تحلیل و معرفی بدافزارهای بسترهای مجازی‌سازی

فهرست مطالب

۱ مقدمه

مجازی‌سازی روشی است که در آن منابع کامپیوتر به صورت انتزاعی وجود دارند. با مجازی کردن منابع، بستر مورد نظر چندین سیستم‌عامل می‌تواند به صورت همزمان روی یک سخت‌افزار اجرا شود. روش مجازی‌سازی به ابتدای دهه ۷۰ میلادی برمی‌گردد، زمانی که IBM سیستم‌عامل تقسیم زمانی CP/CMS خود را معرفی کرد. مجازی‌سازی منافع بسیاری را برای ما فراهم کرده است، اما یک هکر کامپیوتر می‌تواند با بهره‌برداری از دستورات مجازی‌سازی و ایجاد یک لایه از نرم‌افزار، کنترل سیستم‌عامل اصلی را در اختیار بگیرد. هکر می‌تواند یک بدافزار را در سطح VMM قرار دهد. قرار گرفتن در این سطح می‌تواند بسیار زیان‌آور باشد به‌گونه‌ای که هکر با بالاترین دسترسی عملیات خود را انجام دهد. این بدافزار ممکن است یک ثبت‌کننده‌ی کلید را نصب کند، در حافظه‌ی سیستم‌عامل مهمان به دنبال رمز عبور بگردد و یا به دیسک از راه دور دسترسی داشته باشد. یک روت‌کیت می‌تواند از روش مجازی‌سازی سخت‌افزار استفاده کند که به آن روت‌کیت HVM می‌گویند. اگر شخصی محیط مجازی‌سازی را به خطر بیندازد، می‌تواند کنترل محیط فیزیکی که سیستم روی آن اجرا می‌شود را در دست بگیرد. کشف و بیرون کردن بدافزاری که در این سطح مخفی شده باشد بسیار سخت‌تر از بدافزاری است که در سطح هسته قرار دارد.

در این گزارش، ابتدا بدافزارها را طبقه‌بندی کرده، سپس در مورد بدافزارها و روت‌کیت‌هایی که باعث آلودگی ماشین مجازی و همچنین سیستم‌عامل میزبان می‌شوند و همچنین روش‌های به کار رفته در آنها صحبت می‌کنیم.

۲ طبقه‌بندی بدافزارها

به عنوان تعریفی از بدافزار می‌توان گفت کلاسی از نرم‌افزار است که برای نفوذ یا صدمه‌زدن به یک سیستم کامپیوتری، بدون اجازه‌ی کاربر طراحی شده است. یک بدافزار ممکن است قسمت‌های مختلفی از یک سیستم‌عامل را جعل کند تا کنترل را به سمت کد خود تغییر دهد، و یا به تنهایی به عنوان یک برنامه‌ی کاربردی مستقل بدون تغییر هیچ‌کدام از منابع سیستم اجرا شود. در قسمت بعد کلاس‌های مختلف بدافزار را مبتنی بر نوع روش جعل سیستم‌عامل توصیف می‌کنیم. این طبقه‌بندی توسط Joanna Rutkowska در کنفرانس Black Hat پیشنهاد شد و به طور گسترده‌ای مورد پذیرش قرار گرفته است.

۲-۱ نوع صفر بدافزار

همان‌گونه که در شکل ۱ نشان داده شده است، این نوع از بدافزار به عنوان یک برنامه‌ی کاربردی مستقل عمل می‌کند و هیچ تأثیری روی کد و داده‌ی سیستم عامل ندارد. همچنین، این نوع از بدافزار هیچ تغییری روی رفتار پردازه‌های سطح کاربر نداشته و کد خود را درون هیچ برنامه‌ی باینری تزریق نمی‌کند. بدافزارهای متعلق به این گروه معمولاً فایل‌های مربوط به کاربر را از هر مسیری پاک کرده یا تغییر می‌دهند، و یا

تغییراتی روی کلید رجیستری اعمال می‌کنند. این نوع از بدافزارها به طور کلی به عنوان نوعی آزار تلقی شده و تهدید بزرگی از نظر سیستم در معرض خطر محسوب نمی‌شوند. جاسوس‌افزار[1] یکی از این نوع بدافزارها است.

۲-۲ نوع ۱ بدافزار

نوع ۱ بدافزار قسمت‌های مقاوم از سیستم را جعل می‌کند. معمولاً بدافزار مربوط به این دسته، بخش‌هایی از کد پردازه‌های کاربر یا هسته، جداول مراجعه[2] در فضای کاربر یا هسته، یا رجیسترهای پردازنده را برای اجرای توابع Trampoline تغییر می‌دهد. روش‌های جعل در این دسته از بدافزار، جعل جداول مراجعه[3]، وصله‌کردن کد[4] و جعل رجیسترهای پردازنده می‌باشند.

۲-۳ نوع ۲ بدافزار

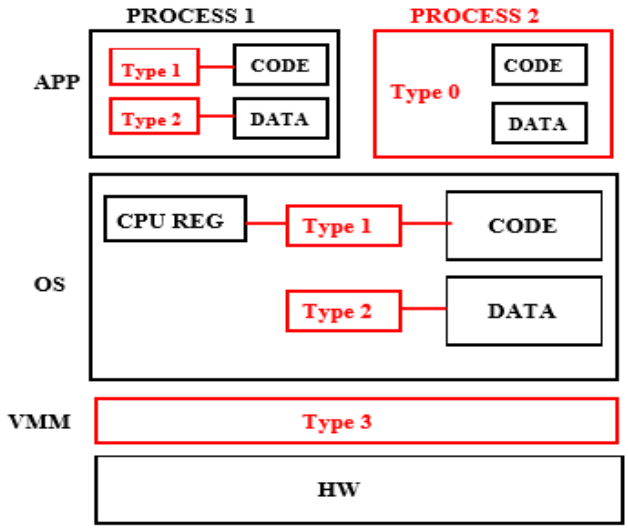
برخلاف نوع ۱ بدافزار، نوع ۲ بدافزار قسمت‌های غیرمقاوم در حافظه را جعل می‌کند. معمولاً بدافزار متعلق به این دسته، بخش‌های داده‌ای در ساختارهای داده‌ی هسته یا بخش‌های داده‌ای پردازه‌ها را تغییر می‌دهد که برای تغییر طراحی شده‌اند. روش‌های استفاده شده در این دسته از بدافزار، جعل شیء در هسته[5] و دست‌کاری مستقیم شیء در هسته[6] می‌باشند.

۲-٤ نوع ۳ بدافزار

این دسته نوع خاصی از بدافزار است که به صورت خاص برای محیط‌های مجازی طراحی شده است. انواع دیگر بدافزارها همیشه در سطح یکسان از سیستم‌عامل عمل می‌کنند، اما نوع ۳ بدافزار میدان نبرد را به یک سطح زیر سیستم‌عامل برده است (شکل ۱). این بدافزار توانسته است به قسمت‌های پنهان سیستم دسترسی پیدا کرده و نه تنها بدون تغییر سیستم‌عامل (بدون هوک‌کردن) بلکه با اعمال نفوذ به سیستم پشتیبانی مجازی‌سازی در نرم افزار، به اندازه سخت‌افزار به سیستم دسترسی پیدا کند. SubVirt، Blue Pill و Vitriol نمونه‌هایی از روت‌کیت‌هایی هستند که در این دسته قرار می‌گیرند.

---

1 Spyware
2 Lookup tables
3 Hooking lookup tables
4 Code patching
5 Kernel object hooking
6 Direct kernel object manipulation



شکل ۱ طبقه‌بندی بدافزارها

۳ روت‌کیت Blue Pill

روت‌کیت Blue Pill توسط Joanna Rutkowska ایجاد شده است. این بدافزار از بسط‌های ماشین مجازی امن AMD64 (SVM) استفاده می‌کند تا در هسته‌ی ویندوز ویستا خراب‌کاری ایجاد کند. ویژگی اصلی روت‌کیت Blue Pill این است که هسته را در حالت اجرا واژگون می‌کند. بنابراین هیچ نیازی به تغییر در BIOS فایل‌های بخش بوت و فایل‌های سیستمی نیست. این بدافزار یک لایه از VMM در زیر سیستم‌عامل نصب می‌کند تا فعالیت‌های مورد نظرخود را درون سیستم‌عامل مهمان کنترل و مشاهده کند.

Blue Pill یک روت‌کیت تحت حافظه است، بنابراین بعد از راه‌اندازی مجدد از بین می‌رود. از طرف دیگر هیچ ردپایی از خود به جا نمی‌گذارد تا با استفاده از تحلیل حافظه کشف شود.

۳-۱ مدل حمله Blue Pill

مدل حمله Blue Pill در شکل ۲ نشان داده شده است. Blue Pill به عنوان یک ماژول درایور در هسته بارگذاری می‌شود. سپس مراحل زیر را اجرا می‌کند تا ماشین مجازی را راه‌اندازی کند:

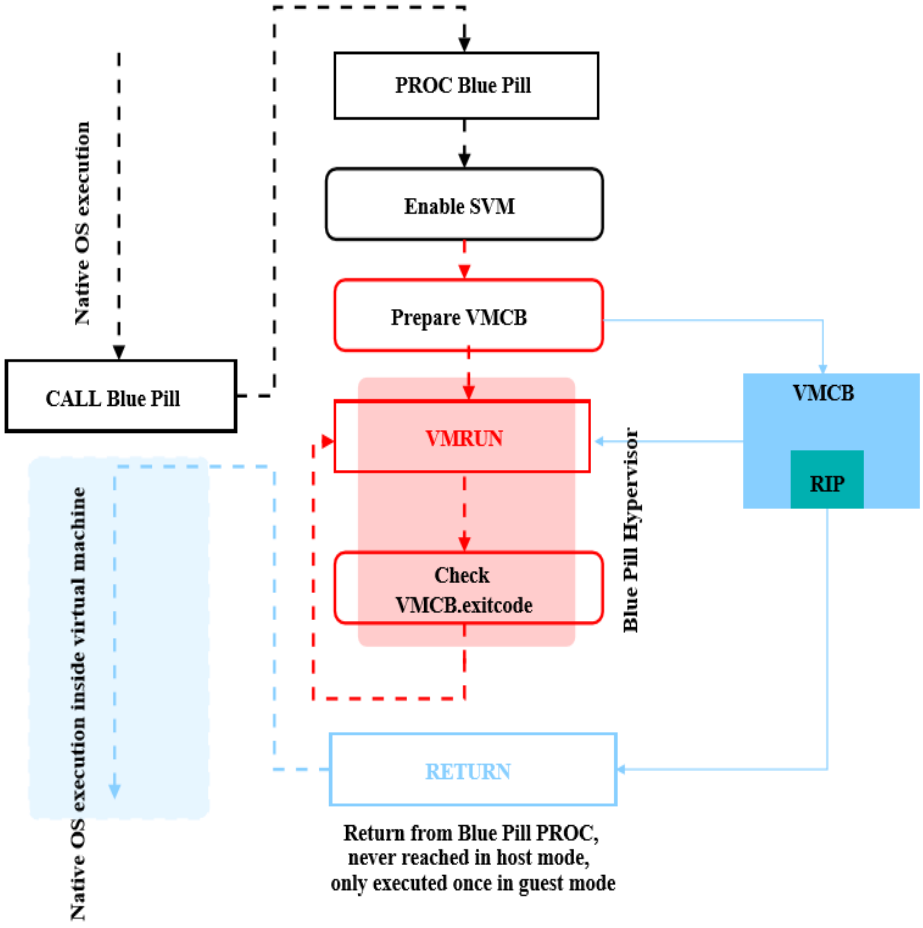
۱) این بدافزار بسط‌های SVM را با تنظیم بیت فعال‌سازی ماشین مجازی امن (SVME) از رجیستر فعال‌سازی ویژگی‌های توسعه داده شده (EFER) فعال می‌کند.

۲) سپس Blue Pill بلاک کنترل ماشین مجازی (VMCB) را مقداردهی می‌کند. در تکنولوژی AMD64 SVM، VMCB داده ساختاری است که حالت سیستم‌عامل مهمان را تعیین و همچنین دستورات و رویدادهایی که توسط VMM رهگیری می‌شوند را تعیین می‌کند.

۳) Blue Pill جدول صفحه‌های خصوصی را برای VMM خود اختصاص می‌دهد.

۴) بعد از راه‌اندازی VMCB، Blue Pill دستورات VMRUN را برای راه‌اندازی ماشین مجازی (سیستم‌عامل مهمان) اجرا می‌کند. سیستم‌عامل مهمان متوجه نمی‌شود که تحت کنترل یک VMM است. هر تلاشی برای اجرای دستورات ویژه توسط سیستم‌عامل مهمان توسط VMM در دام افتاده و باعث می‌شود که رویداد خارج شدن VM اتفاق بیفتد.

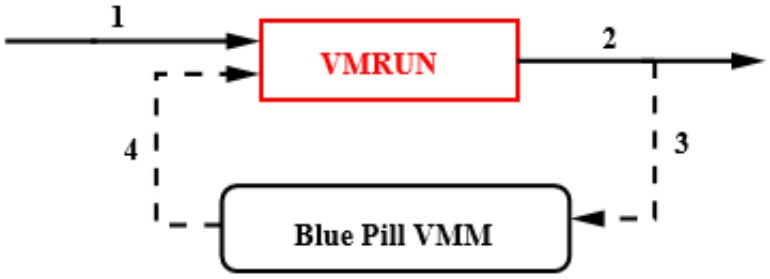
۵) VMM Blue Pill عضو VMCB.exitcode از داده ساختاری VMCB را بررسی می‌کند تا اطلاعات مربوط به رویدادی که باعث خارج شدن می‌شود را پیدا کند. سپس دستورات و رویدادهای ره‌گیری شده را تقلید کرده و اجرای سیستم‌عامل مهمان را با اجرای دستورات VMRUN ادامه می‌دهد.



شکل ۲ مدل حمله Blue Pill

کاربرد VMRUN در شکل ۳ نشان داده شده است. از آنجایی که Blue Pill از VMM استفاده می‌کند، تشخیص آن بسیار سخت می‌شود. همچنین Blue Pill سیستم‌های ورودی و خروجی را مجازی‌سازی نکرده است و بنابراین با اثر مستقیمی که روی سخت‌افزار می‌گذارد قابل تشخیص نیست. Blue Pill VMM همچنین می‌تواند کد مخرب را در کنار تقلیدکردن رویدادهای ره‌گیری شده اجرا کند. همان‌طور

که این عملیات در زیر سیستم‌عامل مهمان انجام می‌شود، تمام زمینه‌های مخرب که توسط Blue Pill VMM راه‌اندازی شده است به صورت کامل درون سیستم عامل مهمان مخفی می‌شود.



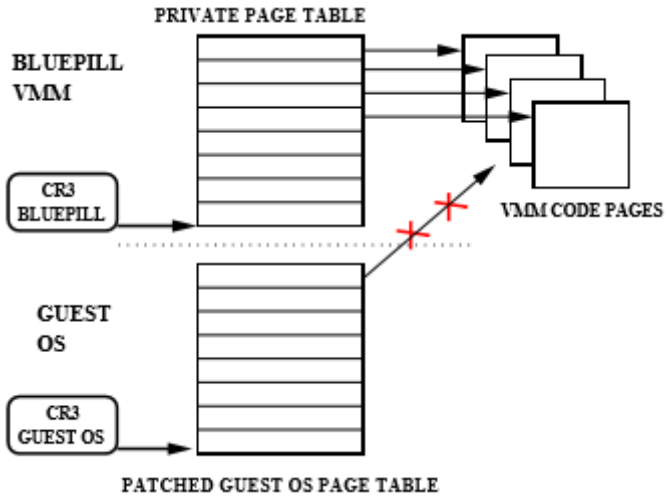
شکل ۳ کاربرد دستورات VMRUN

در ادامه به توصیف مراحل نشان داده شده در شکل ۳ می‌پردازیم.

۱. روت‌کیت Blue Pill، VMRUN را برای راه‌اندازی ماشین مجازی اجرا می‌کند.
۲. ماشین مجازی (سیستم‌عامل مهمان) اجرا می‌شود.
۳. سیستم‌عامل مهمان توسط Blue Pill VMM ره‌گیری می‌شود.
۴. Blue Pill VMM، VMRUN را برای ادامه‌ی اجرای ماشین مجازی اجرا می‌کند.

۲-۳ پنهان‌کردن حافظه

Blue Pill از جدول صفحه‌های خصوصی برای پنهان‌کردن صفحات کد VMM از سیستم‌عامل مهمان استفاده می‌کند. Blue Pill VMM، CR3 خصوصی خود را دارد. پردازنده این مقدار CR3 را به صورت مستقیم در رجیستر CR3 بارگذاری می‌کند، زمانی که یک رویداد خروج VM وجود دارد. Blue Pill از سیستم پشتیبانی سیستم‌عامل مهمان برای راه‌اندازی صفحات VMM استفاده می‌کند. Blue Pill جدول صفحه‌ها را به مقادیر خود اختصاص می‌دهد و تمام ردیف‌های جدول صفحه متعلق به Blue Pill VMM را کپی می‌کند. سپس این ورودی‌ها را در سیستم‌عامل مهمان که جدول صفحه‌ها را به مقادیر "garbage" اختصاص داده است وصله می‌کند. به این طریق Blue Pill قادر است که صفحات کد VMM خود را از سیستم‌عامل مهمان مخفی کند. این روش در شکل ۴ دیده می‌شود. روت‌کیت دیگر به نام Vitriol ایجاد شده است تا در سیستم‌عامل Mac با استفاده از تکنولوژی سخت افزار Intel-VT ایجاد خراب‌کاری کند این درحالی است که کد منبع آن مانند Blue Pill منبع‌باز نمی‌باشد.



شکل ۴ جدول صفحه خصوصی

۴ روت‌کیت HVM

روت‌کیت‌های HVM به هیچ‌کدام از اعمالی که سیستم‌عامل انجام می‌دهد آسیب‌پذیر نیستند، زیرا این روت‌کیت‌ها در حالت‌هایی با دسترسی بیشتری از سیستم‌عامل اجرا می‌شوند. یک ابرناظر[۷] حتی نیاز به حضور در حافظه ندارد که برای سیستم‌عامل قابل دسترس باشد. وقتی ابرناظر خود را به صورت خودکار راه‌اندازی می‌کند، باعث اجرای هر دستور یا دسترسی به حافظه‌ای می‌شود که حضور خود را با دسترسی بیشتری از سیستم‌عامل فاش می‌کند. وقتی این دستورات اجرا می‌شوند، پردازنده در ابرناظر به دام افتاده و اجازه می‌دهد که نتیجه عوض شود. بنابراین، ابرناظر نیاز به هیچ تغییری در سیستم‌عامل ندارد تا حضور خود را مخفی کند. ابرناظر می‌تواند هر کدام از این تغییرات را ایجاد کند و باعث شود که آنها توسط سیستم‌عامل، غیرقابل تشخیص شوند.

دو محقق به نام‌های Dino Dai Zovi و Joanna Rutkowska به موازات هم روی اثبات مفهوم روت‌کیت HVM کار می‌کردند. Zovi یک چارچوب برای روت‌کیت HVM در Intel VT پیاده‌سازی کرد و Rutkowska مشابه آن را برای روت‌کیت HVM با AMD-V پیاده‌سازی کرد. هر دو ادعا کردند روی نمونه‌های اولیه به نام‌های Vitriol و Blue Pill کار کردند اما کد منبعی از آن‌ها در اختیار ندارند. Rutkowska ادعا کرد که یک روت‌کیت کاملاً غیر قابل تشخیص طراحی کرده است که با توجه به عدم اثبات در دسترس و ناتوانی در آزمون این ادعا باعث ایجاد جدالی در جامعه‌ی تحقیقاتی شد.

[7] Hypervisor

محققان علاقه‌مند بودند که روت‌کیت HVM خود را بسازند. حدود یک سال بعد از ارائه‌ی Black Hat هنوز نمونه‌هایی از HVM، به جز کد توزیع شده برای پروژه Xen توسط مهندسانی از Intel و AMD، در دسترس نبود. متأسفانه کد Xen بسیار پیچیده‌تر از چیزی بود که برای پیاده‌سازی روت‌کیت HVM مورد نیاز است. Xen به گونه‌ای طراحی شده است تا از VMهای مهمان و چندین معماری پردازنده و شمایی از معماری مجازی‌سازی خاص با مجموعه‌ای از متاساختار خود پشتیبانی کند.

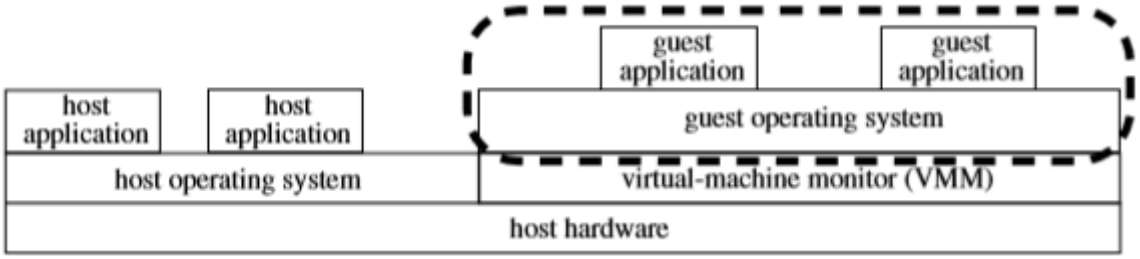
برخلاف ابرناظر معمولی که قبل از روشن کردن VM مهمان بارگذاری می‌شود، یک روت‌کیت HVM درون سیستم‌عاملی که از قبل بارگذاری شده، بار شده و به VM مهمان خود تبدیل می‌شود. بنابراین روت‌کیت باید توابع ابرناظر را مقداردهی کند و به صورت پویا به عنوان میزبان در نظر گرفته شود و سیستم‌عامل در حال اجرا را به مهمان تبدیل کند. ابرناظر و سیستم‌عامل به صورت همزمان اجرا نمی‌شوند و همچنین سیستم‌عامل نیاز ندارد تغییر کند یا به جایی برود.

۱-٤ پیش‌نیازها

یک ابرناظر AMD-V اجرای مهمان را با VMRUN شروع می‌کند. دستور VMRUN در بستر سطح صفر از درایور حالت هسته عمل می‌کند. روت‌کیت HVM باید با درایور شروع کند. اما وقتی ابرناظر نصب می‌شود، آن درایور در ماشین مهمان قرار دارد و ممکن است حضور ابرناظر را برای مهمان آشکار کند. به جای پنهان‌کردن درایور در حالت عادی روت‌کیت، درایوری را انتخاب می‌کنیم که یک منطقه حافظه صفحه‌بندی‌نشده را برای داشتن ابرناظر اختصاص دهد. سپس کد ابرناظر را در آنجا کپی کرده و درایور را از هسته برمی‌داریم. بنابراین درایوری که ابرناظر را نصب کرده باید به عنوان یک بارکننده برای ابرناظر و نه به عنوان محیط حامل آن، عمل کند. پس از این‌که ابرناظر نصب شد، فایل درایور باید از روی دیسک و شاید از روتین بار نشده‌ی درایور پاک شود.

۵ روت‌کیت Subvirt

برای کشف این تهدید، دو مفهوم VMBR برای پلت‌فرم‌های x86 با استفاده از Virtual PC و VMware Workstation VMM پیاده‌سازی شده‌اند. همان‌طور که در شکل ۵ مشاهده می‌شود هر دو مفهوم از معماری VMM استفاده می‌کنند که به سیستم‌عامل میزبان نفوذ کرده تا به سخت‌افزار لایه‌ی زیرین دسترسی داشته باشند. Virtual PC VMBR از نسخه کوچک‌شده‌ی ویندوز XP برای سیستم‌عامل میزبان استفاده می‌کند و VMware VMBR از لینوکس Gentoo استفاده می‌کند. برای پیاده‌سازی VMBR، هسته ویندوز XP میزبان، Virtual PC و هسته لینوکس میزبان را تغییر می‌دهیم.



شکل ۵ روش‌های رایج استفاده شده در VMM

۵-۱ نصب

در ساختار کلی VMBR، یک VMBR در زیر سیستم‌عامل موجود و برنامه‌های کاربردی آن اجرا می‌شود. برای انجام این کار VMBR باید خود را در زیر سیستم‌عامل مورد نظر قرار دهد و آن را به عنوان مهمان اجرا کند (شکل ۶). برای قرار گرفتن در زیر سیستم موجود، VMBR باید مراحل بوت سیستم را با مهارت انجام دهد تا مطمئن شود که VMBR قبل از سیستم‌عامل هدف و برنامه‌های کاربردی آن بارگذاری می‌شود. بعد از بارگذاری VMBR، سیستم عامل هدف را با استفاده از VMM بوت می‌کند. در نتیجه سیستم عامل هدف به صورت نرمال اجرا می‌شود اما VMBR به صورت آرام در زیر آن قرار دارد.

برای نصب VMBR روی یک کامپیوتر، مهاجم باید در درجه‌ی اول به سیستم دسترسی کافی داشته باشد تا بتواند مراحل بوت سیستم را تغییر دهد. راه‌های بسیار زیادی برای یک مهاجم وجود دارد تا به این سطح دسترسی برسد. برای مثال، یک مهاجم می تواند از یک آسیب‌پذیری بهره برداری کرده، کاربر را فریب دهد تا یک نرم‌افزار مخرب را نصب کند و یا یک CD-ROM یا یک تصویر DVD موجود در یک شبکه نقطه به نقطه را خراب کند. در بسیاری از سیستم‌ها مهاجم که دسترسی ریشه یا مدیر را به دست آورده می‌تواند مراحل بوت سیستم را دست‌کاری کند. در سیستم‌های دیگر یک مهاجم باید کد را در هسته اجرا کند تا مراحل بوت را تغییر دهد. فرض می‌کنیم که مهاجم می‌تواند کد دلخواه را در سیستم هدف با دسترسی ریشه یا مدیر اجرا کند و ماژول‌های هسته را در صورت نیاز نصب کند.

پس از این که مهاجم دسترسی ریشه را به دست آورد، باید حالت VMBR را در یک محل ذخیره مداوم نصب کند. مناسب‌ترین فرم ذخیره‌ی مداوم برای حالت VMBR دیسک است. مهاجم می‌تواند از سیستم‌عامل هدف برای اختصاص بلوک‌های دیسک (از طریق فایل‌های سیستمی) استفاده کند و یا ساختارهای روی دیسک را برای پیدا کردن بلوک‌های استفاده نشده تجزیه نماید. زمانی که سیستم هدف، ویندوز XP است، می‌توان حالت VMBR را در ابتدای قسمت اول فعال دیسک ذخیره کرد. داده‌ی موجود در این بلوک‌های دیسک را به بلوک‌های استفاده نشده در هر جای دیسک انتقال می‌دهیم. زمانی که سیستم

هدف، لینوکس است جابجایی را غیرفعال کرده و از قسمت تعویضی برای ذخیره حالت مداوم VMBR استفاده می‌شود. هر دو روش نصب بیشتر داده‌های هدف را در مکان اصلی روی دیسک باقی می‌گذارند.

مرحله بعدی نصب یک VMBR، تغییر مراحل بوت سیستم است تا مطمئن شود که VMBR قبل از سیستم‌عامل هدف بارگذاری می‌شود. مناسب‌ترین راه برای VMBR برای دست‌کاری مراحل بوت سیستم، تغییر رکوردهای بوت روی دیسک سخت اولیه است. بسیاری از آنتی‌ویروس‌های رایج، تغییرات بلوک‌های بوت روی دیسک سخت را تشخیص می‌دهند. این پیاده‌سازی در تلاش است تا با دست‌کاری بلوک‌های بوت، در حین مراحل نهایی خاموش شدن و بعد از اینکه بیشتر پردازش‌ها و زیرسیستم‌های هسته خارج شدند، مانع این نوع تشخیص شود.

وقتی سیستم مورد نظر ویندوز XP است، از یک ماژول هسته استفاده می‌کنیم که کنترل‌کننده‌ی رویداد LastChanceShutdown Notification را ثبت می‌کند. این ماژول در مراحل آخر خاموش شدن و بعد از این‌که فایل‌های سیستمی پاک شدند فراخوانی می‌شود. وقتی ویندوز این کنترل‌کننده‌ی رویداد را فراخوانی می‌کند، ماژول هسته کد بوت VMBR را در قسمت فعال دیسک کپی می‌کند و موجب می شود که سیستم، VMBR را در بوت بعدی سیستم بارگذاری کند. از آنجایی که کد حمله در سیستم‌عامل اجرا می‌شود، کنترل کافی را روی سیستم داریم تا حتی اگر در حین فرآیند خاموش شدن اجرا شود مانع نرم‌افزار ضد بدافزار شود.

وقتی سیستم مورد نظر لینوکس است، مراحل بوت را با استفاده از کد در حالت کاربر تغییر می‌دهیم. اسکریپت خاموش شدن را تغییر داده تا کد نصب بعد از اینکه تمام پردازش‌ها کشته شدند اما قبل از خاموش شدن سیستم اجرا شود. رکورد بوت دیسک اصلی را با استفاده از بلوک دستگاه هارد لینوکس بازنویسی کرده تا VMBR در بوت سیستم به جای سیستم عامل هدف بارگذاری شود.

پس از نصب، فضای دیسک سیستم مورد نظر درون دیسک مجازی قرار می‌گیرد. بعد از بوت شدن دوباره، VMM دیسک مجازی مورد نظر را به گونه‌ای برمی‌گرداند که به موقعیت روی دیسک فیزیکی مربوطه دسترسی داشته باشد. برای اجرای پشتیبانی تغییر مکان بر روی دیسک برای VMBR مبتنی بر Virtual PC، ماژول مجازی‌سازی دیسک VMM را تغییر می‌دهیم. برای VMBR مبتنی بر VMware دستگاه بلوک هارد درایو لینوکس را تغییر می‌دهیم.

۲-۵ سرویس‌های مخرب

پس از نصب VMBR، می‌توان سرویس‌های مخرب را اجرا کرد. در این بخش در مورد تکنیک‌هایی صحبت می‌کنیم که توسط VMBR مورد استفاده قرار می‌گیرد تا انواع سرویس‌های مخرب را پیاده‌سازی کند.

بدافزارهای معمولی اغلب راحتی پیاده‌سازی را با توانایی جلوگیری از تشخیص مبادله می‌کنند. این بدافزارها در حالت کاربر که در سیستم‌عامل هدف اجرا می‌شوند راحتی پیاده سازی را ترجیح می‌دهند زیرا نویسندگان بدافزار می‌توانند از هر زبان برنامه‌نویسی برای نوشتن این سرویس‌های مخرب استفاده کنند. همچنین، بدافزارهای حالت کاربر به تمام کتابخانه‌ها و منابع سطح سیستم‌عامل دسترسی دارند تا انجام برخی از عملیات را آسان کند. اگرچه، این بدافزار می‌تواند توسط نرم‌افزار امنیتی اجرا شده در سیستم‌عامل هدف تشخیص داده شود زیرا تمام حالت‌ها و رویدادهای مخرب برای سیستم‌عامل هدف قابل دیدن هستند.

VMBR از یک حمله جداگانه به سیستم‌عامل برای گسترش بدافزار استفاده می‌کند که از دید سیستم‌عامل هدف مخفی است اما هنوز هم پیاده‌سازی آن راحت است. هیچ‌کدام از حالت‌ها و رویدادهای حمله سیستم‌عامل از درون سیستم‌عامل هدف قابل دیدن نیست، بنابراین هر کدی که درون حمله سیستم‌عامل هدف اجرا شود کاملاً مخفی نیست. توانایی اجرای سرویس‌های مخرب مخفی در حمله‌ی سیستم‌عامل، به مزاحمان این آزادی را می‌دهد که از کد حالت کاربر با ترس کمتری از تشخیص استفاده کنند.

ما سرویس‌های مخرب را به سه دسته تقسیم‌بندی کردیم. آنهایی که نیاز به تعامل با سیستم‌عامل هدف ندارند، آنهایی که اطلاعاتی در مورد سیستم‌عامل هدف را مشاهده می‌کنند و آنهایی که عمداً مزاحم اجرای سیستم‌عامل هدف می‌شوند. در ادامه‌ی این بخش در مورد این‌که چگونه VMBR هر دسته از سرویس را پشتیبانی می‌کند صحبت می‌کنیم.

دسته‌ی اول از سرویس‌های مخرب با سیستم‌عامل هدف ارتباط برقرار نمی‌کنند. مثال‌هایی از این سرویس‌ها انتشار اسپم[8]، زامبی‌های خودداری از سرویس توزیع‌شده و جعل وب‌سرویس‌ها است. یک VMBR این سرویس‌ها را پشتیبانی می‌کند تا در حمله به سیستم‌عامل اجرا شوند. در نتیجه، بدون این‌که سرویس‌های مخرب به درون سیستم‌عامل هدف افشا شوند، باعث اجرای آسان در حالت کاربر می‌شود.

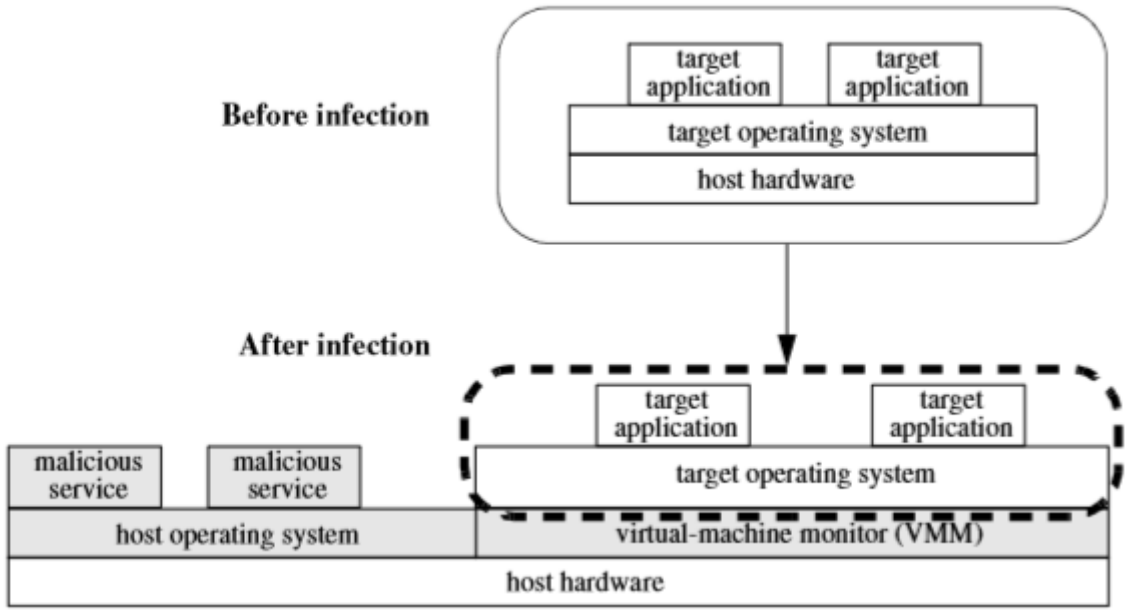
دسته‌ی دوم از سرویس‌های مخرب داده یا رویداد از سیستم‌عامل هدف را مشاهده می‌کنند. VMBR ثبت داده در سطح سخت‌افزار را به صورت پنهانی (ضربه‌زدن به کلید، بسته‌های شبکه) با تغییر نرم‌افزار تقلید از دستگاه VMM فعال می‌کند. این تغییر تأثیری بر دستگاه‌های مجازی موجود در سیستم‌عامل هدف ندارد. برای مثال، یک VMBR می‌تواند تمام بسته‌های شبکه را با تغییر کارت‌های شبکه تقلید شده VMM ثبت

[8] Spam relays

کند. این تغییرات از دید سیستم‌عامل هدف پنهان است زیرا رابط کارت شبکه تغییر نمی‌کند اما VMBR هنوز هم می‌تواند تمام بسته‌های شبکه را ضبط کند.

درون‌گرایی ماشین مجازی سرویس‌های مخرب را فعال می‌کند تا اجرای سیستم‌عامل هدف یا برنامه‌های کاربردی را در هر دستور دلخواهی به دام اندازد. وقتی این تله اتفاق می‌افتد، یک سرویس مخرب می‌تواند از درون‌گرایی ماشین مجازی استفاده کرده و داده را از سیستم هدف دوباره‌سازی کند. برای مثال اگر یک برنامه هدف از یک سوکت رمز شده استفاده کند، مهاجمین می‌توانند از درون‌گرایی ماشین مجازی استفاده کرده تا تمام فراخوانی‌های نوشتن سوکت SSL را به دام انداخته و داده‌های متن آشکار را قبل از رمزشدن ثبت کنند. این ثبت کردن برای سیستم‌عامل هدف و برنامه‌های آن واضح است زیرا کد مخرب بیرون از سیستم هدف اجرا می‌شود و همچنین درون‌گرایی ماشین مجازی مزاحم حالت سیستم هدف نمی‌شود.

دسته‌ی سوم از سرویس مخرب عمداً اجرای سیستم هدف را تغییر می‌دهد. برای مثال یک سرویس مخرب می‌تواند ارتباطات شبکه را تغییر دهد، پیام‌های ایمیل را پاک کند یا اجرای برنامه‌ی هدف را تغییر دهد. یک VMBR می‌تواند لایه تقلید دستگاه VMM را به گونه‌ای ایجاد کند تا داده سطح سخت‌افزار را تغییر دهد. همچنین یک VMBR می‌تواند داده یا اجرای درون هدف را از طریق درون‌گرایی ماشین مجازی تغییر دهد.



شکل ۶ چگونگی اجرای سیستم موجود درون ماشین مجازی فراهم شده توسط VMM

۳-۵ مثال‌هایی از سرویس‌های مخرب

با استفاده از مفهوم VMBR، چهار سرویس مخرب را تولید کردیم که تعدادی از سرویس‌هایی که نویسنده نرم‌افزار مخرب می‌خواهد گسترش دهد را نشان می‌دهد. ما جعل سرویس‌دهنده‌ی وب، ثبت‌کننده‌ی

کلیدهای صفحه کلید، سرویسی که جعل کردن فایل‌های سیستمی هدف را برای فایل‌های حساس اسکن می‌کند و دفاع متقابل که به تشخیص‌دهنده‌های ماشین مجازی غلبه می‌کند، را پیاده‌سازی کردیم. برای گسترش این سرویس‌ها از سیستم‌عامل میزبان به عنوان حمله به سیستم‌عامل استفاده می‌کنیم و نیز برای بعضی از سرویس‌ها VMM را تغییر می‌دهیم.

با استفاده از VMBR مبتنی بر VMware، سرویس‌دهنده‌ی وب را جعل کرده که بدافزاری را نشان می‌دهد که هیچ تعاملی با سیستم‌عامل هدف ندارد. سرویس‌دهنده‌های وب جعل شده برای گسترش وب‌سایت‌هایی که شبیه کارهای قانونی است استفاده می‌شود و کاربران را برای وارد کردن اطلاعات شخصی مانند شماره کارت اعتباری و رمز عبور آن فریب می‌دهد. مهاجمین معمولاً از سیستم‌های در معرض خطر برای گسترش این وب‌سایت‌های مخرب استفاده می‌کنند. برای پیاده‌سازی سایت جعل شده، از وب سرور httpd اجرا شده در حمله به سیستم‌عامل استفاده کردیم. ما تنظیمات شبکه مجازی را به گونه‌ای تغییر دادیم که بیشتر ترافیک شبکه به هدف برسد اما هر درخواست TCP وارد شده روی پورت ۸۰۸۰ به سرور جعل شده می‌رسد. این سرویس‌دهنده‌ی وب نیازی به هیچ کد جدیدی ندارد زیرا به سرویس‌دهنده‌ی وب موجود نفوذ کرده و تنظیمات شبکه مجازی موجود را تنظیم می‌کند و هنوز قادریم یک سرویس‌دهنده‌ی وب تمام عیار را درون محیط VMBR اجرا کنیم به گونه‌ای که هیچ حالت یا رویدادی نداشته باشد که درون سیستم عامل هدف قابل دیدن باشد.

با استفاده از VMBR مبتنی بر Virtual PC، یک سرویس برای ثبت کلیدهای صفحه کلید را پیاده‌سازی کردیم. این سرویس بدافزاری را نشان می‌دهد که داده‌ی سطح سخت‌افزار مربوط به اجرای سیستم هدف را مشاهده می‌کند. مهاجمین از ثبت‌کننده‌های کلید صفحه کلید برای به دست آوردن اطلاعات حساس مثل رمز عبور استفاده می‌کنند. برای پیاده‌سازی این ثبت‌کننده، ماژول تقلید کنترل‌کننده‌ی صفحه کلید را درون Virtul PC VMM تغییر داده و بنابراین تمام ضربات صفحه کلید به یک برنامه در حمله به سیستم‌عامل قبل از رسیدن به سیستم‌عامل هدف فرستاده می‌شود.

٤-٥ حفظ کنترل

برای جلوگیری از حذف، یک VMBR باید حالت خود را از طریق حفظ کنترل سیستم حفاظت کند. تا زمانی‌که VMBR سیستم را کنترل می‌کند، می‌تواند هر تلاشی توسط سیستم هدف را برای تغییر حالت VMBR خنثی کند. حالت VMBR حفاظت می‌شود زیرا سیستم هدف تنها به دیسک مجازی و نه دیسک فیزیکی دسترسی دارد.

تنها زمانی که VMBR کنترل سیستم را از دست می‌دهد زمانی است که بعد از این‌که سیستم روشن می‌شود هنوز VMBR روشن است. هر کدی که در این زمان اجرا می‌شود می‌تواند به صورت مستقیم به حالت

VMBR دسترسی داشته باشد. اولین کدی که در این زمان اجرا می‌شود سیستم BIOS است. سیستم BIOS دستگاه‌ها را مقداردهی کرده و انتخاب می‌کند که کدام واسط بوت شروع شود. در سناریوی معمولی BIOS بعد از این‌که VMBR کنترل سیستم را دوباره به دست آورد VMBR را بوت می‌کند. با این وجود، اگر BIOS یک برنامه را روی یک واسط دیگر بوت کند آن برنامه می‌تواند به حالت VMBR دسترسی داشته باشد.

از آنجایی که VMBR کنترل را در زمانی که سیستم خاموش شد از دست می‌دهد، آن‌ها تلاش می‌کنند تعداد زمان‌های خاموش شدن کامل سیستم را کاهش دهند. رویدادها به صورت معمول باعث می‌شوند چرخه‌ی برق دوباره راه‌اندازی شده و خاموش شود. VMBR راه‌اندازی مجدد را با دوباره روشن کردن سخت‌افزار مجازی به جای تنظیم کردن دوباره سخت‌افزار فیزیکی زیرین مدیریت می‌کند. با دوباره روشن کردن سخت‌افزار مجازی، VMBR فریبی برای تنظیم مجدد سخت‌افزار فیزیکی بدون از دست دادن کنترل را فراهم می‌کند. هر واسط قابل بوت متناوبی که بعد از راه‌اندازی مجدد هدف استفاده می‌شود، تحت کنترل VMBR اجرا می‌گردد.

علاوه بر مدیریت راه‌اندازی مجدد، VMBR می‌تواند سیستم خاموش شدن را تقلید کند به‌گونه‌ای که سیستم ظاهراً خاموش شده باشد اما VMBR در حال اجرا بر روی سیستم باقی بماند.

۶ **Crisis**: بدافزار پیشرفته

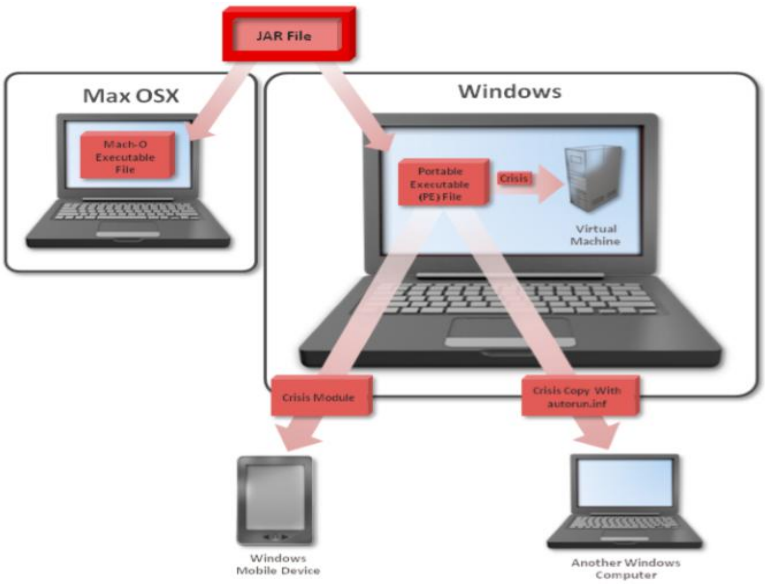
تا چند سال اخیر تعدادی بدافزار پیشرفته ایجاد شد تا در کامپیوترهای Mac اجرا شود. همزمان با افزایش استفاده از Mac، بدافزارهای مربوط به آن نیز افزایش پیدا کرد. برای مثال در سال گذشته بدافزارهای جدیدی برای Mac کشف شده است که شامل OSX.Flashback, OSX.Imuler و OSX.Sabpa می‌باشد. اخیراً ما OSX.Crisis را کشف کردیم. بدافزار Crisis یک بدافزار پیشرفته است که هم روی ویندوز و هم روی کامپیوترهای Mac قابل اجراست. کاربرد آن دزیدن اطلاعات است که شامل فعالیت‌های مرورگر و فهرست تماس‌ها است. همین‌طور توانایی ضبط اطلاعات دیداری و شنیداری از طریق میکروفون و دوربین کامپیوترها را دارد.

ویژگی‌های پیدا شده در این نرم‌افزار مشخص کرد که این بدافزار اهداف تحقیقات خصوصی یا جاسوسی دارد و خیلی پیشرفته‌تر از متوسط بدافزارهای دزدی اطلاعات است. به علاوه نسخه‌ی ویندوزی این بدافزار ماژول‌های خود را روی ابزارهای موبایل ویندوزی ایجاد می‌کند. همچنین این نرم‌افزار مخرب ممکن است اولین بدافزاری باشد که تلاش می‌کند به ماشین‌های مجازی نفوذ کند.

۱-۶ ساختار بدافزار

۱-۱-۶ فایل انتقال دهنده نرم افزار جاوا

Crisis نفوذ را از نرم‌افزار جاوا شروع کرد. این بدافزار سیستم عامل کامپیوتر در معرض خطر را بررسی می‌کند و یک نرم افزار قابل نصب مناسب بر روی کامپیوتر قرار می‌دهد.



شکل ۷ روش نفوذ Crisis

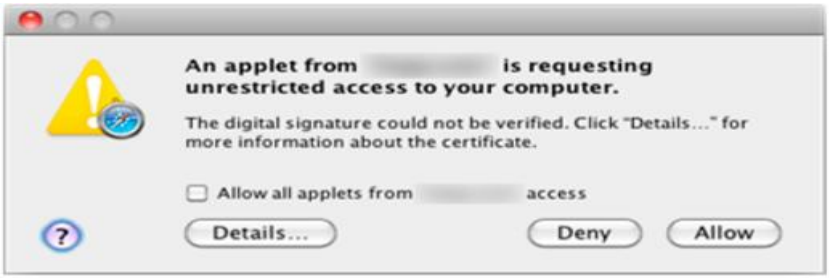
این بدافزار از هیچ آسیب‌پذیری برای قراردادن اجزای خود روی کامپیوتر بهره‌برداری نمی‌کند اما یک امضای عددی برای تولید یک فایل محلی و اجرای آن دارد. ما از روش‌هایی که نویسنده‌ی بدافزار برای مجبور کردن کاربر به بارکردن نرم‌افزار استفاده کرده است آگاه نیستیم، اما این امکان وجود دارد که نویسنده از حقه‌های مهندسی اجتماعی استفاده کرده باشد. زیرا این بدافزار از هیچ آسیب‌پذیری سوءاستفاده نکرده است.

در حالت کلی نرم‌افزارهای جاوا نمی‌توانند به منابع محلی از قبیل فایل‌های سیستمی بدون بهره‌برداری از آسیب‌پذیری دسترسی داشته باشند، اما اگر این نرم‌افزار امضا شده باشد می‌تواند یک دسترسی کامل برای اجرای هر عملیاتی را به دست آورد.

```
if (isWindows()){
str2=str2+”win”;
}
else if (isMac()){
Str2=str2+”mac”;
}
```

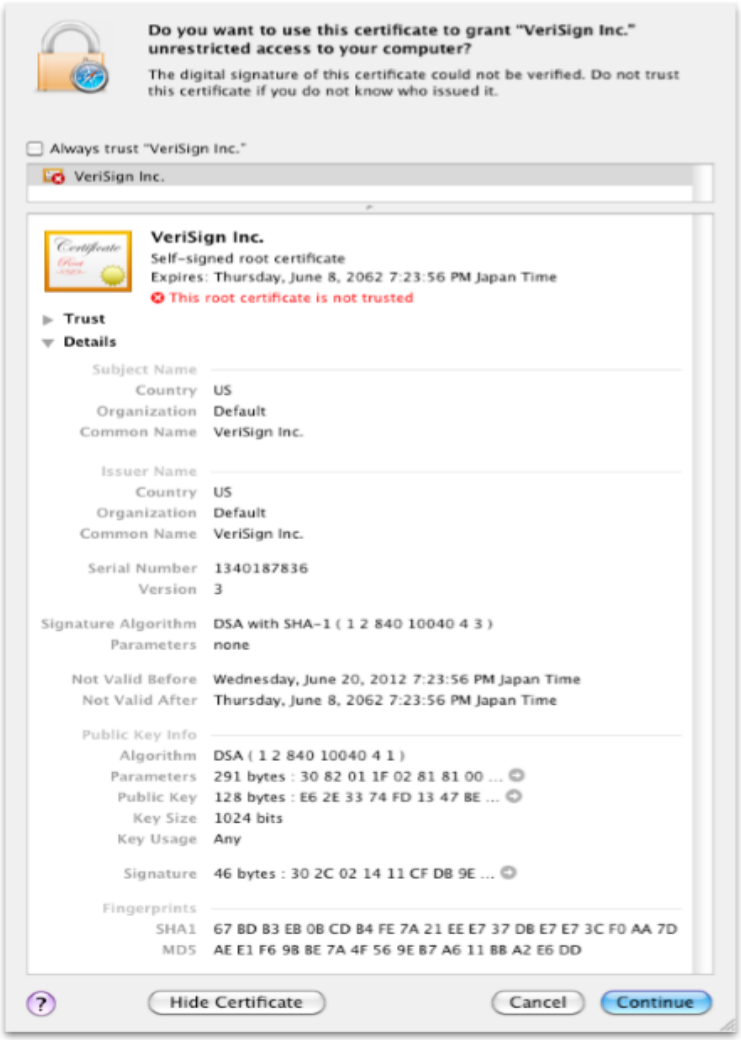
```
else{
System.out.println("Unknown operating system, quitting!");
System.exit (0);
}
```

در حالی که اغلب حملات از آسیب‌پذیری‌های جاوا به عنوان اولین قدم برای حمله به درایور از طریق دانلود سوءاستفاده می‌کنند، Crisis به این طریق کار نمی‌کند. چرا که نویسنده Crisis نمی‌خواهد ریسک تشخیص داده شدن توسط نرم‌افزارهای آنتی‌ویروس را بپذیرد، زیرا اگر از آسیب‌پذیری‌ها بهره‌برداری می‌کرد امکان تشخیص داده شدنش بیشتر می‌شد.



شکل ۸ این پیام وقتی نشان داده می‌شود که نرم افزار مورد نظر اجرا شود.

اگر بدافزار از هیچ آسیب‌پذیری استفاده نکند حمله به یک کامپیوتر سخت‌تر می‌شود در غیر این صورت بدافزار باید از روش‌های مهندسی اجتماعی استفاده کند که موفقیت این عملیات نیز به کاربر بستگی دارد.



شکل ۹ گواهی‌نامه شامل هیچ جزئیاتی از امضا نیست.

۶-۲ نفوذ چندبستری

فایل انتقال‌دهنده‌ی نرم‌افزار جاوا تنها یک فایل نصب برای هر بستر در یک پوشه موقت قرار می‌دهد سپس این فایل اجزای مهم را منتقل می‌کند.

۶-۳ فایل باینری

جداول ۱ و ۲ نام و مسیر فایل‌های باینری نصب شده، نوع فایل و عملیات سیستم‌های‌عامل مربوطه را نشان می‌دهد.

۶-۳-۱ ویندوز

فایل‌های باینری تحت ویندوز در مسیر % UserProfile%\Local Settings\jlc3V7we نصب می‌شوند.

جدول ۱ نام و مسیر فایل‌های باینری نصب شده، نوع فایل و عملیات سیستم‌عامل ویندور

Table 1
Windows binaries

File name or path	File type	Function
6EaqyFfo.zIK	x86_64, executable	Driver
IZsROY7X.-MP	i386, dll	Core module
WeP1xpBU.wA-	i386, executable	Driver
hypn4cqI.HSC	i386, dll	Copy of pstorec.dll
IUnsA3Ci.Bz7	i386, dll	Speex module
t2HBeaM5.OUk	x86_64, dll	64-bit process injection

Mac ۲-۳-۶

فایل‌های باینری Mac در مسیر $HOME\Library\Preferences\jlc3V7we.app نصب می‌شوند.

جدول ۲ : نام و مسیر فایل‌های باینری نصب شده، نوع فایل و عملیات سیستم‌عامل Mac

Table 2
Mac binaries

File name or path	File type	Function
IZsROY7X.-MP	i386, executable	Core module
IUnsA3Ci.Bz7	UB(i386, x86_64), dylib	Core module
mWgpX-aI.8Vq	UB(i386, x86_64), executable	XPC module
WeP1xpBU.wA	i386, dylib	Kernel extension
6EaqyFfo.zIK	x86_64, dylib	Kernel extension
Contents/Resources/WeP1xpBU.wA-.kext/Contents/MacOS/WeP1xpBU.wA	Copy of the above file	-
Contents/Resources/6EaqyFfo.zIK.kext/Contents/MacOS/6EaqyFfo.zIK	Copy of the above file	-
$HOME/Library/ScriptingAdditions/appleHID/Contents/MacOS/IUnsA3Ci.Bz7	Copy of the above file	-

Note: UB stands for Universal Binary, which contains multiple binaries for multiple CPUs.

۴-۶ نقطه بارگذاری

اگر کامپیوتر در معرض خطر، بعد از نصب نرم‌افزار خاموش و دوباره روشن شود Crisis تلاش می‌کند دوباره اجرا شود. در ادامه در مورد نقاط بارگذاری که توسط Crisis استفاده می‌شود، صحبت می‌شود.

۱-۴-۶ ویندوز

این بدافزار کلید رجیستری زیر را ایجاد می‌کند تا وقتی ویندوز شروع به کار کرد اجرا شود.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"*J7PugHy" = "%System%\rundll32.exe,%UserProfile%\Local Settings\jlc3V7we\IZsROY7X.-"MP,F1dd208

۶-۴-۲ Mac

این بدافزار در Mac از اسکریپت‌های بیشتری نیز استفاده می‌کند. این اسکریپت‌های اضافه روشی ایجاد می‌کنند که عملیات اضافه‌ای را که در AppleScript استفاده می‌شود، انتقال دهند. این کدهای اضافه وظیفه‌ی بررسی رویدادهای Apple و رویدادهای داده‌های تهدیدآمیز Apple را بر عهده دارند. هر زمان برنامه‌ای اجرا شود Crisis به صورت خودکار اجرا می‌شود. در زیر قسمتی از لیست ویژگی‌های این اسکریپت اضافه دیده می‌شود.

```
<key>OSAXHandlers</key>
<dict>
<key>Events</key>
<dict>
      <key>RCSeload</key>
      <dict>
            <key>Context</key>
            <string>Process</string>
            <key>Handler</key>
            <string>InjectEventHandler</string>
            <key>ThreadSafe</key>
            <false/>
      </dict>
</dict>
</dict>
```

۶-۵ مشترکات

این بخش عملیات مشترکی را که بر روی هر دو نسخه ویندوزی و Mac توسط این بدافزار انجام شده را توضیح می‌دهد.

۶-۵-۱ مبهم‌سازی فایل نصب

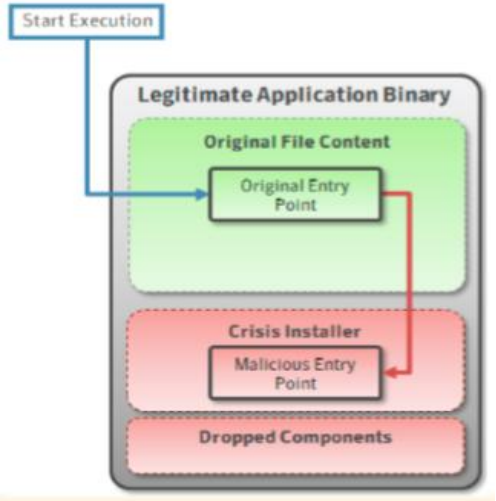
فایل‌های باینری Crisis برای هیچ هدف و مقصودی نه مبهم می‌شوند و نه بسته‌بندی، با این وجود فایل اجرایی نصب مبهم‌سازی شده است. با توجه به سیستم‌عامل کامپیوتر در معرض خطر، فایل نصب مورد نظر منتقل شده و توسط نرم افزار جاوا اجرا می‌شود.

۶-۵-۲ ویندوز

در حال حاضر دو نوع فایل نصب برای ویندوز وجود دارد. نوع اول یک فایل سالم است که تغییر داده شده است. کد فایل نصب به یک نرم افزار قابل اطمینان اضافه شده و نقطه ورودی اصلی برای راه اندازی کد اضافه شده تغییر یافته است. همچنین اجزای قرار داده شده بر روی سیستم به انتهای فایل اضافه گردیده است.

یکی از نمونه‌ها شناسایی شده یک برنامه کاربری SSH است که به گونه‌ای تغییر کرده تا به فایل نصب Crisis تبدیل شود. نمونه‌های دیگر به گونه‌ای به نظر می‌رسند که توسط نویسنده Crisis با استفاده از یک

زبان برنامه‌نویسی به نام scratch ایجاد شده‌اند. این نمونه‌ها از کتابخانه مرتبط شده Lua استفاده کرده و با استفاده از UPX بسته بندی می‌شوند.



شکل ۱۰ فایل باینری تغییریافته‌ی نرم‌افزار

۳-۵-۶ Mac

فایل نصب برای Mac کمی پیچیده است. اگر این فایل را با استفاده از ابزار تحلیل مانند IDA Pro باز کنید کدی مانند کد نشان داده شده در شکل ۱۱ را می‌توان مشاهده کرد.

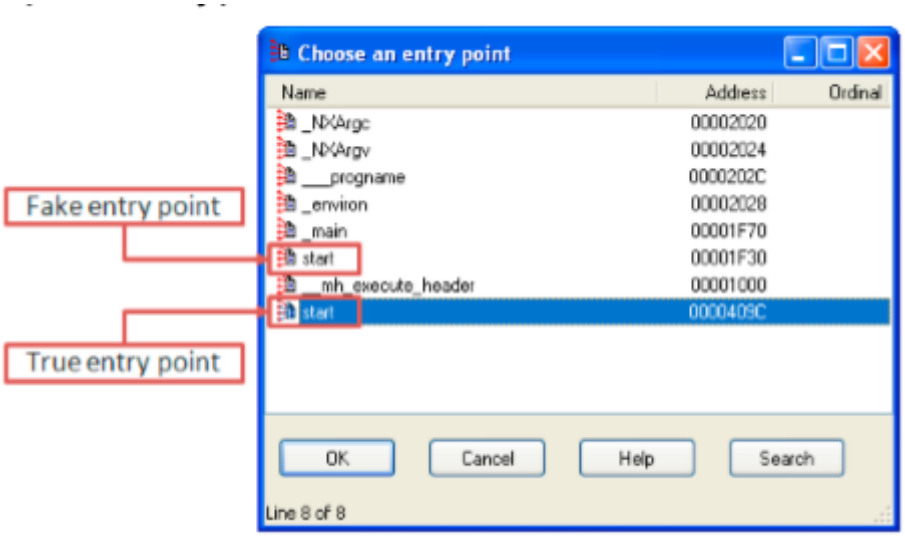
```
                public _main
_main           proc near               ; CODE XREF: start+30↑p

var_8           = dword ptr -8
var_4           = dword ptr -4

                push    ebp
                mov     ebp, esp
                sub     esp, 8
                mov     [ebp+var_8], 0
                mov     eax, [ebp+var_8]
                mov     [ebp+var_4], eax
                mov     eax, [ebp+var_4]
                add     esp, 8
                pop     ebp
                retn
_main           endp
```

شکل ۱۱ قطعه کد فایل نصب Mac

تابع اصلی در این بخش از کد که در شکل ۱۱ مشاهده می‌شود در ظاهر کاری انجام نمی‌دهد اما اگر بیشتر دقت کنید می‌توانید نقطه ورودی تغییر داده شده را ببینید.



شکل ۱۲ نقطه ورودی تکرار شده

نقطه ورودی اصلی در یک قسمت مخفی قرار دارد و EIP این آدرس را با استفاده از دستور بارگذاری LC_UNIXTHREAD قرار می‌دهد.

```
Load command 11
        cmd LC_UNIXTHREAD
    cmdsize 80
     flavor i386_THREAD_STATE
      count i386_THREAD_STATE_COUNT
    eax 0x00000000 ebx    0x00000000 ecx 0x00000000 edx 0x00000000
    edi 0x00000000 esi    0x00000000 ebp 0x00000000 esp 0x00000000
    ss  0x00000000 eflags 0x00000000 eip 0x0000409c cs  0x00000000
    ds  0x00000000 es     0x00000000 fs  0x00000000 gs  0x00000000
```

تمام کدهای مهم در بخش مخفی قرار داده شده‌اند بنابراین نویسنده Crisis می‌تواند به راحتی فایل‌های باینری جدیدی ایجاد یا نرم‌افزار مطمئن دیگری را انتخاب کند و به یک فایل نصب Crisis جدید تبدیل کند. در واقع هر فایل اجرایی می‌تواند به یک فایل نصب Crisis تبدیل شود.

۴-۵-۶ دزدی اطلاعات

هدف اصلی بدافزار Crisis دزدی اطلاعات است. این بدافزار می‌تواند اطلاعات و داده‌های تولید شده توسط خیلی از نرم‌افزارها یا فعالیت‌های انجام شده روی کامپیوتر را جمع‌آوری کند. سپس اطلاعات جمع‌آوری شده را به مهاجم راه دور می‌فرستد. شکل ۱۳ عملیات بی‌شماری که توسط Crisis نظارت می‌شوند را نشان می‌دهد.

شکل۱۳ عملیات نظارت شده توسط Crisis

جدول ۳ عملیات رایج یک بدافزار

Table 3
Details of functions monitored by Crisis

Function	Details
File system	Upload/download files from/onto the compromised computer.
Creating process	Creates a new process and gets the result.
Recording	Audio and video recording using the microphone and the webcam.
Key logging	Records all key strokes that are typed by the user.
Clipboard	Data held in the clipboard.
Screen shot	Takes screen shots.
Wi-Fi	Gets Wi-Fi information, such as SSID and RSSI. This function is called "position" in the Windows version of Crisis, which could be used to determine the location of the compromised computer.
Address book	Steals contact lists.
Browser	Steals Web browser activities.
Instant messenger	Steals instant messenger activities.

توابع موجود جدول ۳ عملیات رایج یک بدافزار است که ما هر روز با آنها مواجه می‌شویم. اگرچه این اولین باری است که تمام آنها را در یک زمان برای سیستم‌های‌عامل ویندوز و Mac می‌بینیم. البته همان‌طور که در جدول ۴ می‌بینیم نرم‌افزارهای مورد نظر بین ویندوز و Mac متفاوتند.

جدول ۴ برنامه‌های کاربردی موجود برای ویندوز و Mac

Table 4

Targeted applications for each platform

	Windows	Mac
Browser	Internet Explorer Mozilla Firefox Google Chrome Opera	Safari Mozilla Firefox
Contact list	Windows Live Mail Windows Mail Microsoft Outlook Mozilla Thunderbird	Address Book
Instant messenger	Google Talk Skype Yahoo Messenger Trillian	Adium Microsoft Messenger Skype

جدول ۴ نشان می‌دهد که بدافزار Crisis بیشتر بر اساس سیستم‌عامل ویندوز تولید شده است زیرا که لیست نرم‌افزارهای تحت پوشش نسخه ویندوزی بیشتر است. به علاوه نسخه ویندوزی بدافزار Crisis شامل قابلیت دزدیدن جزئیات حساب و رمز عبور مربوط به نرم‌افزارهای لیست شده است اما نسخه Mac این قابلیت را ندارد.

در واقع داده‌های مربوط به تقریباً تمام فعالیت‌های انجام شده در کامپیوتر در معرض خطر، می‌توانند توسط Crisis دزدیده شوند که این امر باعث همه‌گیر شدن این بدافزار شده است.

۶-۵-۵ سرویس‌دهنده‌ی فرماندهی و کنترل (C&C)

تمام نمونه‌های Crisis که تا کنون تحلیل کردیم به سرویس‌دهنده‌های C&C واقع در انگلند متصل هستند که از آدرس‌های IP ایستا استفاده می‌کنند. Crisis برای ویندوز و Mac به سرویس‌دهنده‌ی یکسانی متصل می‌شود و فایل پیکربندی سرویس‌دهنده برای هر دو فایل JASON است که با AES128 رمز شده است.

جالب توجه است که میزبان سرویس‌دهنده‌ی C&C، یک سرویس VPS (سرویس‌دهنده‌ی خصوصی مجازی) شناخته شده در انگلند می‌باشد. سرویس VPS به طور عمده برای ماشین‌های مجازی لینوکس استفاده می‌شود اما URLای که توسط بدافزار Crisis استفاده می‌شود شامل یک فایل با پسوند asp. است. به طور کلی فایل asp. برای وب سرویس نرم‌افزار ویندوزی استفاده می‌شود.

۶-۶ ویژگی‌های منحصر به نسخه ویندوزی

این بخش تنها قابلیت‌هایی که نسخه ویندوزی بدافزار Crisis دارد را توصیف می‌کند. برخلاف نسخه Mac، نسخه ویندوزی شامل بعضی قابلیت‌های پیشرفته است.

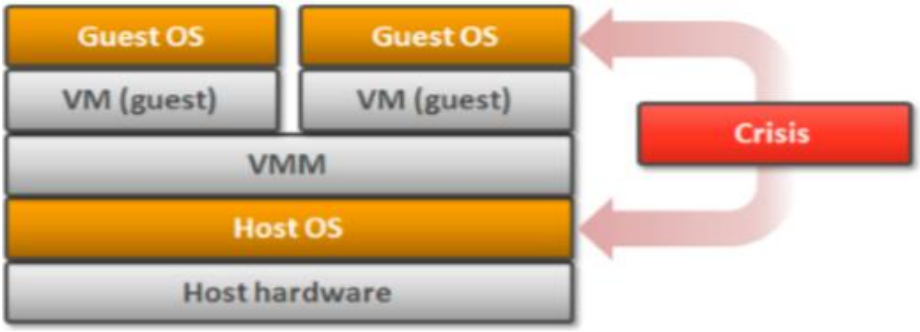
۱-۶-۶ Social

یک تابع با نام Social که برای دزدیدن اطلاعات از سرویس‌های شبکه اجتماعی Facebook و Twitter استفاده می‌شود. این بدافزار علاوه بر دزدیدن پست‌های این سایت‌ها، لیست دوستان و دنباله‌روها را نیز می‌دزدد. تابع Social همچنین برای دزدیدن ایمیل‌ها از سرویس ایمیل تحت وب gmail استفاده می‌کند.

۲-۶-۶ آلوده کردن ماشین مجازی

ماشین‌های مجازی برای اهداف متفاوتی از قبیل توسعه وتحلیل نرم‌افزار مفید هستند. یک ماشین مجازی به طور عمده شامل یک میزبان، یک نظاره‌گر ماشین مجازی (VMM)، نرم‌افزار و یک مهمان است. VMM به کاربر اجازه می‌دهد تا کامپیوترهای مهمان زیادی را در سیستم‌عامل میزبان اجرا کند. به طور کلی، کاربران می‌توانند هر سیستم‌عاملی که توسط VMM پشتیبانی می‌شود را نصب کنند. روی سیستم‌عامل میزبان، تصویر ماشین مجازی شامل فایل‌هایی از قبیل فایل‌های تنظیمات و تصاویر دیسک وجود دارد. این ویژگی هدف نسخه ویندوزی بدافزار Crisis می‌باشد.

نسخه ویندوزی بدافزار Crisis قابلیت پخش شدن به درون ماشین مجازی را دارد. در حال حاضر، این بدافزار به گونه‌ای طراحی شده است که به برخی محصولات نرم افزار VMware محدود است اما روشی که استفاده می‌شود می‌تواند برای تهیه بسیاری محصولات VMware گسترش یابد.



شکل ۱۴ روش آلوده کردن VM

این تهدید، عملیات زیر را به هنگام آلوده کردن ماشین مجازی VMware انجام می‌دهد.

۱. فایل VMware preference را باز می‌کند. فایل VMware preference می‌تواند در مکان ٪UserProfile%\Application Data\VMware\preferences.ini یافت شود.

```
.encoding = "windows-1252"
pref.eula.count = "1"
pref.eula0.product = "VMware Player"
pref.eula0.build = "812388"
vmWizard.guestKey = "windows7-64"
vmWizard.physicalBackend = "D:"
pref.mruVM0.filename = "C:\Users\%USERNAME%\Documents\Virtual Machines\VictimGuest
VictimGuest.vmx"
pref.mruVM0.displayName = "VictimGuest"
pref.mruVM0.index = "0"
```

مثال بالا یک ماشین مجازی به نام VictimGuest دارد.

۲. فایل preference را تجزیه کرده تا مسیر فایل vmx. را پیدا کند. فایل vmx. یک فایل تنظیمات برای تصویر ماشین مجازی است که درون فایل preference قرار دارد.

۳. فایل vmx. را تجزیه کرده تا مسیر فایل vmdk. را پیدا کند. فایل vmx. شامل مسیر فایل vmdk. است که مربوط به فایل تصویر دیسک ماشین مجازی می‌باشد.

```
scsi0.pciSlotNumber = "160"
scsi0.present = "TRUE"
scsi0.sasWWID = "50 05 05 68 67 f6 eb 00"
scsi0.virtualDev = "lsisas1068"
scsi0:0.fileName = "VictimGuest.vmdk"
scsi0:0.present = "TRUE"
scsi0:0.redo = ""
serial0.fileType = "thinprint"
serial0.present = "TRUE"
```

مثال بالا بخشی از فایل vmx. است که شامل نام فایل vmdk. می‌باشد.

۴. دو ورودی رجیستری را باز کرده تا مسیر فایل vixDiskMountServer.exe که به صورت زیر می باشد را پیدا کند:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\vmplayer.exe\"@" = "C:\\ Program Files (x86)\\VMware\\VMware Player\\vmplayer.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\vmplayer.exe\"Path" = "C:\\Program Files (x86)\\VMware\\VMware Player\\"

مسیر بالا فقط یک مثال است. این مسیر وقتی ماشین مجازی نصب می‌شود می تواند تغییر کند.

۵. فایل vmdk. را مانند درایو Z بارگذاری می‌کند. فایل vixDiskMountServer.exe یک ابزار است که با برنامه VMware نصب می‌شود. این فایل می‌تواند برای بارگذاری تصویر vmdk. استفاده شود. بدافزار Crisis به جستجوی یک دستگاه است که نامی شامل "vstor2" دارد و در درایو Z قرار می‌گیرد.

۶. فایل نصب خود را در پوشه startup در درایو Z کپی می‌کند. بدافزار فایل نصب خود را در پوشه startup زیر در درایو Z کپی می‌کند:

- Z:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\mWgpX-al.exe
- Z:\Documents and Settings\All Users\Start Menu\Programs\Startup\mWgpX-al.exe

اولی برای ویندوز ویستا و ویندوز ۷ است و دومی برای ویندوز XP است. اگرچه زمانی که تلاش کند تا فایل نصب را روی ویندوز XP کپی کند فرآیند شکست می‌خورد. بنابراین فرآیند نفوذ ماشین مجازی که در حال حاضر در حال اجراست تنها زمانی می‌تواند موفق شود که سیستم عامل مهمان ویندوز ویستا یا ویندوز ۷ باشد. این می‌تواند یک اشتباه در کد باشد اما نمی‌توانیم به طور قطعی بگوییم که این یک اشکال است.

در گذشته هر زمان تشخیص داده می‌شد که یک بدافزار در یک محیط مجازی در حال اجرا است بدافزار عملیات را متوقف می‌کرد، بدین وسیله تلاش برای خنثی کردن تحلیل این تهدید نیز متوقف می‌شد. Crisis به این طریق کار نمی‌کند زیرا این اولین بدافزار بیرون از ماشین مجازی است که فعالانه تلاش می‌کند به درون ماشین مجازی گسترش یابد نه اینکه اجرای آن را متوقف کند. این طبیعت عرصه بدافزار است که وقتی یک مفهوم جدید پیاده‌سازی شد دیگر نویسندگان بدافزار سریع آن روش را برای کد مخرب خود تطبیق دهند. به این معنی که احتمال دارد در آینده با روش‌های بیشتری که بدافزار برای گسترش به درون ماشین مجازی به کار می‌گیرد آشنا شویم.

در ابتدا، ماشین‌های مجازی برای اهداف محدودی از قبیل ابزار حرفه‌ای برای توسعه و تحلیل و سرویس‌دهنده‌های بزرگ تولید شده بودند. اما این روزها استفاده از ماشین‌های مجازی خیلی شایع هستند. ما همچنین از وب سرویس‌های زیادی استفاده می‌کنیم که روی سرویس‌های VPS اجرا می‌شوند. بدافزار Crisis یک سری حملات جدید که ماشین مجازی را هدف گرفته است، را نشان می‌دهد. خوشبختانه، بدافزار Crisis از هیچ آسیب‌پذیری در نرم‌افزار VMware بهره‌برداری نمی‌کند و همچنین نمی‌تواند به تمام ماشین‌های مجازی در این زمان نفوذ کند در واقع این بدافزار تنها به VMware Workstation نفوذ می‌کند و نه VMware ESX اما ما باید خود را برای نسل بعدی بدافزار Crisis آماده کنیم.

در این گزارش ما در مورد فرآیند آلوده کردن ماشین مجازی میزبان به مهمان بحث کردیم. احتمال دیگری که می‌توان بررسی کرد آلوده کردن ماشین مجازی مهمان به میزبان است. سناریوی نفوذ میزبان به مهمان

به صورت مستقیم بستگی به امتیاز دسترسی به تصویر دیسک VM دارد. با این وجود اگر نفوذ مهمان به میزبان واقعیت پیدا کند، احتمال زیادی دارد که باعث آسیب‌پذیری در VMM شود. اگرچه همان‌طور که قبلاً در این گزارش گفته شد، Crisis از هیچ آسیب‌پذیری در نرم‌افزار VMware در این نقطه در زمان بهره‌برداری نمی‌کند. نفوذ مهمان به میزبان بر این موضوع دلالت دارد که نرم‌افزار قادر است از جعبه شن ماشین مجازی فرار کند. در حال حاضر روش دوم ممکن نیست اما اگر واقعاً این امکان وجود داشته باشد این دو روش نفوذ متقاطع می‌توانند باعث وقوع سناریوی کابوس‌واری شوند که نفوذ مهمان به مهمان نیز می‌تواند اتفاق بیفتد. در این صورت این اتفاق ممکن است ایمنی مورد نظر در مورد ایزوله کردن ماشین مجازی را مورد هدف قرار دهد.

در نهایت، بررسی این مسأله که آیا نویسنده‌ی برنامه‌ی بدافزار Crisis مسئول آزادکردن این تهدید به جهان است یا نه ارزش دارد. بعضی از فروشندگان محصولات امنیتی و محققان باور دارند که یک گروه در ایتالیا بدافزار Crisis را به عنوان محصولی برای فروش به سازمان‌های اجرای قانون تولید کردند. در واقع تعدادی از توابع بدافزار Crisis از قبیل ضبط صدا و دزدیدن اطلاعات دفترچه آدرس برای تحقیقات خصوصی و جاسوسی مناسب است. متن روی وب سایت گروه و قابلیت‌های بدافزار Crisis در واقع کاملاً شبیهند. با این وجود نمی‌توان لزوماً اثبات کرد که چه کسی مسئول ایجاد Crisis است.

در حالت کلی، دنبال کردن منبع برنامه مخرب مشکل است زیرا نویسنده اغلب بسیار طولانی کد زده است تا از فاش شدن هویتش جلوگیری کند. با این وجود بخشی از داده که در شکل ۱۵ دیده می‌شود از تحلیل فایل نصب Crisis به‌دست آمده است و شامل نام نویسنده می‌باشد.

```
.rdata:004421EB                 db  8Ch ; Î
.rdata:004421EC                 db    2
.rdata:004421ED                 db    0
.rdata:004421EE                 db    0
.rdata:004421EF                 db    0
.rdata:004421F0 $_projectPath   db 'C:\Users\[illegible]\documents\visual studio 2010\Projects\Win3'
.rdata:004421F0                 db '2Test\Release\Win32Test.pdb',0
.rdata:0044224D                 db    0
.rdata:0044224E                 db    0
.rdata:0044224F                 db    0
```

شکل ۱۵ نام نویسنده در کد دیده می‌شود

داده شامل مسیر فایل پروژه و مسیری می‌باشد که نام کاربر را دربردارد. با تحقیق به دنبال این اسم در اینترنت کشف کردیم که کاربر یکی از اعضا گروهی در ایتالیا است. در نتیجه این احتمال وجود دارد که اعضا گفته شده که برنامه Crisis را ایجاد کردند از این گروه باشند. با وجود کشف کردن این ارتباط ما هنوز هویت درستی از کسی که پشت این برنامه است نداریم. همان طور که در بخش مبهم‌سازی فایل نصب گفته

شد این فایل می‌تواند هر نرم‌افزاری باشد که تغییر یافته است بنابراین دیگر نمی‌تواند همان نرم افزار قبلی باشد.

۶-۷ نتیجه‌گیری

قطعاً امکان پذیر است که بدافزار Crisis در ابتدا برای اهداف اجرای قانون تولید شده باشد تا تحقیقات خصوصی یا جاسوسی انجام دهد، مانند قابلیت‌هایی که درون کد وجود دارد و بسیار پیشرفته و مناسب است. این بدافزار قابلیت نفوذ چندبستری را برای سیستم‌های‌عامل مایکروسافت ویندوز و Mac بر روی Apple فراهم می‌کند همچنین توانایی پخش از طریق محیط ماشین مجازی را دارد. می‌دانیم که این بدافزار می‌تواند ماژول‌های خود را روی بستر ویندوز موبایل قرار دهد اما متأسفانه ماژول‌های موجود برای تحلیل را نداشته و بنابراین هیچ مدرکی از قابلیت‌های آن روی موبایل نداریم.

Crisis می‌تواند اولین بدافزاری باشد که قابلیت پخش به درون ماشین مجازی را دارد. کاربرد روش VM هر روز زیاد می‌شود بنابراین ویژگی‌های پیدا شده در Crisis پیامدهای قابل توجهی را برای صنعت امنیت به همراه دارد. قابل توجه است که قابلیت انتشار مانند قابلیت دزدیدن اطلاعات در Crisis تنها برای بستر ویندوزی ایجاد شده است. علاوه براین حتی توابع رایج در هردو نسخه ویندوزی و Mac پیاده سازی بهتری روی بستر ویندوزی دارند.