شکار تهدید باج‌افزار Anatova

شکار تهدیدات

آکادمی راوین

علی طباطبایی
طه توکلی

نسخه ۰.۱

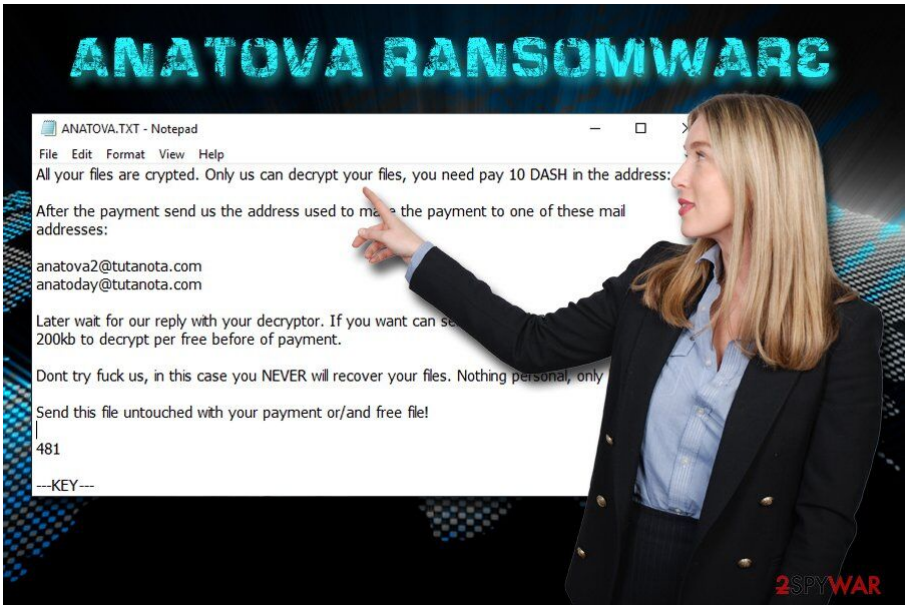
۲۵ بهمن ۱۴۰۰

فهرست مطالب

فهرست شکل‌ها

۱.۰ مقدمه

این باج‌افزار در سال ۲۰۱۹ توسط کمپانی McAfee کشف شده است. باج‌افزاری که از string

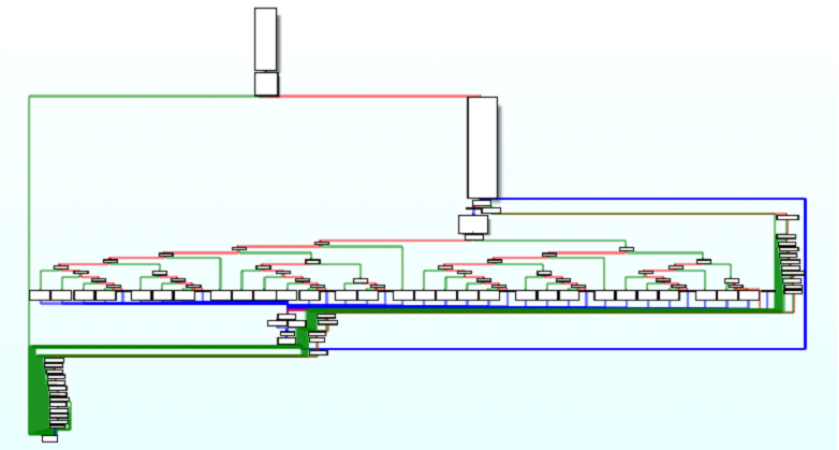


encryption و dynamic api استفاده می‌کند.

این بخش به تحلیل باج‌افزار Anatova می‌پردازد.

۲.۰ تحلیل باج‌افزار

تعداد کمی API در IAT این باج‌افزار وجود دارند. مهم‌ترین آن‌ها LoadLibrary و GetProcAddress هستند که از این دو برای resolve کردن api ها به صورت داینامیک استفاده می‌شود. تابعی که مسئولیت این کار را دارد، به صورت زیر است:



شکل ۱ شمای تابع بدست آورنده‌ی آدرس

تعدادی string که encrypt شده‌اند به یک متغیر انتقال داده می‌شوند. همین‌طور تعدادی عدد به یک متغیر انتقال داده می‌شوند.

```
000000000040587D mov     eax, 12
0000000000405882 mov     [rbp+var_125], al
0000000000405888 mov     eax, 11h
000000000040588D mov     [rbp+var_125+1], al
0000000000405893 mov     eax, 7
0000000000405898 mov     [rbp+var_125+2], al
000000000040589E mov     eax, 13h
00000000004058A3 mov     [rbp+var_125+3], al
00000000004058A9 mov     eax, 13h
00000000004058AE mov     [rbp+var_125+4], al
00000000004058B4 mov     eax, 19h
00000000004058B9 mov     [rbp+var_125+5], al
00000000004058BF mov     eax, 0Ah
00000000004058C4 mov     [rbp+var_125+6], al
00000000004058CA mov     eax, 0Ch
00000000004058CF mov     [rbp+var_125+7], al
00000000004058D5 mov     eax, 5
00000000004058DA mov     [rbp+var_125+8], al
00000000004058E0 mov     eax, 0Fh
00000000004058E5 mov     [rbp+var_125+9], al
00000000004058EB mov     eax, 0Ah
00000000004058F0 mov     [rbp+var_125+0Ah], al
00000000004058F6 mov     eax, 0Ah
00000000004058FB mov     [rbp+var_125+0Bh], al
```

شکل ۲ نمونه کدهایی برای رمزنگاری

```
000000000040570B lea     rax, aZeXymMCo  ; "Ze~xym`M``co"
0000000000405712 mov     [rbp+var_108], rax
0000000000405719 lea     rax, aGxcedpWctt ; "Gxcedp}Wctt"
0000000000405720 mov     [rbp+var_108+8], rax
0000000000405727 lea     rax, aWuhdbtt45anuts ; "Wuhdbtt45AnutsP"
000000000040572E mov     [rbp+var_108+10h], rax
0000000000405735 lea     rax, aCvCaPv    ; "\\cv}Ca|pv``"
000000000040573C mov     [rbp+var_108+18h], rax
0000000000405743 lea     rax, aGvaZRgvcaPv ; "Gva~z}rgvCa|pv``"
000000000040574A mov     [rbp+var_108+20h], rax
0000000000405751 lea     rax, aZuvjQxwU  ; "Zuvj|Qxw}u|"
0000000000405758 mov     [rbp+var_108+28h], rax
000000000040575F lea     rax, aZxeioyy98dor ; "Zxeioyy98Dor~]"
0000000000405766 mov     [rbp+var_108+30h], rax
000000000040576D lea     rax, aIxiCAchi  ; "_ixI~~c~Achi"
0000000000405774 mov     [rbp+var_108+38h], rax
000000000040577B lea     rax, aBQvVqHaCdpiqpl ; "B`qV|vq`hA`cdpiqPLIdkbpdb`"
0000000000405782 mov     [rbp+var_108+40h], rax
0000000000405789 lea     rax, aLJnJbzJwn ; "L}jn{jBz{jwN"
0000000000405790 mov     [rbp+var_108+48h], rax
0000000000405797 lea     rax, aMoFkyOxxex ; "Mo~Fky~Oxxex"
000000000040579E mov     [rbp+var_108+50h], rax
00000000004057A5 lea     rax, aMoFemcikfnxcOy ; "Mo~FemcikfNxc|oy"
00000000004057AC mov     [rbp+var_108+58h], rax
00000000004057B3 lea     rax, aZkXmMvvuqUiJwx ; "Zk|xm|Mvvuq|ui*+Jwxijqvm"
00000000004057BA mov     [rbp+var_108+60h], rax
```

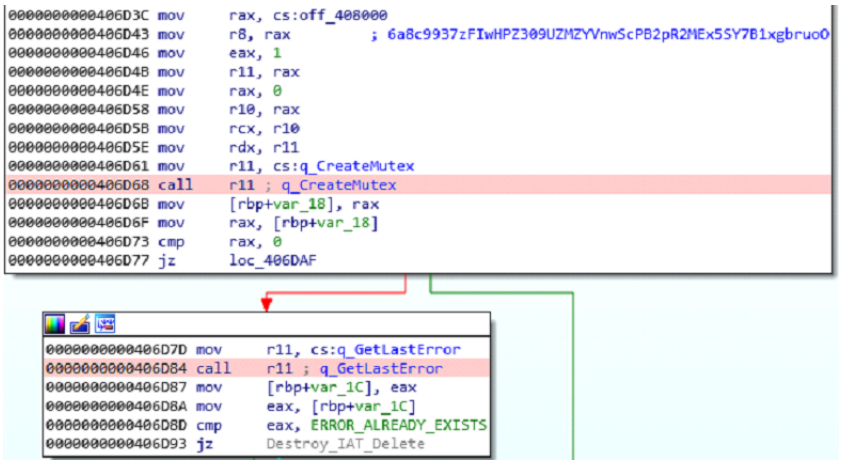
شکل ۳ نمونه کدهایی رمز شده

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

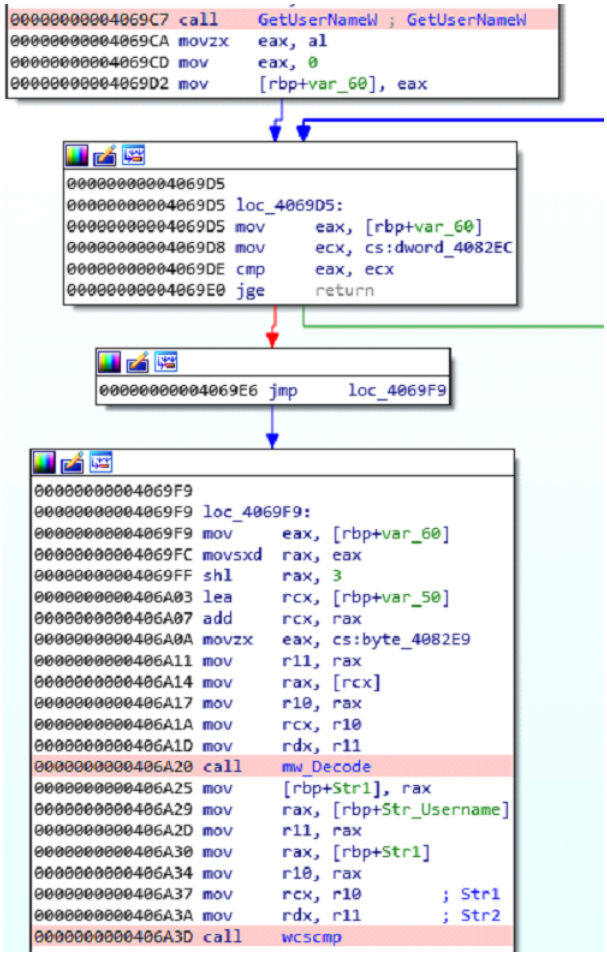
```
def decode(string, value):
    o = ""
    for i in range(len(string)):
        o += chr(ord(string[i]) ^ value)
    return o
print(decode("\\cv}Ca|pv``", 19)) # OpenProcess
```

شکل ۴ تابع رمزگشا

بعد از آن، باج‌افزار یک mutex با اسمی hardcode شده درست می‌کند. اگر این mutex وجود داشت، باج‌افزار artifact های خود در سیستم را پاک می‌کند. باج‌افزار سپس username سیستم را در مقابل لیستی از اسم‌ها چک می‌کند.



شکل ۵ ایجاد mutex

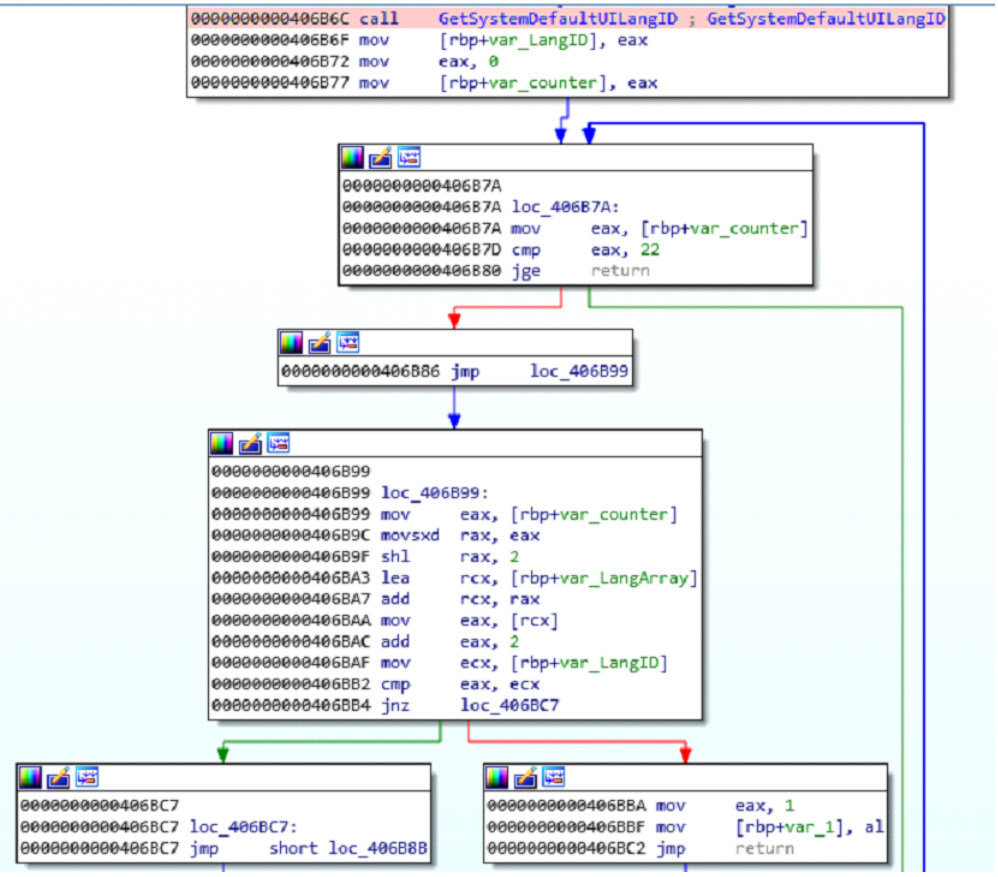


شکل ۶ بررسی username

در ادامه لیستی از Username هایی که باج‌افزار به آن‌ها حساس است آمده‌است.

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

سپس باج‌افزار زبان اول سیستم را در مقابل لیستی از زبان‌ها چک می‌کند. زبان‌هایی [1] که باج‌افزار به آن‌ها حساس است و باعث جلوگیری از آلوده‌سازی سیستم می‌شود: سپس باج‌افزار، لیستی از فرآیندهای جاری سیستم را در مقابل لیستی از اسم فرآیندها چک می‌کند. در صورتی که پروسسی با این نام وجود داشت، آن را terminate می‌کند.



شکل ۷ بررسی زبان سیستم

[1] 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

```
0000000000402397 call    _wcsicmp
000000000040239C mov     [rbp+var_154], eax
00000000004023A2 mov     rax, [rbp+Str2]
00000000004023A9 mov     r10, rax
00000000004023AC mov     rcx, r10
00000000004023AF call    mw_VirtualFree
00000000004023B4 mov     eax, [rbp+var_154]
00000000004023BA cmp     eax, 0
00000000004023BD jnz     loc_402456

00000000004023C3 mov     eax, dword ptr [rbp+arg_0]
00000000004023C6 cmp     eax, 0
00000000004023C9 jz      loc_402456

00000000004023CF mov     rax, [rbp+var_140]
00000000004023D6 add     rax, 8
00000000004023DA mov     ecx, [rax]
00000000004023DC mov     r8, rcx         ; dwProcessId
00000000004023DF mov     eax, 0
00000000004023E4 mov     r11, rax
00000000004023E7 mov     eax, 1
00000000004023EC mov     r10, rax
00000000004023EF mov     rcx, r10        ; dwDesiredAccess
00000000004023F2 mov     rdx, r11        ; bInheritHandle
00000000004023F5 mov     r11, cs:OpenProcess
00000000004023FC call    OpenProcess ; OpenProcess
00000000004023FF mov     [rbp+var_160], rax
0000000000402406 mov     rax, [rbp+var_160]
000000000040240D cmp     rax, 0FFFFFFFFFFFFFFFFh
0000000000402411 jz      loc_402456

0000000000402417 mov     eax, 0
000000000040241C mov     r11, rax
000000000040241F mov     rax, [rbp+var_160]
0000000000402426 mov     r10, rax
0000000000402429 mov     rcx, r10
000000000040242C mov     rdx, r11
```

شکل ۹ بررسی فرآیندهای جاری سیستم

اسامی فرآیندهایی که توسط باج‌افزار چک می‌شود:

```
"msftesql.exe"
"sqlagent.exe"
"sqlbrowser.exe"
"sqlwriter.exe"
"oracle.exe"
"ocssd.exe"
"dbsnmp.exe"
"synctime.exe"
"agntsvc.exeisqlplussvc.exe"
"xfssvccon.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 باج‌افزار از encrypt کردن های‌folder زیر جلوگیری می‌کند.

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

شکل ۱۱ فولدرهای محافظت شده

و در اواخر کار، Shadow Volume Copy ها را با command زیر پاک می‌کند. سپس باج‌افزار باینری خود را با command زیر از سیستم پاک می‌کند.

در نهایت code خود را nop می‌کند و IAT ساخته شده در run-time را از بین می‌برد.

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

شکل ۱۲ حذف فایل‌های پشتیبان

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

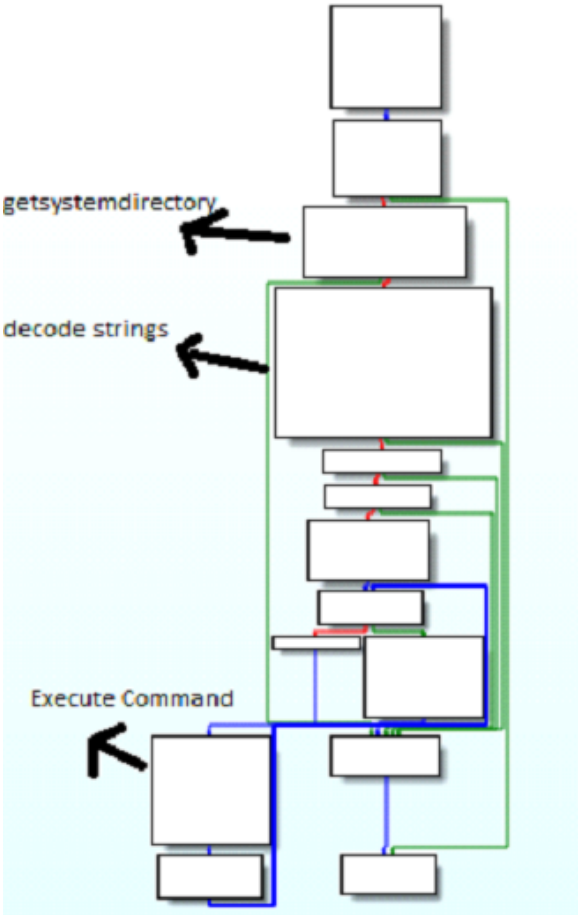
شکل ۱۳ حذف فایل‌های پشتیبان

```
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:SetErorrMode, 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 ۱۴ حذف IAT 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 ۱۵ حذف کدهای اجرایی از حافظه



شکل ۱۶ جریان اجرایی باج‌افزار

۳.۰ نمونه آشکارسازها

۱.۳.۰ چکیده ها

جدول ۱ آشکارساز رویداد 96069

96069		
تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2019-03-08	2a0da563f5b88c4d630aefbcd212a35e	md5
	366770ebfd096b69e5017a3e33577a94	md5
	596ebe227dcd03863e0a740b6c605924	md5
	61139db0bbe4937cd1afc0b818049891	md5
	9d844d5480eec1715b18e3f6472618aa	md5
	170fb7438316f7335f34fa1a431afc1676a786f1ad9dee63d78c3f5efd3a0ac0	sha256
	75371ff38823885b47aa21d2883792a5470e9bf1f3d2dc93f512725f35491820	sha256
	97fb79ca6fc5d24384bf5ae3d01bf5e77f1d2c0716968681e79c097a7d95fb93	sha256
	ab8a76b64448b943dc96a3e993b6e6b37af27c93738d27ffd1f4c9f96a1b7e69	sha256
	bd422f912affcf6d0830c13834251634c8b55b5a161c1084deae1f9b5d6830ce	sha256
	f9ce8aecbcd1d718d4c5b710456579b71ad3383844e3e594b8837c00c4b9e4ca	sha256
	775dd73a14d07fb8ed837d931842e7066b88367850ef7770edfaca534cbfd8df	sha256

جدول ۲ آشکارساز رویداد 13632

13632		
تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2019-01-23	2a0da563f5b88c4d630aefbcd212a35e	md5
	366770ebfd096b69e5017a3e33577a94	md5
	9d844d5480eec1715b18e3f6472618aa	md5
	61139db0bbe4937cd1afc0b818049891	md5
	596ebe227dcd03863e0a740b6c605924	md5

جدول ۳ آشکارساز رویداد 13196

13196		
تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2019-01-23	2a0da563f5b88c4d630aefbcd212a35e	md5
	366770ebfd096b69e5017a3e33577a94	md5
	9d844d5480eec1715b18e3f6472618aa	md5
	61139db0bbe4937cd1afc0b818049891	md5
	596ebe227dcd03863e0a740b6c605924	md5

فهرست نمادها