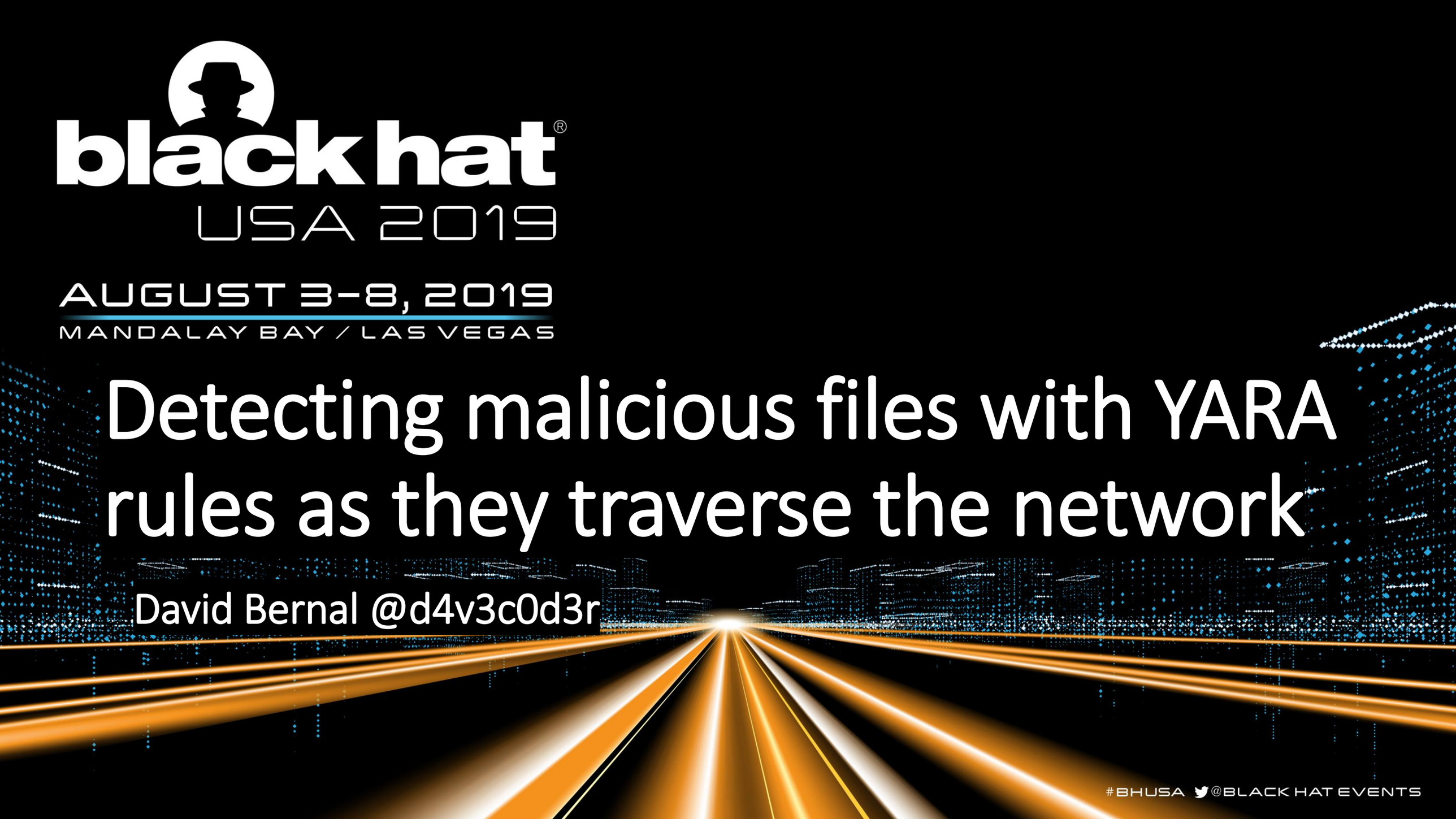


Detecting malicious files with YARA rules as they traverse the network

David Bernal @d4v3c0d3r

#whoami

- Lead Security Researcher of SCILabs
- 10 years of experience in DFIR
- 9 GIAC Certifications, SANS Mentor for Latin America
- I like playing the piano and exercising in my free time

SCI LABS
SCITUM CYBER INTELLIGENCE LABORATORIES


A VOUS DE JOUER !
make a gif.com

I want to help blue teamers detect malicious files on the network using **YARA** rules, **Zeek** framework and a custom script I developed, all are open source projects.

- Open source tool created by Victor Alvarez (@plusvic) from Virus Total
- Identification and classification of malware samples
- Create descriptions for malware families

```
rule SampleRule
{
    meta:
        my_identifier_1 = "Some string data"
    strings:
        $my_text_string = "text here"
        $my_hex_string = { E2 34 A1 C8 FB }
    condition:
        $my_text_string or $my_hex_string
}
```

Metadata section (optional): rule description, sharing restrictions, author

Strings section (optional, but almost always used): text, hex or regular expressions

Condition section (required): Determines the condition for detecting a file

Source: https://yara.readthedocs.io/en/v3.4.0/writingrules.html

```
rule Office_doc_AutoOpen {
  meta:
    author = "David Bernal - Scilabs"
    description = "Detects Microsoft Office documents with strings related to macro code and AutoExecution. “
    license = “https://creativecommons.org/licenses/by-nc/4.0/”
  strings:
      $auto1 = "AutoOpen"
      $auto2 = “AutoClose"
      $macro = "ThisDocument"
      $macro2 = "Project“
  condition:
      uint32(0) == 0xe011cfd0 and uint32(4) == 0xe11ab1a1 and
            all of ($macro*) and 1 of ($auto*)
  }
```

Author, description and license

AutoOpen or AutoClose-> automatic execution ThisDocument and Project -> macro

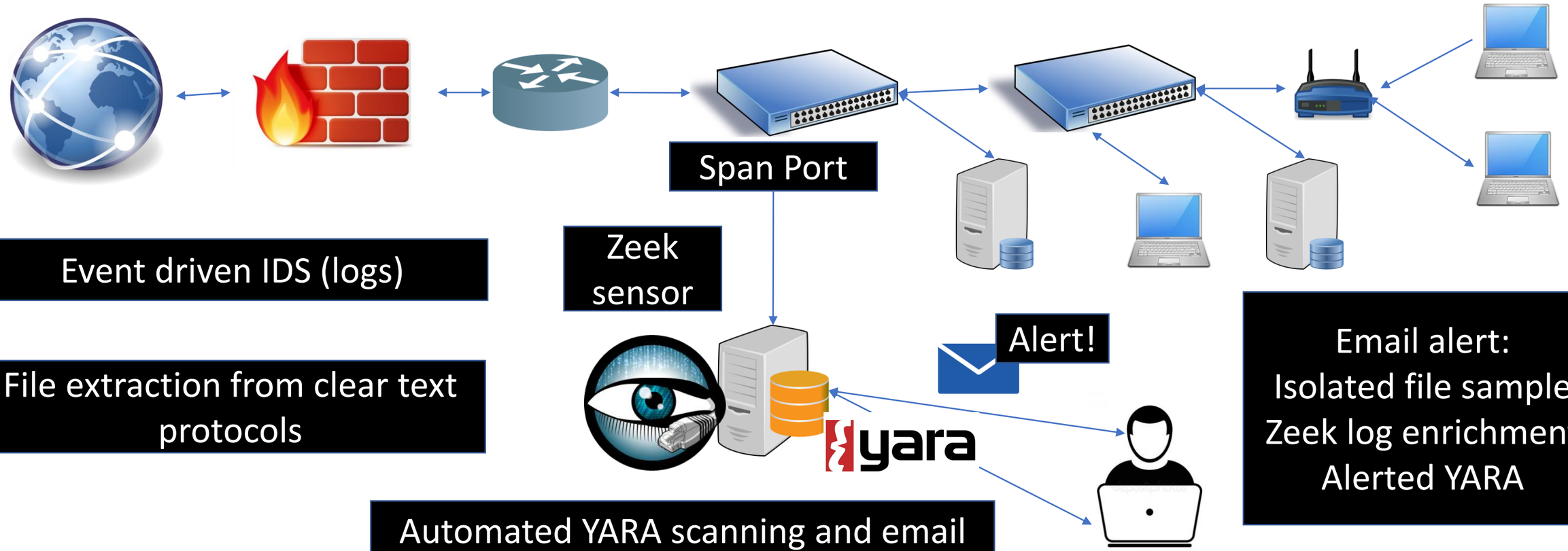
Uint32 -> define file magic number for office files and how strings are used

Zeek Network Security Monitor

- Formerly bro
- Event driven sensor
- Creates logs of the network traffic
- Can natively extract files from the network

- YARA has traditionally been used on the endpoint to detect malicious files. We can complement this detection on the network, for an increased coverage
- While some commercial products exist to support network based YARA detection, **it can be implemented with open source tools**!!: Zeek and YARA

Typical Enterprise Network Diagram



Event driven IDS (logs)

File extraction from clear text protocols

Automated YARA scanning and email based alerting with log enrichment

Email alert:
Isolated file sample
Zeek log enrichment
Alerted YARA

Enabling file extraction capabilities in Zeek

Zeek will trigger the event (f:fa_file) when it observes a new file in a supported clear text protocol

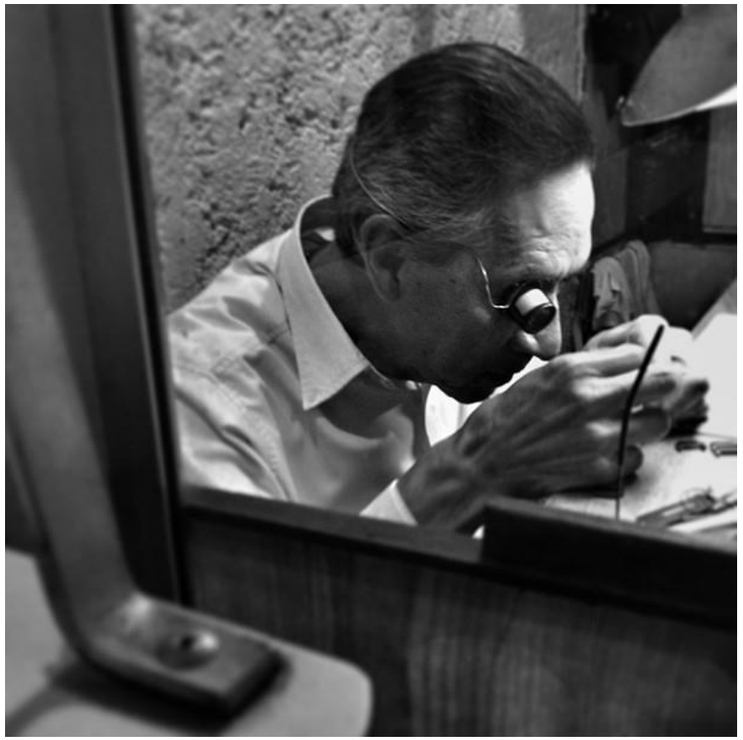
1. Add extraction script in main.bro
2. Enable the provided script:

@load frameworks/files/extract-all-files

3. Deploy Zeek configuration: Broctl deploy

Tuning file extraction in Zeek

- Increased sensor performance
- Files are retained for longer
- Potential evasion opportunity if an unexpected mime-type is used



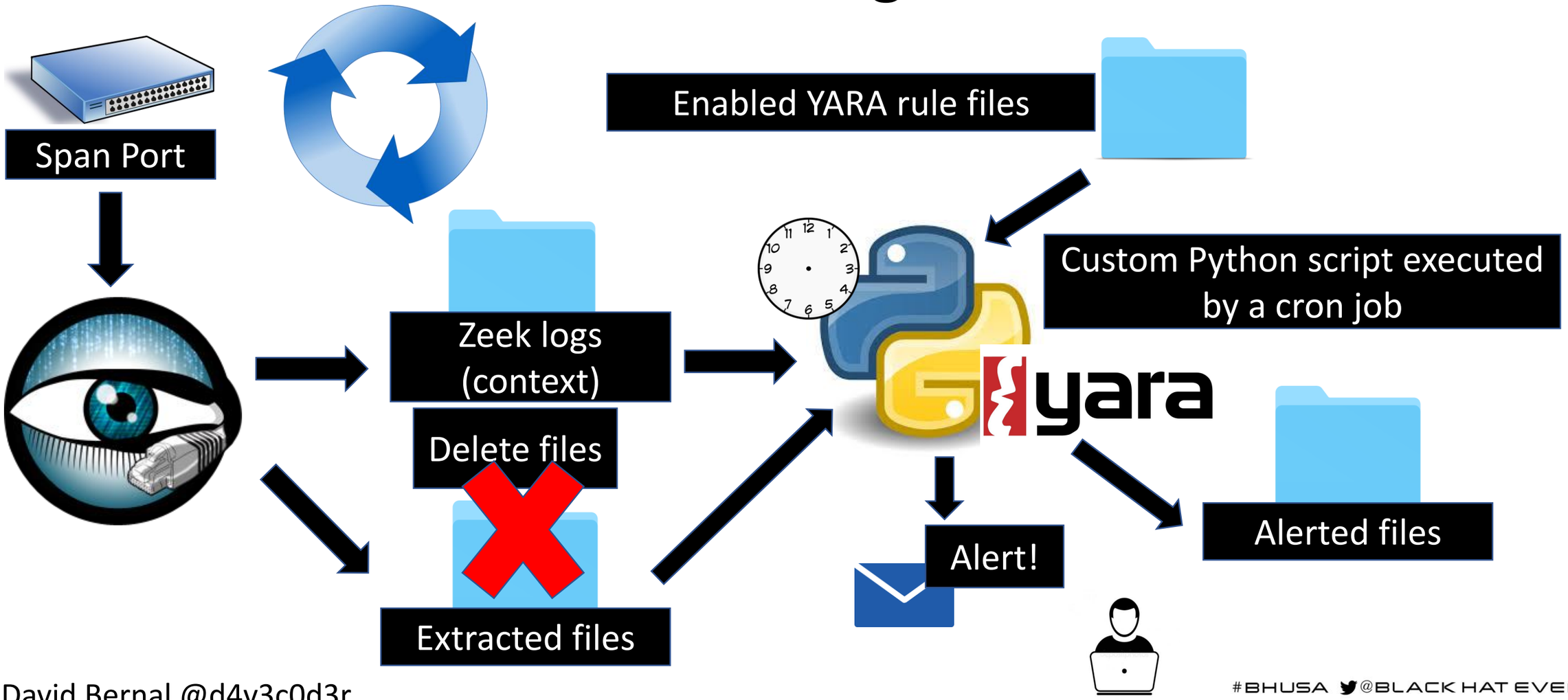
Tuning file extraction in Zeek

Target specific mime-types commonly used for malware delivery

- Compressed files
- Microsoft Word (old and new format)
- PDF files
- RTF files
- TXT files (detecting powershell, vbs)

Sample Zeek configuration file for targeted extraction based on mime-types is available on the white paper

Automated YARA Scanning



David Bernal @d4v3c0d3r

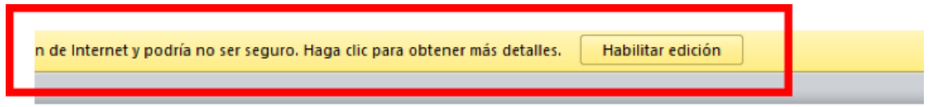
What YARA rules should you enable?

Develop and use your own YARA rules for the campaigns you detect.

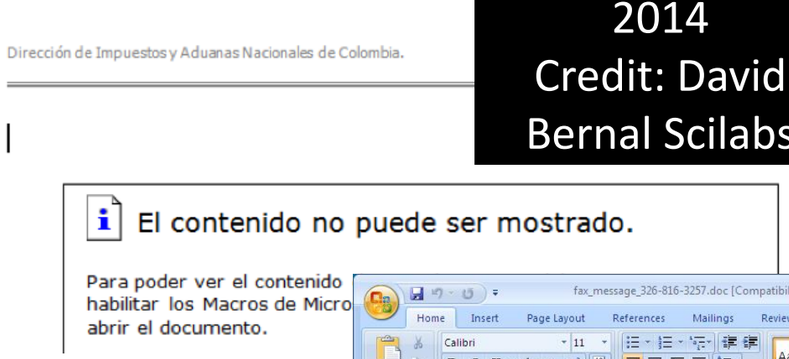
Use third party YARA rules from trusted sources, the community has great resources!

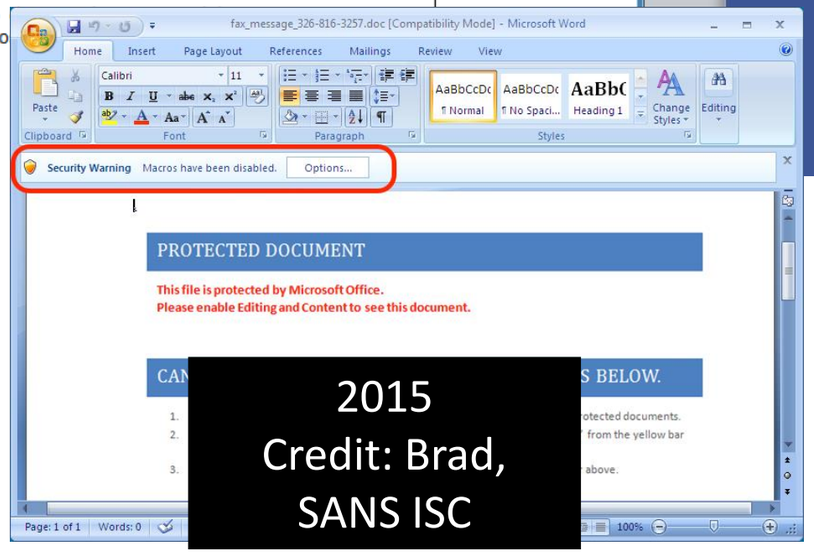
- CSIRT-CERT teams
- Florian Roth's rules https://github.com/Neo23x0/signature-base
- YARA Rules project https://github.com/Yara-Rules/rules
- Public threat research papers by various Security Vendors and Security Researchers
- Closed threat research groups (YARA Exchange community)

Detection Demo: malicious word files with macros

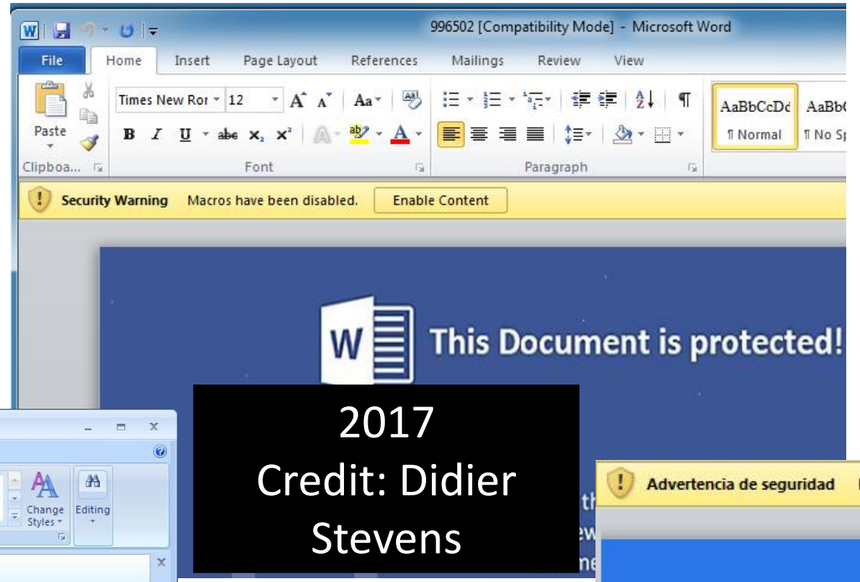


2014
Credit: David Bernal Scilabs





2015
Credit: Brad, SANS ISC



2017
Credit: Didier Stevens

5 years later…
still used!!

July 2019
Credit: Brad @malware_traffic

Full references on the white paper

Detection Demo: malicious word file with macros

Hello,

This email confirms that you submitted this total amount for processing:

Deposit Date: June 16, 2019

Merchant Id: 4596

Amount: $3,739.00 USD

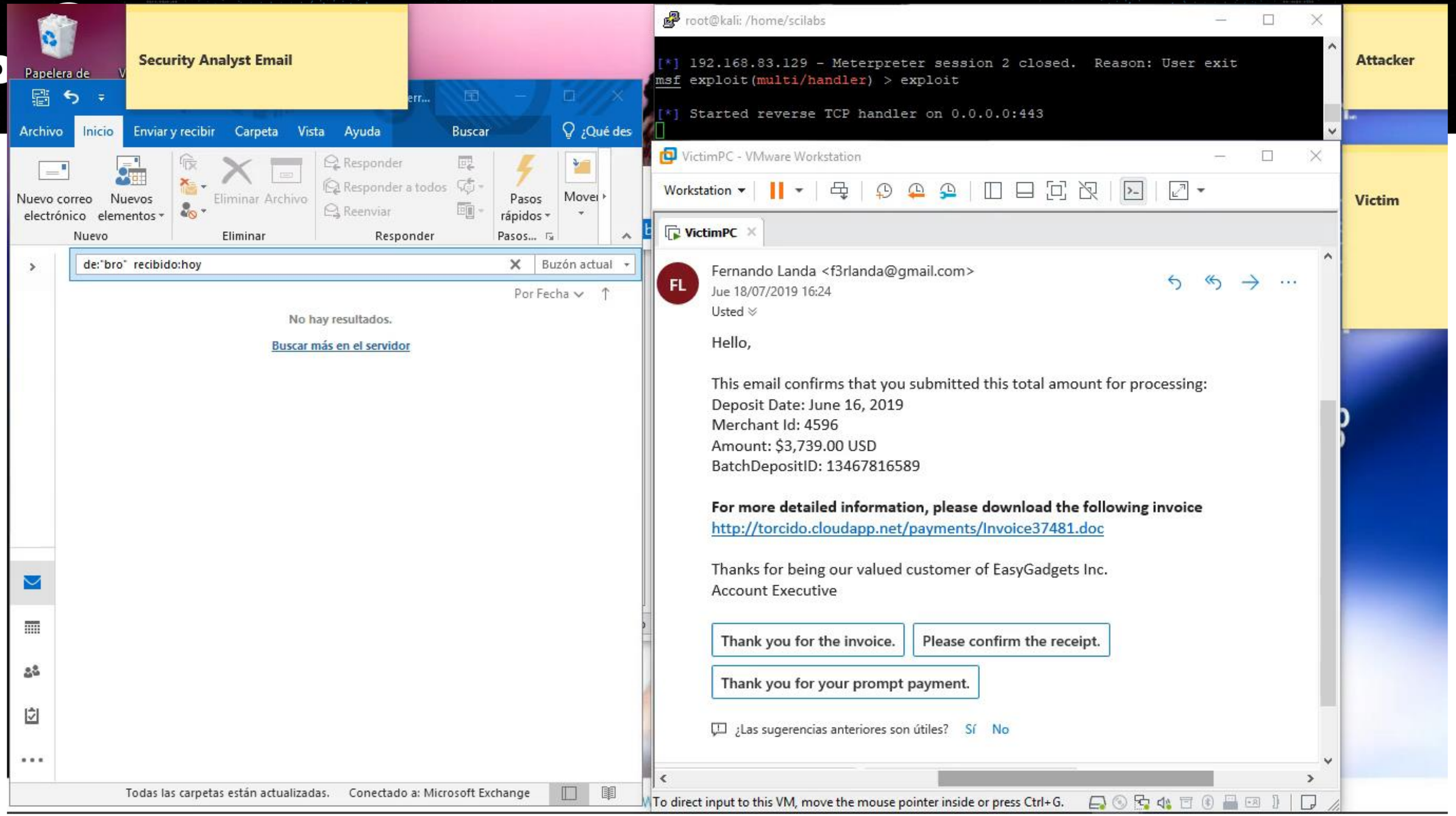
BatchDepositID: 13467816589

For more detailed information, please download the following invoice

http://torcido.cloudapp.net/payments/Invoice37481.doc

Thanks for being our valued customer of EasyGadgets Inc.

Account Executive

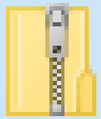

Papelera de
Security Analyst Email
Archivo
Inicio
Enviar y recibir
Carpeta
Vista
Ayuda
Buscar
Nuevo correo electrónico
Nuevos elementos
Nuevo
Eliminar
Archivo
Responder
Responder a todos
Reenviar
Pasos rápidos
Pasos...
de:"bro" recibido:hoy
Buzón actual
Por Fecha
No hay resultados.
Buscar más en el servidor
Todas las carpetas están actualizadas.
Conectado a: Microsoft Exchange
root@kali: /home/scilabs
[*] 192.168.83.129 - Meterpreter session 2 closed. Reason: User exit
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 0.0.0.0:443
VictimPC - VMware Workstation
Workstation
VictimPC
FL
Fernando Landa <f3rlanda@gmail.com>
Jue 18/07/2019 16:24
Usted
Hello,
This email confirms that you submitted this total amount for processing:
Deposit Date: June 16, 2019
Merchant Id: 4596
Amount: $3,739.00 USD
BatchDepositID: 13467816589
For more detailed information, please download the following invoice
http://torcido.cloudapp.net/payments/Invoice37481.doc
Thanks for being our valued customer of EasyGadgets Inc.
Account Executive
Thank you for the invoice.
Please confirm the receipt.
Thank you for your prompt payment.
¿Las sugerencias anteriores son útiles? Sí No
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Attacker
Victim

miércoles 17/07/2019 09:25 p. m.

bro@scitum.com.mx

YARA Alert

Para David Eduardo Bernal Michelena



HTTP-F5RH0B4Yv40fchollc.doc.zip
17 KB

More Yara detections: higher confidence

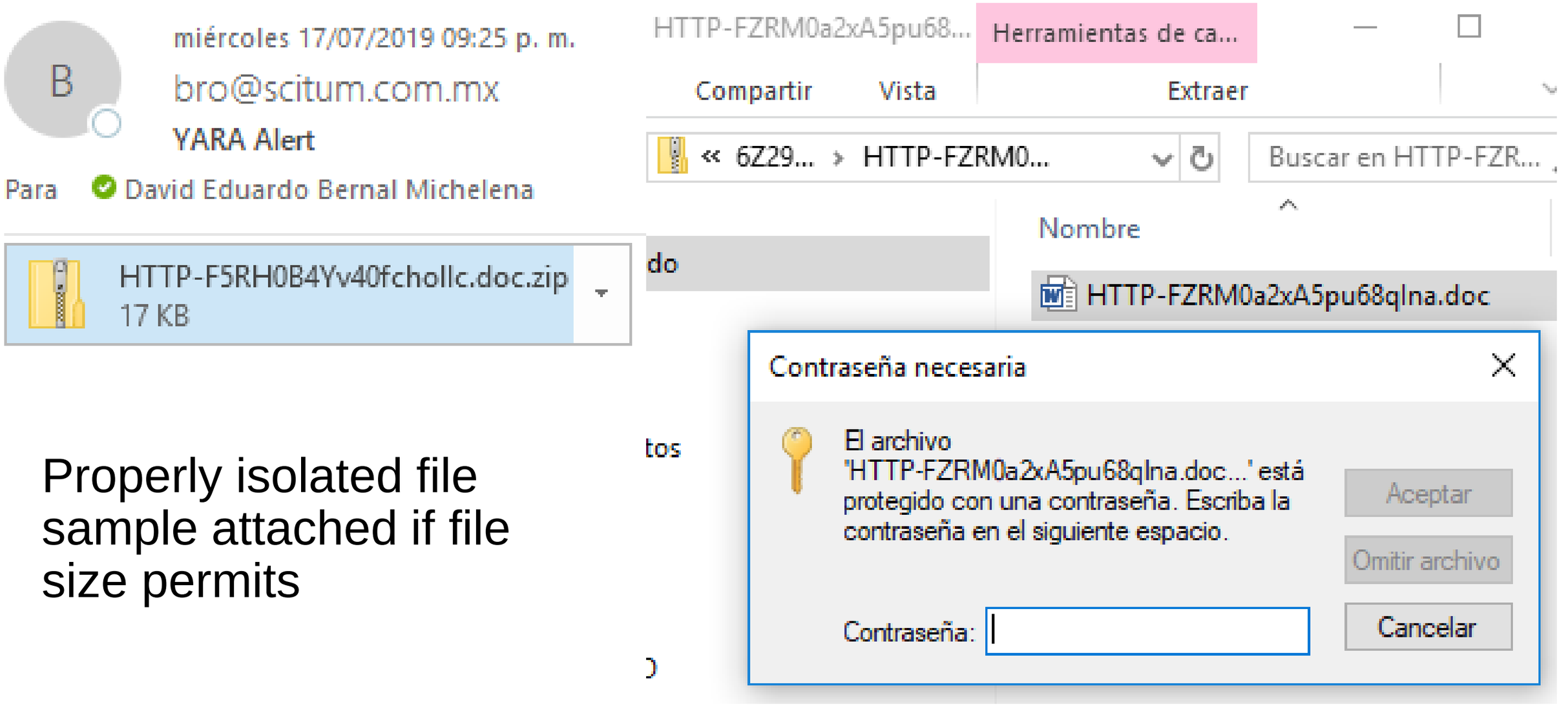
2 of my rules alerted

1 additional from a trusted third party

alerted rules: ['Office_doc_AutoOpen', 'Office_doc_Execution', 'Office_AutoOpen_Macro']
filepath: /home/bro/extracted/HTTP-F5RH0B4Yv40fchollc.doc
md5sum : e4b827195b5ee3ef85f3085852a26012
sha1sum: bf7668ec23feeac9dad987e1338945e2bb8fa0fb
sha256sum: 99b2b9973349d796a3658c37bda3d3cad2af46b793536bd3c54a036b44a416d4

saved Zip file: /home/bro/YARA/alertedFiles/HTTP-F5RH0B4Yv40fchollc.doc.zip

context: 2019-07-17T21:24:28-0500 F5RH0B4Yv40fchollc 13.94[redacted] 172[redacted]
CUNdaY2zRjiVYQjLnh HTTP 0 MD5,EXTRACT,SHA1 application/msword
- 0.798037 F F 47616 47616 0 0 F -
e4b827195b5ee3ef85f3085852a26012
bf7668ec23feeac9dad987e1338945e2bb8fa0fb - /home/bro/extracted/HTTP-
F5RH0B4Yv40fchollc.doc F -
2019-07-17T21:24:27-0500 CUNdaY2zRjiVYQjLnh 172[redacted] 36642 13.94[redacted]
80 3 GET torcido.cloudapp.net /payments/Invoice37481.doc -
1.1 Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0;
.NET4.0C; .NET4.0E; ms-office; MSOffice 14) 0 47616 200 OK - -
(empty)- - - - - - F5RH0B4Yv40fchollc -
application/msword



Properly isolated file sample attached if file size permits

Challenges / Next Steps

- Fine tuning
- Automatic event creation on MISP
- Integration with Elasticsearch and Syslog
- Exclusions
- Encrypted protocols
- Migration to Python 3
- Sandbox integration
- Integration with SOAR

Custom script

- This script can be freely downloaded from SCILabs github https://github.com/SCILabsMX/yaraZeekAlert

- The white paper is available on Black Hat media server

Key Takeaways

- YARA detection can not only be implemented on the endpoint, but on the network too
- Network based YARA detection can be implemented with Zeek
- Network based YARA detection does not stress the endpoints and is generally faster, (several GB against several hundreds GB)

Thanks for your contributions!!!

Zeek Project (@zeekurity)
https://docs.zeek.org

YARA
https://yara.readthedocs.io/

Security researchers than share with the community

- Víctor M Álvarez
- Mila Parkour & YARA Exchange, DeepEndResearch Community
- Florian Roth
- Didier Stevens
- Brad from malware-traffic-analysis.net, SANS ISC
- CERT Teams, Security Vendors that release public YARA rules

SCITUM CYBER INTELLIGENCE LABORATORIES

David Bernal

@d4v3c0d3r

davidbernalmichelena@gmail.com