بسمه تعالی

عنوان مستند

تحلیل و بررسی بدافزار "Wapomi"

فهرست مطالب

۱ معرفی بدافزار

Wapomi ویروسی است که رفتاری تروجان مانند دارد. این ویروس در اصل سالها پیش کشف شد، اما هنوز نیز فعال است و به حیات خود ادامه داده است. در این گزارش نگاهی به بعضی از عملکردهای آن شده است تا ماهیت آن کمی روشن شود.

این بدافزار پس از اجرا، دارای قابلیت تکثیر خود و آلوده کردن فایل ها و برنامه های دیگر است. این ویروس می تواند فضای هارد و حافظه را اشغال نموده و باعث کند شدن یا متوقف شدن سیستم شود. همچنین می تواند باعث حذف یا خرابی داده ها، پاک کردن دیسک سخت، سرقت اطلاعات شخصی کاربر شود. این ویروس در system32 رایانه می نشیند و به اکثر فایلهای اجرایی حمله و آنها را حذف می کند. این بدافزار همچنین توانایی خاتمه دادن به محصولات آنتی ویروس، مخفی کردن فایل ها، فرایندها و ورودی های رجیستری خود را دارد. این بدافزار به اینترنت برای دانلود اجزاء و قطعات خود متصل می شود.

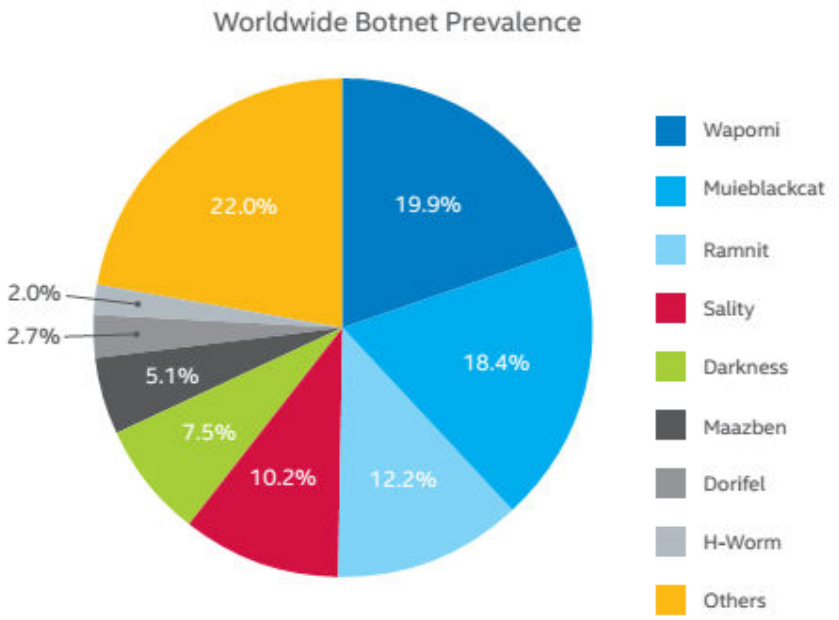
پس از آلودگی، این ویروس یک کپی از خود در سیستم ایجاد و تنظیمات سیستم را تغییر می دهد به طوری که در هر بار شروع ویندوز اجرا می شود.

W32.wapomi ممکن است برخی از علائم زیر را نمایش دهد:

- ممکن است کاربر احساس کند کسی در حال کنترل سیستم است.
- تنظیمات سیستم ممکن است تغییر کند.
- فایلها ممکن است در رجیستری ظاهر، ناپدید و تغییر کنند.
- ممکن است سرعت کامپیوتر را به طور چشمگیری کاهش دهد.

۲ آمار آلودگی

طبق گزارش تهدیدات آزمایشگاه مکافی در August سال ۲۰۱۵ ، گسترش این ویروس ۱۹,۹ درصد در سراسر جهان بوده است.



۳ مشخصات فایل تحلیل شده

مشخصات فایل تحلیل شده بدین شرح است:

File name: f56536e29f17a960a8e6081582a8232db61531ba.exe

Type: Portable Executable 32

MD5: 07738194E8634FE5EB01E65135583B76

SHA-1: F56536E29F17A960A8E6081582A8232DB61531BA

۴ روشهای انتشار بدافزار

نمونه های Wapmi از طریق آلودگی فایل و یا درایورهای قابل جابجایی انتشار می یابند. این ویروس با پیوست کردن خود به یک فایل با پسوند ".exe" گسترش می یابد.

فایل آلوده پوشه زیر را در دستگاه های قابل جابجایی ایجاد می کند:

- recycle.{CLSID}

و یک کپی از خودش را در آن قرار می دهد:

- recycle.{CLSID}\uninstall.exe

و یک فایل AUTORUN.INF برای اجرای خودکار کپی خود، به پوشه اضافه می کند. فایل INF. شامل رشته های زیر است:

```
[autorun]
OPEN=recycle.{CLSID}\uninstall.exe
shell\open=´ò¿ª(&O)
shell\open\Command=recycle.{CLSID}\uninstall.exe Show
shell\open\Default=1
shell\explore=×ÊÔ´¹ÜÀíÆ÷(&X)
shell\explore\Command=recycle.{CLSID}\uninstall.exe Show
```

```
add     esp, 0Ch
push    104h            ; Size
push    0               ; Val
lea     eax, [ebp+PathName]
push    eax             ; Dst
call    memset
add     esp, 0Ch
push    offset byte_4120A4
push    [ebp+arg_0]
push    offset aSS_1    ; "%s%s"
lea     eax, [ebp+PathName]
push    eax             ; LPSTR
call    ds:wsprintfA
add     esp, 10h
push    104h            ; Size
push    0               ; Val
lea     eax, [ebp+FileName]
push    eax             ; Dst
call    memset
add     esp, 0Ch
push    offset aUninstall_exe ; "uninstall.exe"
lea     eax, [ebp+PathName]
push    eax
push    offset aSS_0    ; "%s\\%s"
lea     eax, [ebp+FileName]
push    eax             ; LPSTR
call    ds:wsprintfA
add     esp, 10h
push    800h            ; Size
push    0               ; Val
lea     eax, [ebp+String1]
push    eax             ; Dst
call    memset
add     esp, 0Ch
push    offset aShow    ; "Show"
push    offset aUninstall_exe ; "uninstall.exe"
push    offset byte_4120A4
push    offset aShow    ; "Show"
push    offset aUninstall_exe ; "uninstall.exe"
push    offset byte_4120A4
push    offset aUninstall_exe ; "uninstall.exe"
push    offset byte_4120A4
push    offset aX@6p    ; "$++X@6P-"
lea     eax, [ebp+String1]
push    eax             ; LPSTR
call    ds:wsprintfA
```

۵ روشهای شناسایی و پاکسازی

۱- برای انجام اسکن کامل سیستم، قبل از اسکن System Restore را غیر فعال کنید.

۲- فایلهای زیر را جستجو از سیستم حذف کنید:

- C:\Windows\System32\dmlocalsvc.dll
- C:\Windows\System32\{random}.sys

۳- کلید رجیستری زیر را حذف کنید:

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\08151f4a.exe

۴- سیستم را جستجو و پوشه زیر را حذف کنید:

- {drive leter}:\recycle.{CLSID}

۵- سیستم را جستجو و فایلهای زیر را حذف کنید:

C:\Windows\System32\49AE0164.tmp

- C:\Users\Infotmp.txt
- C:\Document and Setting\Infotmp.txt

۶- سیستم را جستجو و فایل AUTORUN.INF ساخته شده توسط ویروس wapomi را حذف کنید.

این فایل شامل رشته های زیر می باشد:

- [autorun]
- OPEN=recycle.{CLSID}\uninstall.exe
- shell\open=´ò¿ª(&O)

- shell\open\Command=recycle.{CLSID}\uninstall.exe Show
- shell\open\Default=1
- shell\explore=×ÊÔ´¹ÜÀíÆ÷(&X)
- shell\explore\Command=recycle.{CLSID}\uninstall.exe Show

۷- سیستم را توسط یکی از محصولات آنتی ویروس اسکن کنید.

۸- فایلهای زیر را از backup ویندوز به سیستم برگردانید.

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network

- C:\Windows\System32 \drivers\etc\hosts

- C:\Windows\System32 \appmgmts.dll
- C:\Windows\System32 qmgr.dll
- C:\Windows\System32 \shsvcs.dll
- C:\Windows\System32 \mspmsnsv.dll
- C:\Windows\System32 \xmlprov.dll
- C:\Windows\System32 \es.dll
- C:\Windows\System32 \ntmssvc.dll
- C:\Windows\System32 \upnphost.dll
- C:\Windows\System32 \ssdpsrv.dll
- C:\Windows\System32 \netman.dll
- C:\Windows\System32 \mswsock.dll
- C:\Windows\System32 \tapisrv.dll
- C:\Windows\System32 \browser.dll
- C:\Windows\System32 \cryptsvc.dll
- C:\Windows\System32 pchsvc.dll
- C:\Windows\System32 regsvc.dll
- C:\Windows\System32 schedsvc.dll

۶ سطح تهدید فایل تحلیل شده

نتیجه بررسی فایل تحلیل شده با استفاده از تارنمای Virustotal.com در جدول ذیل ارایه شده است. همانطور که مشاهده می‌شود از بین ۵۱ موتور تشخیص بدافزار ۴۴ عدد این فایل را به عنوان بدافزار وغالباً تحت عنوان بدافزار wapomi تشخیص داده‌اند.

Antivirus	Result	Update
AVware	Virus.Win32.Otwycal.ab (v)	20150901
Ad-Aware	Win32.VJadtre.3	20150909
Agnitum	Win32.Otwycal.Gen.2	20150908
AhnLab-V3	Win32/Wampori	20150908
Antiy-AVL	Virus/Win32.Otwycal.a	20150909
Arcabit	Win32.VJadtre.3	20150909
Avast	Win32:Evo-gen [Susp]	20150909
Avira	W32/Jadtre.A	20150909
Baidu-International	Virus.Win32.Otwycal.$a	20150909
BitDefender	Win32.VJadtre.3	20150909
Bkav	HW32.Packed.9AD8	20150908
CAT-QuickHeal	W32.Otwyacal.C	20150908
CMC	Virus.Win32.Otwycal.1!O	20150908
ClamAV	W32.Virus.Wapomi-1	20150909
Comodo	Virus.Win32.Wapomi.AA	20150909
Cyren	W32/Injector.A.gen!Eldorado	20150909
DrWeb	Win32.HLLP.Protil.1	20150909

ESET-NOD32	Win32/Wapomi.AA	20150909
Emsisoft	Win32.VJadtre.3 (B)	20150909
F-Secure	Win32.VJadtre.3	20150909
Fortinet	W32/Agent.R!tr	20150909
GData	Win32.VJadtre.3	20150909
Ikarus	Backdoor.Win32.Agent	20150909
Jiangmin	Win32/Protil.e	20150907
K7AntiVirus	Virus (002401471)	20150909
K7GW	Virus (002401471)	20150909
Kaspersky	Virus.Win32.Otwycal.a	20150909
Kingsoft	Win32.Otwycal.xp.112128	20150909
McAfee	W32/Simfect	20150909
McAfee-GW-Edition	BehavesLike.Win32.Fujacks.dc	20150908
MicroWorld-eScan	Win32.VJadtre.3	20150909
Microsoft	Virus:Win32/Mikcer.A	20150909
NANO-Antivirus	Virus.Win32.Otwycal.dszex	20150908
Panda	Generic Suspicious	20150909
Qihoo-360	HEUR/Malware.QVM19.Gen	20150909
Sophos	W32/Patched-AG	20150909
Symantec	W32.Wapomi.C!inf	20150908
Tencent	Virus.Win32.Dropper.a	20150909
TrendMicro-HouseCall	PE_WAPOMI.SM	20150909
VBA32	Virus.Otwycal.a	20150909
VIPRE	Virus.Win32.Otwycal.ab (v)	20150908
ViRobot	Win32.Otwycal.A[h]	20150909
Zoner	Win32.Wapomi.A	20150909
nProtect	Win32.VJadtre.3	20150909

۷ گزارش تحلیل

۷-۱ تحلیل بدافزار Wapomi

در ابتدا وقتی فایل آلوده (یا ویروس) اجرا می شود، جزء اصلی بدافزار آزاد و اجرا می شود. این جزء فرایند تزریق به سایرین را به عهده دارد.

بدافزار Wapomi فایل اجرایی 08151f4a.exe را به سیستم اضافه میکند. پس از اجرا Wapomi بدنه بدافزار را تجزیه می کند تا بدنبال executable image بگردد که برای فایل رهاکننده استفاده خواهد شد. ابتدا MZ header را جستجو می کند. تصویر فایل اجرایی به هیچ شکلی رمزگذاری یا کدگذاری نشده است و صرفا یک تصویر ساده جاسازی شده است.

بدافزار سپس تصویر اجرایی را بوسیله تابع WriteFileدر فایلی در مسیر '%System Root%\08151f4a.exe' می نویسد و آن فایل را با CloseHandle می بندد. در نهایت Wapomi فایل اضافه شده را با WinExec فعال می کند.

۷-۲ تحلیل فایل اضافه شده (08151f4a.exe)

فایل رهاشده ('%System Root%\08151f4a.exe') تمام قابلیت های بدخواه را که بدافزار لازم دارد را در خود دارد که بوسیله ابزار فشرده سازی ASPack بسته بندی شده است.

بعد از بازشدن، چندین گام از روال آماده سازی خود را انجام می دهد که شامل بدست آوردن نام پوشه temp٪، نام پوشه %system% و نام ماژول است. این کارها را به ترتیب توسط APIهای زیر انجام می‌دهد: GetTempPathA, GetSystemDirectoryA , GetModuleFileNameA.

این فایل اضافه شده توسط wapomi فایلهای با پسوند exe. و فایلهای rar. شامل فایلهای exe. را آلوده می‌کند، این فایل بعد از اجرا خودش را حذف می کند.

۷-۲-۱ عملکرد فایل اضافه شده توسط بدافزار wapomi

۷-۲-۱-۱ ایجاد یک کپی با پسوند tmp

فایل اضافه شده یک کپی از خودش با پسوند tmp در مسیر زیر ایجاد می کند:

C:\Windows\System32\49AE0164.tmp

```
004026FE
004026FE loc_4026FE:
004026FE call    sub_40246E
00402703 and     eax, 0FFFF0000h
00402708 mov     ecx, dword_414D40
0040270E and     ecx, 0FFFFh
00402714 or      eax, ecx
00402716 push    eax
00402717 push    offset a_8x_tmp ; "%.8X.tmp"
0040271C push    offset byte_414D20 ; LPSTR
00402721 call    ds:wsprintfA
00402727 add     esp, 0Ch
0040272A mov     VersionInformation.dwOSVersionInfoSize, 9Ch
00402734 push    offset VersionInformation ; lpVersionInformation
00402739 call    ds:GetVersionExA
0040273F call    sub_40246E
00402744 push    eax
00402745 push    offset byte_414960
0040274A push    offset aS_8x_log ; "%s%.8X.log"
0040274F push    offset byte_414D44 ; LPSTR
00402754 call    ds:wsprintfA
0040275A add     esp, 10h
0040275D push    0               ; lpOverlapped
0040275F lea     eax, [ebp+NumberOfBytesRead]
00402762 push    eax             ; lpNumberOfBytesWritten
00402763 push    2D4h            ; nNumberOfBytesToWrite
00402768 push    offset VersionInformation ; lpBuffer
0040276D push    [ebp+hFile]     ; hFile
00402773 call    ds:WriteFile
00402779 push    [ebp+hFile]     ; hObject
0040277F call    ds:CloseHandle
00402785 jmp     loc_40284D
```

۷-۲-۱-۲ اضافه کردن فایلهای DLL و SYS

فایل اضافه شده توسط wapomi در بخش Resource خود دو فایل دارد. این فایلها یک فایل dll و یک فایل sys می باشند.

```
00402F1D mov     ebp, esp
00402F1F sub     esp, 14h
00402F22 mov     [ebp+var_8], 1
00402F29 and     [ebp+lpBuffer], 0
00402F2D and     [ebp+hResInfo], 0
00402F31 and     [ebp+Src], 0
00402F35 and     [ebp+Size], 0
00402F39 push    offset Type     ; "FILE"
00402F3E movzx   eax, [ebp+arg_8]
00402F42 push    eax             ; lpName
00402F43 push    [ebp+hModule]   ; hModule
00402F46 call    ds:FindResourceA
00402F4C mov     [ebp+hResInfo], eax
00402F4F push    [ebp+hResInfo]  ; hResInfo
00402F52 push    [ebp+hModule]   ; hModule
00402F55 call    ds:SizeofResource
00402F5B mov     [ebp+Size], eax
00402F5E push    [ebp+hResInfo]  ; hResInfo
00402F61 push    [ebp+hModule]   ; hModule
00402F64 call    ds:LoadResource
00402F6A mov     [ebp+Src], eax
00402F6D push    [ebp+Src]       ; uNumber
00402F70 call    ds:SetHandleCount
00402F76 push    40h             ; flProtect
00402F78 push    3000h           ; flAllocationType
00402F7D push    [ebp+Size]      ; dwSize
00402F80 push    0               ; lpAddress
00402F82 call    ds:VirtualAlloc
00402F88 mov     [ebp+lpBuffer], eax
00402F8B push    [ebp+Size]      ; Size
00402F8E push    [ebp+Src]       ; Src
00402F91 push    [ebp+lpBuffer]  ; Dst
00402F94 call    memcpy
00402F99 add     esp, 0Ch
00402F9C push    [ebp+Src]       ; hResData
00402F9F call    ds:FreeResource
00402FA5 mov     eax, [ebp+lpBuffer]
3,493) 00002F46 00402F46: sub_402F1C+2A
```

زمانی که فایل اضافه شده اجرا می شود فایلهای Dll و Sys توسط apiهای FindResourceA وLoadResourceA از قسمت Resource لود و در سیستم کپی می شوند. این دو فایل در مسیر های زیر ایجاد می شوند.

- %System%\dmlocalsvc.dll
- %System%\{random}.sys

(%System% معمولا C:\Windows\System32 می باشد)

این بدافزار برای دانلود فایلهای مخرب از فایل DLL و برای پنهان کردن حضور خود از فایل SYS استفاده می کند.

۳-۱-۲-۷ اجرای بدافزار در هربار شروع ویندوز

این فایل مخرب اضافه شده توسط wapomi، ورودی های رجیستری زیر را برای اجرا در هربار شروع ویندوز ایجاد می کند.

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[random]\"ImagePath" = "%SystemRoot%\[random].sys"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[random]\"Start" = "3"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[random]\"Type" = "1"

۴-۱-۲-۷ خاتمه دادن به فرایندهای در حال اجرا

این فایل آلوده اگر فرآیندهای زیر را در حال اجرا در حافظه سیستم پیدا کند به آنها پایان می دهد:

- 360tray.exe
- Explorer.exe
- KSafeTray.exe
- MPMon.exe
- MPSVC.exe
- MPSVC1.exe
- MPSVC2.exe
- RavMonD.exe
- RsAgent.exe

همچنین این فایل آلوده با ایجاد مدخل زیر در رجیستری، از اجرای چندین فرآیند مرتبط امنیتی جلوگیری می کند:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options نام فایل.exe\"Debugger" = "ntsd -d"

فرآیندهایی که توسط این رجیستری غیر فعال می شوند شامل:

360hotfix.exe	avgnt.exe	kmailmon.exe	McSACore.exe	safeboxTray.exe
360rp.exe	avguard.exe	kpfw32.exe	Mcshield.exe	ScanFrm.exe
360rpt.exe	avmailc.exe	kpfwsvc.exe	mcsysmon.exe	sched.exe
360safe.exe	avp.exe	krnl360svc.exe	mcvsshld.exe	seccenter.exe
360safebox.exe	avshadow.exe	ksmgui.e	MpfSrv.exe	SfCtlCom.exe
360sd.exe	avwebgrd.exe	ksmsvc.exe	MPMon.exe	spideragent.exe
360se.exe	bdagent.exe	kswebshield.exe	MPSVC.exe	SpIDerMl.exe
360SoftMgrSvc.exe	CCenter.exe	KVMonXP.kxp	MPSVC1.exe	spidernt.exe
360speedld.exe	ccSvcHst.exe	KVSrvXP.exe	MPSVC2.exe	spiderui.exe
360tray.exe	dwengine.exe	kwatch.exe	msksrver.exe	TMBMSRV.exe
afwServ.exe	egui.exe	livesrv.exe	qutmserv.exe	TmProxy.exe
ast.exe	ekrn.exe	Mcagent.exe	RavMonD.exe	Twister.exe
AvastUI.exe	FilMsg.exe	mcmscsvc.exe	RavTask.exe	UfSeAgnt.exe

avcenter.exe	kavstart.exe	McNASvc.exe	RsAgent.exe	
avfwsvc.exe	kissvc.exe	Mcods.exe	rsnetsvr.exe	
zhudongfangyu.exe	vsserv.exe	McProxy.exe	RsTray.exe	

۷-۲-۱-۵ تغییر تنظیمات safe mode

فایل اضافه شده توسط بدافزار، برای تغییر تنظیمات safe mode زیرکلیدهای رجیستری زیر را حذف می کند:

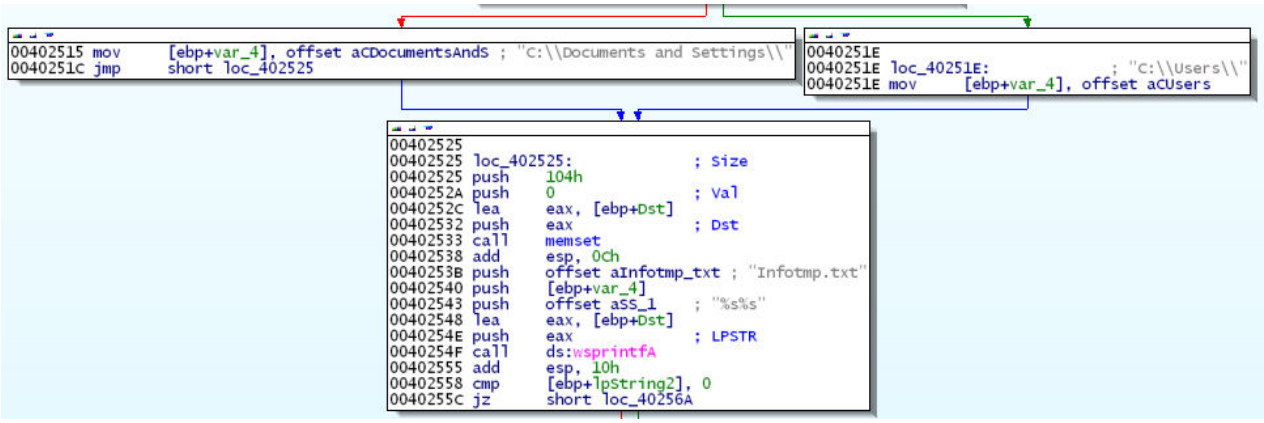
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal

```
00403788 pszSubKey= byte ptr -620h
00403788 var_220= byte ptr -220h
00403788 var_114= dword ptr -114h
00403788 FileName= byte ptr -110h
00403788 lDistanceToMove= dword ptr -8
00403788 BytesReturned= dword ptr -4
00403788
00403788 push    ebp
00403789 mov     ebp, esp
0040378B sub     esp, 0A38h
00403791 and     [ebp+lDistanceToMove], 0
00403795 and     [ebp+var_114], 0
0040379C and     [ebp+BytesReturned], 0
004037A0 push    offset aMinimal ; "Minimal"
004037A5 push    offset aSafeboot ; "SafeBoot"
004037AA push    offset aControl ; "Control"
004037AF push    off_412CFC
004037B5 push    offset aSSSS    ; "%s\\%s\\%s\\%s"
004037BA lea     eax, [ebp+pszSubKey]
004037C0 push    eax             ; LPSTR
004037C1 call    ds:wsprintfA
004037C7 add     esp, 18h
004037CA lea     eax, [ebp+pszSubKey]
004037D0 push    eax             ; pszSubKey
004037D1 push    80000002h       ; hkey
004037D6 call    ds:SHDeleteKeyA
004037DC push    offset aNetwork ; "Network"
004037E1 push    offset aSafeboot ; "SafeBoot"
004037E6 push    offset aControl ; "Control"
004037EB push    off_412CFC
004037F1 push    offset aSSSS    ; "%s\\%s\\%s\\%s"
004037F6 lea     eax, [ebp+pszSubKey]
004037FC push    eax             ; LPSTR
004037FD call    ds:wsprintfA
00403803 add     esp, 18h
00403806 lea     eax, [ebp+pszSubKey]
0040380C push    eax             ; pszSubKey
```

۷-۲-۱-۶ روتین keylogging

همچنین این فایل اضافه شده توسط بدافزار، فایل Infotmp.txt را برای انجام روتین keylogging و جمع آوری اطلاعات از سیستم در یکی از مسیر های زیر ایجاد می‌کند:

- %System Root%\Users\Infotmp.txt
- %System Root%\Document and Setting\Infotmp.txt



پس از اجرای بدافزار محتوی این فایل به صورت زیر است:

œ ± Service Pack 1

C:\08151f4a.exe
0930B0AA0.tmp

C:\Users\maryam\AppData\Local\Temp\093B1216.log

۷-۱-۲-۷ تغییر فایل HOSTS

فایل HOSTS مرجع اولیه ویندوز برای Name Resolution می باشد که در مسیر زیر قرار دارد:

- %windir%\system32\drivers\etc\hosts

این فایل آلوده فایل های HOSTS سیستم را برای تغییر مسیر ترافیک شبکه بازنویسی می کند:

- 127.0.0.1 localhost

```
push    ebp
mov     ebp, esp
sub     esp, 118h
mov     [ebp+lpBuffer], offset a127_0_0_1Local ; "127.0.0.1       localhost\r\n"
and     [ebp+NumberOfBytesWritten], 0
or      [ebp+hObject], 0FFFFFFFFh
mov     eax, ds:SetFileAttributesA
mov     [ebp+var_10], eax
push    104h            ; Size
push    0               ; Val
lea     eax, [ebp+Dst]
push    eax             ; Dst
call    memset
add     esp, 0Ch
push    offset dword_414A70
push    offset aSDriversEtcHos ; "%s\\drivers\\etc\\hosts"
lea     eax, [ebp+Dst]
push    eax             ; LPSTR
call    ds:wsprintfA
add     esp, 0Ch
push    80h
lea     eax, [ebp+Dst]
push    eax
call    [ebp+var_10]
push    0               ; hTemplateFile
push    80h             ; dwFlagsAndAttributes
push    3               ; dwCreationDisposition
push    0               ; lpSecurityAttributes
push    3               ; dwShareMode
push    0C0000000h      ; dwDesiredAccess
lea     eax, [ebp+Dst]
push    eax             ; lpFileName
call    ds:CreateFileA
mov     [ebp+hObject], eax
push    0               ; lpOverlapped
lea     eax, [ebp+NumberOfBytesWritten]
push    eax             ; lpNumberOfBytesWritten
push    [ebp+lpBuffer]  ; lpString
call    ds:lstrlenA
push    eax             ; nNumberOfBytesToWrite
push    [ebp+lpBuffer]  ; lpBuffer
push    [ebp+hObject]   ; hFile
call    ds:WriteFile
push    [ebp+hObject]   ; hFile
call    ds:SetEndOfFile
```

۷-۲-۱-۸ اتصال به اینترنت

این فایل آلوده برای بررسی اتصال به اینترنت به آدرس زیر متصل می شود:

- www.baidu.com

```
                        ; CODE XREF: sub_409F63+63↓j
push    offset name     ; "www.baidu.com"
call    ds:gethostbyname
test    eax, eax
jnz     short loc_409FC8
cmp     [ebp+arg_0], 0FFFFFFFFh
jz      short loc_409FBB
call    ds:GetTickCount
sub     eax, [ebp+var_194]
cmp     eax, [ebp+arg_0]
jb      short loc_409FBB
xor     eax, eax
jmp     short locret_409FD1
```

۸ جمع بندی

Wapomi به دلیل عملکرد رهاکردن فایل معمولا به عنوان یک Trojan و یا Worm تشخیص داده می شود.

تحلیل های انجام شده نشان می دهد که این ویروس:

- فایلهای آلوده و ورودی های رجیستری را به سیستم تزریق می کند.
- تنظیمات safe mode را تغییر می دهد.
- ویروس های دیگر را توسط باز کردن درهای پشتی در سیستم آلوده نصب می کند.
- اطلاعات شخصی و سیستمی را جمع آوری می کند.
- با دانلودهایی که از اینترنت انجام میدهد به سیستم کاربر حمله می کند.
- سرعت و عملکرد سیستم را به طور چشمگیری کاهش می دهد.