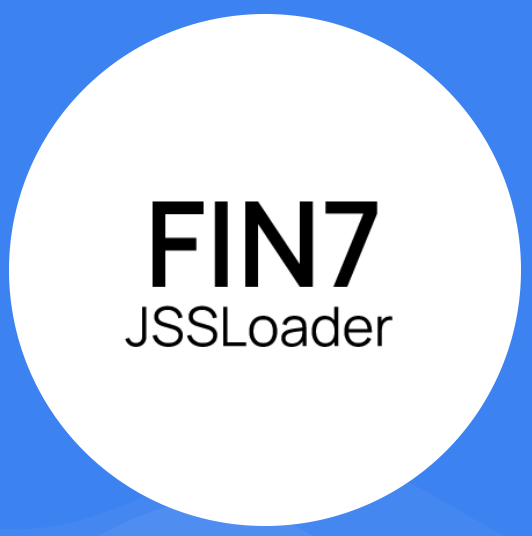
Detecting XLL files used for dropping FIN7 JSSLoader with Wazuh



May 24th 2022 I by Chris Bassey I Wazuh 4.3

JSSLoader is a remote access trojan by the Russian FIN7 hacking group. There has been an increase in the number of JSSLoader infections this year. These infections have been utilizing Microsoft Excel add-in files (XLL files) to drop the JSSLoader trojan to victim machines.

In this blog post, we use Wazuh to detect when an XLL file is used as a dropper for the JSSLoader trojan on a Windows endpoint. It is important to detect this dropper activity so we can respond to the JSSLoader infection before it takes root.

XLL dropper behavior

The recent infection chain leverages email to deliver the XLL file. Once the file is downloaded and opened, the malicious code in the file is loaded and executed by Excel. Then the following behavior is observed:

- **Execution of unsigned binaries:** An Excel popup appears, which asks the user if the add-in should be executed because it's unsigned. In the logs of the infected machine, we see this activity as an image loaded by Excel with its signed status as false.

Related **content**

Detecting malicious URLs using Wazuh and URLhaus
October 31, 2024

Ransomware protection on Windows with Wazuh
October 17, 2024

How to configure Rsyslog client to send events to Wazuh
August 15, 2024

Integrating Imperva cloud web application firewall (CWAF) with Wazuh
July 31, 2024

Use **cases**

Log Data Analysis

```
Company: Govert van Drimmelen
OriginalFileName: ExcelDna.xll
Hashes: SHA1=6B8F41B0BD35C0C4E6972A2C6B9D4ABEBF0861E9,MD5=8728DF136AF405
Signed: false
```

- **DNS query for a malicious domain**: From the execution logs, we see a DNS query for physiciansofficenews[.]com by Excel to retrieve the JSSLoader trojan. Other domains identified as being used for delivery of the trojan include thechinastyle[.]com and divorceradio[.]com.

```
UtcTime: 2022-04-05 07:58:50.837
ProcessGuid: {ef5984a4-f69d-624b-dd04-000000000500}
ProcessId: 4976
QueryName: physiciansofficenews[.]com
QueryStatus: 0
QueryResults: ::ffff:209[.]99[.]64[.]51;
Image: C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
```

- **Creation and execution of an executable temporary file with DNA prefix**: The XLL file downloads a `.tmp` file with the DNA prefix in the `%TEMP%` directory of the user, then executes this temporary file. The `.tmp` file downloaded is the JSSLoader trojan.

```
Image: C:\Users\chris\AppData\Local\Temp\DNAxxx.tmp
CommandLine: C:\Users\chris\AppData\Local\Temp\DNAxxx.tmp
CurrentDirectory: C:\Users\chris\Documents\
User: DESKTOP-PQKPK46\chris
LogonGuid: {ef5984a4-0f92-624c-8023-030000000000}
LogonId: 0x32380
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=CE2AA4C6A7A2235C3C9F7233933DD7CD9DD44D09,MD5=22616070ACE3C7
ParentProcessGuid: {ef5984a4-2de5-624c-1402-000000000700}
ParentProcessId: 6820
ParentImage: C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
```

The use of the `.tmp` extension is to bypass malware scanners and monitoring tools that may be looking for the creation of executable files (.exe, .bin, etc.) but not temporary files. The temporary file created can still be executed and is just a way of masquerading.

Detection with Wazuh

Wazuh provides rules for threat and anomaly detection. We can extend some of these base rules to improve coverage for malicious behavior by FIN7 XLL dropper files.

Requirements

- An installed Wazuh manager.

- Download Sysmon from the Microsoft Sysinternals page.
- Download the Sysmon configuration file.
- Launch the CMD as an administrator and install Sysmon using the command below:

```
Sysmon64.exe -accepteula -i sysconfig.xml
```

- Edit the `ossec.conf` file to specify the location to collect Sysmon logs:

```
<localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
```

- Restart the Wazuh agent for changes to apply.

On the Wazuh manager

We proceed to create rules to detect the identified XLL dropper file behaviors by adding the following rules in our `local_rules.xml` file.

- **Execution of unsigned binaries:** For execution of unsigned binaries, we create rules to detect when Excel loads an add-in as it is a popular source for running malicious files. Then we detect if the add-in loaded is unsigned.

```
<group name="malware_detection,fin7,">
  <rule id="100002" level="0">
    <if_sid>61609</if_sid>
    <field name="win.eventdata.image" type="pcre2">(?i)excel.exe</field>
    <description>Application $(win.eventdata.imageLoaded) loaded by excel
    <mitre>
      <id>T1204</id>
      <id>T1137</id>
    </mitre>
  </rule>

  <rule id="100003" level="3">
    <if_sid>100002</if_sid>
    <field name="win.eventdata.imageLoaded" type="pcre2">(?i)(.xll|.xla|.
    <description>Add-in $(win.eventdata.originalFileName) loaded by excel
    <mitre>
      <id>T1137</id>
      <id>T1137.001</id>
    </mitre>
  </rule>

  <rule id="100004" level="7">
    <if_sid>100003</if_sid>
    <field name="win.eventdata.signed" type="pcre2">^false$</field>
    <description>Unsigned add-in $(win.eventdata.originalFileName) loadec
    <mitre>
      <id>T1204</id>
      <id>T1204.002</id>
      <id>T1137</id>
```

- **DNS query for a malicious domain:** Here, we create rules to detect when Excel makes a DNS query for a known JSSLoader distributor domain.

```
<group name="malware_detection,fin7,">
  <rule id="100005" level="0">
    <if_sid>61600</if_sid>
    <field name="win.eventdata.image" type="pcre2">(?i)excel.exe</field>
    <field name="win.system.eventID" type="pcre2">^22$</field>
    <description>Excel made a network request.</description>
  </rule>

  <rule id="100006" level="15">
    <if_sid>100005</if_sid>
    <field name="win.eventdata.queryName" type="pcre2">(?i)(physiciansoff
    <description>Excel made a network request to JSSLoader dropper domair
    <mitre>
      <id>T1105</id>
    </mitre>
  </rule>
</group>
```

- **Creation and execution of an executable temporary file with DNA prefix:** For this behavior, we create rules to detect when a `.tmp` file is loaded for execution. We also create rules to detect if the file loaded has a DNA prefix which is an indicator that it is a FIN7 JSSLoader file.

```
<group name="malware_detection,fin7,">
  <rule id="100007" level="0">
    <if_sid>61603</if_sid>
    <field name="win.eventdata.parentImage" type="pcre2">(?i)excel.exe</f
    <description>$(win.eventdata.image) Process launched by excel.</descr
    <mitre>
      <id>T1059</id>
    </mitre>
  </rule>

  <rule id="100008" level="7">
    <if_sid>100007</if_sid>
    <field name="win.eventdata.image" type="pcre2">(?i).tmp</field>
    <description>$(win.eventdata.image) executable masquerading as a TMP
    <mitre>
      <id>T1036</id>
      <id>T1059</id>
      <id>T1059.005</id>
    </mitre>
  </rule>

  <rule id="100009" level="15">
    <if_sid>100008</if_sid>
    <field name="win.eventdata.image" type="pcre2">(?i)DNA</field>
    <description>$(win.eventdata.image) executable masquerading as a .TMF
    <mitre>
      <id>T1036</id>
      <id>T1059</id>
      <id>T1059.005</id>
    </mitre>
  </rule>
</group>
```

Upon execution of the malicious XLL dropper file on an endpoint that is enrolled to Wazuh, we see that the rules created detect the malicious behavior and generate alerts.

Security Alerts

Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Apr 6, 2022 @ 16:27:07.576	T1036 T1059 T1059.005	Defense Evasion, Execution	C:\\Users\\chris\\AppData\\Local\\Temp\\DNAxxx.tmp executable masquerading as a .TMP file launched by excel. DNA prefix is typically associated with FIN7 JSSLoader.	15	100009
Apr 6, 2022 @ 16:27:07.516	T1105	Command and Control, Lateral Movement	Excel made a network request to JSSLoader dropper domains.	15	100006
Apr 6, 2022 @ 16:26:31.393			Service startup type was changed	3	61104
Apr 6, 2022 @ 16:25:27.362	T1204 T1204.002 T1137 T1137.001	Execution, Persistence	Unsigned add-in ExcelDna.xll loaded by excel.exe. Possible malicious activity.	7	100004

Conclusion

In this article, we successfully created rules to detect when a malicious XLL dropper file is being used to download and execute the FIN7 JSSLoader RAT. It is also possible for Wazuh to detect and remove a malicious file like the XLL dropper before it is executed by a user. We illustrate this in our proof of concept guide where we check the hash of a downloaded file in Virustotal and then perform an active response on the file if it is malicious.

References

- New JSSLoader Trojan Delivered through XLL Files.