Descubriendo amenazas a nivel gubernamental

DIEZ AÑOS FORTALECIENDO LA CIBERSEGURIDAD NACIONAL

Dani Creus, Palo Alto Networks
Vicente Díaz, Kaspersky Lab

Chapter One

APTs y adversarios en el 2016

GRUPOS/OPERACIONES

Espionaje – Propaganda - Disrupción

JULY 2016 – SAURON / REMSEC

Objetivos de alto nivel seleccionados (Gob, Científico, Mil, Telecos, Finanzas)

Distribución controlada – Rusia, Irán y Ruanda (+ China, Suecia y Bélgica, según Symantec).

Infraestructura única por víctima – haciendo los IOCs inútiles

Excelente Seguridad Operacional – pero costosa

Duqu:

- Use of intranet C2s (where compromised target servers may act as independent C2s)
- Running only in memory (persistence on a few gateway hosts only)
- Use of different encryption methods per victim
- Use of named pipes for LAN communication

Flame:

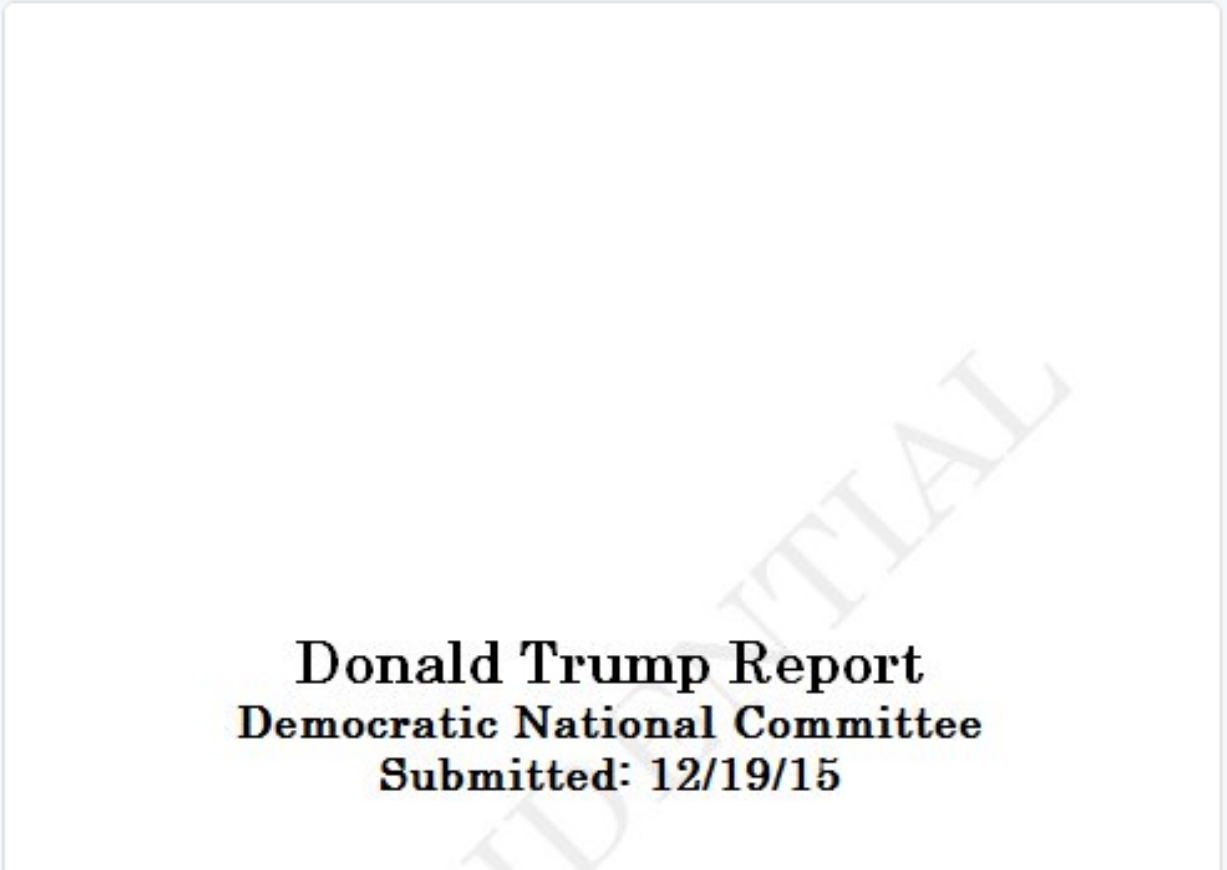
- LUA-embedded code
- Secure file deletion (through data wiping)
- Attacking air-gapped systems via removable devices

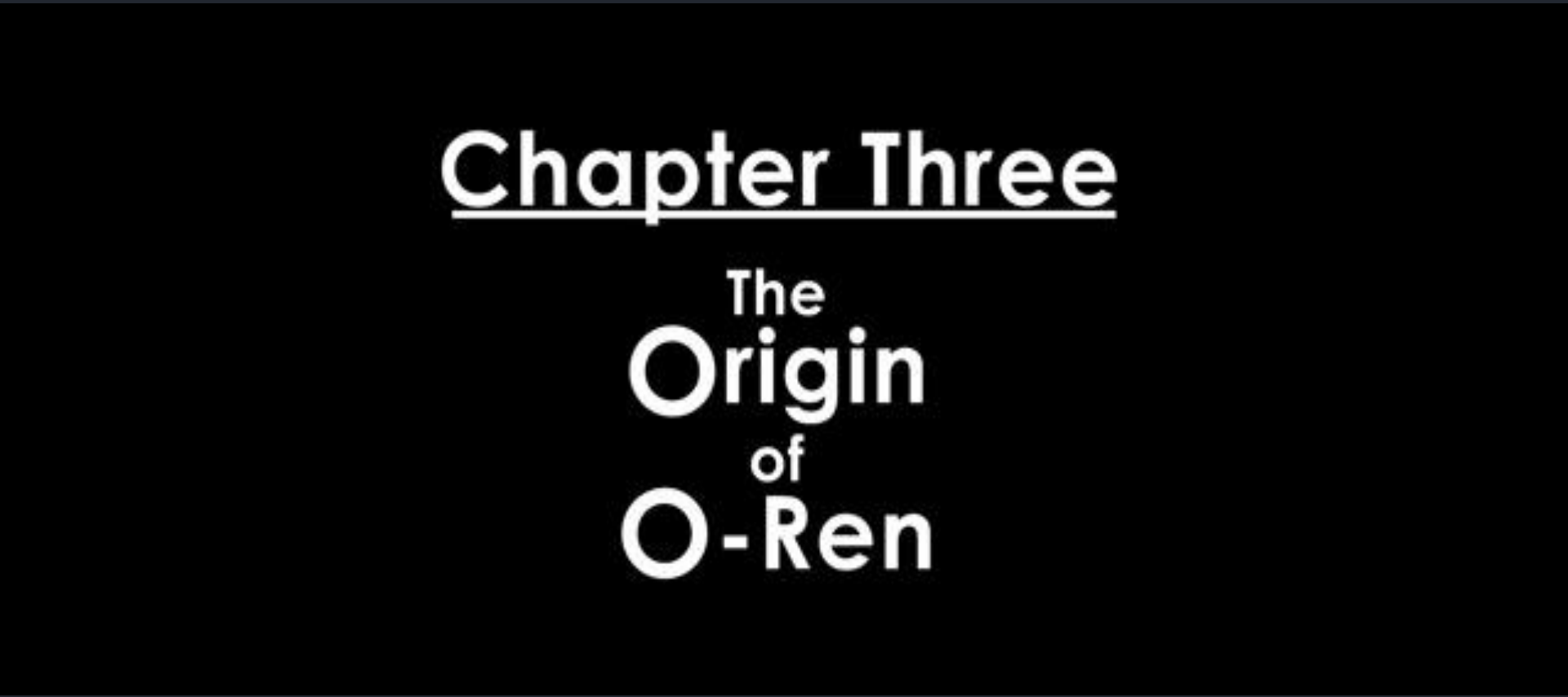
Equation and Regin:

- Usage of RC5/RC6 encryption
- Virtual Filesystems (VFS)
- Attacking air-gapped systems via removable devices
- Hidden data storage on removable devices

GUCCIFER 2.0 @GUCCIFER_2 · 20 jun.

#Guccifer2 #DNC's servers hacked by a lone hacker. #Trump report guccifer2.wordpress.com/2016/06/15/dnc/

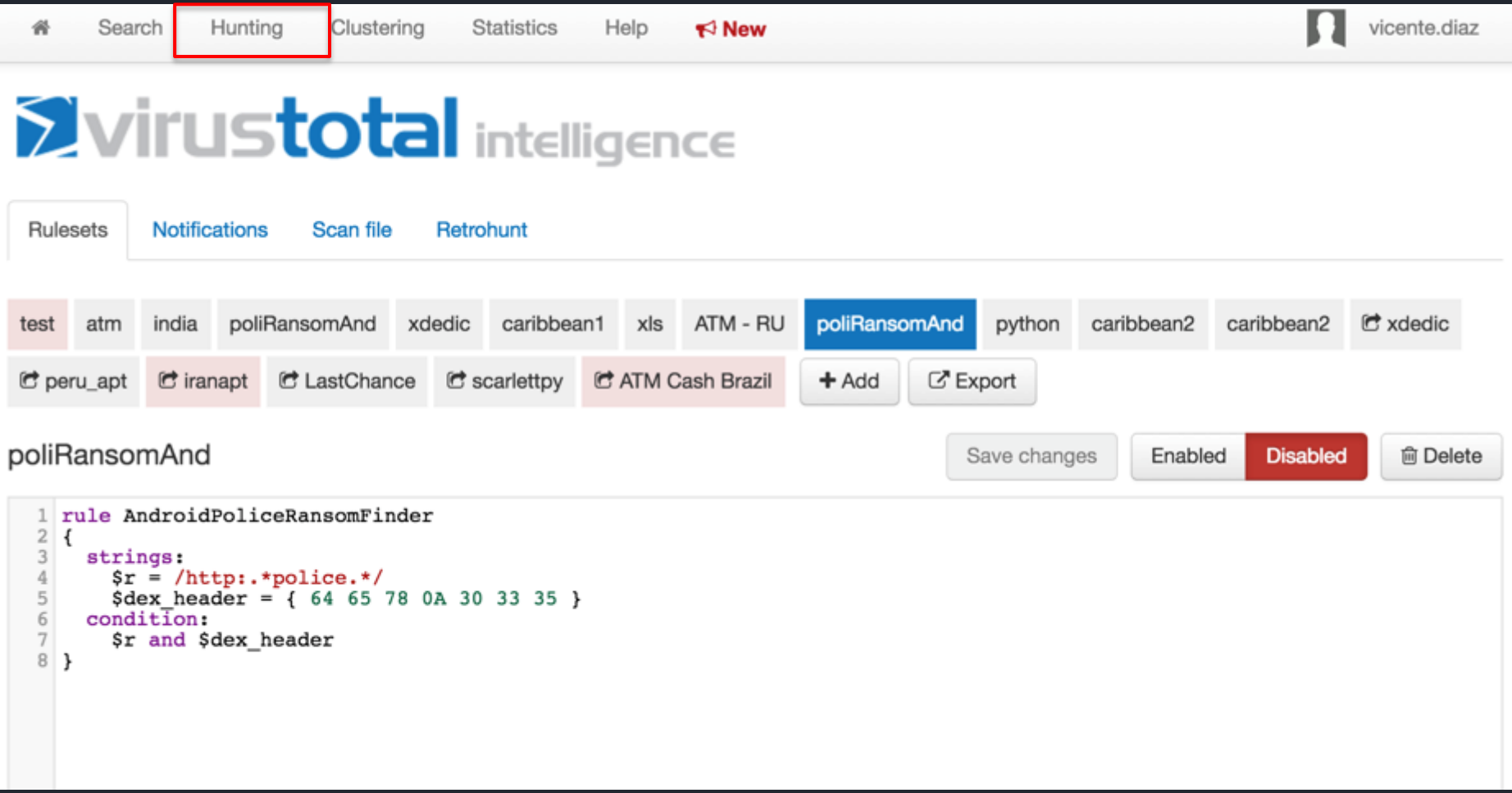




APT HUNTING

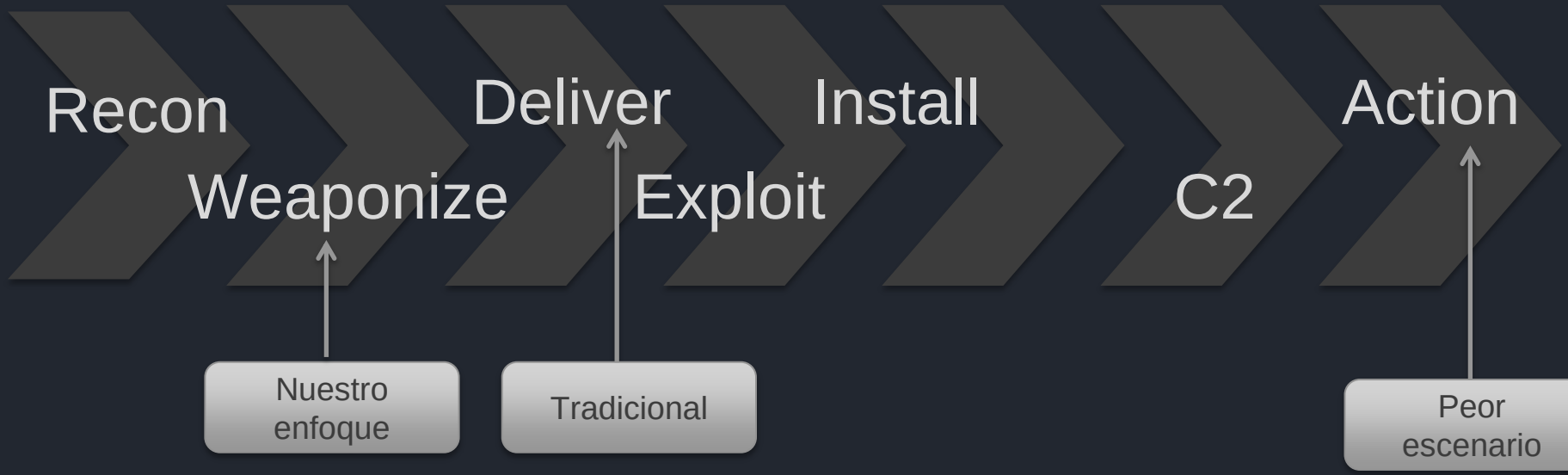
The pattern matching swiss knife for malware researchers (and everyone else)

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```


Search
Hunting
Clustering
Statistics
Help
New
vicente.diaz
virustotal intelligence
Rulesets
Notifications
Scan file
Retrohunt
test
atm
india
poliRansomAnd
xdedic
caribbean1
xls
ATM - RU
poliRansomAnd
python
caribbean2
caribbean2
xdedic
peru_apt
iranapt
LastChance
scarlettpy
ATM Cash Brazil
Add
Export
poliRansomAnd
Save changes
Enabled
Disabled
Delete
rule AndroidPoliceRansomFinder
{
strings:
$r = /http:.*police.*/
$dex_header = { 64 65 78 0A 30 33 35 }
condition:
$r and $dex_header
}

Nuestro método: detección de anomalías con conocimiento 0

KILL CHAIN


Recon
Weaponize
Deliver
Exploit
Install
C2
Action
Nuestro enfoque
Tradicional
Peor escenario

Ejemplo – “Cebos” usados por SOFACY

MH17 Malaysian Airlines crash
International Military.rtf
Exercise_Noble_Partner_16.rtf
Putin_Is_Being_Pushed_to_Prepare_for_War.rtf
Russia anti-Nato troops.rtf
Iran_nuclear_talks.rtf
IDF_Spokesperson_Terror_ Attack_011012.doc
APEC Media list 2013 Part1.xls
APEC Media list 2013 Part2.xls
Europejskie Siły Żandarmerii.doc (The European Gendarmerie Force)
Norwegian Defence ADL Conference 2012. Map.doc
JMAA CONTACT INFORMATION.doc
Speech-US John Hopkins.doc

Víctimas confirmadas de Sofacy

Worker in vatican embassy in Iraq
Military officials and attaches from several countries
Pakistani military officials - Jan 2014
Polish gov employees
Japanese targets Sept 14
ACADEMI, formerly Blackwater (United States)
Broadcasting companies in various countries
Ministry of Defense (France)
Ministry of Defense (Hungary)
Multinational company based in Germany
OSCE (Austria)
SAIC (United States)
U.S. Department of State

Las fuerzas iraquíes entran por primera vez en Mosul

Fuerzas antiterroristas y tropas iraquíes luchan contra el Estado Islámico en el distrito de Karama, a las afueras de la ciudad tomada por los yihadistas

Un miliciano chiita hace el símbolo de la victoria en un pueblo al sur de Mosul (Ahmad Al-rubaye / AFP)

EFE, Bagdad
31/10/2016 14:05 | Actualizado a 31/10/2016 19:50

Lo + Visto


La propietaria de un restaurante desmonta a Alberto Chicote


Se buscan cien familias para acoger a niños de hasta 6 años


Se estrella un avión en Colombia que transportaba al equipo brasileño Chapecoense


Si tu hijo te dice que no quiere ir al colegio, ¡escúchale!

Creamos detección basada en:

- Corpus de Conocimiento Genérico

- Eventos Relevantes

Los artefactos detectados nos proporcionan los elementos necesarios para una búsqueda refinada basada en metadatos.

Crea

- C

- E

Los a

búsc

a una

```
strings:

        //GENERIC
         $generic1 = "confidencial"
         $generic2 = "confidential"
         $generic3 = "secreto"
         $generic4 = "secret"

        //INFORMATION CLASSIFICATION
         $infoclass1 = "FOUO"   // US for official use only
         $infoclass2 = "SBU"    // US sensitive but classified
         $infoclass3 = "LES"    // US Law Enforcement Sensitive
         $infoclass4 = "CTS"    // US Cosmic Top Secret
         $infoclass5 = "NS"     // NATO Secret
         $infoclass6 = "NC"     // NATO Confidential
         $infoclass7 = "NR"     // NATO Restricted

        //TERMS
         $terms1 = "implant"
         $terms2 = "cyber weapon"
         $terms3 = "cyber warfare"
         $terms4 = "cyber exploitation"
         $terms5 = "kinetic"
         $terms6 = "effects assessment"
         $terms7 = "intended cyber effect"
         $terms8 = "cyberspace operations"
```

Un miliciano chiíta hace el símbolo de la victoria en un pueblo al su

```
al"
al"


TION
// US for official use only
// US sensitive but classified
// US Law Enforcement Sensitive
// US Cosmic Top Secret
// NATO Secret
// NATO Confidential
```

Comparte en Facebook | Comparte en Twit

EFE, Bagdad
31/10/2016 14:05 | Actualizado a 31/10/2016 19:50

issions | ITW | Comments

Date	File name	Source	Country
2016-11-07 15:27:18	7f7aa85afdfa6b6732f00fe26d733086.virus	22b3c7b0 (api)	CA
2016-10-31 10:33:08	Operation_in_Mosul.rtf	ff7a1448 (web)	AL

DEMO

Ejemplo 1 – Sofacy “DealersChoice”

European Parliament Press Release

European Parliament Press Unit

European Parliament Press Release

Para: Danil.Sytnikov@uarpa.com

15 de agosto de 2016, 10:53

Archivo adjunto al mensaje.rtf

Bulletin.doc

‘DealersChoice’ is Sofacy’s Flash Player Exploit Platform

By Robert Falcone and Bryan Lee

October 17, 2016 at 11:00 PM

Category: Unit 42 Tags: adobe, DealersChoice, exploit, Flash Player, Sofacy

7,039 0

dc2c3314ef4e6186b519af29a246679caa522acd0c44766ecb9df4d2d5f3995b New doc 3 months ago

Ejemplo 2 – Dukes y elecciones US

```
rule SpytermsV5
{
strings:
            $a1= “trump”
            $a2 = “election”
            $a3 = “US”
condition:

   (
    file_type contains "msoffice" or
            file_type contains "pdf" or
            file_type contains "rtf" or
            file_type contains "document" or
            file_type contains "internet email" or
            file_type contains "outlook" or
            file_type contains "email"
    )

   and

    (
     any of ($a*)
    )
}
```

PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs

Posted on November 9, 2016 by Steven Adair

In the wake of the 2016 United States Presidential Election, not even six hours after Donald Trump became the nation's President-Elect, an advanced persistent threat (APT) group launched a series of coordinated and well-planned spear phishing campaigns. Volexity observed five different attack waves with a heavy focus on U.S.-based think tanks and non-governmental organizations (NGOs). These e-mails came from a mix of attacker created Google Gmail accounts and what appears to be compromised e-mail accounts at Harvard's Faculty of Arts and Sciences (FAS). These e-mails were sent in large quantities to different individuals across many organizations and individuals focusing in **national security**, **defense**, **international affairs**, **public policy**, and **European and Asian studies**. Two of the attacks purported to be messages forwarded on from the **Clinton Foundation** giving insight and perhaps a postmortem analysis into the elections. Two of the other attacks purported to be eFax links or documents pertaining to the election's outcome being revised or rigged. The last attack claimed to be a link to a PDF download on "*Why American Elections Are Flawed.*" Volexity believes a group it refers to as **The Dukes** (also known as APT29 or Cozy Bear) is responsible for post-election attack activity.

Sometimes you can see things happen right in front of your eyes and still jump to the wrong conclusions.

Jodi Picoult

Técnicas aplicables a fuentes abiertas, pero especialmente a internas y entornos sensibles donde nuestro conocimiento puede ser mayor.

Con APTs actuales un análisis completo no puede estar únicamente basado en aspectos técnicos. La prevención puede venir del conocimiento del adversario, lo que pertenece a la disciplina de inteligencia tradicional.

x@thedatacult.com

- **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**