Intelligence Driven Intrusion Detection

Matthias Wübbeling: *matthias.wuebbeling@cs.uni-bonn.de*
Arnold Sykosch: *sykosch@cs.uni-bonn.de*

Friedrich-Wilhelms-Universität Bonn: Working Group IT Security

Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE: Cyber Security Department

universitätbonn

OVERVIEW

- Threat Intelligence in a Nutshell
- Exchange of TI
- Utilization of TI
- STIX2Suricata
- STIX2GRR

Threat Intelligence in a Nutshell

- What do you need TI for?
  - Identify emerging threats before being targeted by an attacker.
  - Share intelligence information of ongoing or finished attacks.
  - Common sense:
    To survive, a gazelle must run faster than the slowest gazelle.

(image from http://quoteinvestigator.com)

  - „Common sense is not so common“ (unknown source).
  - How about this quote in the field of Internet attacks / APT?

Threat Intelligence in a Nutshell

- How about the hunters and the hunted in the Internet age?
  - To survive: You have to be faster than the fastest attacker!

Threat Intelligence in a Nutshell

- How about the hunters and the hunted in the Internet age?
  - To survive: You have to be faster than the fastest attacker!

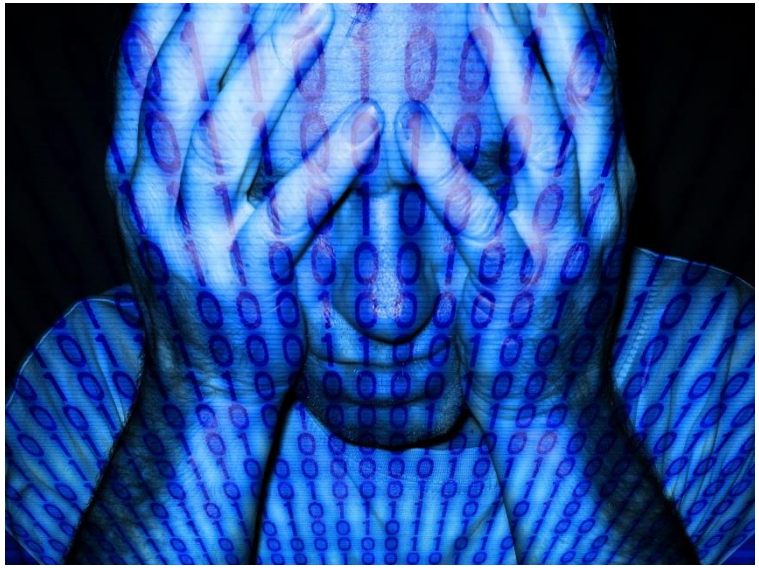
- Common goal: Being faster than 85%-99% of the attackers.

Exchange of Threat Intelligence

- Common data exchange format: XML
- Existing standards for TI data:
  - OpenIOC
  - STIX/CybOX
- OpenIOC
  - “OpenIOC is an extensible XML schema for the description of technical characteristics that identify a known threat, an attacker’s methodology, or other evidence of compromise. OpenIOC was created by MANDIANT” (www.openioc.org)
- STIX/CybOX
  - Developed by MITRE.
  - At least as expressively as OpenIOC.
  - Therefore: => we use STIX/CybOX.
- How to get Threat Intelligence?
  - Become part of a TI sharing community
  - Buy TI feeds or get the free ones (e.g. from hailataxii.com)

Utilization of Threat Intelligence

- How to use Threat Intelligence to protect your infrastructure?
  - Have an employee consuming TI the whole day extracting the relevant information?

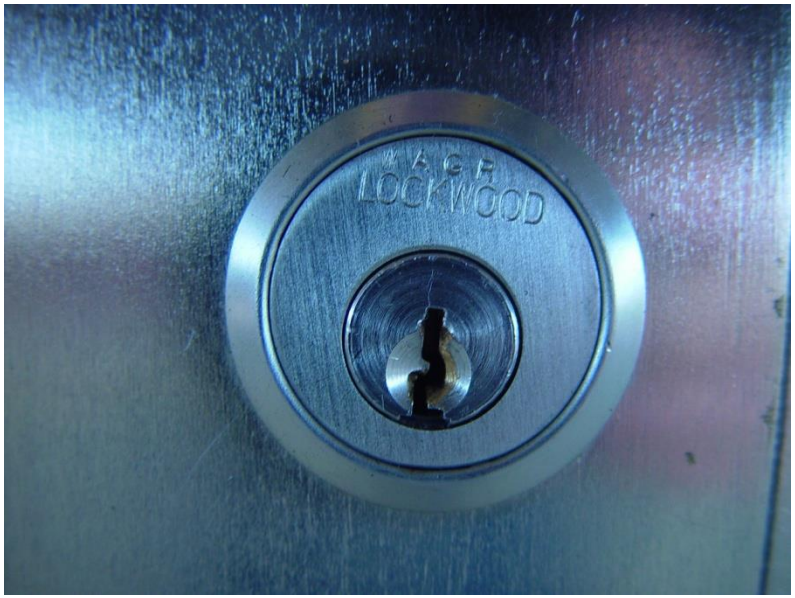


Utilization of Threat Intelligence

- How to use Threat Intelligence to protect your infrastructure?
  - Have an employee consuming TI the whole day extracting the relevant information?
    Better not!

Utilization of Threat Intelligence

- How to use Threat Intelligence to protect your infrastructure?
  - Have an employee consuming TI the whole day extracting the relevant information?
    Better not!
  - Enable your security equipment to understand STIX/CybOX?



Utilization of Threat Intelligence

- How to use Threat Intelligence to protect your infrastructure?
  - Have an employee consuming TI the whole day extracting the relevant information?
    Better not!
  - Enable your security equipment to understand STIX/CybOX?
    Not possible if you use security appliances.

Utilization of Threat Intelligence

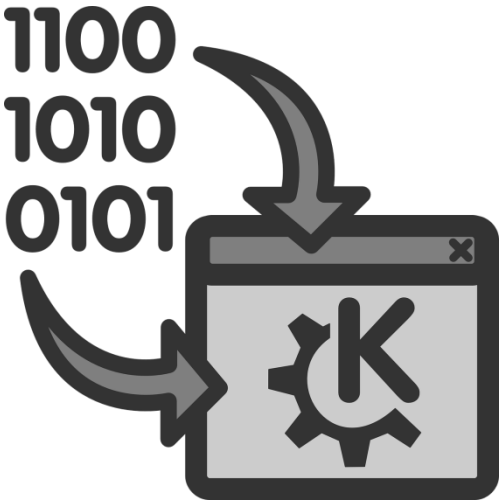
- How to use Threat Intelligence to protect your infrastructure?
  - Have an employee consuming TI the whole day extracting the relevant information?
    Better not!
  - Enable your security equipment to understand STIX/CybOX?
    Not possible if you use security appliances.
  - Beg the vendor or your appliance to implement STIX/CybOX?

Utilization of Threat Intelligence

- How to use Threat Intelligence to protect your infrastructure?
  - Have an employee consuming TI the whole day extracting the relevant information?
    Better not!
  - Enable your security equipment to understand STIX/CybOX?
    Not possible if you use security appliances.
  - Beg the vendor or your appliance to implement STIX/CybOX?
    Sure you do! Will take a while.

Utilization of Threat Intelligence

- How to use Threat Intelligence to protect your infrastructure?
  - Have an employee consuming TI the whole day extracting the relevant information?
    Better not!
  - Enable your security equipment to understand STIX/CybOX?
    Not possible if you use security appliances.
  - Beg the vendor or your appliance to implement STIX/CybOX?
    Sure you do! Will take a while.
  - Map STIX/CybOX information to the applications'/appliances' configuration!



Utilization of Threat Intelligence

- How to use Threat Intelligence to protect your infrastructure?
  - Have an employee consuming TI the whole day extracting the relevant information?
    Better not!
  - Enable your security equipment to understand STIX/CybOX?
    Not possible if you use security appliances.
  - Beg the vendor or your appliance to implement STIX/CybOX?
    Sure you do! Will take a while.
  - Map STIX/CybOX information to the applications'/appliances' configuration!

    Might be a good chance to get it now!

Utilization of Threat Intelligence

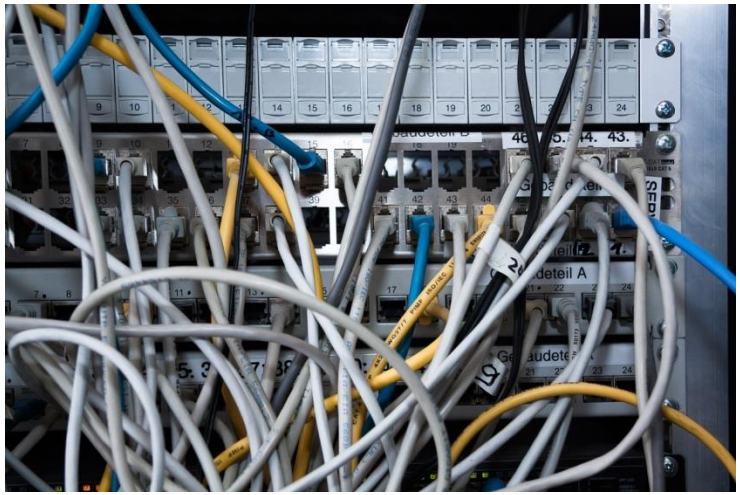
- How to use Threat Intelligence to protect your infrastructure?
  - Have an employee consuming TI the whole day extracting the relevant information?
    Better not!
  - Enable your security equipment to understand STIX/CybOX?
    Not possible if you use security appliances.
  - Beg the vendor or your appliance to implement STIX/CybOX?
    Sure you do! Will take a while.
  - Map STIX/CybOX information to the applications'/appliances' configuration!

    Might be a good chance to get it now!
  - We just started to map STIX to a Host and a Network IDS:
    Suricata (NIDS; same rule syntax as SNORT)
    GRR Rapid Response (HIDS; "hunting for artifacts")

STIX2Suricata

- Goal: Generate Suricata rules based on STIX/CybOX TI.
  - 1st Step: Identify relevant data fields in STIX/CybOX.
  - 2nd Step: Mapping identified fields to Suricata rule elements.
  - 3rd Step: Implement tool for automated rule generation.

- STIX/CybOX elements relevant for network intrustion detection systems:
  - Address, NetworkConnection, Packet, Port, Socket
  - ArchiveFile, DNSQuery, DNSRecord, DomainName, EmailMessage, File, Hostname, HTTPSession, Link, NetFlow, URI, X509Certificate



STIX2Suricata

- Suricata rule syntax:
  - <Action> <Header> <Options>

STIX2Suricata

- Suricata rule syntax:
  - <Action> <Header> <Options>
- <Action>
  - Pass
  - Drop
  - Reject
  - Alert

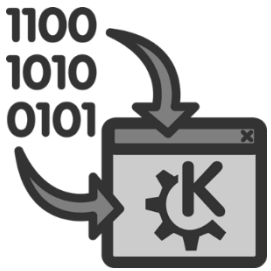
STIX2Suricata

- Suricata rule syntax:
  - <Action> <Header> <Options>
- <Action>
  - Pass
  - Drop
  - Reject
  - Alert
- <Header>
  - Protocol: (IP/UDP/TCP + some application layer protocols)
  - Source IP-Address
  - Source TCP/UDP-Port
  - Direction of traffic
  - Destination IP-Address
  - Destination TCP/UDP-Port
- STIX2Suricata mapping for <Header> elements:
  - Address, NetworkConnection, Packet, Port, Socket

- <Header> mapping example:

  - STIX/Cybox data:

```
<indicator:Observable  id="example:Observable-1c798262-a4cd-434d-a958-884d6980c459">
   <cybox:Object id="example:Object-1980ce43-8e03-490b-863a-ea404d12242e">
     <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
       <AddressObject:Address_Value condition="Equals" apply_condition="ANY">
          10.1.0.1##comma##10.2.0.2##comma##10.3.0.3
        </AddressObject:Address_Value>
        </cybox:Properties>
      </cybox:Object>
 </indicator:Observable>
```



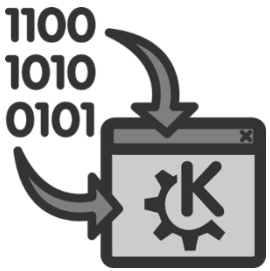
  - Resulting Suricata rule:
    alert ip [10.1.0.1, 10.2.0.2, 10.3.0.3] any <> any any (<Options>)

STIX2Suricata

- Suricata rule syntax:
  - <Action> <Header> <Options>
- <Options>
  - msg
  - sid
  - rev
  - gid
  - classtype
  - reference
  - priority
  - metadata
  - content
- STIX2Suricata mapping for <Options> elements:
  - ArchiveFile, DNSQuery, DNSRecord, DomainName, EmailMessage, File, Hostname, HTTPSession, Link, NetFlow, URI, X509Certificate

- <Options> mapping example:
  - STIX/Cybox data:

```
<EmailMessageObj:Header>
 <EmailMessageObj:From category="e-mail">
  <AddressObj:Address_Value condition="StartsWith">
   match@state.gov
  </AddressObj:Address_Value>
 </EmailMessageObj:From>
</EmailMessageObj:Header>
…
<cybox:Related_Objects>
 <cybox:Related_Object>
  <cybox:Properties xsi:type="FileObj:FileObjectType">
   <FileObj:File_Extension>pdf</FileObj:File_Extension>
   <FileObj:Size_In_Bytes>87022</FileObj:Size_In_Bytes>
  </cybox:Properties>
</cybox:Related_Object>
</cybox:Related_Objects>
```



  - Resulting Suricata rule:

```
alert tcp any any <> any any (msg:"STIX2Suricata: Malicious Email"; flow:established;
    content:From: match@state.gov; nocase; fileext:"pdf"; sid:513000; )
```

STIX2Suricata

- Current development status:
  - Python prototype maps data relevant for NIDS to Suricata rules.
  - Integration into [large company name here] Threat Intelligence tool.

STIX2GRR

- GRR Rapid Response (GRR)
  - “GRR is forensic framework focused on scalability enabling powerful analysis.” (https://github.com/google/grr)
  - A forensic framework is not a Host IDS !!!11 ?
  - But: It is possible to use GRR to remotely get the state of host systems.
- Why GRR and not OSSEC or similar?
  - GRR is state based – as STIX/CybOX data is
- GRR is hunt based
  - Define artifact to look for.
  - Select target hosts.
  - Start hunt.
  - Wait for “rapid responses”.

- GRR Rapid Response (GRR)
  - GRR is highly extensible and written in python.

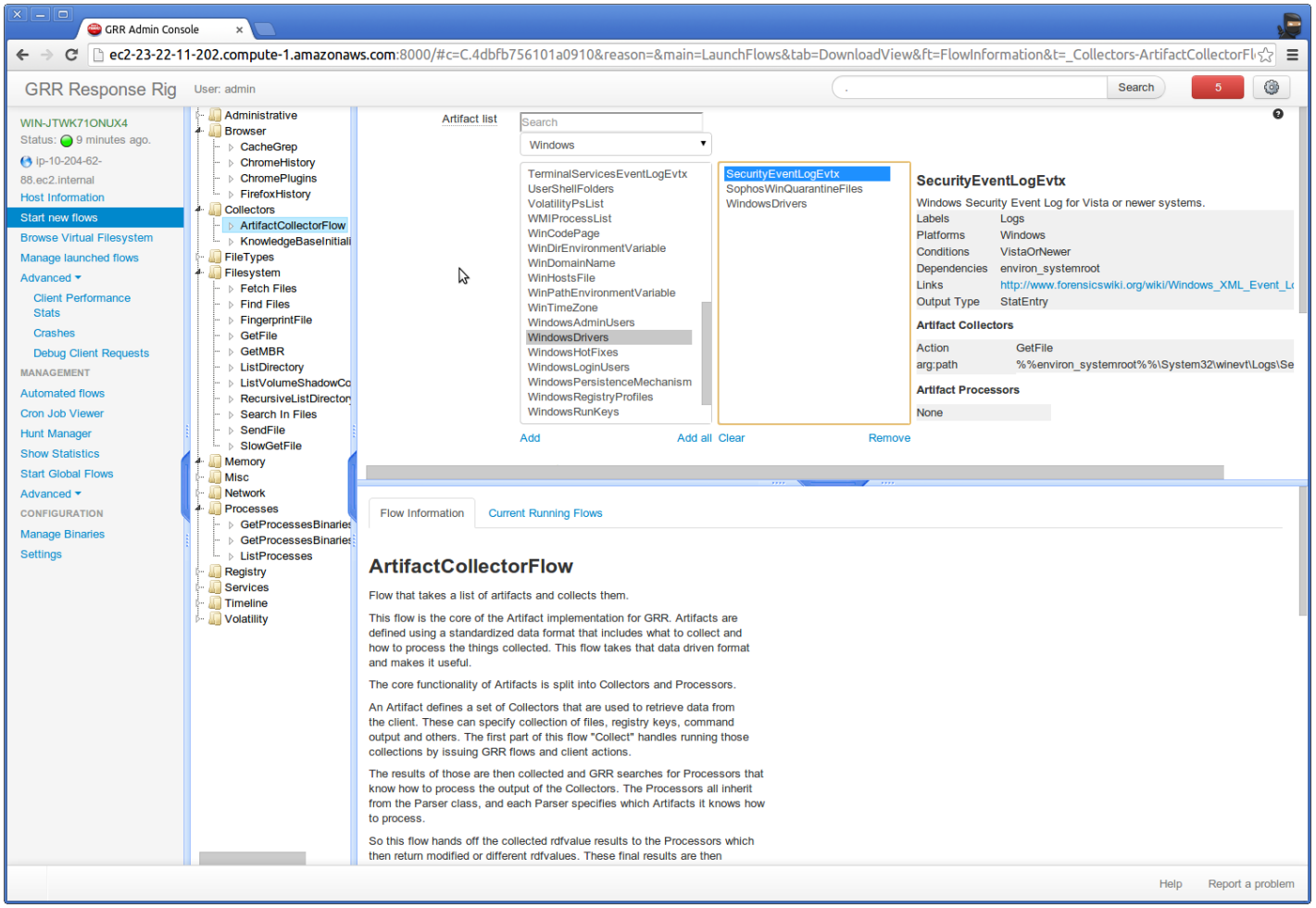


Image from: https://github.com/google/grr

STIX2GRR

- Mapable STIX/CybOX data fields:
  - WindowsDriver, ArchiveFile, File, ImageFile, PDFFile, UnixFile, WindowsExecutableFile, WindowsFile, Mutex, Address, DomainName, DNSQuery, EmailMessage, HTTPSession, NetworkConnection, SocketAddress, URI, Process, UnixProcess, WindowsProcess, WindowsRegistryKey

- Goal: Generate hunts for given STIX/CybOX TI data:
  - 1st Step: Identify relevant data fields in STIX/CybOX.
  - 2nd Step: Mapping identified fields to artifacts.
  - 3rd Step: Implement tool for automated hunt generation (+ artifact support).

STIX2GRR

- Current development status:
  - Python prototype maps data relevant for HIDS and creates hunts directly in GRR server system.
  - Integration into [large company name here] Threat Intelligence tool.

Conclusion

- Identified relevant Objects in STIX/CybOX.
- Created mapping for STIX/CybOX => (N|H)IDS.
- Implemented prototype as proof-of-concept.
- Integrated it into a TI management framework.

Questions?

Thank you very much for your attention

Credits: Image „Lion and Gazelle“ from quoteinvestigator.com.
Image „GRR hunt“ from github.com/google/grr
Other images from pixabay.com (CC License)