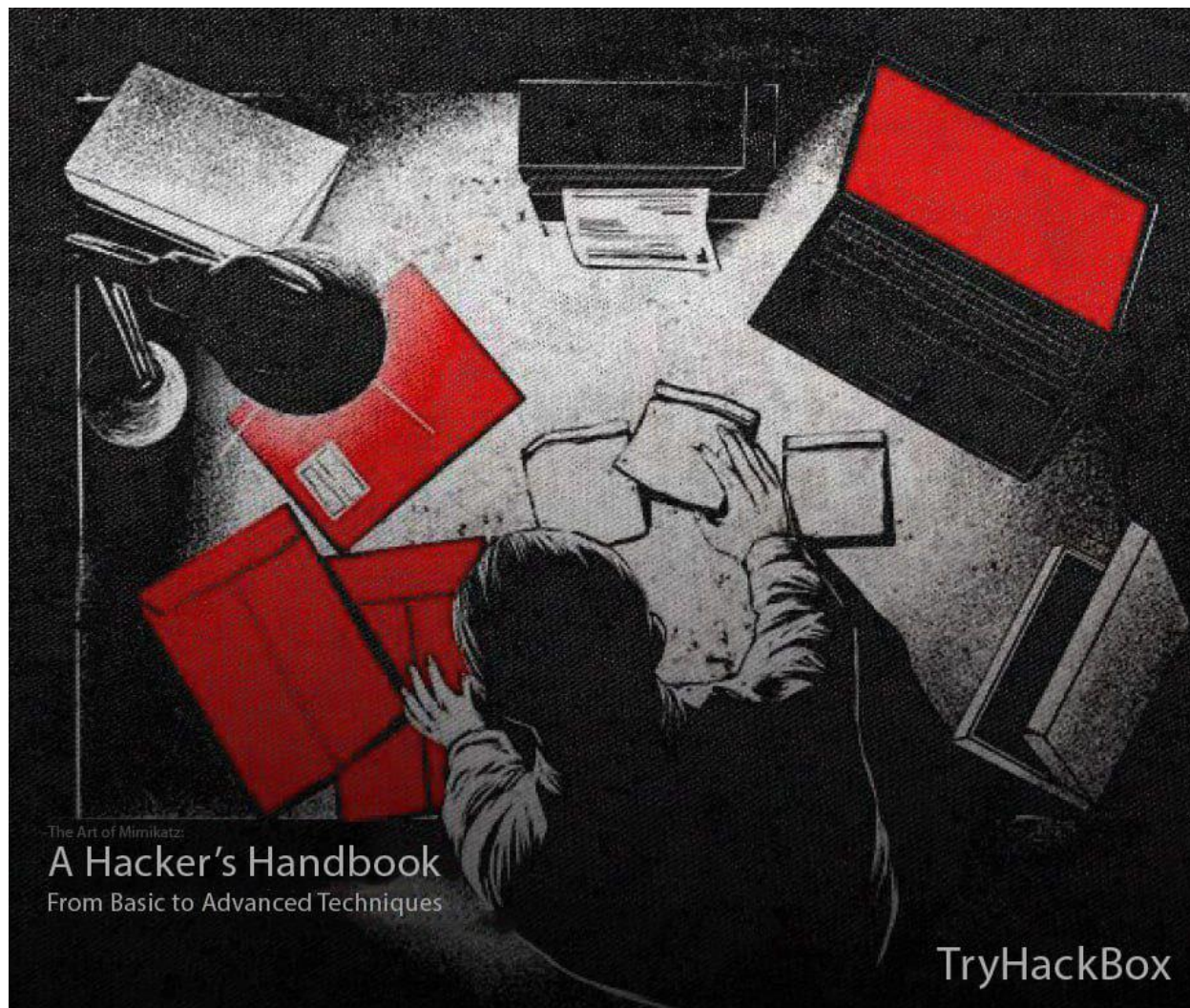


آشنایی مقدماتی با Mimikatz



تهیه شده توسط : کاوه

فهرست :

Mimikatz چیست ؟

آیا Mimikatz هنوز در ویندوز ۱۰ کار می کند؟

نسخه های رسمی Mimikatz .

چرا Mimikatz هنوز مؤثر است؟

آیا Mimikatz هنوز در ویندوز ۱۰ کار می کند؟

تاریخچه کوتاه Mimikatz و ویندوز .

چرا Mimikatz هنوز کار می کند؟

قابلیت های کلیدی Mimikatz .

چرا Mimikatz خطرناک است؟

Mimikatz چقدر امروزه مورد استفاده قرار می گیرد؟

نمونه هایی از حملات واقعی که از Mimikatz استفاده کردن.

لیست MITRE و Mimikatz .

چرا Mimikatz اینقدر محبوب است؟

گروه های تهدید و استفاده از Mimikatz

گروه Cobalt و استفاده از Cobalt Strike

آیا Mimikatz قادر به عبور از نرم افزارهای امنیتی Endpoint است؟

Mimikatz چیست ؟

Mimikatz یک ابزار قدرتمند است که هم توسط هکرها و هم توسط متخصصان امنیتی برای استخراج اطلاعات مهم مثل پسوردها و اطلاعات ورود به سیستم‌ها از حافظه کامپیوتر استفاده می‌شود. این ابزار معمولاً برای نفوذ به شبکه‌ها، سیستم‌ها یا برنامه‌ها و انجام کارهای مخرب مثل دسترسی به قسمت‌های حساس سیستم یا Lateral Movement در شبکه به کار می‌رود.

توجه: نسخه Mimikatz که در Metasploit وجود دارد، نسخه ۱.۰ است. اما سازنده این ابزار، Benjamin Delpy، نسخه ۲.۰ آن را به صورت جداگانه روی سایت خود منتشر کرده است. این موضوع مهم است چون بسیاری از دستورات و روش‌های استفاده از Mimikatz در نسخه ۲.۰ تغییر کرده‌اند.

Mimikatz رو می‌شه به روش‌های مختلفی استفاده کرد که بستگی به هدف شخص استفاده‌کننده داره. مثلاً می‌شه ازش برای کارهای زیر استفاده کرد:

۱. استخراج پسوردها و اعتبارنامه‌ها از حافظه سیستم

- توضیحات Mimikatz: می‌تواند پسوردها و اعتبارنامه‌ها را از حافظه سیستم استخراج کند.
- هدف مهاجم: دسترسی غیرمجاز به شبکه‌ها، سیستم‌ها یا برنامه‌ها.

۲. دور زدن مکانیزم‌های احراز هویت

- توضیحات Mimikatz: می‌تواند با سرقت اعتبارنامه‌ها، مکانیزم‌های احراز هویت مانند احراز هویت چندعاملی (Multi-Factor Authentication) را دور بزند.
- هدف مهاجم: استفاده از اعتبارنامه‌های سرقت‌شده برای دسترسی به سیستم‌ها.

۳. افزایش دسترسی (Privilege Escalation)

- توضیحات Mimikatz: می‌تواند دسترسی‌های یک کاربر معمولی را به سطح مدیر (Admin) ارتقا دهد.
 - هدف مهاجم: دسترسی به داده‌های حساس یا انجام اقدامات مخرب دیگر.
-

۴. حرکت جانبی در شبکه (Lateral Movement)

- توضیحات Mimikatz: می‌تواند به مهاجم اجازه دهد تا در شبکه Lateral Movement کند و به سیستم‌ها یا شبکه‌های اضافی دسترسی پیدا کند.
- هدف مهاجم: گسترش دسترسی در شبکه و کنترل سیستم‌های بیشتر.

نسخه‌های رسمی Mimikatz :

نسخه‌های رسمی Mimikatz هنوز هم توی سایت GitHub نگهداری می‌شن. علاوه بر این، Mimikatz توی چندتا ابزار و فریم‌ورک معروف که بعد از نفوذ به سیستم استفاده می‌شن (Post-Exploitation) هم قرار داده شده. مثلاً توی این ابزارها می‌تونید Mimikatz رو پیدا کنید:

- Metasploit
- Cobalt Strike
- Empire
- PowerSploit

- و ابزارهای مشابه

چرا Mimikatz هنوز مؤثر است؟

1. سازگاری با سیستم‌های جدید Mimikatz: به‌طور مداوم به‌روزرسانی می‌شود تا با سیستم‌عامل‌ها و پروتکل‌های جدید سازگار باشد.
۲. استفاده گسترده: این ابزار در بسیاری از فریم‌ورک‌های تست نفوذ و حملات سایبری گنجانده شده است.
۳. انعطاف‌پذیری Mimikatz: می‌تواند برای اهداف مختلف، از استخراج اعتبارنامه‌ها تا Lateral Movement در شبکه، استفاده شود.

Mimikatz از چندین ماژول (قطعه کد) تشکیل شده که هر کدام برای یه کار خاص یا یه نوع حمله طراحی شدن. بعضی از ماژول‌های مهم و پرکاربردش ایناست:

۱. ماژول Crypto

- توضیحات: این ماژول برای دستکاری توابع CryptoAPI استفاده می‌شود.
- کاربردها:
 - تقلید توکن‌ها (Token Impersonation): اجازه می‌دهد مهاجم به جای کاربر دیگری عمل کند.
 - اصلاح (Patching) توابع قدیمی CryptoAPI: برای دور زدن مکانیزم‌های امنیتی قدیمی.

۲. ماژول Kerberos

- توضیحات: این ماژول از طریق **Microsoft Kerberos API** مکان ایجاد بلیط‌های طلایی (Golden Tickets) را فراهم می‌کند.
- کاربردها:
 - ایجاد بلیط‌های جعلی برای دسترسی طولانی‌مدت به سیستم‌ها.

۳. ماژول Lsadbump

- توضیحات: این ماژول برای دستکاری پایگاه داده **SAM** (Security Account Manager) استفاده می‌شود.
- کاربردها:
 - دسترسی به پسوردها از طریق **LM Hash** یا **NTLM**.
 - کاربرد روی سیستم‌های زنده یا نسخه‌های پشتیبان‌گیری‌شده (Offline) از hive های SAM .

۴. ماژول Process

- توضیحات: این ماژول پروسس‌های در حال اجرا را لیست می‌کند.
- کاربردها:
 - مفید برای شناسایی پروسس‌ها و انجام **Pivot** در شبکه.

۵. ماژول Sekurlsa

- توضیحات: این ماژول برای استخراج داده‌ها از **LSASS** (Local Security Authority Subsystem Service) استفاده می‌شود.
- کاربردها:
 - استخراج بلیط‌ها (Tickets) ، پین‌کدها، کلیدها و پسوردها از حافظه.

۶. ماژول Standard

- توضیحات: این ماژول اصلی Mimikatz است و دستورات پایه و عملیات اصلی را مدیریت می‌کند.
 - کاربردها:
 - اجرای دستورات اصلی و مدیریت کلی ابزار.
-

۷. ماژول Token

- توضیحات: این ماژول برای کشف و دستکاری محدود توکن‌ها (Tokens) استفاده می‌شود.
- کاربردها:
 - شناسایی توکن‌ها و تغییر محدود آن‌ها.

آیا Mimikatz هنوز در ویندوز ۱۰ کار می‌کند؟

آره، Mimikatz هنوز هم کار می‌کند. مایکروسافت تلاش کرده تا با آپدیت‌ها و پیچ‌های امنیتی، کارایی این ابزار رو محدود کنه، اما این تلاش‌ها معمولاً موقتی و بی‌نتیجه بودن Mimikatz. مدام در حال توسعه و به‌روزرسانی‌ست و همیشه راهی پیدا می‌کنه تا از این پیچ‌ها عبور کنه و به کارش ادامه بده. یعنی هرچی مایکروسافت سعی می‌کنه جلوش رو بگیره، سازنده‌های Mimikatz یه راهی برای دور زدنش پیدا می‌کنن!

تاریخچه کوتاه Mimikatz و ویندوز:

- اولین تمرکز روی WDigest :
در ابتدا، Mimikatz روی یه نقطه ضعف در ویندوز به نام WDigest تمرکز کرده بود. قبل از سال ۲۰۱۳، ویندوز پسوردهای رمزنگاری‌شده رو به همراه کلید رمزگشایی‌شان در حافظه سیستم نگه می‌داشت Mimikatz. این پروسس رو ساده کرد و با استخراج این اطلاعات از حافظه، پسوردها و اطلاعات لاگین رو لو می‌داد.
- به‌روزرسانی‌های مایکروسافت:
با گذشت زمان، مایکروسافت متوجه این مشکل شد و تغییراتی در ویندوز ایجاد کرد تا جلوی این نوع حملات رو بگیره. اما Mimikatz همیشه خودش رو به‌روز کرده تا با این تغییرات سازگار بشه و همچنان کار کنه.
- رفع مشکلات بعد از ویندوز ۱۰ نسخه ۱۸۰۹:
مثلاً بعد از آپدیت ویندوز ۱۰ نسخه ۱۸۰۹، بعضی از قابلیت‌های Mimikatz (مثل ماژول sekurlsa::logonpasswords) از کار افتاده بود. اما توسعه‌دهنده‌های Mimikatz این مشکلات رو برطرف کردن و دوباره این ابزار رو فعال و قابل استفاده کردن.

خلاصه اینکه، Mimikatz یه ابزاریه که همیشه خودش رو با تغییرات ویندوز تطبیق داده و هنوز هم می‌تونه از ضعف‌های سیستم‌عامل سوءاستفاده کنه. مایکروسافت سعی کرده جلوش رو بگیره، اما Mimikatz همیشه یه قدم جلوتر بوده!

چرا Mimikatz هنوز کار می‌کند؟

۱. توسعه مداوم Mimikatz: به‌طور مداوم به‌روزرسانی می‌شود تا با تغییرات سیستم‌عامل ویندوز سازگار بماند.
۲. انعطاف‌پذیری: این ابزار از روش‌های مختلفی برای استخراج اعتبارنامه‌ها استفاده می‌کند و به راحتی خود را با تغییرات تطبیق می‌دهد.
۳. سوءاستفاده از آسیب‌پذیری‌های جدید: حتی با وجود وصله‌های امنیتی، آسیب‌پذیری‌های جدیدی کشف می‌شوند که Mimikatz از آن‌ها استفاده می‌کند.

```
.#####. mimikatz 2.2.0 (x64) #18362 Aug 14 2019 01:31:47
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 176409 (00000000:0002b119)
Session : Interactive from 1
User Name : sphil
Domain : SPHIL2AB1
Logon Server : SPHIL2AB1
Logon Time : 11/4/2019 2:45:19 PM
SID : S-1-5-21-3123691167-3462951650-3668972122-1000

msv :
[00000003] Primary
* Username : sphil
* Domain : SPHIL2AB1
* NTLM : d3b4230029c4a099823fd08451c14194
* SHA1 : 6d99a0126dd45d142f92d81d8bac7eb4ed458af9
tspkg :
wdigest :
* Username : sphil
* Domain : SPHIL2AB1
```

Mimikatz از هر دو معماری ۶۴ بیتی (x64) و ۳۲ بیتی (x86) پشتیبانی می‌کند و برای هر کدام نسخه‌های جداگانه‌ای ارائه شده است. یکی از دلایل خطرناک بودن Mimikatz، توانایی آن در بارگذاری DLL در حافظه است. این قابلیت به مهاجمان اجازه می‌دهد بدون نیاز به نوشتن فایل‌ها روی دیسک، حملات خود را انجام دهند.

قابلیت‌های کلیدی Mimikatz :

۱. پشتیبانی از هر دو معماری x64 و x86:

- Mimikatz برای سیستم‌های ۶۴ بیتی و ۳۲ بیتی به صورت جداگانه کامپایل شده است.

- این ویژگی باعث می‌شود که Mimikatz روی طیف وسیعی از سیستم‌ها قابل اجرا باشد.

۲. بارگذاری DLL در حافظه:

- Mimikatz می‌تواند DLL خود را به صورت (بدون نیاز به ذخیره‌سازی روی دیسک) در حافظه بارگذاری کند.
- این قابلیت باعث می‌شود که تشخیص حمله توسط ابزارهای امنیتی سنتی (مانند آنتی‌ویروس‌ها) دشوارتر شود.

۳. استفاده با PowerShell (Invoke-Mimikatz):

- Mimikatz می‌تواند از طریق PowerShell و اسکریپت‌هایی مانند **Invoke-Mimikatz** اجرا شود.
- این روش به مهاجمان اجازه می‌دهد بدون نیاز به ذخیره‌سازی فایل‌های مخرب روی دیسک، حملات خود را انجام دهند.

۴. حملات بدون تماس با دیسک (Fileless Attacks):

- با ترکیب Mimikatz و PowerShell، مهاجمان می‌توانند حملات بدون تماس با دیسک انجام دهند.
- این نوع حملات به دلیل عدم وجود ردپای فایل‌های مخرب، تشخیص و مقابله با آن‌ها را دشوارتر می‌کند.

چرا Mimikatz خطرناک است؟

- عدم نیاز به ذخیره‌سازی روی دیسک: بارگذاری DLL و استفاده از PowerShell باعث می‌شود که Mimikatz به راحتی توسط ابزارهای امنیتی سنتی شناسایی نشود.
- انعطاف‌پذیری بالا: Mimikatz از روش‌های مختلفی برای استخراج اعتبارنامه‌ها استفاده می‌کند و به راحتی خود را با تغییرات سیستم عامل تطبیق می‌دهد.
- استفاده گسترده در حملات پیشرفته: Mimikatz در بسیاری از حملات پیشرفته مانند **Pass-the-Hash**، **Golden Ticket** و **Lateral Movement** استفاده می‌شود.

Mimikatz چقدر امروزه مورد استفاده قرار می‌گیرد؟

امروزه Mimikatz هنوز هم یکی از ابزارهای خیلی محبوب و پر استفاده در حملات سایبری. خیلی از بدافزارها و تهدیدهای بزرگ یا مستقیماً از Mimikatz استفاده می‌کنن یا از ابزارهایی شبیه به اون برای دزدیدن پسوردها و حرکت تو شبکه‌ها بهره می‌برن. مثلاً بدافزارهای معروفی مثل NotPetya و BadRabbit از Mimikatz برای دزدیدن اطلاعات لاگین استفاده کردن. حتی بدافزار جدیدتری مثل Trickbot هم از یه نسخه مشابه Mimikatz برای دزدیدن پسوردها و پخش شدن تو شبکه‌ها استفاده می‌کنه.

خلاصه اینکه، Mimikatz هنوز هم به ابزار خطرناک و پرکاربرده که هکرها از آن برای نفوذ به سیستم‌ها و شبکه‌ها استفاده می‌کنند.

نمونه‌هایی از حملات واقعی که از Mimikatz استفاده کردند:

۱. BadRabbit، NotPetya :

این بدافزارهای معروف از Mimikatz برای دزدیدن پسوردها و پخش شدن تو شبکه‌های قربانی استفاده کردند. یعنی بعد از نفوذ به یک سیستم، با Mimikatz پسوردها رو دزدیدن و به سیستم‌های دیگر هم دسترسی پیدا کردند.

۲. Trickbot :

این بدافزار هم از یک نسخه تغییر داده شده Mimikatz برای دزدیدن پسوردها و حرکت تو شبکه استفاده می‌کنه. Trickbot با این کار می‌تونه به سیستم‌های بیشتری نفوذ کنه و خرابکاری‌های بیشتری انجام بده.

۳. گروه‌های هکری حرفه‌ای (APT Groups) :

خیلی از گروه‌های هکری حرفه‌ای از Mimikatz تو حملاتشون استفاده می‌کنند. بعضی از این گروه‌ها عبارتند از:

- Oilrig
- APT28 (Fancy Bear)
- Lazarus
- Cobalt Group
- Turla
- Carbanak
- FIN6
- APT21

این گروه‌ها معمولاً هدف‌های بزرگ مثل سازمان‌های دولتی یا شرکت‌های بین‌المللی رو هدف قرار می‌دن و از Mimikatz برای دزدیدن اطلاعات حساس و نفوذ به سیستم‌ها استفاده می‌کنند.

خلاصه اینکه، Mimikatz به ابزار محبوبه که هم هکرها معمولی و هم گروه‌های حرفه‌ای از آن برای انجام حملات خطرناک استفاده می‌کنند.

لیست MITRE و Mimikatz :

به زبان ساده، MITRE ATT&CK به لیست بزرگه که تکنیک‌ها و ابزارهایی که هکرها استفاده می‌کنند رو جمع‌آوری کرده. تو این لیست، Mimikatz به عنوان یک ابزار مهم و پرستفاده شناخته شده که گروه‌های هکری حرفه‌ای از آن برای نفوذ به سیستم‌ها و دزدیدن اطلاعات استفاده می‌کنند. پس Mimikatz نه تنها یک ابزار ساده نیست، بلکه یک سلاح قویه که هکرها بهش اعتماد دارند!

چرا Mimikatz اینقدر محبوب است؟

۱. کارایی بالا Mimikatz: می‌تواند اعتبارنامه‌ها را به راحتی از حافظه سیستم استخراج کند.
۲. انعطاف‌پذیری: این ابزار می‌تواند برای اهداف مختلف، از سرقت اعتبارنامه‌ها تا Lateral Movement در شبکه، استفاده شود.
۳. توسعه مداوم Mimikatz: به‌طور مداوم به‌روزرسانی می‌شود تا با تغییرات سیستم‌عامل و وصله‌های امنیتی سازگار بماند.

SOFTWARE		Techniques Used			ATT&CK® Navigator Layers
Mimikatz		Domain	ID	Name	Use
MimiPenguin		Enterprise	T1134	.005 Access Token Manipulation: SID-History Injection	Mimikatz's <code>ntsc::ntsssl</code> module can append any SID or user/group account to a user's SID-History. Mimikatz also utilizes <i>SID-History injection</i> to expand the scope of other components such as generated Kerberos Golden Tickets and DCSync beyond a single domain. ^{[2][3]}
Miner-C		Enterprise	T1098	Account Manipulation	The Mimikatz credential dumper has been extended to include Skeleton Key domain controller authentication bypass functionality. The <code>LSADUMP::ChangeNTLM</code> and <code>LSADUMP::SehNTLM</code> modules can also manipulate the password hash of an account without knowing the clear text value. ^{[2][4]}
MiniDuke		Enterprise	T1547	.005 Boot or Logon Autostart Execution: Security Support Provider	The Mimikatz credential dumper contains an implementation of an SSP. ^[5]
MirageFox		Enterprise	T1555	Credentials from Password Stores	Mimikatz performs credential dumping to obtain account and password information useful in gaining access to additional systems and enterprise network resources. It contains functionality to acquire information about credentials in many ways, including from the credential vault and DPAPI. ^{[1][3][6][7][8]}
Mis-Type				.003 Credentials from Web Browsers	Mimikatz performs credential dumping to obtain account and password information useful in gaining access to additional systems and enterprise network resources. It contains functionality to acquire information about credentials in many ways, including from DPAPI. ^{[1][3][6][7]}
Misdat				.004 Windows Credential Manager	Mimikatz contains functionality to acquire credentials from the Windows Credential Manager. ^[6]
Mispadu		Enterprise	T1003	.001 OS Credential Dumping: LSASS Memory	Mimikatz performs credential dumping to obtain account and password information useful in gaining access to additional systems and enterprise network resources. It contains functionality to acquire information about credentials in many ways, including from the LSASS Memory. ^{[1][3][4][7]}
Mivast				.002 OS Credential Dumping:	Mimikatz performs credential dumping to obtain account and password information useful in
MobileOrder					
MoleNet					
Moneybird					
Mongall					
Monokle					
MoonWind					
More_eggs					
Mori					
Mosquito					
Multilayer Wiper					
MURKYTOP					
Mythic					
...					

Groups That Use This Software		
ID	Name	References
G0050	APT32	[1][2][3][4]
G0016	APT29	[1][2][3][4][5][6][7][8]
G1006	Earth Lusca	[21]
G0046	FIN7	[22]
G0079	DarkHydruS	[23][24]
G0092	TA505	[25]
G1030	Agrius	Agrius used Mimikatz to dump credentials from LSASS memory.[26]
G0060	BRONZE BUTLER	[27][28][29]
G0034	Sandworm Team	[30]
G0064	APT33	[31]
G1024	Akira	[32]
G0131	Tonto Team	[33]
G0087	APT39	[34][35][36][37]
G0108	Blue Mockingbird	[38]
G0080	Cobalt Group	[39][40][41]
G0027	Threat Group-3390	Threat Group-3390 has used a modified version of Mimikatz called Wrapikatz.[42][43][44][45][46]

گروه‌های تهدید و استفاده از Mimikatz :

همه این گروه‌ها روش‌های خاص خود را برای فراخوانی یا تزریق Mimikatz توسعه می‌دهند تا موفقیت حمله را تضمین کنند و از کنترل‌های امنیتی نقطه پایانی (Endpoint Security Controls) که ممکن است مانع شوند، عبور کنند.

گروه Cobalt و استفاده از Cobalt Strike :

گروه **Cobalt** به‌خصوص به دلیل استفاده از ابزار **Cobalt Strike** شناخته شده است. یک ابزار همکاری‌محور برای تیم‌های قرمز (Red Team) و شبیه‌سازی مهاجمان (Adversary Simulation) است. همان‌طور که قبلاً اشاره شد، Mimikatz به‌عنوان یکی از قابلیت‌های اصلی در Cobalt Strike گنجانده شده است.

نکته نگران‌کننده‌تر این است که Cobalt Strike این توانایی را دارد که Mimikatz را مستقیماً در حافظه و از طریق هر پروسس مناسب (Context-Appropriate Process) که **Beacon Payload** در آن تزریق شده است، فراخوانی کند. این نوع حمله بدون تماس با دیسک (**Fileless**) نه تنها از خواندن/نوشتن روی دیسک جلوگیری می‌کند، بلکه می‌تواند بسیاری از محصولات امنیتی مدرن و "نسل بعدی" را که قادر به نظارت دقیق بر رویدادها/فعالیت‌های خاص سیستم‌عامل نیستند، دور بزند.

مثال : Mimikatz و Cobalt Strike

- **Beacon Payload :** Cobalt Strike از Beacon برای ایجاد یک کانال ارتباطی مخفی با سیستم قربانی استفاده می کند.
- **تزریق Mimikatz در حافظه :** Beacon می تواند Mimikatz را مستقیماً در حافظه فراخوانی کند و از آن برای سرقت اعتبارنامه ها یا انجام سایر فعالیت های مخرب استفاده کند.

آیا Mimikatz قادر به عبور از نرم افزارهای امنیتی Endpoint است؟

اگر سیستم عامل نتواند در برابر Mimikatz مقاومت کند، آیا راهکارهای امنیتی ارائه شده توسط شرکت های دیگر می توانند از سیستم ها در برابر حملات Mimikatz محافظت کنند؟ پاسخ به این سوال به شرایط بستگی دارد Mimikatz . برای کنترل های امنیتی سنتی Endpoint ، مانند آنتی ویروس های قدیمی و حتی برخی ابزارهای به اصطلاح "نسل بعدی"، یک چالش بزرگ محسوب می شود. همان طور که قبلاً گفته شد، اگر این ابزارها رفتارهای حافظه یا رویدادهای خاص سیستم عامل را زیر نظر نگیرند، ممکن است اصلاً متوجه حمله نشوند یا نتوانند از آن جلوگیری کنند.

علاوه بر این، Mimikatz برای اجرا نیاز به دسترسی Administrator یا SYSTEM روی سیستم هدف دارد. این بدان معناست که مهاجمان باید کد خود را در یک پروسس با سطح دسترسی مناسب تزریق کنند یا راهی برای افزایش دسترسی (Privilege Escalation) پیدا کنند که بتواند برخی از نرم افزارهای آنتی ویروس را دور بزند، به خصوص اگر این نرم افزارها تمایل به Whitelisting پروسس های "مطمئن" سیستم عامل داشته باشند.

جمع بندی

حقیقت این است که Mimikatz تقریباً به طور فراگیری در ابزارهای مهاجمان امروزی جای گرفته است. این ابزار در حملات با هر سطحی از پیچیدگی و علیه انواع مختلف اهداف مورد استفاده قرار می گیرد. با وجود گذشت بیش از ۱۲ سال از زمان توسعه آن، Mimikatz نه تنها همچنان کارآمد است، بلکه به طور مداوم بهبود می یابد و فناوری های قدیمی و منسوخ محافظت از نقاط پایانی را تحت فشار قرار می دهد.

<https://github.com/Off3nsivePwn/>

<https://www.x.com/kavehxnet>

<https://t.me/KavehAPT>

<https://t.me/TryHackBox>

