



آکادمی راورین

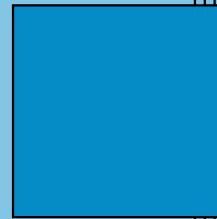
شکار تهدید باج افزار Anatova

شکار تهدیدات

آکادمی راورین

نسخه ۰.۱

۲۵ بهمن ۱۴۰۰



فهرست مطالب

پ	فهرست شکل‌ها
چ	تحلیل باج‌افزار
چ	۱.۰ تحلیل باج‌افزار
س	آشکارسازی
س	۲.۰ نمونه آشکارسازها
س	۱.۲.۰ چکیده‌ها
ص	فهرست نمادها



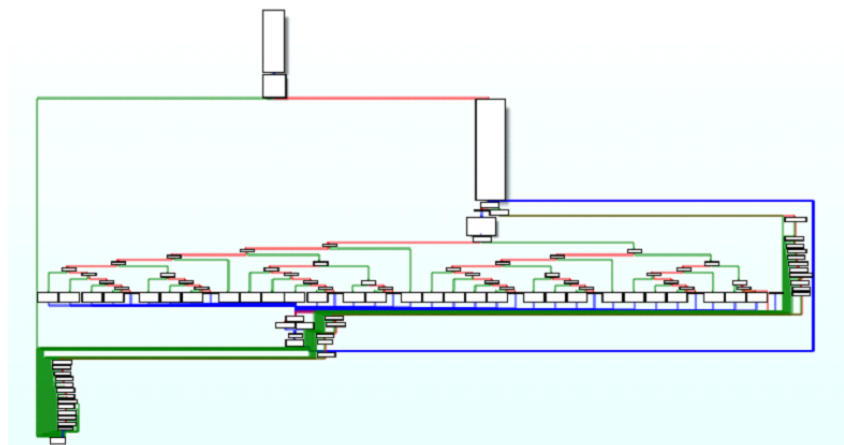
۱	شمای تابع بدست آورنده‌ی آدرس	چ
۲	نمونه کدهایی برای رمزنگاری	ح
۳	نمونه کدهایی رمز شده	ح
۴	تابع رمزگشا	ح
۵	ایجاد mutex	خ
۶	بررسی username	خ
۷	بررسی زبان سیستم	د
۸	بررسی زبان سیستم	ذ
۹	بررسی فرآیندهای جاری سیستم	ذ
۱۰	بررسی اسامی فرآیندها	ر
۱۱	فولدرهای محافظت شده	ر
۱۲	حذف فایل‌های پشتیبان	ز
۱۳	حذف فایل‌های پشتیبان	ز
۱۴	حذف IAT از حافظه	ز
۱۵	حذف کدهای اجرایی از حافظه	ژ
۱۶	جریان اجرایی باج‌افزار	ژ

این بخش به تحلیل باج افزار Anatova می پردازد.

۱.۰ تحلیل باج افزار

این باج افزار در سال ۲۰۱۹ توسط کمپانی McAfee کشف شده است. باج افزاری که از string encryption و dynamic api استفاده می کند. تعداد کمی API در IAT این باج افزار وجود دارند. مهم ترین آن ها LoadLibrary و GetProcAddress هستند که از این دو برای resolve کردن api ها به صورت داینامیک استفاده می شود. تابعی که مسئولیت این کار را دارد، شکل ۱

شکل ۱ شمای تابع بدست آورنده ی آدرس



برای عملیات‌های مانند درهم‌سازی و اضافه کردن پیچیدگی به کد مشاهده می‌شود که تعدادی string که encrypt شده‌اند به یک متغیر انتقال داده می‌شوند. همین‌طور تعدادی عدد به یک متغیر انتقال داده می‌شوند.

```
00000000040587D mov     eax, 12
000000000405882 mov     [rbp+var_125], al
000000000405888 mov     eax, 11h
00000000040588D mov     [rbp+var_125+1], al
000000000405893 mov     eax, 7
000000000405898 mov     [rbp+var_125+2], al
00000000040589E mov     eax, 13h
0000000004058A3 mov     [rbp+var_125+3], al
0000000004058A9 mov     eax, 13h
0000000004058AE mov     [rbp+var_125+4], al
0000000004058B4 mov     eax, 19h
0000000004058B9 mov     [rbp+var_125+5], al
0000000004058BF mov     eax, 0Ah
0000000004058C4 mov     [rbp+var_125+6], al
0000000004058CA mov     eax, 0Ch
0000000004058CF mov     [rbp+var_125+7], al
0000000004058D5 mov     eax, 5
0000000004058DA mov     [rbp+var_125+8], al
0000000004058E0 mov     eax, 0Fh
0000000004058E5 mov     [rbp+var_125+9], al
0000000004058EB mov     eax, 0Ah
0000000004058F0 mov     [rbp+var_125+0Ah], al
0000000004058F6 mov     eax, 0Ah
0000000004058FB mov     [rbp+var_125+0Bh], al
```

شکل ۲ نمونه کدهایی برای رمزنگاری

```
00000000040570B lea     rax, aZeXymfCo ; "Ze~xym`M`co"
000000000405712 mov     [rbp+var_108], rax
000000000405719 lea     rax, aGxcdpWctt ; "Gxcdp}Wctt"
000000000405720 mov     [rbp+var_108+8], rax
000000000405727 lea     rax, aWuhdbtt45Anuts ; "Wuhdbtt45AnutsP"
00000000040572E mov     [rbp+var_108+10h], rax
000000000405735 lea     rax, aCvCaPv ; "\\cv}Ca|pv`"
00000000040573C mov     [rbp+var_108+18h], rax
000000000405743 lea     rax, aGvaZRgvCaPv ; "Gva~z}rgvCa|pv`"
00000000040574A mov     [rbp+var_108+20h], rax
000000000405751 lea     rax, aZuvjQxwU ; "Zuvj}Qxw|u|"
000000000405758 mov     [rbp+var_108+28h], rax
00000000040575F lea     rax, aZxeioyy98Dor~ ; "Zxeioyy98Dor~]"
000000000405766 mov     [rbp+var_108+30h], rax
00000000040576D lea     rax, aIxiAchi ; "_ixInnc~Achi"
000000000405774 mov     [rbp+var_108+38h], rax
00000000040577B lea     rax, aBQvVqHaCdpiqpl ; "B`qV|vq`hA`cdpiqPLIdkbpdb`"
000000000405782 mov     [rbp+var_108+40h], rax
000000000405789 lea     rax, aLJnJbzJwn ; "L}jn{jBz{jwN"
000000000405790 mov     [rbp+var_108+48h], rax
000000000405797 lea     rax, aMoFkyOxxex ; "Mo~Fky~Oxxex"
00000000040579E mov     [rbp+var_108+50h], rax
0000000004057A5 lea     rax, aMoFemcikfNxc|oy ; "Mo~FemcikfNxc|oy"
0000000004057AC mov     [rbp+var_108+58h], rax
0000000004057B3 lea     rax, aZkXmHvvuqUiJwx ; "Zk|xm|Hvvuq|ui*+Jwxiqvm"
0000000004057BA mov     [rbp+var_108+60h], rax
```

شکل ۳ نمونه کدهایی رمز شده

هر string با عدد متناظر به یک تابع فرستاده می‌شود. این تابع وظیفه decrypt کردن string ها را دارد.

```
def decode(string, value):
    o = ""
    for i in range(len(string)):
        o += chr(ord(string[i]) ^ value)
    return o
print(decode("\\cv}Ca|pv`", 19)) # OpenProcess
```

شکل ۴ تابع رمزگشا

بعد از آن، باج‌افزار یک mutex با اسمی hardcoded شده درست می‌کند. اگر این mutex وجود داشت، باج‌افزار artifact های خود در سیستم را پاک می‌کند.


```

000000000406D3C mov     rax, cs:off_408000
000000000406D43 mov     r8, rax          ; 6a8c9937zFIwHPZ309UZMZYVnwScPB2pR2MEx5SY7B1xgbruo0
000000000406D46 mov     eax, 1
000000000406D48 mov     r11, rax
000000000406D4E mov     rax, 0
000000000406D58 mov     r10, rax
000000000406D5B mov     rcx, r10
000000000406D5E mov     rdx, r11
000000000406D61 mov     r11, cs:q_CreateMutex
000000000406D68 call    r11 ; q_CreateMutex
000000000406D6B mov     [rbp+var_18], rax
000000000406D6F mov     rax, [rbp+var_18]
000000000406D73 cmp     rax, 0
000000000406D77 jz      loc_406DAF

```

شکل ۵ ایجاد mutex

```

000000000406D7D mov     r11, cs:q_GetLastError
000000000406D84 call    r11 ; q_GetLastError
000000000406D87 mov     [rbp+var_1C], eax
000000000406D8A mov     eax, [rbp+var_1C]
000000000406D8D cmp     eax, ERROR_ALREADY_EXISTS
000000000406D93 jz      Destroy_IAT_Delete

```

باج افزار سپس username سیستم را در مقابل لیستی از اسم ها چک می کند.

شکل ۶ بررسی username

```

0000000004069C7 call    GetUserNameW ; GetUserNameW
0000000004069CA movzx   eax, al
0000000004069CD mov     eax, 0
0000000004069D2 mov     [rbp+var_60], eax

```

```

0000000004069D5 loc_4069D5:
0000000004069D5 mov     eax, [rbp+var_60]
0000000004069D8 mov     ecx, cs:dword_4082EC
0000000004069DE cmp     eax, ecx
0000000004069E0 jge     return

```

```

0000000004069E6 jmp     loc_4069F9

```

```

0000000004069F9 loc_4069F9:
0000000004069F9 mov     eax, [rbp+var_60]
0000000004069FC movsxd  rax, eax
0000000004069FF shl     rax, 3
000000000406A03 lea     rcx, [rbp+var_50]
000000000406A07 add     rcx, rax
000000000406A0A movzx   eax, cs:byte_4082E9
000000000406A11 mov     r11, rax
000000000406A14 mov     rax, [rcx]
000000000406A17 mov     r10, rax
000000000406A1A mov     rcx, r10
000000000406A1D mov     rdx, r11
000000000406A20 call    mw Decode
000000000406A25 mov     [rbp+Str1], rax
000000000406A29 mov     rax, [rbp+Str_Username]
000000000406A2D mov     r11, rax
000000000406A30 mov     rax, [rbp+Str1]
000000000406A34 mov     r10, rax
000000000406A37 mov     rcx, r10          ; Str1
000000000406A3A mov     rdx, r11          ; Str2
000000000406A3D call    wcsncmp

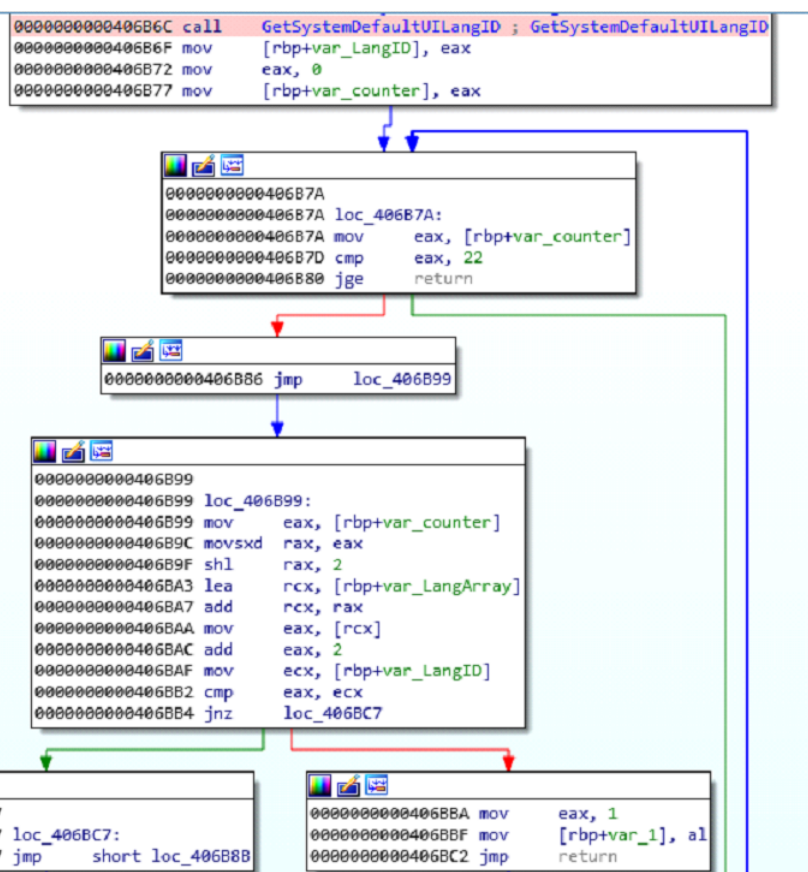
```

در ادامه لیستی از Username هایی که باج افزار به آن ها حساس است آمده است.

- tester
- Tester
- LaVirusLera
- analyst
- Analyst
- lab
- Lab
- malware
- Malware

سپس باج افزار زبان اول سیستم را در مقابل لیستی از زبان ها چک می کند.

شکل ۷ بررسی زبان سیستم



مقادیر زبانهایی^۱ که باج افزار به آن ها حساس است و باعث جلوگیری از آلوده سازی سیستم می شود در ادامه آمده است.

^۱ زبان کشورهایی مثل عراق، مصر، هند، مراکش و ...

```

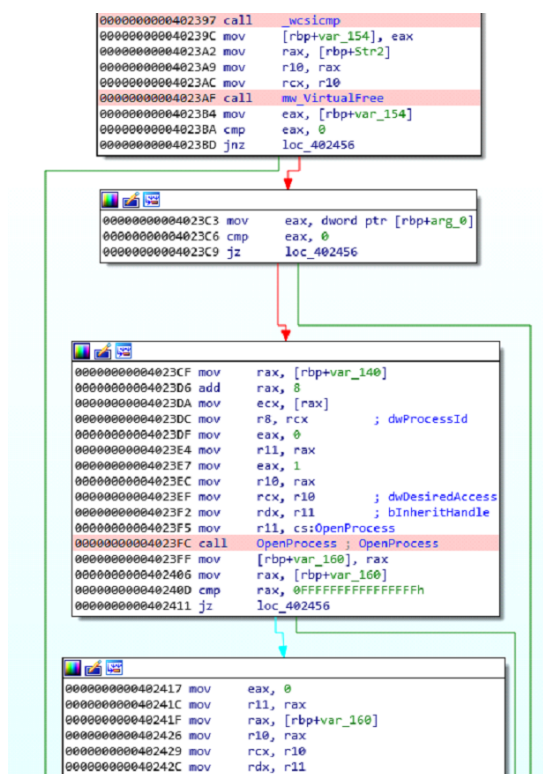
eax=419
eax=422
eax=423
eax=428
eax=42b
eax=42c
eax=437
eax=43f
eax=440
eax=442
eax=443
eax=444
eax=818
eax=819
eax=82c
eax=843
eax=45a
eax=2801
eax=439
eax=c01
eax=1801
eax=801

```

شکل ۸ بررسی زبان سیستم

سپس باج افزار، لیستی از فرآیندهای جاری سیستم را در مقابل لیستی از اسم فرآیندها چک می‌کند. در صورتی که بررسی با این نام وجود داشت، آن را terminate می‌کند.

شکل ۹ بررسی فرآیندهای جاری سیستم



اسامی فرآیندهایی که توسط باج افزار چک می شود:

```
-----
"msftesql.exe"
"sqlagent.exe"
"sqlbrowser.exe"
"sqlwriter.exe"
"oracle.exe"
"ocssd.exe"
"dbsnmp.exe"
"synctime.exe"
"agntsvc.exeisqlplussvc.exe"
"xfssvcon.exe"
"sqlservr.exe"
"mydesktopservice.exe"
"ocautoupds.exe"
"agntsvc.exeagntsvc.exe"
"agntsvc.exeencsvc.exe"
"firefoxconfig.exe"
"tbirdconfig.exe"
"mydesktopqos.exe"
"ocomm.exe"
"mysqld.exe"
"mysqld-nt.exe"
"mysqld-opt.exe"
"dbeng50.exe"
"sqbcoreservice.exe"
"excel.exe"
"infopath.exe"
"msaccess.exe"
"mspub.exe"
"onenote.exe"
"outlook.exe"
"powerpnt.exe"
"steam.exe"
"thebat.exe"
"thebat64.exe"
"thunderbird.exe"
"visio.exe"
"winword.exe"
"wordpad.exe"
```

شکل ۱۰ بررسی اسامی فرآیندها

بعد از encrypt کردن درایوهای remote ، باج افزار از encrypt کردن های زیر جلوگیری می کند.

```
Recycle Bin
Program Files
Program Files (x86)
Windows
ProgramData
Tor Browser
Local Settings
IETLdCache
Boot
All Users
```

شکل ۱۱ فولدرهای محافظت شده

در اواخر کار، Shadow Volume Copy ها را با command زیر پاک می کند.

شکل ۱۲ حذف فایل های پشتیبان

```
0000000000405545 call    ShellExecuteA ; ShellExecuteA
0000000000405545 cmd.exe /c vssadmin delete shadows /all /quiet
```

سپس باج افزار باینری خود را با command زیر از سیستم پاک می کند.

شکل ۱۳ حذف فایل های پشتیبان

```
0000000000405352 call    r11 ; ShellExecuteA
0000000000405352 "cmd /c timeout -c 9 & del "C:\PATH_To_Binary" /f /q"
```

در نهایت code خود را nop می کند و IAT ساخته شده در run-time را از بین می برد.

شکل ۱۴ حذف IAT از حافظه

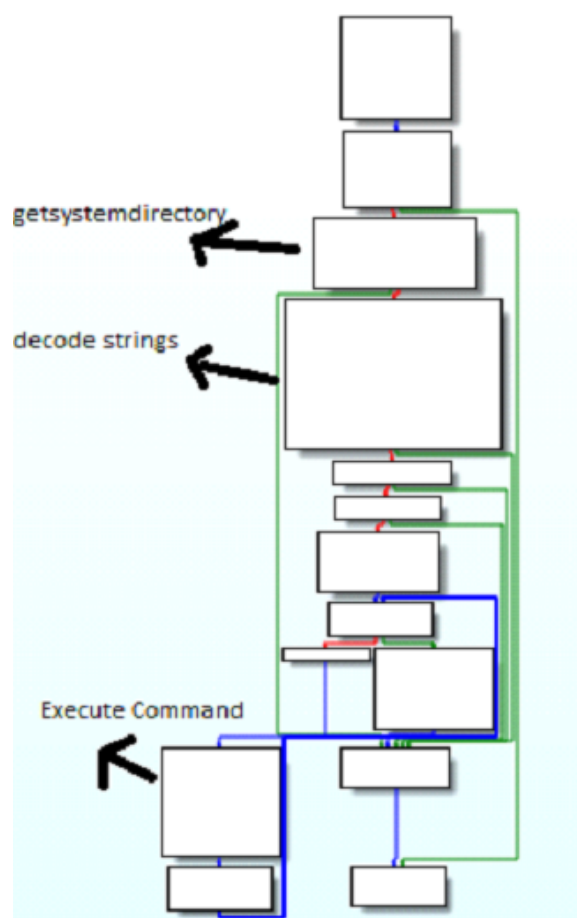
```
0000000000401E11 mov     rax, 0
0000000000401E1B mov     cs:OpenProcess, rax
0000000000401E22 mov     rax, 0
0000000000401E2C mov     cs:TerminateProcess, rax
0000000000401E33 mov     rax, 0
0000000000401E3D mov     cs:CloseHandle, rax
0000000000401E44 mov     rax, 0
0000000000401E4E mov     cs:SetErrorMode, rax
0000000000401E55 mov     rax, 0
0000000000401E5F mov     cs:CreateMutex, rax
0000000000401E66 mov     rax, 0
0000000000401E70 mov     cs:GetLastError, rax
0000000000401E77 mov     rax, 0
0000000000401E81 mov     cs:VirtualAlloc, rax
0000000000401E88 mov     rax, 0
0000000000401E92 mov     cs:VirtualFree, rax
0000000000401E99 mov     rax, 0
0000000000401EA3 mov     cs:GetSystemDefaultUILangID, rax
```

شکل ۱۵ حذف کدهای اجرایی از حافظه

```

0000000000406FEA mov     eax, 90h
0000000000406FEF mov     r11, rax
0000000000406FF2 lea     rax, main
0000000000406FF9 mov     r10, rax
0000000000406FFC mov     rcx, r10      ; Dst
0000000000406FFF mov     rdx, r11      ; Val
0000000000407002 call    memset
    
```

شکل ۱۶ جریان اجرایی باج افزار



۲.۰ نمونه آشکارسازها

چکیده ها

۱.۲.۰

جدول ۱ آشکارساز رویداد 96069

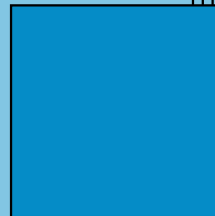
96069		
تاریخ	آشکارساز یا ج افزار	تابع چکده ساز
2019-03-08	2a0da563f5b88c4d630aefbcd212a35e	md5
	366770ebfd096b69e5017a3e33577a94	md5
	596ebe227dcd03863e0a740b6c605924	md5
	61139db0bbe4937cd1afc0b818049891	md5
	9d844d5480eec1715b18e3f6472618aa	md5
	170fb7438316f7335f34fa1a431afc1676a786f1ad9dee63d78c3f5efd3a0ac0	sha256
	75371ff38823885b47aa21d2883792a5470e9bflf3d2dc93f512725f35491820	sha256
	97fb79ca6fc5d24384bf5ae3d01bf5e77f1d2c0716968681e79c097a7d95fb93	sha256
	ab8a76b64448b943dc96a3e993b6e6b37af27c93738d27ffd1f4c9f96a1b7e69	sha256
	bd422f912affcf6d0830c13834251634c8b55b5a161c1084deae1f9b5d6830ce	sha256
	f9ce8aecbcd1d718d4c5b710456579b71ad3383844e3e594b8837c00c4b9e4ca	sha256
	775dd73a14d07fb8ed837d931842e7066b88367850ef7770edfaca534cbfd8df	sha256

جدول ۲ آشکارساز رویداد 13632

13632		
تاریخ	آشکارساز باج افزار	تابع چیکده ساز
2019-01-23	2a0da563f5b88c4d630aefbcd212a35e	md5
	366770ebfd096b69e5017a3e33577a94	md5
	9d844d5480eec1715b18e3f6472618aa	md5
	61139db0bbe4937cd1afc0b818049891	md5
	596ebe227dcd03863e0a740b6c605924	md5

جدول ۳ آشکارساز رویداد 13196

13196		
تاریخ	آشکارساز باج افزار	تابع چیکده ساز
2019-01-23	2a0da563f5b88c4d630aefbcd212a35e	md5
	366770ebfd096b69e5017a3e33577a94	md5
	9d844d5480eec1715b18e3f6472618aa	md5
	61139db0bbe4937cd1afc0b818049891	md5
	596ebe227dcd03863e0a740b6c605924	md5



فهرست نمادها

چ	جدول آدرس توابع ورودی	IAT
ح	باج افزار	Ransomware
ح	رابط برنامه نویسی کاربردی	API
ح	رمز شده	encrypt
ح	رشته	string
ح	رمزگشایی	decrypt
ح	مشخصه	artifact
ح	انحصار متقابل	mutex
د	نام کاربری	Username
ر	راه دور	remote
ز	دستور	command
ز	زمان اجرا	run-time
ز	آپ کد خالی	nop