

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

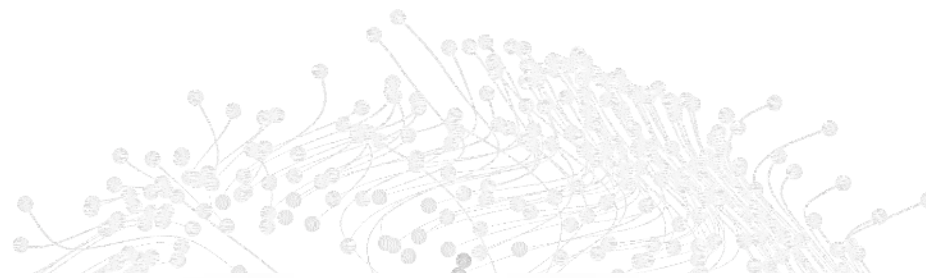
OPERACIONES DE FALSA BANDERA



- David Barroso @lostinsecurity
- CounterCraft
- dbarroso@countercraft.eu

- “Las **operaciones de bandera falsa** son operaciones encubiertas llevadas a cabo por gobiernos, corporaciones y otras organizaciones, diseñadas para aparecer como si fueran llevadas a cabo por otras entidades.”
- El nombre se deriva del concepto militar de izar colores falsos; esto quiere decir la bandera de un país diferente al propio.

TV5Monde



A tener en cuenta

- Fallos de OPSEC: ¿intencionados o inadvertidos?
 - Mala compartimentación de operaciones
 - Tensiones geo-políticas
 - Eventos de relevancia
 - TTPs – fácil reutilización
-
- Es necesario mezclar HUMINT + aspectos técnicos y operativos en el mundo 'ciber'.
 - Sólo al alcance de LEAs, militares y servicios de inteligencia.

Importante

1. La atribución es casi imposible
2. Es binario: o se puede conocer o no.
3. La propia evidencia es auto-explicativa. Lo difícil es encontrarla. No hace falta más análisis.

- Límites: inteligencia, recursos/habilidades, tiempo y OPSEC del adversario

“No sólo hay que encontrar una pistola humeante, sino también tiene que estar caliente, con el asesino sosteniéndola en su mano”

¿Cómo se atribuía hace unos años?

South Korea traces cyber-attacks to Chinese IP address

Suspicion for simultaneous shutdown still focused on North Korea despite discovery of attack's apparent origin



Customers use automated teller machines at a branch of Shinhan Bank in Seoul. Tens of thousands of computers

Most cyber attacks on India show Chinese IP address

Cyber attacks have grown nearly five times in the last three years and most of them have been found to be originating from the IP addresses located in China. "Most of the cyber attacks that we have tracked show IP addresses located in China but we are unable to establish if the attacker is from China. We need international cooperation for handling such crimes," NTRD Director of Cyber Security Operations Alok Vijayant said at Ground Zero Summit.

Government's cyber security arm Computer Emergency Response Team-India (CERT-In) reported 62,189 cyber security incidents in the first five months of the current calendar year.

These attacks have been found to be originating from the cyber space of a number of countries including the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE, according to the official report. The National Technical Research Organisation (NTRO) Director said that foreign countries are investing heavily in cyber espionage to gather crucial data and India needs to seriously consider a strategy to counter this strategy.

India has seen increase in cyber attacks from about 13,000 in 2011 to 62,000 till mid-2014. The country has been unable to identify cyber criminals in majority of the case due to absence of international cooperation on the issue.

The smoking gun on China's US cyberattacks

By John Breeden II Aug 26, 2011

A few weeks ago I wrote a column explaining, step by step, how hackers with a Chinese IP address **attacked a honeypot network** in the GCN Lab that had been set up for just that purpose.

We watched the attacks take place, made notes about what the hackers did, the techniques they used, and tracked them back to several addresses inside China.

In the comments section that followed, a few people complained that I had no evidence that the attack actually came from China, implying that I was slandering them in some way. Given that the Chinese government's official line has always been that it respects the rule of law and would never attack a sovereign nation in cyberspace, I can see why they would have defenders. In truth, other than the IP address of the people who attacked our honeypot, I had no comeback, especially since IP addresses can be spoofed.

No vale todo

[Home](#) > [Technology Industry](#)



SALTED HASH- TOP SECURITY NEWS

By [Steve Ragan](#), Senior Staff Writer, CSO | FEB 2, 2016 3:30 AM PT

About

Fundamental security insight to help you minimize risk and protect your organization

NEWS

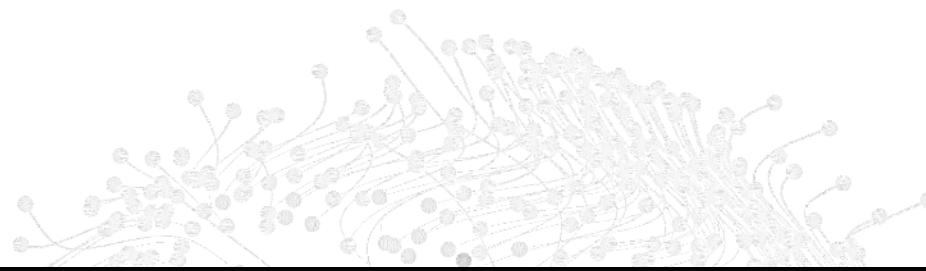
Norse Corp. Deconstructing threat intelligence on Iran

Memo circulated to attack

"It is possible that the Chinese were at it again two years later using compromised Iranian systems, but it is unlikely. The Iranian IP hosts no visible infrastructure and is apparently owned directly by the Telecommunications Company of Iran, running on AS12880. There has never been any public system identified with this IP, or with any of the IPs on this subnetwork, so there has not been any visible server to try to hack. Nor have the Chinese changed their methods from operating openly from their own infrastructure to using that of third parties."

- Malicious Ira

Data collected by AEI and the Norse Corporation indicate that attacks launched from Iranian Internet protocol (IP) addresses increased 128 percent between January 1, 2014, and mid-March 2015. The number of Norse sensors hit by Iranian IPs rose by 229 percent, while the number of distinct IPs used to execute these attacks rose by 508 percent.



If it looks like a duck, walks like a duck and quacks like a duck, then it just may be a duck.

(Walter Reuther)

izquotes.com



Elementos de atribución

- Infraestructura: dominios, direcciones IP, correos, localización
- Cadenas de texto en el binario cliente / servidor
- Metadatos de los binarios: lenguaje, fecha compilación, directorios
- Afectados: sector, país, etc.
- Operaciones: horarios, coincidencias con eventos políticos, religiosos, nacionales
- Reutilización de código - modularidad

CIA - Umbrage

Wikileaks Vault7 data leak – the Umbrage team was tasked by the Central Intelligence Agency for false flag hacking operations.

WikiLeaks has **obtained** thousands of files allegedly originating from a CIA high-security network that details CIA hacking tools and capabilities. Digging in the huge trove of files, it is possible to find information about the ability of the intelligence Agency in fingerprinting hacking techniques used by threat actors in the wild, both state and non-state actors. The CIA has built a specific team of experts code-named as the Umbrage team under the Remote Development Branch inside the CIA's Center for Cyber Intelligence.

CIA - Umbrage

Photo: Martin H. Simon/Press Pool/Getty Images

WIKILEAKS FILES SHOW THE CIA REPURPOSING HACKING CODE TO SAVE TIME, NOT TO FRAME RUSSIA



Kim Zetter

March 8 2017, 8:28 p.m.

ATTRIBUTING HACKING ATTACKS to the correct perpetrators is notoriously difficult. Even the U.S. government, for all its technical resources and expertise, took warranted criticism for [trying to pin](#) a high-profile 2014 cyberattack on North Korea, and more recently faced skepticism when it blamed Russia for hacks against top Democrats during the 2016 election.

NSA Fourth Party

SECRET//COMINT//REL TO USA, FVEY

(U) What is 4th Party



- (S//SI//REL) 4th party collection leverages CCNE accesses to provide Foreign Intelligence from foreign CNE victims
- (U) Types of 4th Party opportunities
 - (U) Passive Acquisition
 - (U) Active Acquisition
 - (U) Victim Stealing / Sharing
 - (U) Re-purposing

The Cuckoo's Egg (1986)

■ **Atribución:**

- Intrusión en Lawrence Berkeley National Laboratory
- Conexión en satélite desde Alemania -> traceada a la Universidad de Bremen
- Honeypot trampa con información falsa (SDI)
- Markus Hess en Hannover -> Venta de información a la KGB
- Objetivo: Entornos militares y de investigación de EEUU

■ **Más información:**

- <http://pdf.textfiles.com/academics/wilyhacker.pdf>

Moonlight Maze (1998)

■ Atribución:

- Direcciones IP a 20km de Moscú
- Trabajan de 8am a 5pm entre semana. Horario de Moscú. No trabajan en los días de fiesta rusos.
- Objetivo: Pentágono, Departamento de Energía, NASA

■ Más información:

- <http://www.sfgate.com/news/article/Russians-Seem-To-Be-Hacking-Into-Pentagon-2903309.php>

Titan Rain (2003)

■ **Atribución:**

- Técnicas militares (PLA)
- Direcciones IP de la provincia china de Guangdong
- Objetivo: Ministerio de defensa EEUU. Contractors: Sandia National Labs, Lockheed Martin, NASA, etc.

■ **Más información:**

- <http://courses.cs.washington.edu/courses/csep590/05au/readings/titan.rain.htm>

Rusia vs Georgia (2008)

■ Atribución:

- Invasión terrestre
- DDoS contra la web del presidente de Georgia: win+love+in+Russia. Inserción de fotos de Hitler
- DDoS y ataques contra prensa, bancos, empresas de Georgia
- Objetivo: Georgia
- Similar: Rusia vs Estonia (2007): DDoS

■ Más información:

- <http://smallwarsjournal.com/blog/journal/docs-temp/639-hellio.pdf>

Stuxnet (2010)

■ **Atribución técnica:**

- Cadena MYRTUS-> My RTUs vs Myrtus -> Hadassah en hebreo, nombre de la Reina judía de Persia
- b:\myrtus\src\objfre_w2k_x86\i386\guava.pdb
- Cifrado 19790509 -> Habib Elghanian, un judío persa, fue ejecutado en Tehran
- Cadena 24 sep 2007 -> Presidente de Irán cuestiona el Holocausto en EEUU
- Multitud de declaraciones de ser una operación conjunta de EEUU + Israel

■ **Atribución:**

- Objetivo: Programa nuclear de Irán

■ **Más información:**

- <http://www.goodreads.com/book/show/18465875-countdown-to-zero-day>

Flame (2012)

■ Atribución:

- Reutiliza alguna técnica de Stuxnet/Duqu
- Programado por un grupo paralelo pero accediendo a los mismos recursos y exploits.
- Objetivos: Irán, Siria, Palestina, Líbano

■ Más información:

- <https://securelist.com/the-flame-questions-and-answers-51/34344/>

Gauss (2012)

■ **Atribución:**

- Reutiliza algunos TTP's de Flame
- "c:\documents and settings\flamer\desktop\gauss_white_1
- Un mes después, el NY Times publica un extenso artículo de cómo Siria blanquea dinero en Líbano
- Objetivo: clientes de bancos del Líbano

■ **Más información:**

- <https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/kaspersky-lab-gauss.pdf>

Shamoon (2012)

■ False flags:

- C:\Shamoon\ArabianGulf\wiper\release\wiper.pdb
- Irán lo llama Persian Gulf
- 15 de agosto: Lailat al Qadr (la noche del poder – celebra la revelación del Corán a Mahoma)
- Wiping a las 11:08am
- El nombre Wiper se usaba también en Flame (ataque a empresas de petróleo de Irán)
- Ataque similar contra RasGas 2 semanas después (Qatar)
- Objetivo: Arabia Saudi – Saudi Aramco

■ Más información:

- <http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html>

Red October (2013)

■ **Atribución:**

- Idioma cirílico
- Cadenas en slang ruso dentro de los binarios
- Utilización de direcciones de e-mail rusos
- Servidores en Rusia, Alemania (Hetzner)
- Registros de dominios en reg.ru, webdrive.ru, webnames.ru, timeweb.ru
- Objetivo: Europa del Este, Asia, antigua URSS, embajadas

■ **Más información:**

- <https://securelist.com/red-october-diplomatic-cyber->

APT1/Comment Crew (2013)

■ Atribución:

- Identificación de personas: UglyGorilla, DOTA, SuperHard. Estudiantes universitarios. Reutilización de nicknames.
- Reutilización de dominios, IPs, direcciones de email
- Número de teléfono real a 600 metros del HQ de la Unit 61398 (habitación en alquiler)
- Lunes a viernes de 8am a 6pm en UTC+4
- Objetivo: EEUU

■ Más información:

- <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>

Corea del Norte vs Corea del Sur (2013)

■ Atribución:

- Dark Seoul
- 20 de marzo a las 2pm: Wiping MBR en varias TVs y bancos. Palabras en MBR: Principes y Hastati (infantería romana). Ataques al BGP de esas empresas
- 1 semana antes: Corea del Norte estuvo 36 horas sin Internet
- 25 de junio: 63º aniversario de la guerra de Corea
- DDoS contra gobierno de Corea del Sur
- Objetivo: Corea del Sur

■ Más información:

- <https://arstechnica.com/security/2013/03/your-hard-drive-will-self-destruct-at-2pm-inside-the-south-korean-cyber-attack/>

Lazarous Group (2007-)

■ **Atribución:**

- Código compartido con otros incidentes
- Infraestructura reutilizada en otros incidentes
- Utilización de alguna dirección IP de Corea del Norte en accesos a C2C
- Objetivos: Corea del Sur, entidades financieras

■ **Más información:**

- [https://securelist.com/files/2017/04/Lazarus Under The Hood PDF final.pdf](https://securelist.com/files/2017/04/Lazarus_Under_The_Hood_PDF_final.pdf)
- <https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf>

Animal Farm (2014)

■ Atribución:

- Tafacalou -> nombre interno del 1st stage.
- Babar
- Nombre del desarrollador: titi (diminutivo de Thierry)
- Idioma de la parte servidora 'fr_FR'
- Inglés extraño
- Zonas horarias de compilación GMT+2 o GMT+3
- Buen inglés pero fallos de no nativos: Exccceeded
- Objetivo: Siria

■ Más información:

- <https://www.gdatasoftware.com/blog/2015/02/24270-babar-espionage-software-finally-found-and-put-under-the-microscope>

Rocket Kitten (2014)

■ Atribución:

- Dominios registrados por grupos que se dedicaban al defacemente (Ajax Security Team).
- Gholee (nombre de función exportada) es un cantante famoso de Irán.
- Cadena: 'bos bos'. Boos es beso en iraní, con lo que pudiera ser xoxo.
- Wool3n.H4T es un usuario de un blog iraní.
- Logs del autor que estaba infectado con su keylogger. Se conecta a AOL con el usuario 'yaserbalaghi'. Experto en C++ que escribe en foros de programación. Realiza un video tutorial de SQL Injection en farsi donde expone su identidad.

■ Más información:

- <https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf>

Careto (2014)

■ Atribución:

- Dominio registrado por 'Victoria Gomez'
- Caguen1aMar como clave de cifrado RC4
- Accept-Language es
- c:\Dev\CaretoPruebas3.0\release32\CDIUninstall32.pdb
- Suplantación de periódicos españoles: El País, El Mundo, Público.
- Objetivos: Marruecos, Cuba, España, Francia, Suiza

■ Más información:

- https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf

Inception / Cloud Atlas (2014)

- De los creadores de Red October. Reutilización de ficheros, víctimas

Red Herrings

- In specific instances where the APT seemed to be under investigation by researchers the actors dropped another piece of malware that is clearly attributable to a previously known Chinese APT: Suggests ties to China
- A large majority of the hacked home routers are in South Korea: Suggests ties to South Korea
- The attackers are most active from 8:00AM to 5:00PM in the Eastern European Timezone: Suggests ties to areas in the GMT+200 timezone
- Some of the comments in the Android malware are in Hindi: Suggests ties to India
- Some text strings in the BlackBerry malware are Arabic: Suggests ties to the Middle East
- The string "God_Save_The_Queen" was found within the Black Berry malware: Suggests ties to the UK
- The word documents show some resemblance to word documents used by the Red October APT: Suggests ties to Ukraine and/or Russia
- The iOS malware was developed by someone using the account name "JohnClerk": Suggests ties to the US or UK
- The encryption key for the iOS malware
"fjkwyreruu665E62C:GWR34285U^%^\#%\$%^\$RXYEUFQ2H89HCHVERWJFKWEhjvvehhewfD63TDYDGTIEDT23Y" appears to be keyboard mashing on a US/US International keyboard: Suggests ties to the US

<https://www.symantec.com/connect/blogs/blue-coat-exposes-inception-framework-very-sophisticated-layered-malware-attack-targeted-milit>

Duqu 2.0 (2014)

■ False flags:

- Cadena ugly.gorilla -> Wang Dong de APT1/Comment Crew
- Cifrado Camellia -> APT1
- Cadena romanian.antihacker -> apuntar a Rumanía
- Algoritmo de compresión raro LZJB -> MiniDuke 2013

■ Atribución:

- Apenas trabaja los viernes y no trabaja los sábados. Su semana empieza los domingos.
- Binarios compilados el 1 de enero
- Zonas horarias de compilación GMT+2 o GMT+3
- Buen inglés pero fallos de no nativos: Exceeded
- Objetivo: Kaspersky

■ Más información:

- https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

Fancy Bear/APT28/Sofacy (2007-)

■ **Atribución:**

- Binarios compilados en idioma ruso.
- Lunes a viernes de 8am a 6pm en UTC+4
- Objetivo: Georgia, Europa del Este, NATO

■ **Más información:**

- <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf>

Yemen Cyber Army (2015)

■ False flags:

- Objetivos: Arabia Saudi
- En una cuenta comprometida, cambiaron el idioma a persa
- Nativos en farsi/persa
- Direcciones IP de Irán
- Utilizan la expresión 'Cutting Sword of Justice' que se utilizó en Shamoon

■ Más información:

- <https://pastebin.com/HqAgaQRj>
- <https://www.recordedfuture.com/iranian-saudi-cyber-conflict/>

DNC Hack (2016)

■ Atribución:

- Crowdstrike y Fidelis: APT28 (FSB) y APT29 (GRU) están presentes
- Reutilización de herramientas, tácticas e infraestructura
 - Misedepatrment.com -> 45.32.129.185 (APT28)
 - C2C reusado: 176.31.112.10 (malware en el parlamento alemán)
 - Certificado SSL reusado (parlamento alemán)
- Metadata de documentos: idioma en ruso, usuario Феликс Эдмундович, errores en cirílico
- Aparece Guccifer 2.0, que dice ser de Rumanía, pero utiliza todo de Francia (OVH, cuenta de AOL francesa, etc.)

■ Más información:

- <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>
- <https://guccifer2.wordpress.com>

Wannacry (2017)

■ Atribución:

- Código compartido con Lazarus Group
- De todos los idiomas, el mejor escrito es el chino

■ Más información:

- <https://www.flashpoint-intel.com/blog/linguistic-analysis-wannacry-ransomware/>
- <http://blog.elevenpaths.com/2017/06/wannacry-chronicles-messi-coreano.html>

Rusia vs Ucrania (2017)

■ **Atribución:**

- Atentado terrorista contra Coronel Maksym Shapoval
- Día del 21^a aniversario de la independencia
- Principal vector de infección: MeDoc, software financiero usado por muchas empresas en Ucrania.
- Visita en la semana pasada de Poroshenko a ver a Trump en Washington
- Objetivo: Ucrania

■ **Más información:**

- <http://dailysignal.com/2017/06/29/russias-hybrid-warfare-battlefield-ukraine-heats/>

A tener en cuenta

- Fallos de OPSEC: ¿intencionados o inadvertidos?
 - Mala compartimentación de operaciones
 - Tensiones geo-políticas
 - Eventos de relevancia
 - TTPs – fácil reutilización
-
- Es necesario mezclar HUMINT + aspectos técnicos y operativos en el mundo 'ciber'.
 - Sólo al alcance de LEAs, militares y servicios de inteligencia.

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@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

