

Một số phương pháp trích xuất malicious AutoIT script

1. Sơ lược về AutoIT

AutoIt là một ngôn ngữ kịch bản miễn phí được thiết kế nhằm tự động hóa các nhu cầu cơ bản của người dùng cũng như các tác vụ liên quan tới GUI Windows. AutoIt thường rất nhỏ và có khả năng thực thi trên tất cả các hệ điều hành Windows mà không đòi hỏi các thư viện "runtimes" như các chương trình được lập trình bằng Visual C++, ... Ngôn ngữ này được sử dụng cho các mục đích như:

- ♦ Mô phỏng lại các tổ hợp phím, thao tác di chuyển chuột và các thao tác điều khiển cửa sổ.
- ♦ Nhận thông tin và tương tác với các thành phần điều khiển như edit boxes, check boxes, list boxes, button, status bar.
- ♦ Tương tác với các tiến trình.
- ♦ Gọi trực tiếp tới các DLL và các hàm Windows API.
- ♦ Các script có thể được biên dịch thành các tập tin thực thi độc lập.
- ♦ ...

Nhờ vào những tính năng tiện lợi ở trên mà việc sử dụng AutoIT để viết phần mềm độc hại không phải là mới. Nó có thể được sử dụng làm keylogger, downloader, hoặc giai đoạn thăm dò trong quá trình lây nhiễm máy tính của nạn nhân. Tại Việt Nam, mã độc dạng này đã xuất hiện từ những năm 2006, điển hình trong đó là mã độc [XRobots](#).

2. Công cụ sử dụng

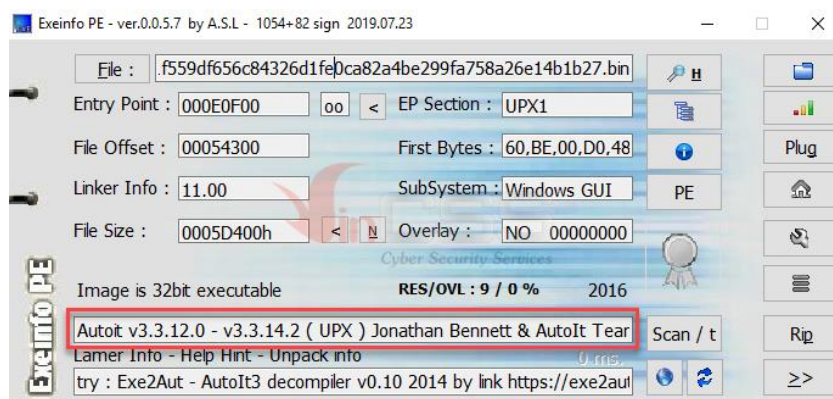
Danh sách các công cụ được sử dụng trong bài viết:

- ♦ [Exeinfo PE/ PESTudio](#)
- ♦ [Hex Editor \(HxD\)](#)
- ♦ [Resource Hacker](#)
- ♦ [Aut2Exe v3 Converter](#)
- ♦ [Exe2Aut Decompiler](#)
- ♦ autoit64to32.py & [AutoItSC.bin \(autoit-v3.2.8.1\)](#)

3. Cách nhận biết AutoIT

Khi phân tích một tập tin nghi ngờ là mã độc, thường người phân tích sẽ sử dụng các công cụ để kiểm tra xem tập tin đó có định dạng gì, được biên dịch bằng ngôn ngữ nào, có bị packed hay không, ... Với AutoIt sẽ có các dấu hiệu nhận biết như sau.

- ♦ Thông qua các công cụ như **Exeinfo PE** hoặc **PEStudio**:



dos-stub (200 bytes)	md5-without-overlay	n/a
file-header (Sep.2018)	sha1-without-overlay	n/a
optional-header (file-checksum)	sha256-without-overlay	n/a
directories (3)	first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
sections (99.88%)	first-bytes-text	MZ
libraries (7/18)	file-size	872448 (bytes)
imports (count)	size-without-overlay	n/a
exports (n/a)	entropy	6.345
tls-callbacks (n/a)	imphash	n/a
resources (Autolt)	signature	Microsoft Visual C++ 8
strings (size)	entry-point	E8 6A CE 00 00 E9 7F FE FF CC CC 57 56 8B 74 24 10 8B 4C 24 14 8B 7C 24 0C 8B C1 8B D1 03 C6 3B
debug (n/a)	file-version	4.1.8.0
manifest (asInvoker)	description	Program Compatibility Assistant
version (3.3.12.0)	file-type	executable
certificate (n/a)	cpu	32-bit
overlay (n/a)	subsystem	GUI
	compiler-stamp	0x5B8F7671 (Wed Sep 05 13:23:45 2018)
	debugger-stamp	n/a
	resources-stamp	empty
	exports-stamp	n/a
	version-stamp	empty
	certificate-stamp	n/a

dos-stub (this program c	entropy	8.000
file-header (Jan.2012)	file-offset	0x000A2600
optional-header (GUI)	size	0x001A3579 (1717625 bytes)
directories (3)	signature	Autolt
sections (27.87%)	first-bytes-hex	A3 48 4B BE 98 6C 4A A9 99 4C 53 0A 86 D6 48 7D
libraries (6/16)	first-bytes-text	.. H K ... I J ... L S ... H }
imports (179/513)	file-ratio	72.09 %
exports (0)		
tls-callbacks (n/a)		
resources (19)		
strings (215/25473)		
debug (n/a)		
manifest (invoker)		
version (3, 3, 8, 1)		
certificate (n/a)		
overlay (Autolt)		

♦ Thông qua Magic number: **A3484BBE986C4AA9994C530A86D6487D**

Khi biên dịch một AutoIt script với công cụ **Aut2Exe**, theo mặc định, một tệp thực thi pack bằng UPX được tạo ra. Mở bằng một trình Hex editor và tìm kiếm chuỗi magic number nói trên, theo sau sẽ là dấu hiệu nhận dạng của AutoIt thông qua chuỗi **AU3!EA06**.

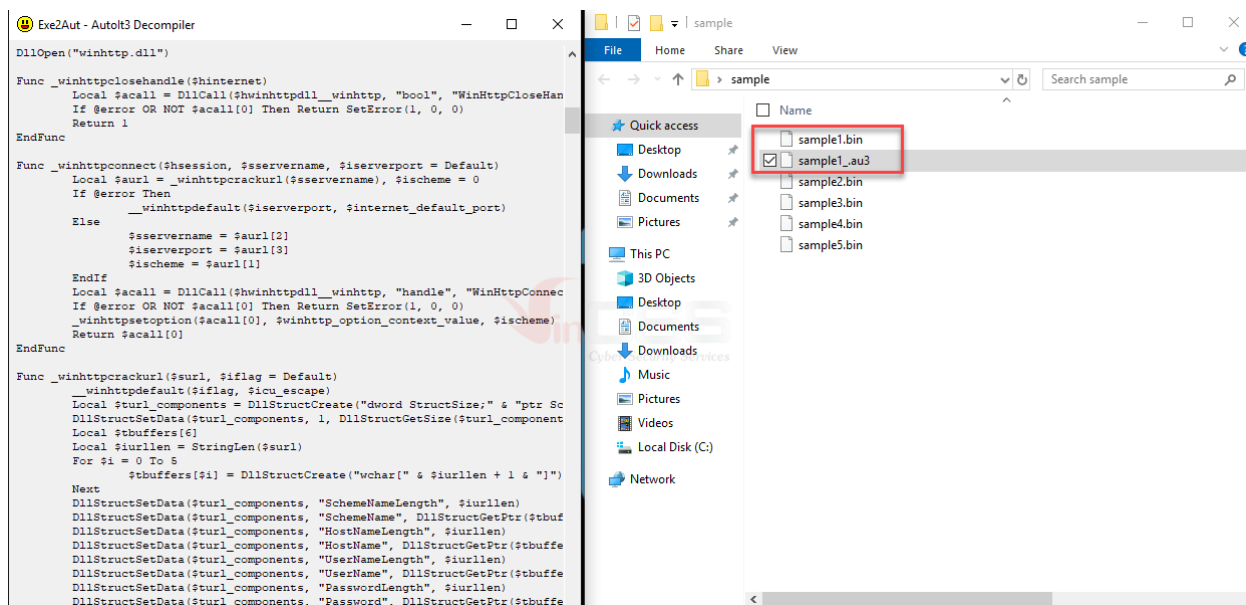
Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000C7180	20	00	63	00	68	00	61	00	72	00	61	00	63	00	74	00	.c.h.a.r.a.c.t.
000C7190	65	00	72	00	20	00	61	00	66	00	74	00	65	00	72	00	e.r. .a.f.t.e.r.
000C71A0	20	00	6B	00	65	00	79	00	77	00	6F	00	72	00	64	00	.k.e.y.w.o.r.d.
000C71B0	2E	00	00	00	00	00	00	00	A3	48	4B	BE	98	6C	4A	A9EHK*~1JG
000C71C0	99	4C	53	0A	86	D6	48	7D	41	55	33	21	45	41	30	36	LS.+OH)AU3!EA06
000C71D0	4D	A8	FF	73	24	A7	3C	F6	7A	12	F1	67	AC	C1	93	E7	M`ys\$S<0z.fg-A"ç
000C71E0	6B	43	CA	52	A6	AD	00	00	E1	BB	3A	21	A5	29	E3	EC	kCER!...á»:¡¥)ãl
000C71F0	E7	0B	98	2E	40	BD	E1	9A	DE	80	46	B1	9D	6B	3B	21	ç.~.@*á\$E€F±.k;!
000C7200	D4	B1	D6	75	3A	C8	3D	C6	D0	33	F7	14	AF	CB	17	A2	Ô±Öu:È=ED3÷.~È.c
000C7210	94	01	8D	13	88	FE	64	95	61	E7	B6	4D	1A	F8	00	00	"...^pd*acQM.ø..
000C7220	0D	D5	ED	C4	2B	1F	97	4D	1E	17	85	46	B4	66	B2	71	.ÖiÄ+.-M....F'f²q
000C7230	FE	BB	40	2C	27	86	59	A9	3B	3E	C8	72	83	6E	77	F8	p»@,'+Y@;>Èrfnwø
000C7240	69	40	1B	AA	BA	2F	39	E3	9D	0A	D0	77	EE	36	09	E6	i@.²°/9Ä..Đwi6.æ
000C7250	3B	9F	C6	24	64	72	8F	0A	79	4F	82	6E	D8	A7	0D	12	;YÆ\$dr..yO,nø\$..
000C7260	DE	B5	2D	FD	C2	1A	02	E7	71	48	B8	E1	4F	F1	96	90	Eu-yÄ..çqH,áoñ-.
000C7270	0F	DA	F2	3F	40	96	AC	FD	1C	4C	D4	39	22	06	A2	94	.Üò?@-ý.LÖ9".c"
000C7280	5D	67	94	88	C5	04	7C	A4	73	5F	D6	31	4E	28	13	99	lg""Ä.¡s Ö1N(.²

4. Phương pháp trích xuất script

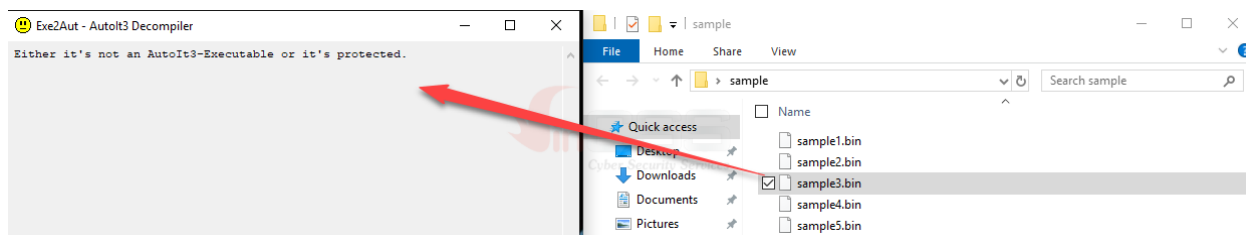
Các phương pháp trình bày dưới đây được tham khảo từ các chuyên gia [@VK Intel](#); [@0xffff0800](#); [@Hexacorn](#)

♦ Phương pháp thứ nhất: "Drag & Drop"

Sở dĩ gọi phương pháp này là "drag & drop" là vì nó rất đơn giản, chỉ việc kéo thả một AutoIt exe-file vào trình **Exe2Aut** để nhận được script gốc. **Exe2Aut** sẽ tự động lưu script tại cùng thư mục với phần mở rộng là <filename>_.au3:

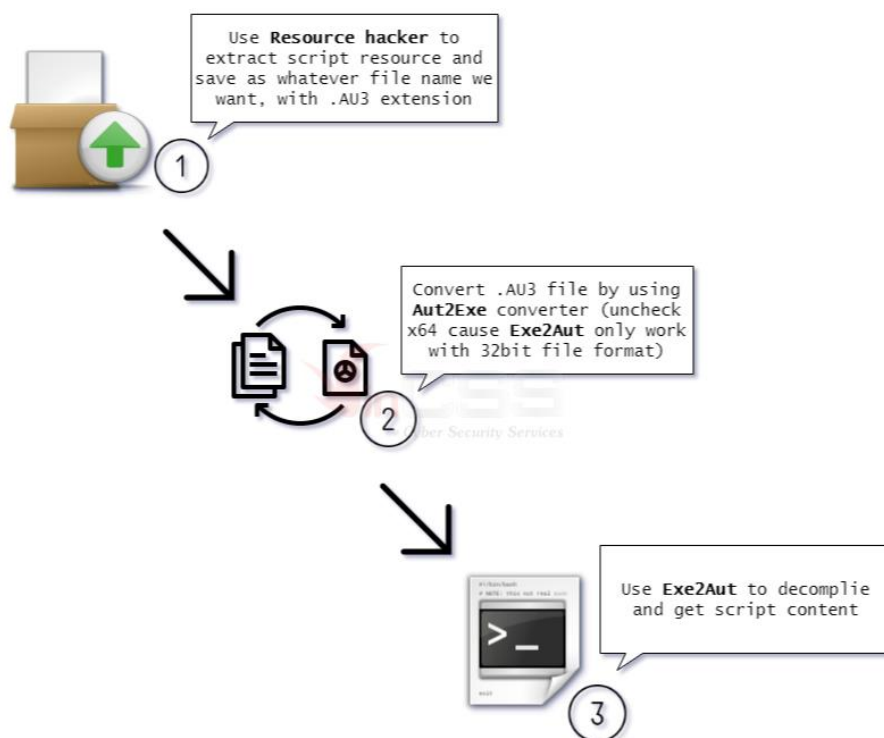


Tuy nhiên, không phải trường hợp nào **Exe2Aut** cũng hoạt động, ví dụ như trường hợp này:



◆ Phương pháp thứ hai

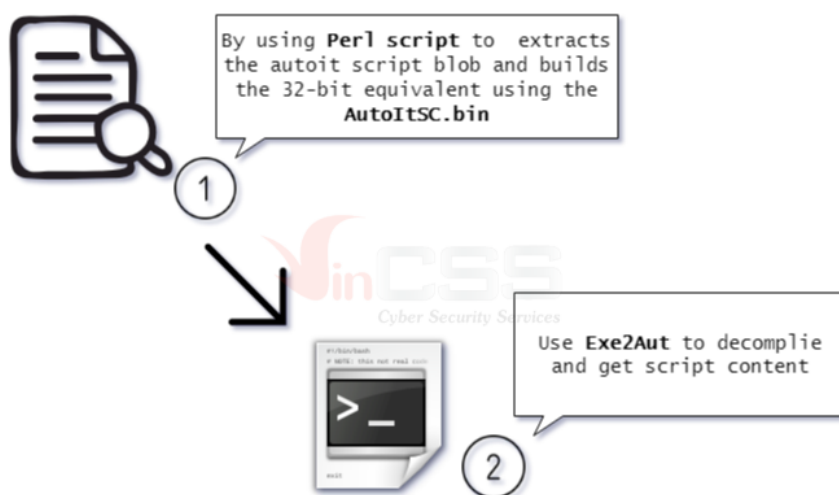
Để khắc phục cho trường hợp không trích xuất được bằng phương pháp đầu, phương pháp này sử dụng **Resource Hacker** để trích xuất script resource, lưu lại với tên bất kỳ với phần mở rộng là .au3. Tiếp theo, chuyển đổi file đã lưu sang định dạng PE bằng công cụ **Aut2Exe**. Lưu ý bỏ tùy chọn "Compile for system x64" trong quá trình thực hiện vì **Exe2Aut** không hỗ trợ x64 executables.



Dưới đây là phần demo minh họa cho phương pháp này

♦ Phương pháp thứ 3

Sử dụng Python script (được convert từ [autoit64to32.pl \(Perl script\)](#) của [@Hexacorn](#)) để trích xuất AutoIT script blob từ file thực thi và chuyển đổi sang định dạng 32 bit tương ứng bằng cách sử dụng **AutoItSC.bin** (32 bit) đi kèm trong bộ **autoit-v3.2.8.1**. File sau chuyển đổi sẽ thông qua **Exe2Aut** để lấy ra nội dung của script:



Nội dung của **autoit64to32.py** như sau:

```

use strict;
use warnings;

my $f=shift || die ("Gimme a file name!");

print STDERR "Processing '$f':\n";
print STDERR "- Reading 'AutoItSC.bin'\n";
open F,"<AutoItSC.bin";
binmode F;
read F,my $a, -s 'AutoItSC.bin';
close F;

print STDERR "- Reading '$f'\n";
open F,"<$f";
binmode F;
read F,my $d, -s $f;
close F;

print STDERR "- Looking for the script\n";
if ($d=~/\xA3\x48\x4B\xBE\x98\x6C\x4A\xA9\x99\x4C\x53\x0A\x86\xD6\x48\x7D/sg)
{
    my $pd=(pos $d)-16;
    print STDERR "- Script found @ ".sprintf("%08lX",$pd)."\n";
    print STDERR "- Creating 32-bit version '$f.a32.exe'\n";
    open F,">$f.a32.exe";
    binmode F;
    print F $a.substr($d,$pd,length($d)-$pd);
    close F;
}
else
{
    print STDERR "- Script not found !\n";
}

```

Dưới đây là phần demo minh họa cho phương pháp này: