باسمه تعالی

عنوان مستند

حمله process Doppelganging

فهرست مطالب

1 مقدمه

یک تیم از محققان امنیتی تکنیکی را کشف کرده اند که به ویروس نویسان کمک می کند تا تمامی آنتی‌ویروس های مدرن و ابزارهای ردیابی سیستم را دور بزنند.

Process Doppelgänging، تکنیک تزریق کد [1] است که از فایل های اصلی ویندوز استفاده می کند و فرآیندهای اجرایی ویندوز را به صورت غیر قانونی اجرا می کند.

Tal Liberman و Eugene Kogan محققان امنیتی گروه ensilo کاشفان حمله Process Doppelgänging هستند، که یافته های خود را در کنفرانس Black Hat 2017 لندن ارائه دادند.

2 جزئیات این حمله

2–1 حوزه فعالیت Process Doppelgänging

حمله ی Process Doppelgänging برروی تمامی ورژن های ویندوز، از ویندوز ویستا تا ویندوز 10 کار می‌کند.

Tal Liberman رهبر تیم تحقیقاتی ensilo ادعا می کند که این تکنیک دور زدن آنتی ویروس، شبیه به حمله Process Hollowing که یک متد جدید برای دور زدن محصولات امنیتی ارائه داده است می باشد.

در حمله Process Hollowing نفوذگر حافظه یک فرآیند قانونی را با کد مخرب جابجا می کند و کد های آن را به جای فرآیند اصلی اجرا می کند.

از زمانی که آنتی ویروس ها و محصولات امنیتی مدرن به روز رسانی شده اند و می توانند حملات Process Hollowing را دفع کنند، استفاده از تکنیک این نوع حملات دیگر ارزشمند نیست. از سوی دیگر، Process Doppelgänging یک رویکرد کاملا متفاوت نسبت به Process Hollowing دارد. این تکنیک جدید با سوءاستفاده از Windows NTFS Transactions و استفاده نامناسب از loader فرآیند های ویندوز که مختص ویندوز XP بود و در تمام نسخه های بعدی ویندوز قابلیت اجرا دارد پیاده سازی شده است.

[1] Code injection

2–2 نحوه حمله Process Doppelgänging

قبل از اینکه بیشتر در مورد نحوه این حمله تزریق کد صحبت کنیم، ابتدا باید درمورد تراکنش های NTFS و اینکه نفوذگر تا چقدر می تواند از آنها برای اقدام های خرابکارانه استفاده کند صحبت کنیم.

NTFS transaction یک ویژگی ویندوز است که ویژگی اتمیک بودن را برای فایل های NTFS سیستم به ارمغان می آورد و به فایل ها و دایرکتوری ها اجازه ساخته شدن، ویرایش، حذف و ... می دهد.

NTFS Transaction یک فضای ایزوله است که به توسعه دهنده های برنامه های ویندوزی اجازه می دهد یک فایل خروجی برای تراکنش های سیستم ایجاد و فعالیت هایی که به صورت کامل انجام شده اند یا شکست خورده اند را مشخص کند.

Process Doppelgänging یک حمله بدون فایل است که در چهار مرحله عمده عمل می‌کند. این مراحل در ادامه ذکر شده‌اند:

Transact: فرآیند مجاز و قابل اجرای سیستمی را در NTFS Transaction پردازش می‌کند سپس آن را با یک فایل مخرب بازنویسی می‌کند.

Load: از فایل اصلاح شده در قسمت transact یا همان کد مخرب یک بخش حافظه ایجاد می‌کند.

RollBack: عقبگرد تراکنش ها (در صورتی که تراکنش شکست بخورد) انجام می دهد. در واقع در این مرحله از روی قصد تراکنش را ناموفق می کنیم که نتیجه ی این کار باعث حذف تمام تغییرات مجاز اجرایی می شود.

Animate: از نسخه قدیمی loader فرآیند های ویندوز برای ساخت یک فرآیند که قبلا در بخش حافظه ایجاد شده است استفاده می کند که در واقع مخرب است و هرگز در دیسک ذخیره نمی شود. این کار فایل مخرب را برای اکثر ابزارهای ذخیره سازی غیرقابل تشخیص می کند.

بیشتر آنتی‌ویروس ها قابلیت تشخیص Process Doppelgänging را ندارند.

Product	Tested OS	Result
Windows Defender	Windows 10	Bypass
AVG Internet Security	Windows 10	Bypass
Bitdefender	Windows 10	Bypass
ESET NOD 32	Windows 10	Bypass
Qihoo 360	Windows 10	Bypass
Symantec Endpoint Protection	Windows 7 SP1	Bypass
McAfee VSE 8.8 Patch 6	Windows 7 SP1	Bypass
Kaspersky Endpoint Security 10	Windows 7 SP1	Bypass
Kaspersky Antivirus 18	Windows 7 SP1	Bypass
Symantec Endpoint Protection 14	Windows 7 SP1	Bypass
Panda	Windows 8.1	Bypass
Avast	Windows 8.1	Bypass

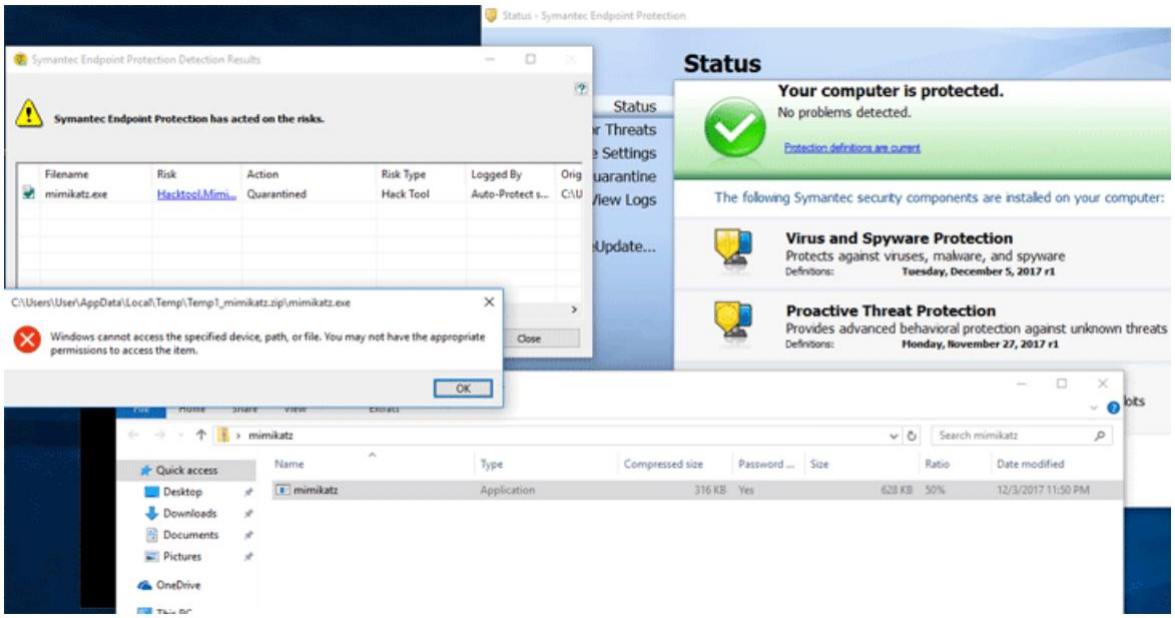
شکل1- آنتی ویروس هایی که با روش Process Doppelgänging قابل دور زدن هستند.

3 جزئیات ردیابی این حمله

Liberman ادعا کرده که طبق خبرهای هکرها، آنها این حملات را روی تمامی محصولات امنیتی مانند Kaspersk، Nod 32، Symantec و... پیاده سازی کردند.

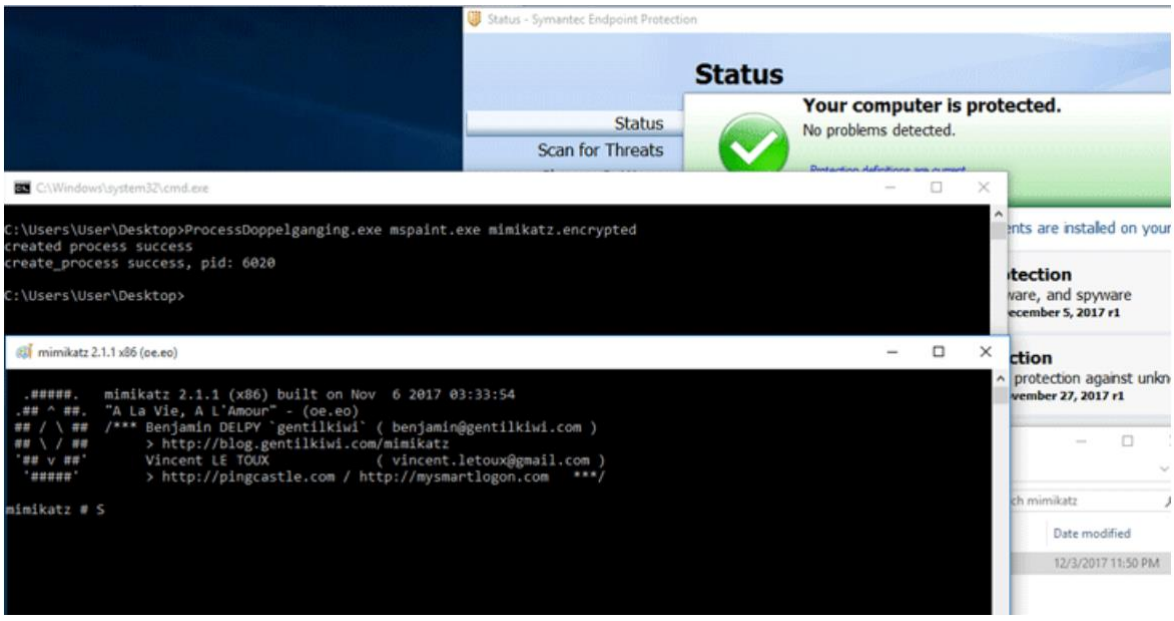
محققان امنیتی از Mimikatz که یک ابزار post-exploitation برای استخراج اطلاعات از سیستم های آسیب دیده است استفاده می کنند و با کمک Process Doppelgänging سعی می‌کند آنتی ویروس را دور بزنند.

همانطور که در شکل 2 می بینید هنگامی که محققان Mimikatz را برروی ویندوز اجرا می کنند، آنتی ویروس symantec بلافاصله این ابزار را تشخیص می دهد:



شکل 2 تشخیص ابزار mimikatz

با این حال زمانی که Mimikatz ، با کمک Process Doppelgänging اجرا شد آنتی ویروس توانایی تشخیص آن را نداشت. شکل 3، اجرای برنامه Mimikatz را پس از استفاده از روش Process Doppelgänging نشان می دهد.



شکل 3

Liberman مدعی است که Process Doppelgänging حتی روی آخرین نسخه های ویندوز 10 به جز نسخه های Windows 10 Redstone و Fall Creators Update (آپدیت های بهاری 2017 مایکروسافت) قابل اجرا شدن است. به علت یک اشکال متفاوت در این دو نسخه مایکروسافت، استفاده از Process Doppelgänging باعث BSOD (صفحه ی آبی مرگ) می شود که کامپیوترهای کاربران را دچار آسیب می‌کرد.

به طرز عجیبی این مشکل در آپدیت های بعدی ویندوز هم قابل مشاهده بود. به همین علت Process Doppelgänging بروی آخرین نسخه ویندوز 10 نیز قابل اجرا شدن است.

از آنتی ویروس ها انتظار می رود که در آپدیت های خود اقدامات لازم برای مقابله با این حمله را انجام دهند.

سورس کد نمونه برای این نوع حملات در آدرس های زیر آمده است، که فرد نفوذگر نسبت به حملات خود می تواند این کد ها را تغییردهد.

- https://github.com/hasherezade/process_doppelganging/commit/fd4856218cf4604b31e4982b5a71caeb25fb2b75
- https://gist.github.com/hfiref0x/a9911a0b70b473281c9da5daea9a177f

4 پیشگیری و پاک سازی

روش رسمی برای جلوگیری از این تکنیک دور زدن ضدویروس ها تاکنون معرفی نشده است، ولی رعایت موارد زیر توصیه می شود:

1. آنتی ویروس یا محصولات امنیتی بروز روی سیستم خود استفاده کنید.
2. نسخه ویندوز خود را به روز رسانی کنید و آخرین پچ های امنیتی را نصب کنید.
3. برنامه ها یا فایل های مورد نیاز خود را از منابع معتبر تهیه کنید.

5 منابع

- https://thehackernews.com/2017/12/malware-process-doppelganging.html
- https://www.bleepingcomputer.com/
- https://www.blackhat.com/
- http://securityaffairs.co/wordpress/66440/hacking/process-doppelganging-attack.html
- https://www.bleepingcomputer.com/
- https://www.youtube.com/watch?v=Cch8dvp836w