JSSLoader: Recoded and Reloaded

proofpoint.com/us/blog/threat-insight/jssloader-recoded-and-reloaded

June 23, 2021

Blog
Threat Insight
JSSLoader: Recoded and Reloaded

June 24, 2021 Dennis Schwarz, Matthew Mesa and Crista Giering

Key Takeaways

- After a months-long absence, the malware loader JSSLoader returned in June 2021 campaigns rewritten from the .NET programming language to C++.
- Rewriting the malware could be an effort by threat actors to evade current detections.
- Current TA543 campaigns delivering JSSLoader are using similar lures to those observed by Proofpoint researchers in 2019 and the emails continue to contain links to a TDS landing page.

Overview

In June 2021, Proofpoint researchers observed a new variant of the downloader JSSLoader in several campaigns impacting a variety of organizations. This version of the malware loader was rewritten from .NET to the C++ programming language. This change, while not unheard of, is not a common occurrence and could be an effort by the threat actors utilizing JSSLoader to evade current detections. JSSLoader is often dropped in the first or second stage of a campaign and has the functionality to profile infected machines and load additional payloads.

The campaigns are ongoing and use similar lures to those initially observed by Proofpoint researchers in 2019. According to our data, the recent campaigns have attempted to target as many as several hundred organizations at a time across a wide range of industries, including finance, manufacturing, technology, retail, healthcare, education, and transportation.

Malware Analysis

Proofpoint researchers initially observed JSSLoader in September 2019. It was written in .NET at the time and being actively developed. Fast forward nearly two years and Proofpoint has now identified this latest variant of the malware loader written in C++. It has much of the same functionality as previous iterations. The following provides a more in-depth look at that early version and the changes the loader has undergone since 2019.

2019 Version of JSSLoader (.NET)

JSSLoader is an initial access malware that was written in .NET and was named after its “JSS” namespace and “jssAdmin” command and control (C&C) panel login page:

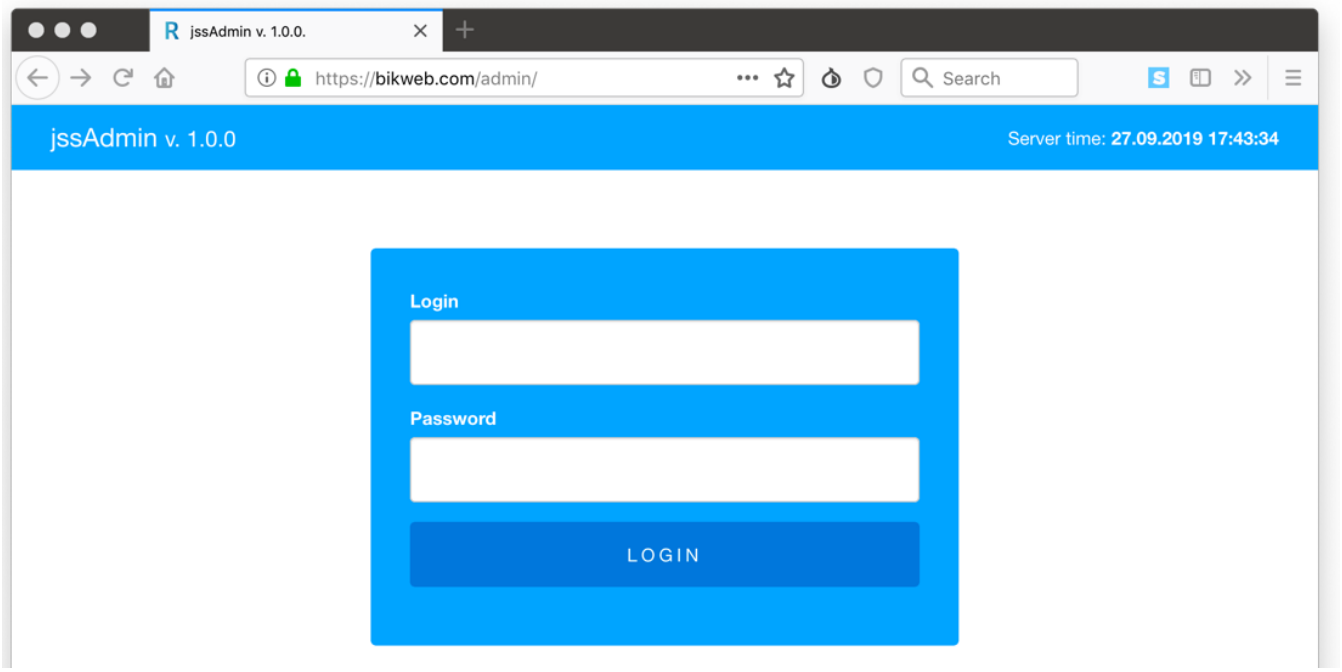


Figure 1. JSSLoader C&C panel login page from September 27, 2019 version.

Its C&C used HTTPS requests with base64-encoded data:

Figure 2. Example C&C request from September 27, 2019 version.

The initial C&C beacon contained verbose system information:

```
0x01. Host information report
=============================================================

HOST: '[redacted]'  DOMAIN: '[redacted]'  USER: '[redacted]'
LOGICAL DRIVES: 'C:\; D:\'
=============================================================

System info
-------------------------------------------------------------

Host Name:                 [redacted]
OS Name:                   Microsoft Windows 7 Ultimate
...
=============================================================

Network info
-------------------------------------------------------------

Windows IP Configuration
...
=============================================================

Process list
-------------------------------------------------------------
   300   conhost
   ...
=============================================================

Desctop file list
-------------------------------------------------------------
     2,014   C:\Users\Public\Desktop\Adobe Reader 9.lnk
     ...
=============================================================

ADInfo
-------------------------------------------------------------
adinformation***no_ad
part_of_domain***yes
pc_domain***[redacted]
pc_dns_host_name***[redacted]
pc_model***[redacted]

=============================================================

End of report
```

Figure 3. Example system information (trimmed for readability) from September 27, 2019 version.

Its commands and functionality focused on executing a next stage executable or JavaScript:

```
switch (theTask.Code)
{
case TaskCode.TASK_FORM:
    AppTask.Execute_TaskForm(theTask.Data, ref result);
    break;
case TaskCode.TASK_JS:
    AppTask.Execute_TaskJS(theTask.Data, ref result);
    break;
case TaskCode.TASK_EXE:
    AppTask.Execute_TaskExe(theTask.Data, theTask.Options, ref result);
    break;
case TaskCode.TASK_UPDATE:
    AppTask.Execute_TaskUpdate(theTask.Data, ref result);
    break;
case TaskCode.TASK_UNINST:
    AppTask.Execute_TaskUninstall(theTask.Data, ref result);
    break;
}
```

Figure 4. Commands from September 27, 2019 version.

2020-2021 JSSLoader Changes (.NET)

Since the initial version of JSSLoader, there have been gradual changes and improvements to the malware in successive campaigns. Morphisec wrote about some of these in a January 2021 paper titled "Threat Profile the Evolution of the FIN7 JSSLoader (PDF)." Two of the most visible changes were a switch from the verbose system information to a JSON object and the addition of new commands. For example, the JSSLoader used in a December 14, 2020 email-based campaign sent the following system information:

```
{
    "domain": "[redacted]",
    "processes": [
        {
            "pid": "1536",
            "name": "svchost.exe"
        },
        ...
    ],
    "system_info": "",
    "logical drives": "",
    "adinfo": {
        "adinformation": "no_ad",
        "pc_domain": "[redacted]",
        "part_of_domain": "yes",
        "pc_dns_host_name": "[redacted]",
        "pc_model": "[redacted]"
    },
    "host": "[redacted]",
    "user": "[redacted]",
    "network_info": "",
    "desktop_file_list": [
        {
            "file": "C:\\Users\\[redacted]\\Desktop\\desktop.ini",
            "size": "282"
        },
        ...
    ]
}
```


Figure 5. Example system information (formatted and trimmed for readability) from December 14, 2020 version.

While the formatting changed, the beacon contained much of the same information as the original version. In addition to the changes in the C&C protocol, several new commands were added. The focus of the new commands was still on executing a next stage:

```
case CommandCd.Cmd_FORM:
    AppCmd.Execute_CmdForm(theCmd.Data, ref result);
    break;
case CommandCd.Cmd_JS:
    AppCmd.FuncEJS1(theCmd.Data, ref result, false);
    break;
case CommandCd.Cmd_EXE:
    AppCmd.FuncECE1(theCmd.Data, theCmd.Options, ref result);
    break;
case CommandCd.Cmd_UPDATE:
    AppCmd.FuncEUP1(theCmd.Data, ref result);
    break;
case CommandCd.Cmd_UNINST:
    AppCmd.FuncEU1(AppCmd.GetME(), theCmd.Data, ref result);
    break;
case CommandCd.Cmd_RAT:
    AppCmd.FuncER1(theCmd.Data, ref result);
    break;
case CommandCd.Cmd_PWS:
    AppCmd.FuncEPWS1(theCmd.Data, ref result);
    break;
case CommandCd.Cmd_VBS:
    AppCmd.FuncEJS1(theCmd.Data, ref result, true);
    break;
case CommandCd.Cmd_RunDll:
    AppCmd.FuncDll1(theCmd.Data, theCmd.Options, ref result);
    break;
case CommandCd.Cmd_Info:
    AppCmd.SendReport(AppInfo.GAI1());
```

Figure 6. Commands from December 14, 2020 version.

After this December 2020 campaign, activity paused and the malware went through a redevelopment phase, according to Proofpoint's visibility.

June 2021 JSSLoader (C++)

In June 2021, email campaigns resumed, but the JSSLoader malware had been redeveloped from using the .NET programming language to C++ (this change was also noticed on infosec Twitter). It is not common for a malware to be redeveloped in a different programming language, but it does happen occasionally. Proofpoint

recently documented another initial access malware known as “Buer Loader” that was redeveloped from the C programming language to Rust. As noted in that blog post, rewriting a malware can enable threat actors to better evade existing detection capabilities.

The C++ version of JSSLoader analyzed here is from a June 8, 2021 email-based campaign. It sets up “registry run” persistence using a value name of “AppJSSLoader” and has similar style of system information beacon as the later .NET versions:


```
{
    "processes": [
        {
            "pid": "4",
            "name": "System"
        },
        ...
    ],
    "desktop_file_list": [
        {
            "file": "desktop.ini",
            "size": "282"
        },
        ...
    ],
    "domain": "[redacted]",
    "adinfo": {
        "adinformation": "[redacted]",
        "pc_domain": "",
        "part_of_domain": "yes",
        "pc_dns_host_name": "",
        "pc_model": ""
    },
    "host": "[redacted]",
    "user": "[redacted]"
}
```


Figure 7. Example system information (formatted and trimmed for readability) from June 8, 2021 C++ version.

The C++ version also has similar command functionality, though they switched from the “Cmd” prefix of the later .NET versions back to the “Task” prefix seen in the earlier .NET samples:

```
if ( command_num == 2 )
{
  v3 = operator new(4u);
  *v3 = &CTaskRunJS::`vftable';
  *command_class = v3;
  return command_class;
}
else if ( command_num == 3 )
{
  v4 = operator new(4u);
  *v4 = &CTaskRunExe::`vftable';
  *command_class = v4;
  return command_class;
}
else if ( command_num == 4 )
{
  v5 = operator new(4u);
  *v5 = &CTaskUpdate::`vftable';
  *command_class = v5;
  return command_class;
}
else if ( command_num == 5 )
{
  v6 = operator new(4u);
  *v6 = &CTaskDelete::`vftable';
  *command_class = v6;
  return command_class;
}
else if ( command_num == 6 )
{
  v7 = operator new(4u);
  *v7 = &CTaskRunPS::`vftable';
  *command_class = v7;
  return command_class;
}
else if ( command_num == 7 )
{
  v8 = operator new(4u);
  *v8 = 0;
  *v8 = &CTaskRunSimplePS::`vftable';
  *command_class = v8;
  return command_class;
}
else if ( command_num == 8 )
{
  v9 = operator new(4u);
  *v9 = &CTaskRunVBS::`vftable';
  *command_class = v9;
  return command_class;
}
else
{
  if ( command_num == 9 )
  {
    v10 = operator new(4u);
    *v10 = &CTaskRunDLL::`vftable';
    *command_class = v10;
  }
```

Figure 8. Commands from June 8, 2021 C++ version.

C&C protocol and command similarity was likely a choice to remain backwards compatible with the existing .NET version's C&C panel software.

Campaign Details

JSSLoader appears to be exclusive to several threat actors. In fact, Proofpoint has only observed two actors using it since the first email campaign in 2019.

Most of the campaigns were attributed to the threat actor tracked by Proofpoint as TA543. They are characterized by their widespread distribution with opportunistic targeting. A typical campaign contains thousands of email messages and targets several hundred organizations. The lures used by TA543 typically focus on invoices and delivery information of packages.

The following sections describe and compare the original campaigns observed by Proofpoint in 2019 to the June 2021 campaigns.

September 2019 Campaign Example

On September 27, 2019 Proofpoint analysts observed a TA543 campaign spoofing Intuit branding. The threat actor used a likely compromised account for an email marketing service to send the malicious emails that purported to be invoices and contained URLs linking to a landing page hosting BlackTDS. The TDS would direct the user to the download another file, a VBS downloader, hosted on SharePoint. The VBS downloader would then download JSSLoader.

During our analysis of JSSLoader, it additionally loaded a Griffon payload which is historically associated with another actor, TA3546, also known as FIN7 or Carbanak. In the following months Proofpoint analysts observed TA543 shift to primarily delivering JSSLoader and/or other loaders that were often observed downloading other TA3546-associated payloads.

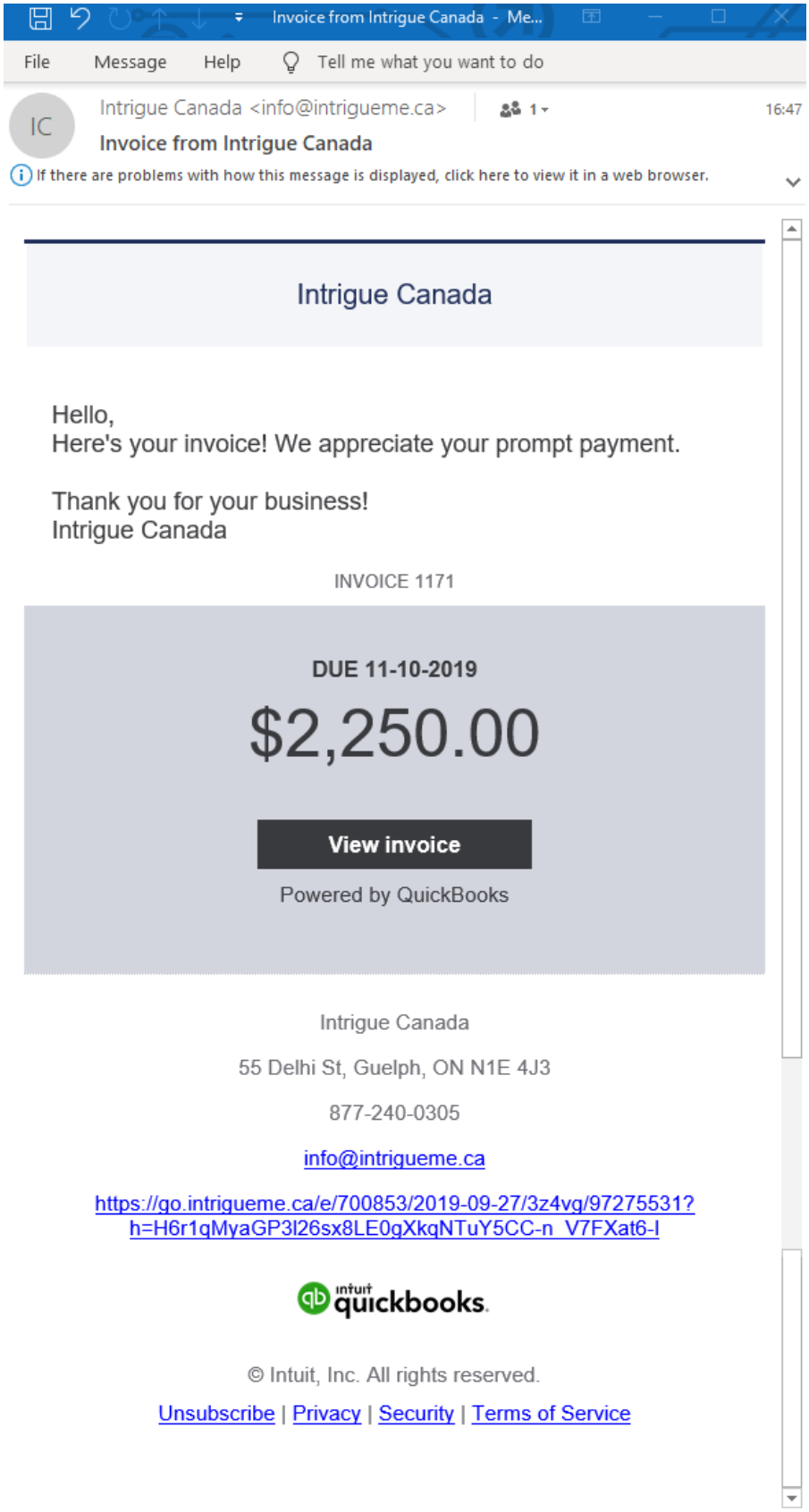
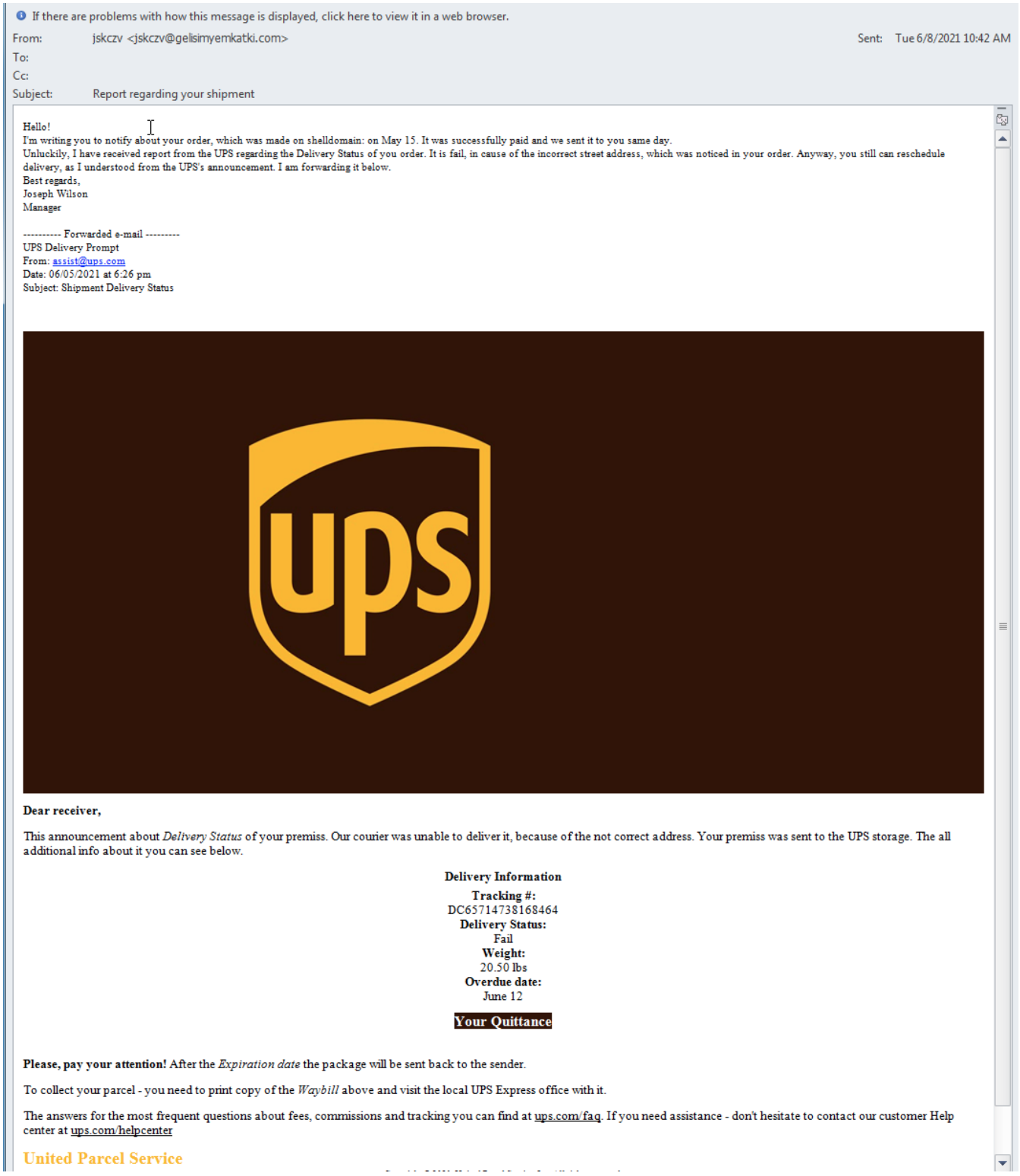


Figure 9. TA543 email that leads to the download of JSSLoader.

June 2021 Campaign Example

On June 8, 2021, Proofpoint analysts observed a TA543 campaign spoofing UPS branding (Figure 10). The email contained URLs linking to a Keitaro TDS landing. In turn, the landing linked to the download of a Windows Scripting File (WSF) hosted on SharePoint. If executed, it downloaded an intermediate script, which then downloaded and executed the C++ version of JSSLoader.



If there are problems with how this message is displayed, click here to view it in a web browser.

From: jskczv <jskczv@gelisimyemkatki.com> Sent: Tue 6/8/2021 10:42 AM
To:
Cc:
Subject: Report regarding your shipment

Hello!
I'm writing you to notify about your order, which was made on shelldomain: on May 15. It was successfully paid and we sent it to you same day.
Unluckily, I have received report from the UPS regarding the Delivery Status of you order. It is fail, in cause of the incorrect street address, which was noticed in your order. Anyway, you still can reschedule delivery, as I understood from the UPS's announcement. I am forwarding it below.
Best regards,
Joseph Wilson
Manager

---------- Forwarded e-mail ---------
UPS Delivery Prompt
From: assist@ups.com
Date: 06/05/2021 at 6:26 pm
Subject: Shipment Delivery Status

Dear receiver,

This announcement about *Delivery Status* of your premiss. Our courier was unable to deliver it, because of the not correct address. Your premiss was sent to the UPS storage. The all additional info about it you can see below.

Delivery Information
Tracking #:
DC65714738168464
Delivery Status:
Fail
Weight:
20.50 lbs
Overdue date:
June 12

Your Quittance

Please, pay your attention! After the *Expiration date* the package will be sent back to the sender.

To collect your parcel - you need to print copy of the *Waybill* above and visit the local UPS Express office with it.

The answers for the most frequent questions about fees, commissions and tracking you can find at ups.com/faq. If you need assistance - don't hesitate to contact our customer Help center at ups.com/helpcenter

United Parcel Service

Figure 10. TA543 email sample from June 8, 2021, that leads to the download of JSSLoader.

Conclusion

The threat actors behind JSSLoader have continuously made modifications since its debut in 2019 and are likely to continue doing so using the 2021 variant. With the redevelopment of the malware into C++, which was possibly done to evade current detections and make analysis more difficult, Proofpoint researchers have not seen the .NET version in play. Instead, researchers anticipate seeing small refinements being made to the 2021 version in future campaigns, keeping in line with the evolution of the .NET version over the past two years.

Indicators of Compromise

Indicator	Type	Notes
dd86898c784342fc11c42bea4c815cb536455ee709e7522fb64622d9171c465d	SHA256	September 27, 2019 JSSLoader Sample
bikweb\.com	Hostname	September 27, 2019 JSSLoader C&C
a062a71a6268af048e474c80133f84494d06a34573c491725599fe62b25be044	SHA256	December 14, 2020 JSSLoader sample
monusorge\.com	Hostname	December 14, 2020 JSSLoader C&C
7a17ef218eebfdd4d3e70add616adcd5b78105becd6616c88b79b261d1a78fdf	SHA256	June 8, 2021 JSSLoader Sample
injuryless\.com	Hostname	June 8, 2021 JSSLoader C&C

ET Signatures

2033072 - ET TROJAN FIN7 JSSLoader Variant Activity (POST)

2033074 - ET TROJAN FIN7 JSSLoader Variant Activity (GET)

2838606 - ETPRO TROJAN Win32/jssLoader CnC Activity

2838607 - ETPRO TROJAN Win32/jssLoader CnC Checkin

2842028 - ETPRO TROJAN JSSLoader CnC Host Checkin

Subscribe to the Proofpoint Blog