MultiKey چیست؟

یکی از نگرانی های برنامه نویسان همواره تامین امنیت نرم افزارها یشان از تحلیل (جهت مهندسی معکوس/مونتاژ) است ، از این رو یکی از مطمئن ترین روش ها استفاده از کلید های سخت افزاری (دانگل) است.

MultiKey یک بسته ی شبیه ساز تجاری(elite) است که قادر است (با توجه به ورژن مورد استفاده) دانگل هایی را شبیه سازی کند ، MultiKey برای سیستم های ۳۲ و ۶۴ بیتی NT طراحی شده که میتواند به توسعه دهندگان نرم افزار و افراد دیگر اجازه دهد که امنیت برنامه ی خود را مورد آزمایش قرار دهند.

برای استفاده از این شبیه ساز نیاز است که تمامی داده های مربوط به دانگل مورد نظر در ریجیستری ویندوز دامپ شود که این فرایند بسته به نوع دیتا ، و نوع کلید متفاوت خواهد بود.یعنی شماتیک یک فایل رجیستری که حاوی دیتای دامپ شده است با نوع های دیگر متفاوت است ،برای اینکه موضوع را بهتر درک کنید ابتدا باید بدانیم که این شبیه ساز از چه برندهایی پشتیبانی میکند

برندهای قابل پشتیبانی درآخرین نسخه MultiKey 20.0.0 (x86, x64) :

- Hasp3 / 4, Hasp HL, Hasp SRM
- Hardlock
- Sentinel superpro, ultrapro , Sentinel Hardware Key (SHK)
- Guardant Stealth I, Stealth II
- Dinkey

محدودیت های این شبیه ساز در نسخه ی دمو :

این شبیه ساز در نسخه ی دمو صرفا برای تست ساخته شده که میتواند توسط سازندگان و افراد دیگر مورد استفاده قرار گیرد اگر بخواهیم محدودیت های آن را ذکر کنیم اینگونه خواهد بود:

۱- امکان نصب به صورت lock pc (نصب محدود بروی یک سیستم با تجهیزات خاص)

۲- وجود باگ در ویندوزهای ۸ تا ۱۰

۳-محدودیت لایسنس برای نسخه های ۶۴ بیتی

۴-تولید مجوز برای محدودیت اجرا فقط برای نوع خاصی از کلید به همراه پسورد

نکته مهم : البته در نسخه های قدیمی (تا 18.x)برای دانگل های sspro و HL محدودیتی نیست اما در نسخه های جدیدتر این محدودیت برای تمامی برندها لحاظ شده است.

برای دانلود شبیه ساز به سایت http://testprotect.com مراجعه کنید

طریقه ی استفاده- نمای عمومی فایل رجیستری برای شبیه ساز-نسخه ی multikey 0.19.1.9 :

قبل از اینکه به نحوه ی کار بپردازیم ابتدا باید با ساختار عمومی فایل رجیستری مورد استفاده در شبیه ساز multikey آشنا باشیم ، این ساختار عمومی شامل ۵ قسمت مجزا است. که در تمام برنده‌ها مورد استفاده قرار میگیرد:

cyberheg.reg - Notepad

File Edit Format View Help

```
REGEDIT4
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Multikey\Dumps\3FAB44CE]



"Name"="AnyThing"
"Copyright"="Copyright (C) 2012 user"
"Created"="07/08/2016 19:41:30"
"DongleType"=dword:00000001

"License"=hex:28,e0,67,40,47,4c,be,e0,85,6e,4e,0b,d2,08,f6,9a

-----------------------------------------------------------------
"SN"=dword:2DB3C188
"Type"=dword:000000EA
"Memory"=dword:00000001


"SecTable"=hex:F2,35,56,15,1C,1D,1C,1D
"NetMemory"=hex:00,00,00,00,00,00,00,00,00,00,FF,FF
"Option"=hex:00,01,02,4A,1F,01,07,07,0C,01,10,29,2F,00
"Data"=hex:\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00
"ColumnMask"=dword:000000DB
```

```
REGEDIT4

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Multikey\Dumps\3FAB44CE]

"Name"="AnyThing"

"Copyright"="Copyright (C) 2012 user"

"Created"="07/08/2016 19:41:30"

"DongleType"=dword:00000001

"License"=hex:28,e0,67,40,47,4c,be,e0,85,6e,4e,0b,d2,08,f6,9a

-----------------------------------------------------------------
```

۱-مسیر رجیستری

[HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ MultiKey \ Dumps \ xxxxxxxx]

همانطور که میبینید Multikey نیاز به مشخص کردن مسیر به شکلی که در بالا میبینید دارد

۲- xxxxxxxx

دراین قسمت پسورد دانگل قرار میگیرد که شامل ۸ کاراکتر در مبنای هگزا است

مثال:

[HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ MultiKey \ Dumps \ 12345678]

نکته : در حالتی که برنامه ی ما از دو یا چند دانگل مختلف ولی از پسورد های یکسان استفاده میکند مسیر رجیستری باید اینگونه تعریف شود:

... MultiKey \ Dumps \ xxxxxxxxa]
... MultiKey \ Dumps \ xxxxxxxx1]

همانطور که میبینید Symbol هایی به انتهای پسورد اضافه شده که حکم یک جداکننده را دارد و شامل کاراکترهای A-Z و 0-9 است

مثال:

[HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ MultiKey \ Dumps \ 12345678a]

[HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ MultiKey \ Dumps \ 123456781]

[HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ MultiKey \ Dumps \ 12345678g]

۳-در این قسمت اطلاعاتی مانند نام برنامه ، کپی رایت ، زمان ساخت قرار میگیرد و میتوان آن را به شکل دلخواه پر کرد

"Name" = "xxx"
"Copyright" = "xxx"
"Created" = "xxx"

مثال:

"Name" = "EDIUS9"
"Copyright" = "IRANLED"
"Created" = "2/2/2016"

۴- در این قسمت نوع دانگل در فیلد x0000000 :به صورت dword مشخص میشود که شامل برندهای قابل پشتیبانی در این شبیه ساز است ، نوع آن به ترتیب با شماره ی ۱ تا ۵ مشخص میشود:

"DongleType" = dword: x 0000000 - key type

1 - HASP (3,4, HL, SRM)
2 - HARDLOCK
3 - SENTINEL (spro, upro)
4 - GUARDANT (I, II)
5 – DINKEY

مثال:

"DongleType" = dword: x 0000002 - key type

که مشخص کننده ی دانگل HARDLOCK است

۵- مجوز

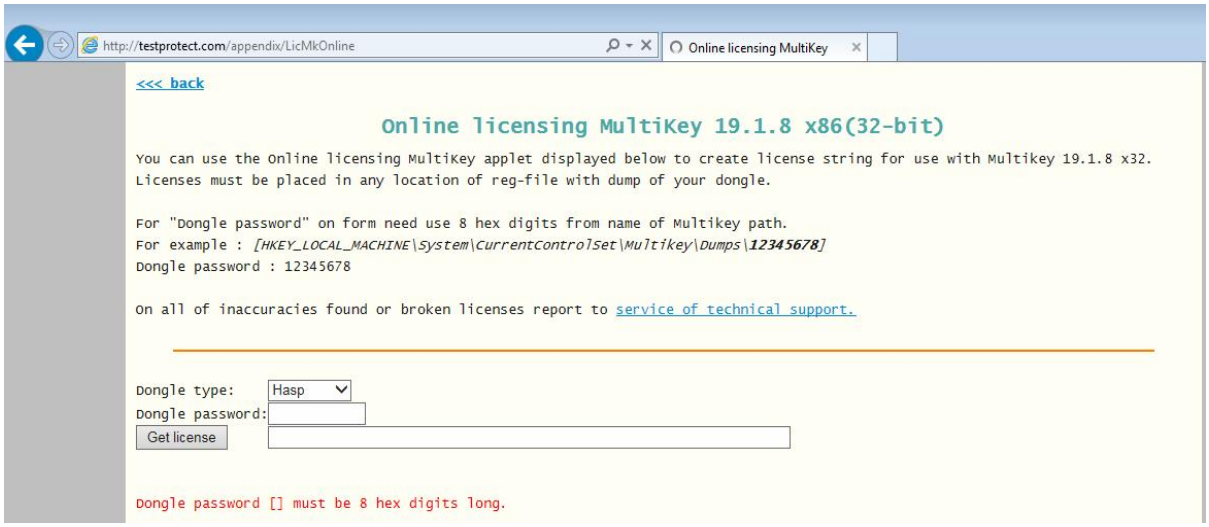
MULTIKEY با دریافت مجوز درواقع ایمولاتور نهایی را محدود میکند این محدودیت شامل آیتم های زیر است :

۱-اجرا بروی یک سیستم

۲-محدودیت اجرا

۳-محدودیت زمان

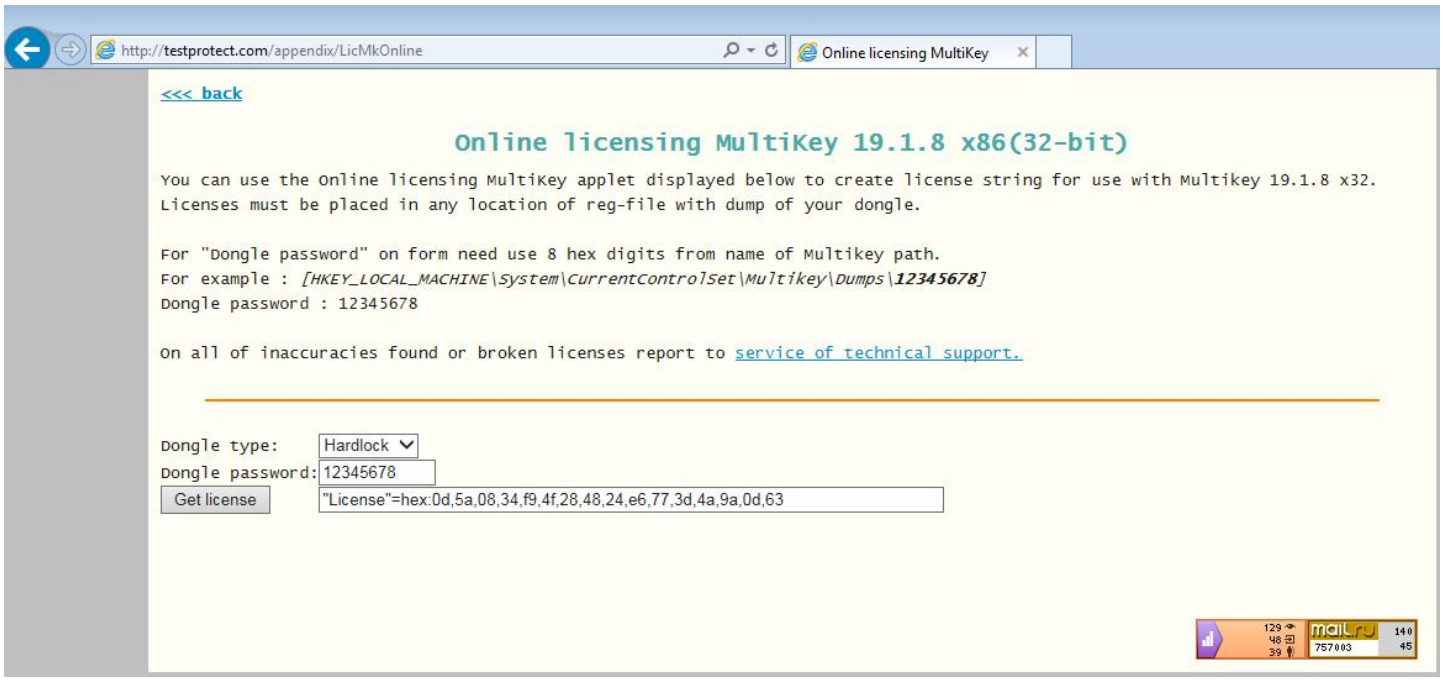
در این قسمت مجوز خود را با توجه به پسورد و نوع دانگل ، را از سایت http://testprotect.com/appendix/LicMkOnline



در قالب کد هگزا برای سیستم های ۳۲ بیتی دریافت کرده و در فایل ریجیستری در قسمت لایسنس قرار دهید :

"License" = hex: xx, xx, xx, xx, xx, xx, xx, xx, xx, xx, xx, xx, xx, xx, xx, xx

مثال:



نکته: محل لاینس را میتوان در هر کجای reg file قرار داد

حال که با چهارچوب عمومی فایل رجیستری برای شبیه ساز MultiKey آشنا شدیم،تک تک برندهای قابل پشتیبانی را تشریح میکنیم:

نکته:ساختار فایل رجیستری شبیه ساز تقریبا برگرفته از شمای داخلی دانگل است ،که فهم آن نیاز آشنایی با نحوه ی کارکرد دانگل و بخصوص نوع آن است،در دانگل هایی که صورت Priv8 شبیه سازی میشوند این فرایند (چیدمان دیتا درون فایل رجیستری) به صورت دستی صورت میگیرد ولی در نسخه های Public این فرایند میتواند دستی همچنین با ابزارهایی مخصوص همان برند به صورت خودکار انجام شود که آن خود مبحثی جدا گانه دارد.

در قسمت بعدی به بررسی ساختار برندهای قابل پشتیبانی در این شبیه ساز میپردازیم