مـــروری بـــر روش‌هـــای

خودحفاظتی بدافزارها

شبکه گستر
شـرکت مهندسی شـبکه گسـتر

عنوان سند: مروری بر روش‌های خودحفاظتی بدافزارها

شناسه سند: SPT-A-۰۱۱۸-۰۱

تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر

تاریخ تهیه: دی ۱۳۹۵

نویسندگان حرفه‌ای بدافزار، وقت و انرژی زیادی را صرف نوشتن کدهای پیچیده‌ای می‌کنند که هدف آنها ماندگاری بیشتر بدافزار بر روی دستگاه قربانی است. رسیدن به این هدف مستلزم توانایی بدافزار در عبور از سد ابزارهای قرنطینه امن (Sandbox)، برنامه‌های ضدویروس و سیستم‌های تحلیلگر بدافزار است.

در سال‌های اخیر، امنیت دنیای فناوری اطلاعات شاهد پیشرفت‌های زیادی بوده و نرم‌افزارها و ابزارهای امنیت سایبری بسیار تواناتر از قبل شده‌اند. متقابلاً نویسندگان بدافزار نیز با رصد عملکرد ابزارها و سیستم‌های امنیتی همواره در حال خلق راه‌های جدید برای رخنه به سیستم‌ها و شبکه‌های کامپیوتری هستند. علاوه بر آن، کم نیستند کاربران و سازمان‌هایی که از ابزارهای ضدبدافزار ناکارامد و یا با تنظیمات ناصحیح استفاده می‌کنند. عواملی که می‌توانند راه ورود بدافزار را هموار کنند.

در این مقاله، به چند روش رایج مورد استفاده نویسندگان بدافزار برای عبور از سد ابزارهای حفاظتی شناسایی‌کننده بدافزار پرداخته شده است.

خودحفاظتی بدافزار

به طور کلی بدافزارها از سه مکانیزم زیر برای جلوگیری از شناسایی و تحلیل شدن توسط ابزارهای امنیتی بهره می‌گیرند:

- ضد ابزارهای امنیت[۱] – هدف از آن، جلوگیری از شناسایی شدن بدافزار توسط ضدویروس، دیواره آتش و سایر سیستم‌های حفاظتی کامپیوترها و شبکه‌ها است.
- ضد قرنطینه امن[۲] – هدف آن شناسایی سیستم‌های تحلیلگر خودکاری است که رفتار بدافزار را بررسی و گزارش می‌کنند.
- ضد تحلیلگر بدافزار[۳] – هدف آن گمراه نمودن و فریب متخصصان و سیستم‌های تحلیلگر است. برای مثال می‌توان به بکارگیری ابزارهای Packer یا ترفندهایی خاص به‌منظور ناتوان کردن برنامه‌های تحلیلگر عملکرد بدافزار، نظیر Process Explorer یا Wireshark از شناسایی بخش مخرب بدافزار اشاره کرد.

برخی تکنیک‌های بدافزارها نیز از تلفیقی از مکانیزم‌های فوق استفاده می‌کنند. برای نمونه، ممکن است بدافزار از ابزار RunPE – که پروسه دیگری از خود را در حافظه اجرا می‌کند - برای عبور از سد ضدویروس و فریب قرنطینه امن و تحلیلگر استفاده کند.

عبور از سد ابزارهای قرنطینه امن

قرنطینه‌های امن، ابزارهای مؤثری برای تحلیل رفتار فایل‌ها و شناسایی بدافزارها محسوب می‌شوند.

> "
> ابزارهای قرنطینه امن، ضمن جدا نگاه داشتن پروسه مورد بررسی با سایر نرم‌افزارهای در حال اجرا، عملکرد و رفتار آن را رصد می‌کنند.
> "

تحلیلگران بدافزار از ابزارهای قرنطینه امن برای بررسی پروسه‌های مشکوک استفاده می‌کنند. در سال‌های اخیر نیز برخی نرم‌افزارها و سخت‌افزارهای ضدبدافزار مجهز به ابزارهای قرنطینه امنی شده‌اند که به‌طور خودکار فایل‌های مشکوک و ناشناس را پویش می‌کنند.

اکثر ابزارهای قرنطینه امن مبتنی بر بسترهای مجازی‌سازی[۴] هستند.

بدیهی است در صورتی که ابزار قرنطینه امن، خود به‌درستی پیکربندی نشده باشد براحتی توسط بدافزار شناسایی می‌شود. در نتیجه آن نیز، بدافزار از اجرا شدن بر روی آن خودداری نموده و ابزار قرنطینه امن فایل بدافزار را پاک و غیرمخرب تشخیص می‌دهد.

---

[۱] Anti-security Tools
[۲] Anti-sandbox
[۳] Anti-analyst
[۴] Virtualization Environment

نویسندگان بدافزار از روش‌های زیر برای بررسی وجود قرنطینه امن استفاده می‌کنند:

- شناسایی نشانی MAC – بسترهای مجازی‌سازی نظیر VMware یا VirtualBox از نشانی‌های MAC اختصاصی استفاده می‌کنند. نشانی MAC معمولاً در مسیر زیر در محضرخانه[۵] ذخیره می‌شود:

  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0000\NetworkAddress

بررسی MAC می‌تواند از طریق رابط برنامه‌نویسی[۶] GetAdapterInfo نیز انجام شود.

```
DWORD GetAdaptersInfo(
          _Out_   PIP_ADAPTER_INFO pAdapterInfo,
          _Inout_ PULONG                   pOutBufLen
);
```

- شناسایی پروسه – برخی بدافزارها قادرند که فعال بودن پروسه‌اهی مرتبط با ابزارهای قرنطینه امن معروف را بر روی سیستم قربانی تشخیص دهند. برای مثال، پروسه‌هایی همچون VmwareService.exe به‌راحتی توسط رابط برنامه‌نویسی CreateToolHelp۳۲Snapshot قابل شناسایی هستند. بدافزار با استفاده از این رابط برنامه‌نویسی می‌تواند یک تصویر لحظه‌ای[۷] از پروسه‌های اجرا شده جاری تهیه کرده و سپس هر یک از پروسه‌ها را با استفاده از دو رابط کاربری Process۳۲Firstو Process۳۲Next فهرست کند.

```
HANDLE WINAPI CreateToolhelp32Snapshot(
          _In_ DWORD dwFlags,
          _In_ DWORD th32ProcessID
);

BOOL WINAPI Process32First(
          _In_    HANDLE           hSnapshot,
          _Inout_ LPPROCESSENTRY32 lppe
);

BOOL WINAPI Process32Next(
          _In_  HANDLE           hSnapshot,
          _Out_ LPPROCESSENTRY32 lppe
);
```

- شناسایی محضرخانه - بسترهای مجازی‌سازی کلیدهایی را در محضرخانه سیستم ایجاد می‌کنند که براحتی توسط بدافزارها قابل شناسایی هستند. برخی نمونه‌های آن عبارتند از:

  - “HARDWARE\\DEVICEMAP\\Scsi\\Scsi Port 0\\Scsi Bus 0\\Target Id 0\\Logical Unit Id 0”
  - “SOFTWARE\\VMware, Inc.\\VMware Tools”
  - “HARDWARE\\Description\\System”

---

[۵] Registry

[۶] Application Programming Interface – API

[۷] Snapshot

```
- “SOFTWARE\\Oracle\\VirtualBox Guest Additions”
- “SYSTEM\\ControlSet001\\Services\\Disk\\Enum”
- “HARDWARE\\ACPI\\DSDT\\VBOX__”
- “HARDWARE\\ACPI\\FADT\\VBOX__”
- “HARDWARE\\ACPI\\RSDT\\VBOX__”
- “SYSTEM\\ControlSet001\\Services\\VBoxGuest”
- “SYSTEM\\ControlSet001\\Services\\VBoxMouse”
- “SYSTEM\\ControlSet001\\Services\\VBoxService”
- “SYSTEM\\ControlSet001\\Services\\VBoxSF”
- “SYSTEM\\ControlSet001\\Services\\VBoxVideo”
```

- بررسی توابع هوک[۸]: هوک اساساً تکنیکی برای تغییر رفتار تابع داخلی یک سیستم عامل یا برنامه است. ابزارهای قرنطینه امن نیز از تکنیک‌های هوک برای تغییر رفتار در جریان رصد و بررسی فایل استفاده می‌کنند. برای مثال، با هوک شدن تابع DeleteFile، بدافزار اجرا شده در ابزار قرنطینه امن ناچار خواهد شد که یک فایل تحت رصد آن ابزار را حذف کرده و عملاً ماهیت خود را در زمان اجرا نمایان کند. این نوع توابع در محلی خاص در بخش هسته[۹] حافظه ذخیره می‌شوند.

بنابراین بدافزار قادر است که استفاده از هوک را با بررسی نشانی تابع فراخوانی شده شناسایی کند. برای مثال اگر نشانی تابع در هسته نباشد، می‌تواند نشانه‌ای از هوک شدن آن باشد.

بدافزار، همچنین می‌تواند از چند تکنیک پیشرفته برای شناسایی یک قرنطینه امن استفاده کند.

عبور از سد ضدویروس

اکثر ابزارهای ضدویروس از سه بخش زیر به‌منظور شناسایی بدافزار استفاده می‌کنند:

- شناسایی مبتنی بر امضاء[۱۰]
- پویشگر[۱۱]
- شناسایی مبتنی بر اکتشاف[۱۲]

بدافزار نیز می‌تواند با استفاده از روش‌های زیر اقدام به عبور از سد بخش‌های مذکور کند:

- فرار از بخش شناسایی مبتنی بر امضاء با تغییر اثر انگشت[۱۳] فایل مخرب ممکن می‌شود. کاری که انجام آن به آسانی تغییر تنها یک بایت فایل است.
- عبور از سد پویشگر می‌تواند از طریق ایجاد یک فایل بزرگ برای فریب برابرساز[۱۴] انجام شود.
- عبور از بخش اکتشافی ضدویروس هر چند دشوارتر اما در هر حال با هوک کردن توابع امکان‌پذیر است.

---

[۸] Hook
[۹] Kernel
[۱۰] Signature
[۱۱] Scanner
[۱۲] Heuristic
[۱۳] Hash
[۱۴] Emulator

راه دیگر برای فرار از سد ابزارهای ضدویروس غیرفعال کردن ضدویروس یا استثناء نمودن پروسه مخرب بدافزار توسط پروسه‌ای مجاز است.

شایان ذکر است که شناسایی نمودن بدافزارها چندشکلی[۱۵] توسط ابزارهای ضدویروس به‌مراتب دشوارتر است.

ضد اشکال‌یابی

تحلیلگران بدافزار از ابزارهای اشکال‌یاب[۱۶] به‌منظور تحلیل عملکرد بدافزار و در حقیقت مهندسی معکوس آن بهره می‌گیرند.

> اشکال‌یاب ابزاری کمکی برای بررسی عملکرد برنامه در جریان ایجاد، آزمایش، اجرا، تغییر و اشکال‌یابی برنامه است.

بدافزار می‌تواند حضور ابزار اشکال‌یاب را بر روی سیستم از طریق توابع زیر شناسایی کند.

- IsDebuggerPresent – در صورتی که پروسه در حالت اشکال‌یابی اجرا نشده باشد خروجی این تابع صفر و در غیر این صورت عددی غیر صفر خواهد بود.

```
BOOL WINAPI IsDebuggerPresent(void);
```

- FindWindow – این تابع می‌تواند برنامه‌های فعال شده بر روی سیستم را بر اساس نام یا کلاس[۱۷] آنها شناسایی کند. همچنین بدافزار قادر است با استفاده از این تابع حضور ابزارهای تحلیلگری همچون Wireshark و Process Explorer را نیز تشخیص دهد.

```
HWND WINAPI FindWindow(
          _In_opt_ LPCTSTR lpClassName,
          _In_opt_ LPCTSTR lpWindowName
);
```

- CsrGetProcessId – این تابع می‌تواند شناسه پروسه سیستمی csrss.exe را پیدا کند. به‌صورت پیش‌فرض، سطح دسترسی SeDebugPrivilege پروسه‌ها در حالت غیرفعال قرار دارد. با این حال زمانی که پروسه توسط یک اشکال‌یاب (نظیر OllyDbg یا WinDbg) اجرا می‌شود، بخش SeDebugPrivilege آن در حالت فعال قرار می‌گیرد. اگر پروسه بتواند csrss.exe را باز کند بدان معناست که پروسه حق دسترسی SeDebugPrivilege را داراست و بنابراین می‌توان این طور نتیجه‌گیری کرد که پروسه در حالت اشکال‌یابی اجرا شده است.

---

[۱۵] Polymorphic Codes
[۱۶] Debugger
[۱۷] Class

ضد دیس‌اسمبلی

ضد دیس‌اسمبلی[۱۸] تکنیک دیگری برای جلوگیری از نمایان شدن عملکرد مخرب بدافزار از طریق مهندسی معکوس کد آن است.

> دیس‌اسمبلر[۱۹] برنامه‌ای کامپیوتری است که زبان ماشین را به زبان اسمبلی تبدیل می‌کند؛ از این برنامه‌ها جهت مهندسی معکوس کد برنامه‌ها استفاده می‌شود.

راه‌های مختلفی برای دشوار نمودن کار تحلیلگر بدافزاری که از دیس‌اسمبلر برای بررسی کد استفاده می‌کند فراهم است:

- گمراه‌سازی فراخوانی رابط‌های کاربری خاص – در صورت استفاده بدافزار از این روش، فراخوانی رابط‌های کاربری خاص بدون استفاده از نام آنها انجام می‌شود. در نتیجه آن، تحلیلگر می‌بایست آن را مهندسی معکوس کرده تا متوجه عملکرد واقعی رابط کاربری شود.
- تزریق کد نامرتبط – نویسنده بدافزار می‌تواند کد نامرتبط را به‌نحوی در بدافزار درج کند که سبب گمراه شدن تحلیلگر و اتلاف وقت او برای شناسایی عملکرد واقعی بدافزار شود. برای مثال، در کدهای فایل دانلود کننده باج‌افزار Cerber چندین متغیر[۲۰] تعریف شده که در بخش‌های مخرب فایل از آنها استفاده نشده و هدف آنها صرفاً گمراه نمودن تحلیلگر است.

[۱۸] Anti-Disassembly
[۱۹] Disassembler
[۲۰] Variable

شبکه گستر

شرکت مهندسی شبکه گستر که در سال ۱۳۷۰ تأسیس گردیده، اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرد. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولید کننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به‌عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد.

پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. در حال حاضر نیز شرکت شبکه گستر به‌عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات درایران اقدام می نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی و انحصاری شرکت آلمانی Astaro، سازنده محصولات "مدیریت یکپارچه تهدیدات" (Unified Threat Management – UTM) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر به‌عنوان نماینده شرکت Sophos ادامه فعالیت داده و اکنون محصولات Astaro سابق را تحت نام جدید Sophos و دیگر محصولات امنیت شبکه این شرکت را در ایران عرضه می‌نماید.

از سال ۱۳۹۱ نیز، شرکت مهندسی شبکه گستر عرضه محصولات ضد ویروس Bitdefender را به‌عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران، آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظاراتی بودند که برخی کاربران و مدیران شبکه‌های کوچک و متوسط داشتند و با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد.

شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین و طولانی مدت‌ترین پروژه‌های طراحی، نصب، راه ندازی و پشتیبانی محصولات نرم‌افزاری ضدویروس و سخت‌افزاری فایروال در کشور بوده است.

این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

CSQ
ISO 9001:2008
Cert No 9150.C528

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

تلفن / دورنگار	۰۲۱-۴۲۰۵۲
تارنمای شرکت	www.shabakeh.net
سامانه پشتیبانی	help.shabakeh.net
خدمات پس از فروش	my.shabakeh.net
مرکز آموزش	events.shabakeh.net
اتاق خبر	newsroom.shabakeh.net