Cyber Investigations and Indicators of Compromise (IOC) Management

I work for Dynamico as the senior security manager of the medium-sized company that outsourced most of its IT services. This activity involves traffic between our branch office in Bismarck, ND, and a known malicious host, moto2.earthsolution.org (IP: 69.195.129.72). My job is to assess the danger that APT actors bring and to study the APT1 group more specifically. This means I have to go through the Internet to search for Indicators of Compromise (IOCs), format them in OpenIOC and STIX format and share the results with others by using the Malware Information Sharing Platform (MISP) (FireEye, 2013).

Section 1: OpenIOC Format

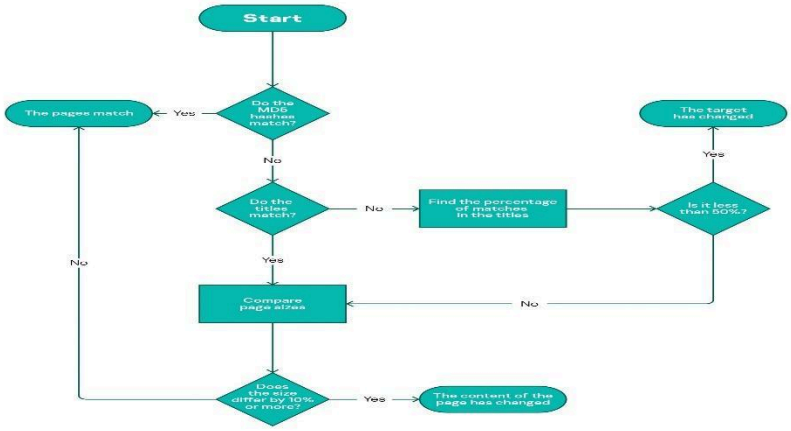
Mandiant released Indicators of Compromise (IOCs) in open domain with the OpenIOC format. They make it possible for a fast dissemination and utilization of IOCs in counteracting existing security risks. In this section, you shall be taken through how you can understand and apply OpenIOC.

1.1 Understanding GDOCUPLOAD Family

The GDOCUPLOAD malware family is connected with the document – upload attacks and aims to use in organizations that deal with important documents. It is spread via e-mail, phishing, and can be downloaded from links which are provided by the malware itself. Researchers have noted that it its operation, once the malware is run, it steals information from the infected system (Barnum, 2014).

Unique Behaviors:

- Establishing C2 Communication: The malware reports stolen information to other external C2 servers and wait for other instructions from the servers. This connection is often encrypted and though traffic analyzing tools (STIX Whitepaper, 2014), this is hard to note.
- Phishing Delivery: GDOCUPLOAD is usually deployed through spam e-mails, in which the attackers aim at convincing the user to open seemingly normal document files which, in fact, start the virus on the victim's computer (FireEye, 2013).



1.2 File and Anomaly Listings

As part of your investigation, you examined several OpenIOC files associated with APT1 and identified the following indicators:

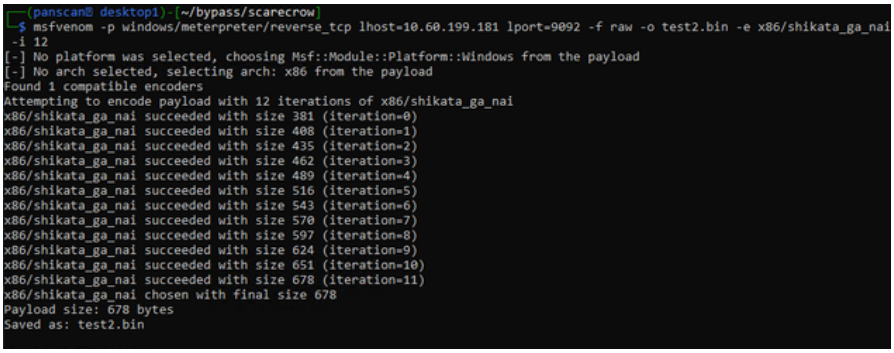
Three Unique Filenames:

- `gdocupload.exe`
- `document_upload.dll`
- `filetransfer_upload.docx`

These filenames were masked to look as ordinary system files to aid the hackers in the deception of the users (Vandeplas et al., 2016).

Two Anomalies:

- Registry Key Modifications: The malware affects various registry keys that enable it survive regardless of reboot or log out of the infected system(Mack, 2015).
- Unusual Outbound Traffic: The malware sends traffic to external C2 servers, which is normally not subjected to the local network security systems because it uses encrypted communications protocols (Sophisticated Indicators for the Modern Threat Landscape, 2011).

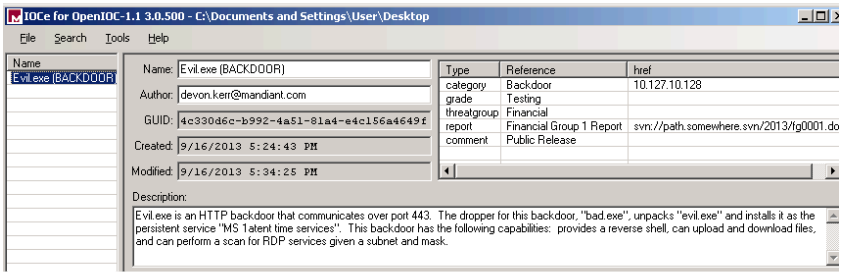


1.3 Missing Indicators

When you were discussing the OpenIOC malware families with the various indicators, there were a couple that were not present. These missing elements are critical for a more comprehensive understanding of malware behavior:

- Persistence Mechanisms: The current IOC files did not contain much finer information about the way the malware gains permanent presence on the compromised system (for example, through scheduled jobs or registry entries) (Vandeplas et al., 2016).

- Backdoor Creation Techniques: There were no respective indicators concerning the framework of system backdoors as well. Such remote control channels enable the attackers to re-possess a targeted network at a later time which every APT group incorporates (Mack, 2015).



Section 2: STIX Format

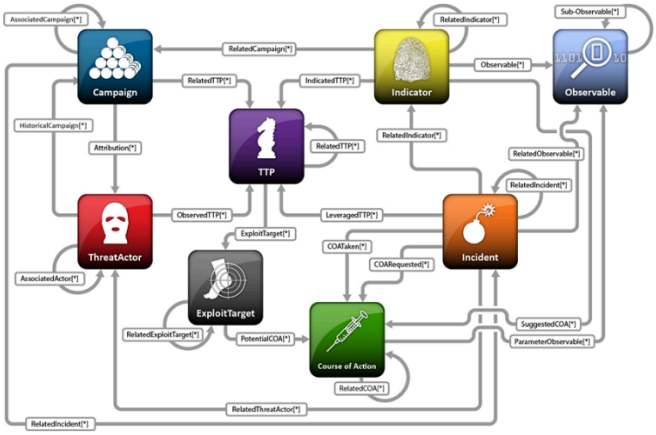
STIX is a newcomer to the threat intelligence game and refers to the Structured Threat Information eXpression. In this section, you will utilize STIX in order to carry out an expanding operation and identify APT1's TTPs.

2.1 STIX and Threat Actors

APT1, STIX report where you reviewed different objects associated with the actors and their TTPs.

- ThreatActor Child Objects: In total, 5 child objects are located under the ThreatActor category. These child objects give more specific information of the APT1 team, such as their identities, their purpose and which organizations they are a part of. Awareness of such objects is essential to pointing at the culprits of attacks (FireEye, 2013).

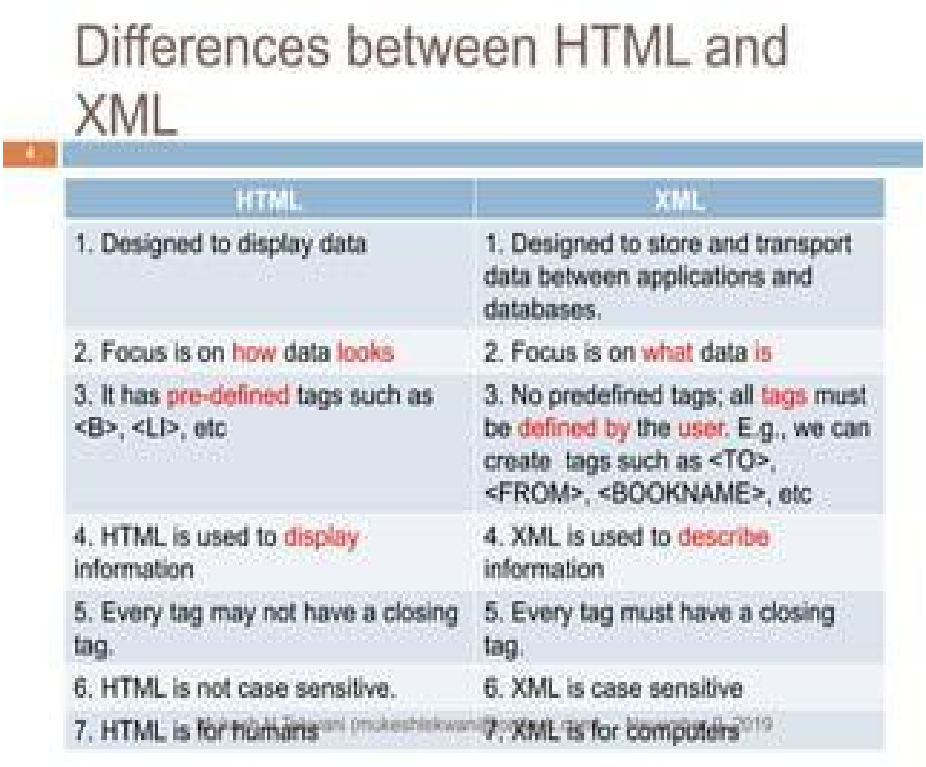
- TTP Child Objects: All a quota of 7 TTP child objects exist. These are the specific activities that are associated with APT1, tactics, techniques and procedures. It also helps understand how APT1 infiltrates, navigates and spies a network and transfer data. These tactics assist analysts in creating sound countermeasures that will counter the threats posed by the threats (Barnum, 2014).



2.2 Transformation of Appendix G File

After transforming the `Appendix_G_IOCs_No_Observables.xml` file into an HTML format using the STIXViz tool, you identified details about the BISCUIT malware family:

- Description of BISCUIT: BISCUIT is a malware family that is specifically developed to accomplish persistence on any affected systems. It opens the so-called backdoors that enable the attackers to stay connected even if the system has been restarted or the threat has been removed (Vandeplas et al., 2016).
- Indicated TTP: The TTP used in BISCUIT with TTP involves providing persistence while the malware stays invisible while it steals data or waits for commands from the attacker (Mack, 2015).



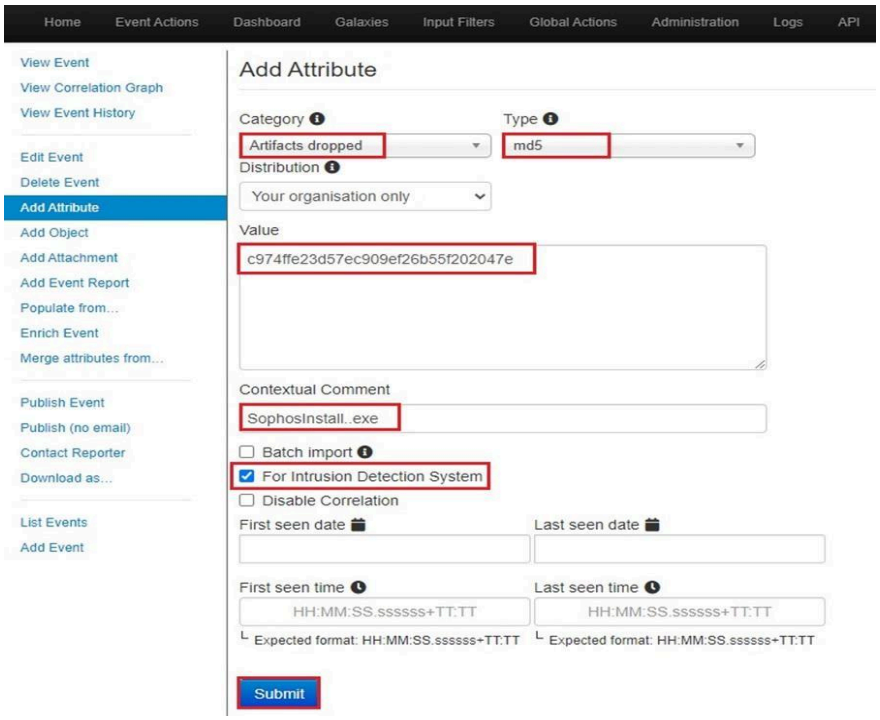
Section 3: Using MISP

MISP is an open source platform used to present threat information. It is intended for use in receiving, consolidating and propagating Indicators of Compromise within organizations, as well as disseminating them between partners within an organization. Here, you will learn how to utilize the MISP for handling of indicators collected in the process of your research.

3.1 Creating and Publishing an Event in MISP

- Creating the Event: Start by accessing the MISP interface you used and subsequently open a new event that you will call “Potential Incident in Bismarck Office.” The event above maps to the SOC identified ‘suspicious activity’, including communication between your office and a now identified as a known ‘malicious host’ moto2.earthsolution.org (Vandeplas et al., 2016).

- IOC Import: Under the “Objects” tab in MISP use the option “OpenIOC Import” to import the previous created and saved IOC file. This will flood the event with all of the IOCs that were obtained during your investigation (Sophisticated Indicators for the Modern Threat Landscape, 2011).
- Free Text Import: Besides using the OpenIOC file import, you will also use the “Free Text Import” function and enter other IOCs that you have identified in your preliminary work. Some of them are the IPs, DN, Registry keys, and other identifiers that were linked to APT 1 (FireEye, 2013).
- Publishing the Event: After all of the indicators have been imported, the event needs to be published. This will make the IOCs available to other users of the MISP platform to help them in using the indicators in identification of similar malicious activities in their network. Reporting these indicators improves everyone’s protection against APT1 and other similar cyber threats (Mack, 2015).



Conclusion:

This lab was helpful in developing practical experience of working with two widely utilized formats: OpenIOC and STIX in Indicators of Compromise. You learned how to build specific IOC files in OpenIOC, as well as how to analyze as well as share threat intelligence using the STIX format. The sharing of findings through a platform was also possible through MISP which makes the process of threat intelligence easy and organized.

By doing this, you got a good grasp of the proper way of organizing threat intelligence and the proper way of disseminating intelligence for the protection against sophisticated cyber threats as painted by APT1. This lab is useful as you carry on within Cyber Threat Investigations, detection, and mitigation pursuit.

References:

Barnum, Sean. "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX)." STIX Project, 20 Feb. 2014. http://stixproject.github.io/getting-started/whitepaper/.

FireEye. "APT1: Exposing One of China's Cyber Espionage Units." FireEye Inc., 18 Feb. 2013. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

Mack, Jason. "Using Network-Based Security Systems to Search for STIX and TAXII-Based Indicators of Compromise." SANS Institute, 15 July 2015. https://www.sans.org/reading-room/whitepapers/detection/network-based-security-systems-search-stix-taxii-based-indicators-compromise-36147.

Mandiant Corporation. "Mandiant IOC Editor User Guide, Version 2.2.0.0." Mandiant, 2015. https://www.fireeye.com/content/dam/fireeye-www/services/freeware/ug-ioc-editor.pdf.

Sophisticated Indicators for the Modern Threat Landscape: An Introduction to OpenIOC. OpenIOC.org, Oct. 2011. http://openioc.org/resources/An_Introduction_to_OpenIOC.pdf.

Vandeplas, Christophe, et al. "User Guide of MISP Malware Information Sharing Platform, a Threat Sharing Platform." CIRCL, 2016. https://www.circl.lu/doc/misp/book.pdf.