Threat intelligence week 6

Jurjen de Jonge
500731921
Hogeschool van Amsterdam

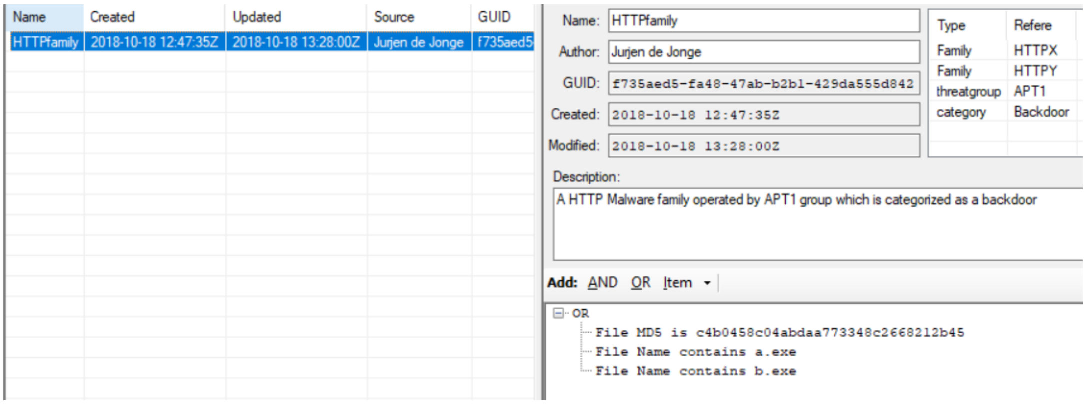
October 21, 2018

Contents

1. *IoC development*

1.1 Developing the IOC

Adding all the given variables to the Mandiant IOCe software was easy to do.



Name	Created	Updated	Source	GUID
HTTPfamily	2018-10-18 12:47:35Z	2018-10-18 13:28:00Z	Jurjen de Jonge	f735aed5

Name: HTTPfamily
Author: Jurjen de Jonge
GUID: f735aed5-fa48-47ab-b2b1-429da555d842
Created: 2018-10-18 12:47:35Z
Modified: 2018-10-18 13:28:00Z

Type	Refere
Family	HTTPX
Family	HTTPY
threatgroup	APT1
category	Backdoor

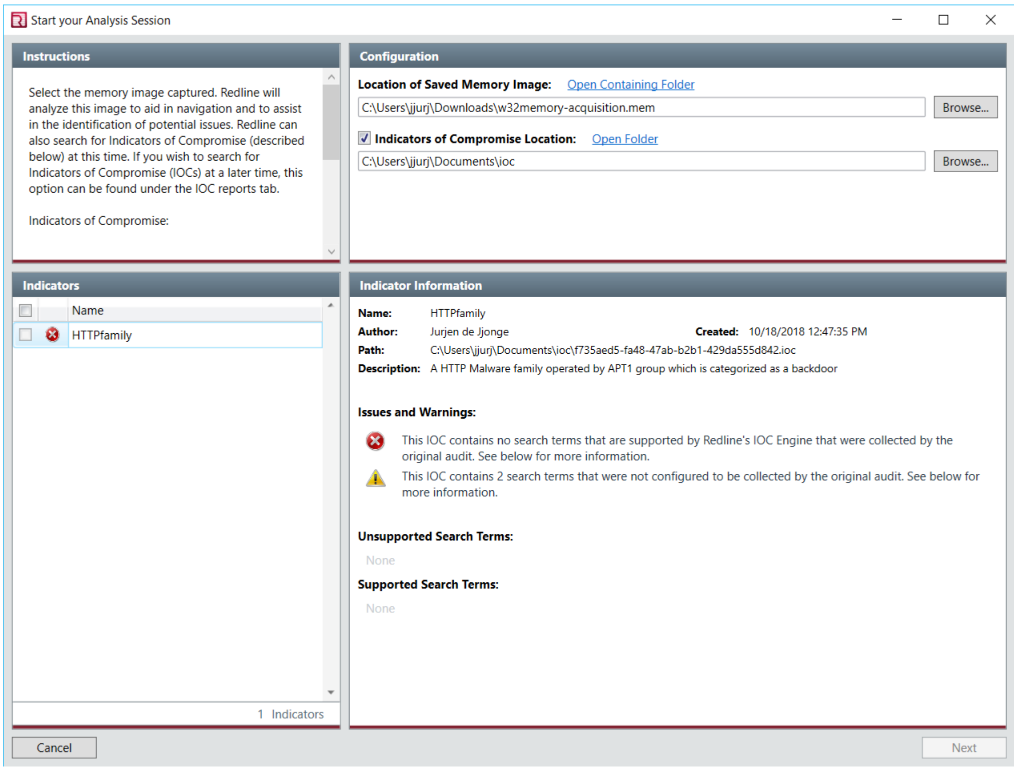
Description:
A HTTP Malware family operated by APT1 group which is categorized as a backdoor

```
OR
  File MD5 is c4b0458c04abdaa773348c2668212b45
  File Name contains a.exe
  File Name contains b.exe
```

Figure 1.1: Usign the MNdiant IOCe software to create an IoC

Adding all the rules is easy, just using the GUI it's very easy to keep on adding rules and logic to the IoC. A large variety of options are available to add to the IoC. Seeming to make the software like a valuable tool.

Sadly when trying to use the rule set made for Mandiant Redline, it will not reconize the IoC search as something to be found back in the memory dump that was given to us.



Start your Analysis Session

Instructions

Select the memory image captured. Redline will analyze this image to aid in navigation and to assist in the identification of potential issues. Redline can also search for Indicators of Compromise (described below) at this time. If you wish to search for Indicators of Compromise (IOCs) at a later time, this option can be found under the IOC reports tab.

Indicators of Compromise:

Configuration

Location of Saved Memory Image: Open Containing Folder

C:\Users\jjurj\Downloads\w32memory-acquisition.mem

☑ **Indicators of Compromise Location:** Open Folder

C:\Users\jjurj\Documents\ioc

Indicators

□		Name
□	☒	HTTPfamily

1 Indicators

Indicator Information

Name: HTTPfamily
Author: Jurjen de Jjonge **Created:** 10/18/2018 12:47:35 PM
Path: C:\Users\jjurj\Documents\ioc\f735aed5-fa48-47ab-b2b1-429da555d842.ioc
Description: A HTTP Malware family operated by APT1 group which is categorized as a backdoor

Issues and Warnings:

☒ This IOC contains no search terms that are supported by Redline's IOC Engine that were collected by the original audit. See below for more information.

⚠ This IOC contains 2 search terms that were not configured to be collected by the original audit. See below for more information.

Unsupported Search Terms:

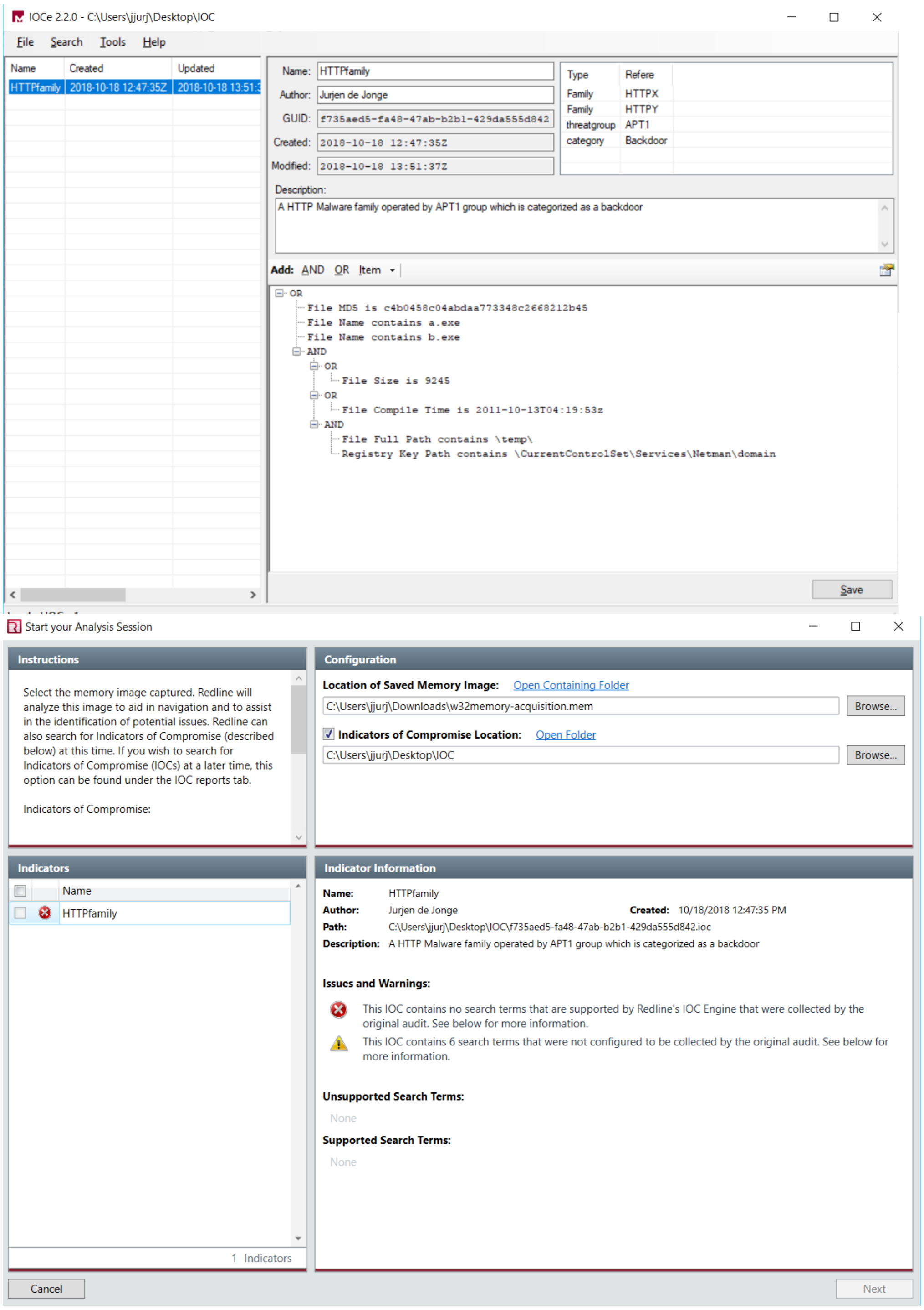
None

Supported Search Terms:

None

Figure 1.2: Error when using the IoC within RedLine

Adding up to the rules was again easy to do, but sadly RedLine showed the same problem with the memory dump as before.



Name	Created	Updated
HTTPfamily	2018-10-18 12:47:35Z	2018-10-18 13:51:3

Name: HTTPfamily
Author: Jurjen de Jonge
GUID: f735aed5-fa48-47ab-b2b1-429da555d842
Created: 2018-10-18 12:47:35Z
Modified: 2018-10-18 13:51:37Z

Type	Refere
Family	HTTPX
Family	HTTPY
threatgroup	APT1
category	Backdoor

Description:
A HTTP Malware family operated by APT1 group which is categorized as a backdoor

```
OR
  File MD5 is c4b0458c04abdaa773348c2668212b45
  File Name contains a.exe
  File Name contains b.exe
  AND
    OR
      File Size is 9245
    OR
      File Compile Time is 2011-10-13T04:19:53z
    AND
      File Full Path contains \temp\
      Registry Key Path contains \CurrentControlSet\Services\Netman\domain
```

Select the memory image captured. Redline will analyze this image to aid in navigation and to assist in the identification of potential issues. Redline can also search for Indicators of Compromise (described below) at this time. If you wish to search for Indicators of Compromise (IOCs) at a later time, this option can be found under the IOC reports tab.

Indicators of Compromise:

Location of Saved Memory Image: C:\Users\jjurj\Downloads\w32memory-acquisition.mem

☑ **Indicators of Compromise Location:** C:\Users\jjurj\Desktop\IOC

□		Name
□	☒	HTTPfamily

1 Indicators

Name: HTTPfamily
Author: Jurjen de Jonge **Created:** 10/18/2018 12:47:35 PM
Path: C:\Users\jjurj\Desktop\IOC\f735aed5-fa48-47ab-b2b1-429da555d842.ioc
Description: A HTTP Malware family operated by APT1 group which is categorized as a backdoor

Issues and Warnings:

☒ This IOC contains no search terms that are supported by Redline's IOC Engine that were collected by the original audit. See below for more information.

⚠ This IOC contains 6 search terms that were not configured to be collected by the original audit. See below for more information.

Unsupported Search Terms:

None

Supported Search Terms:

None

Figure 1.3: Adding more rules to the and RedLine failing again to use these IoC

2. *About STIX & TAXII*

2.1 What is STIX?

Structured Threat Information Expression (STIX) is a format that is used to share cyber threat intelligence with others. It uses JSON format where objects are created. There are twelve STIX domain objects. There objects are linked to each other using the Relationship objects.

This creates a small graph that is easy in use for analyst or processing with tools.

2.2 What is TAXII

Trusted Automated Exchange of Intelligence Information (TAXII) Is protocol designed for communicating Cyber threat information (CTI). It has been specifically designed to transfer STIX. Though TAXII it was designed specifically for STIX it can be used to transport non STIX data.

2.3 Difference between TAXII client and TAXII server

It seems like the difference between the client and server are like every other server ¡-¿ client relationship. The client requests something from the server and it responeds to that request.

3. *STIX*

3.1 Attack pattern

The attack pattern is the description of how adversaries try to compromise targets. It connects towards identity and vulnerability. They indicate that an attack is targeted towards a certain identity or vulnerability in a software.

3.2 Campaign

The campaign is the grouping of adversarial behavior. It's a set of malicious activities or attacks against a specif target. Campaigns are characterized by their objsectives and incidents they cause, targets and resources they use. They are attributed-to to intrusion-set and threat-actor. Which actors and the behavior they show. The targets relationship is identity and vulnerability showing the exploits and type of targets. Using a certain exploit being used or people targeted from a specific sector. The uses relationship will be linked to attack-pattern, malware and tool. This describes how the campaign will go, which actions will be taken and which malware/tools will be used.

3.3 Course of Action

A description of which actions to take to prevent or respond to an attack. Relationships are mitigates and related to attack pattern, malware, tool and vulnerability. Describing how to mitigate them.

3.4 Identity

This identifies actual individuals, organizations or groups. The relationships it has are only reverse relationships.

3.5 Indicator

The indicator will describe, the detected kill chain phases, time window for when the indicator is valid and a pattern to capture detection. The relationships are indications towards attack-pattern, campaign,intrusion-set,malware,threat-actor and tool. It described evidence against the related objects. This could also be secondary evidence.

3.6 Intrusion set

The intrusion set is grouped set of adversarial behaviors and resources with common properties and are believed to be done by a single organization. The set might capture multiple campaigns and share attributes with known and unknown threat actors. Relationships are attributed to a threat actor, targets are identity and vulnerability and uses attack-pattern, malware and tool. All similar to campaign.

3.7 Malware

Malware describes malicious code and software according to family and samples. The relationships are targets, identity and vulnerability. Malware targeting a specific sector or using a specific exploit. uses relationship is tool which documents that the malware is related to a tool. And variant of which describes the variant of a certain type. (TorrentLocker is a variant of CryptoLockers)

3.8 Observed Data

Describes what information was observed on a system. A file, IP-address, network connection or registry key can all be observerd. It does not bring any intelligence with it, just the fact that it was seen. It does not have any relationships.

3.9 Report

Reports are collections of threat intelligence focused on one or more topics. A description of threat actors, malware or attack technique. It does not have any specif relationships. The relationships it has are linked to anything that is related the what is written about in the report.

3.10 Threat actor

These are groups, organizations or individuals that operate with malicious intent. They are characterized by their motives, capabilities, goals, sophistication level, past activities, resources they have access to, and their role in the organization. The relationships are attributed to with identity which describes their real identity, impersonates with identity and describes whom is being impersonated, targets with identity and vulnerability which describes the actors use of exploits and targets, uses towards attack pattern, malware and tool and describes typical behavior, tools and malware being used.

3.11 Tool

Tools are legitimate software that can be used for attacks. The tools have legitimate purposes on systems for power users, admins and even normal users. it characterizes the properties of the software and how they are used in an attack. It has a relationship to targets with identity and vulnerability which again describes an exploit or specific target.

3.12 Vulnerability

The vulnerability describes a mistake in software that can be used by an attacker to gain access to or disrupt a system. It does not have any outgoing relationships.