# تحلیل بدافزار AAEH و ارائه راهکارهای مقابله با آن

## معرفی بدافزار

بدافزار AAEH یکی از شایع‌ترین بدافزارهای فعلی در دنیا است. AAEH در واقع خانواده‌ای از دانلودرهای چندریختی است که هدف اصلی آن‌ها، بارگذاری و نصب سایر بدافزارها (مانند بدافزارهای سرقت کلمه عبور، روتکیت‌ها، آنتی‌ویروس‌های تقلبی و باج‌افزارها) بر روی سیستم‌های قربانی است.

معمولاً این بدافزار از طریق اشتراک‌های شبکه، ابزارهای قابل جابه‌جایی (مانند USB و CD) و از طریق فایل‌های ZIP و RAR منتقل می‌شوند. این خانواده بدافزار با نام Vobfus نیز شناخته می‌شوند. این بدافزار این قابلیت را دارد که به ازای هر آلودگی ساختار خود را نیز تغییر دهد تا تشخیص توسط نرم‌افزارهای ضد بدافزار را دشوار سازد. تعداد نمونه‌های متفاوتی که تا کنون از این بدافزار شناسایی شده‌اند از مرز ۲ میلیون نیز گذشته است.

این بدافزار تاکنون برای نصب بدافزارهای دیگری همچون Zeus، Cryptolocker، ZeroAccess و Cutwail مورد استفاده قرار گرفته است.

## نحوه شناسایی سیستم‌های آلوده از طریق لاگ‌های شبکه

تمامی سیستم‌هایی که نام‌های دامنه زیر را Resolve کرده باشند، آلوده هستند:

- dns0q.net
- ns1.helpupdated.com
- ns1.helpupdated.net
- ns1.helpupdated.org
- ns1.helpupdatek.at
- ns1.helpupdatek.eu
- ns1.helpupdatek.tw
- ns1.helupdates.com

- ns1.helpupdater.net

## نحوه بررسی وجود آلودگی ماشین‌ها

۱. وجود کلید زیر در رجیستری ویندوز (برای اجرای فایلی با نام تصادفی از مسیر Documents And Settings\Username):

\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

۲. وجود فایلی با نام تصادفی در مسیر Documents And Settings\Username

## نحوه پاک‌سازی سیستم

۱. حذف کلید زیر از رجیستری ویندوز:

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/svcname

۲. حذف تمامی فایل‌های اجرایی با نام‌های تصادفی از مسیر Documents And Settings\username

## نحوه بررسی پاک بودن سیستم

۱. نبود کلید زیر در رجیستری ویندوز:

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/svcname

۲. نبود فایل اجرایی با نام تصادفی در مسیر Documents And Settings\Username

## توصیه‌های امنیتی برای پیشگیری

۱. خودداری از اجرای فایل‌های ناشناس (کرک‌های ارایه شده برای نرم‌افزارها توسط تیم‌های ناشناس، فایل‌های دریافتی از اشخاص ناشناس، فایل‌های الحاق شده به ایمیل‌های ناشناس و ...)

۲. به‌روز بودن نرم‌افزار ضدبدافزار نصب شده بر روی سیستم

۳. عدم اتصال فلش و سی‌دی‌های نا آشنا به سیستم

۴. مسدودسازی دسترسی به نام‌های دامنه ذکرشده

## مشخصات فایل تحلیل شده

فایل تحلیل شده، یک فایل اجرایی ویندوز با مشخصات زیر است:

| | |
|---|---|
| MD5 | 4f51a3c9d6f31927593ec931f7e60053 |
| SHA1 | f0aa4cee2fdf5f8ce3a7ec631a232f5a86afe078 |
| SHA256 | 430d1450c027e197c46c302e7156be733d9673ff90d62fe2d3f6a9c15ed49b94 |
| File Size | 86016 bytes |
| File Type | Win32 EXE |
| Magic Literal | PE32 executable for MS Windows (GUI) Intel 80386 32-bit |
| Compiler | Microsoft Visual Basic 6 |
| Encrypted or packed | Not Packed |

## شرح تحلیل

فایل تحلیل شده به زبان Visual Basic نوشته شده که فرآیند تحلیل را با دشواری‌های زیادی مواجهه می‌سازد. علت اصلی این امر، مستند نبودن فرآیندهای داخلی زبان Visual Basic است که کار تحلیل‌گر را بسیار دشوار می‌سازد. بررسی‌های اولیه نشان داد که این فایل احتمالاً توسط یک Packer سفارشی مبهم‌سازی شده است. شکل زیر بخشی از نقاط ورودی فایل تحلیل شده را به نمایش می‌گذارد که بیانگر توسعه بدافزار با استفاده از زبان Visual Basic است.

| Address | Ordinal | Name | Library |
|---|---|---|---|
| 00401000 | | __vbaVarSub | MSVBVM60 |
| 00401004 | | _CIcos | MSVBVM60 |
| 00401008 | | _adj_fptan | MSVBVM60 |
| 0040100C | | __vbaVarMove | MSVBVM60 |
| 00401010 | | __vbaStrI4 | MSVBVM60 |
| 00401014 | | __vbaVarVargNofree | MSVBVM60 |
| 00401018 | | __vbaFreeVar | MSVBVM60 |
| 0040101C | | __vbaCyMul | MSVBVM60 |
| 00401020 | | __vbaAryMove | MSVBVM60 |
| 00401024 | | __vbaLenBstr | MSVBVM60 |
| 00401028 | | __vbaStrVarMove | MSVBVM60 |
| 0040102C | | __vbaEnd | MSVBVM60 |
| 00401030 | | __vbaFreeVarList | MSVBVM60 |
| 00401034 | | _adj_fdiv_m64 | MSVBVM60 |

این فایل یک Downloader می‌باشد که به زبان VB نوشته شده است. این بدافزار در دو مرحله اجرا می‌شود که در مرحله اول فایل اجرایی وظیفه خواندن کدهای قسمت اصلی، رمزگشایی و ایجاد یک Process/Thread برای اجرای آن را دارد. برای اجرای قسمت اصلی از روش code injection استفاده می‌شود.

قسمت دوم پس از اجرا، بعد از بررسی محیط و اطمینان از اینکه در محیط مجازی یا توسط دیباگر اجرا نمی‌شود، سعی در اتصال به سرور خود و دانلود فایل (به احتمال زیاد بدافزارهایی مانند تروجان و ....) می‌کند.

## تحلیل فاز اول اجرا

در این فاز، تنها کد فاز دوم از درون فایل خوانده شده به وسیله یک کلید که در این مورد dulk809838 است، رمزگشایی می‌شود و در نهایت پس از تصحیح سرآیند Image جدید، یک Thread برای آن ایجاد شده و فاز دوم اجرا می‌شود. هدف طراحی فرم‌ها و کنترل‌های زیاد در این فاز مشخص نیست اما می‌تواند آن را به یک حامل قابل استفاده مجدد برای دیگر بدافزارها تبدیل کند. برای مثال کلید رمزگشایی به راحتی می‌تواند درون یک textbox قرار گیرد و طراح نسخه‌های مختلفی را برای مقابله با شناسایی ایجاد کند (تنها

با تغییر این کلید و رمزکردن فاز دوم بر اساس آن). این فاز برای code injection فاز دوم درون یک thread جدید از API های زیر کمک می‌گیرد.

- CreateProcessW(kernel32.dll)
- NtUnmapViewOfSection(ntdll.dll)
- NtAllocatrVirtualMemory(ntdll.dll)
- NtWriteVirtualMemory(ntdll.dll)
- NtGetThreadContext
- NtSetThreadContext
- NtResumeThread

این توابع به طور مستقیم در Import Table بدافزار وجود ندارند و هنگام نیاز آدرس dll مورد نیاز محاسبه و تابع مورد نظر درون آن پیدا و صدا زده می‌شود. کد فاز دوم از بایت ۳۶۳۲۸ به بعد فایل dropper موجود است (به‌صورت رمز شده).

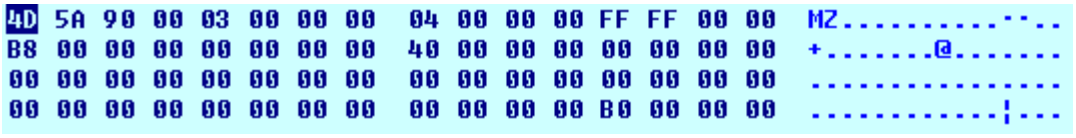
شکل زیر بخش اول فرآیند Code Injection را نشان می‌دهد. در این بخش، یک پروسه جدید از روی همان فایل اصلی بدافزار توسط بدافزار ایجاد می‌شود. این پروسه در حالت Suspended ساخته می‌شود تا مانع از اجرای همان کد Unpacker توسط این پروسه شود.

```
kernel32_CreateProcessW proc near

arg_0= dword ptr  8
arg_4= dword ptr  0Ch
arg_8= dword ptr  10h
arg_C= dword ptr  14h
arg_10= dword ptr  18h
arg_14= dword ptr  1Ch
arg_18= dword ptr  20h
arg_1C= dword ptr  24h
arg_20= dword ptr  28h
arg_24= dword ptr  2Ch

mov     edi, edi
push    ebp
mov     ebp, esp
push    0
push    [ebp+arg_24]
push    [ebp+arg_20]
push    [ebp+arg_1C]
```

در گام بعدی، بدافزار با استفاده از تابع سطح پایین NtWriteVirtualMemory از فایل ntdll.dll تمامی بخش کد را در فضای حافظه پروسه‌ی جدیدی که ایجاد کرده است، بازنویسی می‌کند. بدین صورت بدفزار در واقع یک پروسه با کدی کاملاً مجزا از کد فایل اصلی بدافزار ایجاد نموده است. شکل زیر استفاده از تابع NtWriteVirtualMemory توسط بدافزار که برای بازنویسی مجدد کد پروسه تولید شده مورد استفاده قرار می‌گیرد را نشان می‌دهد.

```
ntdll_NtWriteVirtualMemory proc near
mov     eax, 115h
mov     edx, offset off_7FFE0300
call    dword ptr [edx]
retn    14h
ntdll_NtWriteVirtualMemory endp
```

همچنین شکل زیر بخش اولیه بافری که قرار است در فضای حافظه پروسه تولید شده نوشته شود را نشان می‌دهد. همان‌طور که مشاهده می‌شود، این بافر با حروف MZ شروع می‌شود که نشانگر سرآیند فایل‌های اجرایی ویندوز است.




## تحلیل فاز دوم اجرا

این قسمت هم به‌وسیله زبان VB تولید شده اما به‌صورت P-Code کامپایل شده است. این امر تحلیل آن را سخت‌تر می‌کند.

پس از اینکه این قسمت شروع به اجرا می‌کند، از طریق آدرس رجیستری زیر بررسی می‌کند که آیا درون یک Virtual Machine اجرا شده است یا خیر:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\disk\Enum

در آدرس بالا، بدافزار به دنبال رشته‌هایی می‌گردد که حاوی موارد زیر باشد:

- VIRTUAL
- VMWARE
- VBOX
- QEMU

برای مقابله با عملیات debugging، این بدافزار از یک روش نادر و تابع CsrGetProcessId استفاده می‌کند. این تابع PID پروسه csrss.exe را برمی‌گرداند. در صورتی که یک پروسه در حالت debug باشد، می‌تواند پروسه csrss.exe را بوسیله OpenProcess باز کند. یعنی اگر OpenProcess روی این PID مقدار صفر برنگرداند، یعنی پروسه در حالت debug است. از تابع CsrGetProcessId می‌توان برای شناسایی VMware هم استفاده کرد که چیزی در این بدافزار در این مورد یافت نشد.

در صورتی که بدافزار اطمینان حاصل کند که در حال تست یا در محیط مجازی نیست، سعی می‌کند از طریق HTTPS/SSL به دامنه زیر متصل شود:

dns0q.net

همچنین نمونه‌های دیگر تحلیل شده نیز سعی در برقراری ارتباط با دامنه‌های زیر داشتند:

ns1.helpupdated.com
ns1.helpupdated.net
ns1.helpupdated.org
ns1.helpupdatek.at
ns1.helpupdatek.eu
ns1.helpupdatek.tw
ns1.helupdates.com
ns1.helpupdater.net

آدرس دقیق به دلیل سختی دنبال کردن کد در حالت P-Code پیدا نشد اما آدرس کامل احتمالی می‌تواند به‌صورت زیر باشد:

Snxhk.dns0q.net

در این مورد اجرا و مانیتور کردن بدافزار (تحلیل زمان اجرا)، آدرس دقیق را به راحتی مشخص می‌کند.

عملیات مربوط به پروتکل HTTP به وسیله کامپوننت Microsoft Internet Control انجام می‌شود که پیاده‌سازی آن در ieframe.dll واقع است. به بیانی دیگر بدافزار از اینترنت اکسپلورر برای ارتباط با آدرس بالا استفاده می‌کند. عملیات دانلود در صورت ناموفق بودن هر یک دقیقه انجام می‌شود (از یک Timer در GUI بدافزار استفاده شده است).

پس از تکمیل دانلود ، فایل را با نام runme.exe ذخیره و اجرا می‌کند. نمی‌توان اطلاعاتی در مورد فایلی که دانلود می‌شود بدون بررسی آدرسی که بدافزار به آن متصل می‌شود به‌دست آورد.

شواهدی در کد وجود دارد که بدافزار اطلاعاتی نظیر حجم پارتیشن‌ها و اسم User را به‌دست می‌آورد، اما استفاده دقیق آن در آنالیز استاتیک به طور واضح مشخص نشد. از دیگر موارد موجود، استفاده بدافزار از VBScript برای انجام بعضی عملیات‌های دیگر است.

در نهایت بدافزار برای اطمنیان از اجرای خود پس از راه‌اندازی مجدد سیستم، یک نسخه از فایل اجرایی خود را با یک نام تصادفی در مسیر Documents And Settings\Username کپی نموده و سپس با افزودن کلید زیر در رجیستری، فایل تولید شده را در لیست برنامه‌هایی که پس از بوت سیستم اجرا می‌شوند قرار می‌دهد:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

همان‌طور که اشاره شد، در کل این بدافزار تنها یک دانلودر بوده و غیر از دانلود و اجرای فایل سایر بدافزارها عملکرد خاص دیگری ندارد. از آن‌جا که در طی عملیاتی در سال ۲۰۱۴ تمامی کارگزارهای کنترل و فرمان این بدافزار توسط مراجع قانونی از کار افتاده‌اند، این بدافزار در حال حاضر قادر به دانلود هیچ بدافزار دیگری نیست و تهدید خاصی برای سیستم‌های آلوده به‌شمار نمی‌رود.