will tweet a URL and hashtag.

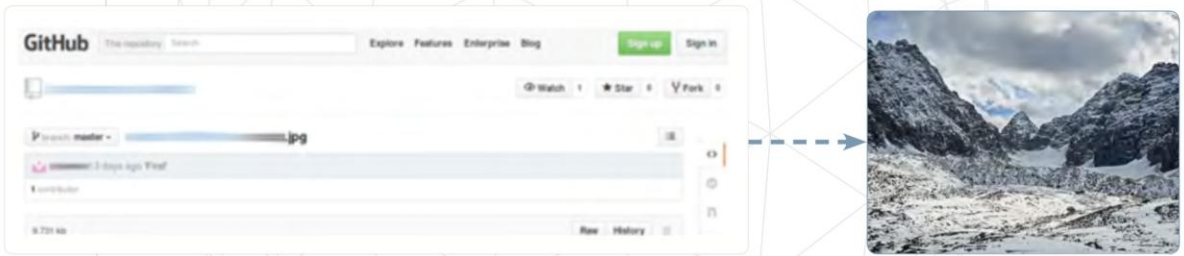
URL: In the case above, the tweet instructs HAMMERTOSS to download the content hosted at the specified URL, including any images on the page. In the example we will discuss later, the tweet included a URL on GitHub.

Hashtag: The tweet also contains a hashtag with information to allow HAMMERTOSS to extract encrypted instructions from an image file. The hashtag indicates that the hidden data is offset 101 bytes into the image file and the characters to be used for decryption are *docto*.

STAGE 3:
Visiting GitHub to Download an Image

APT29's operator registers a GitHub page and uploads an image.

GitHub



STAGE 4:

APT29 Employs Basic Steganography

1. HAMMERTOSS downloads the image from the specified URL, retrieves the image from Internet Explorer's browser cache, and begins the process of decryption.

2. Though the image looks normal, it contains appended and encrypted content.

3. HAMMERTOSS decrypts the image using a hard-coded key appended with the characters obtained from the tweet in Stage 2.

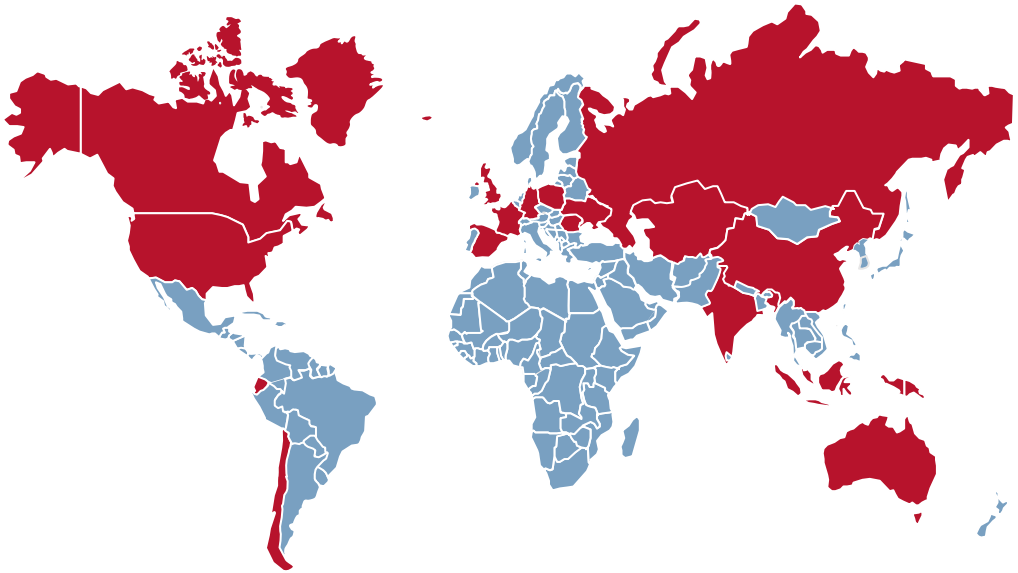
STAGE 5:
Executing Commands and Uploading Victim Data

APT29's operator creates the cloud storage account and can obtain the victim's data from the cloud storage service.

2. HAMMERTOSS is capable of uploading victim data to a cloud storage service.

1. HAMMERTOSS may issue other follow on commands:
`powershell -ExecutionPolicy bypass -WindowStyle hidden -`

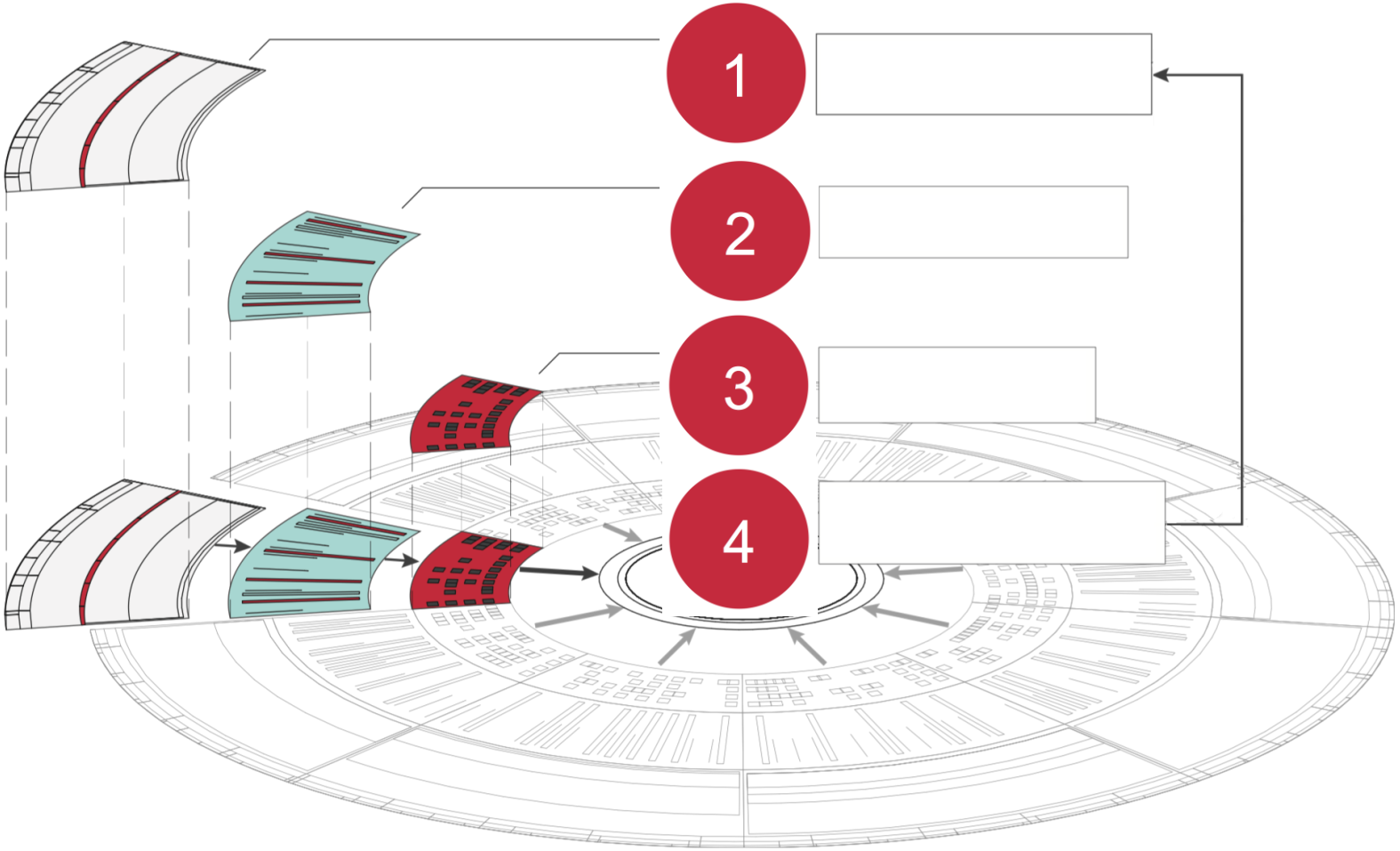
Intel Case Study II: 2015 – WITCHCOVEN



- We track their activities in during 1 Year.
- Selective compromised 100+ websites as part of their infrastructure.
- Scripts and freeware as infection tools
- Massive computing of profiling (CRM)

….E-commerce techniques with total different purposes…

FireEye SECURITY REIMAGINED


1
2
3
4

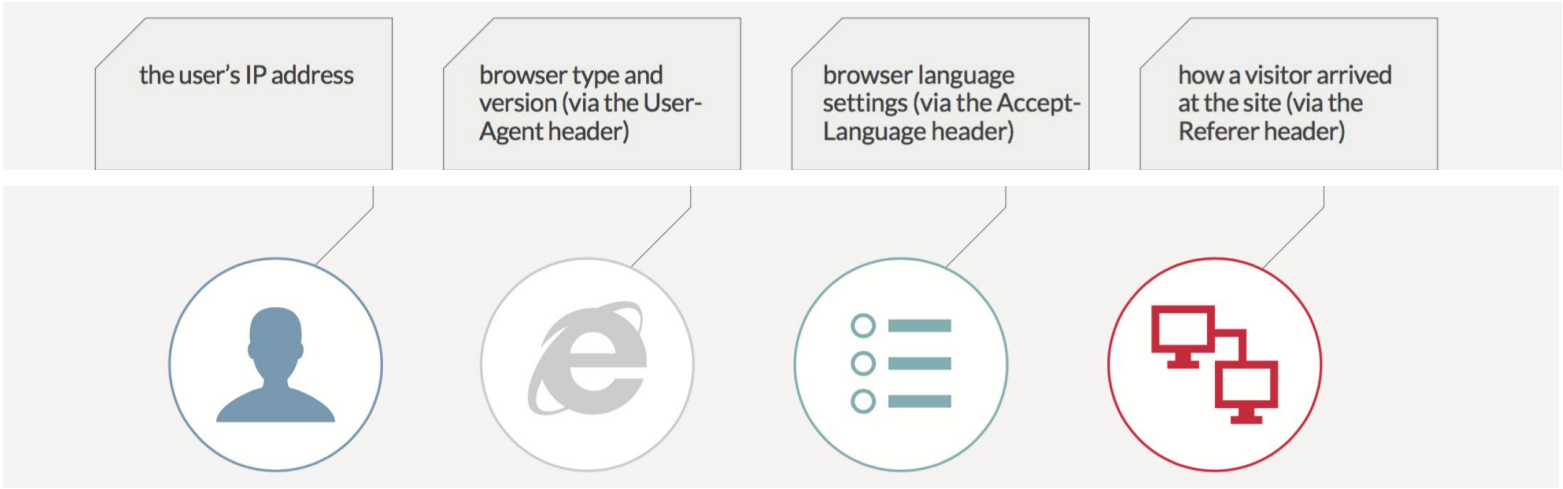
“SUPERCOOKIE”

open source tool “evercookie”..

designed to create “extremely persistent cookies”

alternate storage methods not accessible by common users

- Targeted Exploitation..
- Spear Phishing..
- Human Intelligence…



Conclusions…

Conventional malware is still effective...

No clear “target/no target” attack differentiation by tool..

Malware grows to “legal” CnC infrastructure and freeware.

Intellligence plays HUGE role on risk attribution.

…

Spain is in the “match”…

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sondas@ccn-cert.cni.es
- redsara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Síguenos en Linked in