
تکنیک های حمله و
استخراج اطلاعات از
شبکه هایAir-Gap
By: Meysam Nazemi

تکنیک های نفوذ به شبکه های Air-Gap

بحث هک و نفوذ به شبکه هایی همچون زندان اوین، زندان قزل حصار کرج، شرکت پخش فراورده های نفتی ایران (کارت سوخت) که اخیراً صورت گرفته و همچنین سازمان انرژی اتمی همواره ذهن متخصصین و علاقه مندان به حوزه امنیت را به خود معطوف کرده است. شاید برای شما هم این سوال پیش آماده باشد که چطور این شبکه ها که ایزوله هستند و به اینترنت دسترسی مستقیم نداره مورد هک و نفوذ قرار گرفته اند؟ نفوذگران از چه تکنیک یا تکنیک هایی جهت نفوذ به شبکه های ایزوله شده استفاده می کنند؟ سعی خواهیم کرد در این مقاله به پاسخ سوال هایی از این دست بپردازیم.

شبکه ایزوله یا Air-Gap چیست؟

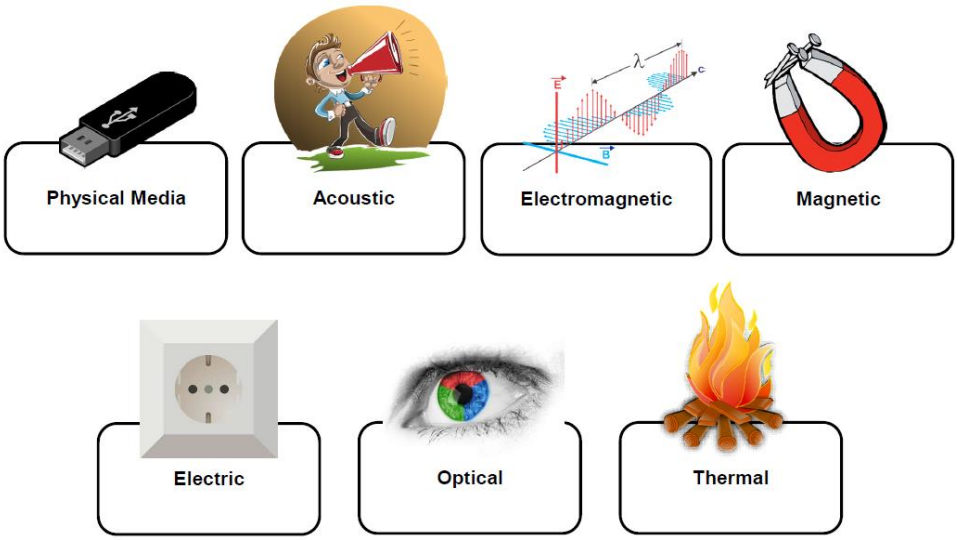
سازمان هایی که با اطلاعات حساس سر و کار دارند از سامانه های امنیتی شبکه برای حفاظت از داده های حیاتی خود بطور گسترده بهره می‌برند. با اینکه چنین سامانه هایی امنیت بیشتری را نسبت به دیگر سیستم‌ها تأمین می‌کنند در عین حال راه هایی برای به خطر انداختن آنها وجود دارد که اجازه می دهد مهاجمان اطلاعات حساس سازمان را به سرقت ببرند. به عنوان مثال سیگنال های رادیویی ساطع شده توسط کارت های گرافیک، کارت صدا و ارتباطات از راه میکروفن و بلندگو جزء سیستم های هستند که اولین بار فورت ناکس اندازه گیری میزان امنیت آن را مورد توجه قرار داد. واژه-Air Gappedبه راهکاری گفته می‌شود که از داده های حیاتی با ایزوله کردن یک یا چند سیستم از شبکه نا امن مانند اینترنت، محافظت می‌نماید. شبکه های Air-Gapped در واقع شبکه های ایزوله ای هستند که مستقل از اینترنت بوده و بصورت کاملاً آفلاین عمل می کنند. این شبکه ها حتی به شبکه بلوتوث و شبکه داخلی نیز دسترسی ندارند و کاملاً ایزوله هستند. مدیران فناوری اطلاعات ممکن است سامانه های حساسی همچون سیستم های نظامی، سیستم های کنترل و نظارت تأسیسات زیر بنایی و حیاتی را به منظور محافظت از داده های آنها در برابر نفوذ، ایزوله نمایند. متأسفانه هیچ سیستمی صد در صد امن نمی باشد و همیشه راهی برای دور زدن و bypass تدابیر امنیتی وجود خواهد داشت. حتی به نظر می رسد برخی از این روش های نفوذ بطور مستقیم از داستان های علمی تخیلی نشأت گرفته باشد!.

توجه: شبکه های Air-Gap را با نام هایی همچون: شبکه شکاف هوا، شبکه های ایزوله شده، شبکه های محدود و بدون دسترسی به اینترنت هم می شناسند.

کامپیوتر Air-Gapped چیست؟

کامپیوترهای Ari-Gapped، سیستم هایی هستند که از اینترنت، شبکه های محلی، بلوتوث جدا شده اند و بنابراین اعتقاد بر این است که امن ترین دستگاه ها هستند و نفوذ یا نفوذ به آنها دشوار است.

امروزه مهاجمان با انگیزه بالا می توانند از بدافزارهای طراحی شده ویژه برای استخراج داده ها از یک کامپیوتر Air-Gapped از طریق نور، صدا، گرما، الکترومغناطیسی، مغناطیسی، مادون قرمز و امواج اولتراسونیک استفاده کنند.



شبکه های Ari-Gap کجا استفاده می شوند؟

نمونه هایی از انواع شبکه ها یا سیستم هایی که ممکن است در آنها از Air-Gapped Networkها شوند عبارتند از:

- شبکه های نظامی
- شبکه های دولتی
- سیستم های مالی، مانند بورس اوراق بهادار
- سیستم های کنترل صنعتی، مانند SCADA در زمینه های نفت و گاز
- سیستم های حیاتی، مانند کنترل نیروگاه های هسته ای
- رایانه های مورد استفاده در هواپیمایی و هوانوردی، مانند FADECs، ترافیک هوایی کنترل سیستم ها و avionics
- تجهیزات پزشکی رایانه ای
- سیستم های بسیار ساده، که در وهله اول نیازی به به خطر انداختن امنیت نیست، مانند: واحد کنترل موتور و سایر دستگاه های موجود در CAN bus در اتومبیل، یک ترموستات دیجیتال برای تنظیم دما و کمپرسور در HVAC و سیستم های برودتی خانگی
- کنترل کننده آب پاش های الکترونیکی برای آبیاری چمن ها
- و...

مثال هایی از شبکه های Air-Gap

شبکه های دارای شکاف هوا یا Ari-Gapped Networkها کاملاً ایمن نیستند، راه های مختلفی برای استخراج اطلاعات یا اصطلاحاً Exfiltration از کامپیوترهای جدا شده از اینترنت وجود دارد. هر تکنیک برای انجام داده ها، از امواج صوتی تا امواج الکترومغناطیسی، بر بردار متفاوتی متکی است.

تکنیک های نفوذ و استخراج اطلاعات از شبکه های Air-Gapped

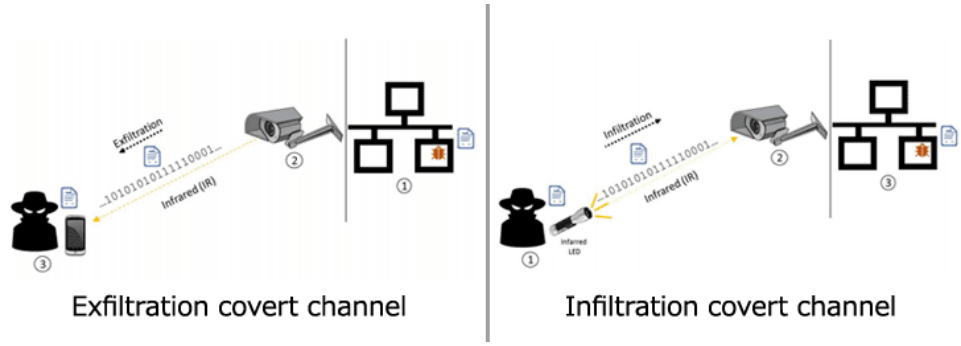
اولین بار محققیق امنیتی از دانشگاه Ben-Gurion (بن گوریون) کشور اسرائیل تکنیک هایی را در قالب Cover Channel که هدف آنها کامپیوترهای شبکه های Air-Gapped هست ارائه کردند. بطور کلی ۱۲ تکنیک جهت هک ماشین های air-gap توسط این محقیق در جریان کنفراس Black-hat سال ۲۰۱۸ ارائه شده که همگی این تکنیک ها مبتنی بر ارتباطات کاملاً درون شبکه ای می باشند. اسلاید مربوط به کنفرانس تکنیک های نفوذ و استخراج اطلاعات از شبکه های Air-Gapped در جریان کنفرانس امنیتی Black-hat:

https://i.blackhat.com/us-18/Wed-August-8/us-18-Guri-AirGap.pdf

روش کار هر یک از این تکنیک ها را بطور کلی در ادامه این مقاله مطرح خواهیم کرد.

تکنیک aIR-Jumper

در این حمله اطلاعات حساس از کامپیوترهای Air-Gapped به کمک دوربین های CCTV مجهز به infrared که برای دید در شب مورد استفاده قرار می گیرند استخراج می شود. در این حمله به طور کلی از ۲ سناریو می توان بهره برد استخرجا یا Exfiltration اطلاعات حساس از شبکه Air-Gapped توسط تکنیک aIR-Jumper و ارسال داده ها یا Infiltration به شبکه Air-Gapped توسط تکنیک aIR-Jumper به شبکه Air-Gapped. در ادامه به توضیح هر یک از دو سناریو خواهیم پرداخت.



سناریو Exfiltration یا استخراج داده از شبکه Air-Gapped توسط تکنیک aIR-Jumper

در این روش حمله کنندگان می توانند از دوربین های نظارتی نور مادون قرمز برای ایجاد کانال ارتباط پنهان دو طرفه بین شبکه های داخلی سازمان ها و مهاجمان از راه دور ایجاد کنند. نشت داده ها از شبکه Air-Gap و نفوذ و ارسال اطلاعات به شبکه Air-Gap شده توسط دوربین های نظارت و امنیت مجهز به LEDهای اکسفیلتراسیون IR، که برای دید شب استفاده می شوند با استفاده از روش aIR-Jumper امکان پذیر می باشد.

در این سناریو نرم افزارهای مخرب در داخل سازمان دسترسی و روشنایی IR دوربین های نظارتی در سراسر شبکه محلی را که در محیط Air-Gap واقع شده است، کنترل می کند. اطلاعات حساس مانند کدهای پین، رمزهای عبور و کلید رمزگذاری سپس تعدیل می شوند و توسط سیگنال‌های IR دوربین نظارتی فرستاده می‌شوند. یک مهاجم در یک منطقه عمومی (به عنوان مثال، در خیابان) با یک خط دید مناسب به دوربین نظارت سیگنال های IR را ثبت و رمزگشایی می کند به این صورت سناریوی نشت اطلاعات از محیط Air-Gap پیاده سازی می شود.

سناریو Infiteration یا ارسال داده به شبکه Air-Gapped توسط تکنیک aIR-Jumper

و اما در سناریوی دوم یعنی ارسال داده به شبکه مذکور، یک مهاجم ایستاده در یک منطقه عمومی (به عنوان مثال، در خیابان) از LEDهای IR برای ارسال سیگنال های پنهان به دوربین های نظارت استفاده می کند. داده های باینری مانند فرمان و کنترل (C&C) در بالای سیگنال های IR رمزگذاری می شوند. سیگنال ها سپس در جریان ویدئو پنهان شده و پس از آن توسط بدافزار ساکن در شبکه Air-Gap شده رمزگشایی می شوند. ارزیابی های صورت گرفته مشخص می کند که از Cover Channel مذکور داده ها را می توان به طور مخفیانه از یک exfiltrated با سرعت ۲۰ بیت / ثانیه در هر دوربین نظارت به فاصله یک تا ده ها متر دورتر ارسال کرد. همچنین در سناریوی دوم یعنی ارسال داده ها به صورت مخفیانه به شبکه Air-Gap شده یک سازمان با سرعت بیش از ۱۰۰ بیت / ثانیه در هر دوربین نظارت از فاصله صدها متر تا کیلومتر دور امکان پذیر می باشد. البته برای افزایش سرعت نرخ انتقال می‌توان از چند دوربین نظارتی در این سناریوها استفاده کرد و یا با منطقه بندی بین بخش های مختلف، کدهای اختصاصی برای هر بخش ارسال نمود.

در ادامه می‌توانید دو فیلم مربوط به روش aIR-Jumper را در زیر مشاهده کنید.

https://youtu.be/auoYKSzdOj4
https://youtu.be/om5fNqKjj2M
https://www.youtube.com/watch?v=jHb9vOqviGA

جهت کسب اطلاعات بیشتر در تکنیک aIR-Jumper به مقاله مربوطه در آدرس زیر مراجعه نمایید:
https://arxiv.org/ftp/arxiv/papers/1709/1709.05742.pdf

تکنیک MOSQUITO

در این تکنیک از دو یا چند PC که در داخل یک شبکه Air-Gapped و در یک اتاق هستند می توان با استفاده از امواج ultrasonic اطلاعات حساس را استخراج کرد. برای چنین حملاتی لازم است تنها در سیستم ایزوله صنعتی فقط یک اسپیکر یا یک هدفون معمولی حتی بدون میکروفون متصل باشد.
در واقع در سال ۲۰۱۶ همین جمع از محقیقین کشور اسرائیل نشان دادند که چگونه مهاجمان می توانند بطور مخفیانه به مکالمات خصوصی در اتاق شما گوش دهند، فقط با استفاده از بدافزار، هدفون های شما (متصل به رایانه آلوده) را به میکروفون متصل کنند.
در سال ۲۰۱۸، همین جمع از محققان با آخرین تحقیقات خود را به سطح بالاتری رسانده و راهی برای تبدیل برخی از بلندگوها/هدفون ها/گوشی هایی که در اصل برای عملکرد به عنوان میکروفون طراحی نشده اند به یک دستگاه شنود - در حالی که میکروفون استاندارد وجود ندارد، یا mute شده و یا خاموش نیست، شنود نمود.

از آنجاییکه برخی از بلندگوها/هدفون‌ها/گوشی‌ها به‌خوبی به محدوده فراصوت (۱۸ کیلوهرتز تا ۲۴ کیلوهرتز) پاسخ می‌دهند، محققان دریافتند که چنین سخت افزاری می‌تواند به عنوان میکروفون معکوس شود.

علاوه بر این، وقتی صحبت از یک ارتباط مخفی به میان می آید، بدیهی است که دو کامپیوتر نمی توانند با استفاده از بلندگوها و هدفون، داده‌ها را از طریق صداهای شنیداری مبادله کنند. بنابراین، امواج فراصوت نامشهود بهترین کانال مخفی صوتی را برای ارتباط بلندگو به بلندگو ارائه می دهد.
ویدئوهای زیر در جهت اثبات تکنیک MOSQUITO ارائه شده اند:

https://youtu.be/O_jz2mDwAew

https://youtu.be/ZD8CNxYe5dk

در صورت تمایل جهت کسب اطلاعات بیشتر در خصوص تکنیک MOSQUITO می توانید به مقاله ارائه شده آن به آدرس زیر مراجعه نمایید:

https://arxiv.org/pdf/1803.03422.pdf

تکنیک Fansmitter

روشی جهت استخراج داده های حساس از طریق صدای منتشر شده به وسیله فن های رایانه های Air-Gapped می باشد. در تاریخ ژوئن ۲۰۱۶ خبر آمد که پژوهشگران حوزه امنیت در کشور اسرائیل موفق به طراحی بدافزاری شدند که بر مبنای فن کامپیوترها قادر است به سرقت داده ها بپردازد. یک تیم از پژوهشگران دانشگاهی Ben-Gurion مدعی شده‌اند، بدافزاری طراحی کرده اند که توانایی استخراج داده ها از یک کامپیوتر ایزوله را بدون نیاز به یک ارتباط اینترنتی یا سخت افزار خاص صوتی یا دوربین دارد. این بدافزار صدایی که توسط پردازشگر ماشین و فن های مربوط به آن تولید می شود را برای سرقت داده ها مورد استفاده قرار می‌دهد.

در این روش یک نرم افزار مخرب که بر روی رایانه ایزوله شده هدف قرار می‌گیرد می‌تواند از فن های دستگاه برای ارسال بیت های داده به گوشی های تلفن همراه در مجاورت آن و یا یک رایانه دیگر که مجهز به میکروفن باشد، استفاده کند. در این تکنیک از چندین نوع فن می‌توان استفاده کرد، اما فن های پردازنده و کیس از همه بهتر هستند، چرا که می‌توان آنها را از طریق نرم افزارهای بسیار زیادی کنترل کرد.

در حالیکه روش های دیگر بر مبنای امواج مافوق صوتی که از طریق اسپیکرهای ماشین ها تولید می شود، متمرکز هستند، روش مورد استفاده توسط این گروه از محققان با کنترل و گوش کردن به سرعت فن های یک ماشین و پردازنده مرکزی آن انجام می شود. در این روش نیازی به هیچ اسپیکر، دوربین یا سخت افزار جانبی نیست. پژوهشگران این مکانیزم حمله را اینگونه تشریح کرده اند: «در این روش ما

موفق شدیم، داده ها را از طریق یک شکاف هوایی به وجود آمده توسط کامپیوتر و بدون نیاز به تجهیزات صوتی به یک اسمارت فون دریافت کننده در همان اتاق ارسال کنیم. متد می تواند نشتی داده ها در انواع مختلفی از تجهیزات مورد استفاده در دنیای فناوری اطلاعات، سامانه های توکار و دستگاه های اینترنت اشیاء یا IoT که هیچگونه سخت افزار صوتی ندارند، اما دارای فن هایی در ابعاد و اندازه های مختلف هستند را شناسایی کرده و به استخراج آنها بپردازد.»

مدل حمله Fansmitter چگونه است؟

بطور معمول در این حمله، انتقال دهنده یک کامپیوتر دسکتاپ معمولی و دریافت کننده تلفنی است که در مجاورت آن قرار دارد. در مرحله اول، انتقال دهنده و دریافت کننده توسط هکر در معرض تهدید قرار می‌گیرند. در این مکانیزم حمله برای آلوده سازی یک شبکه بسیار ایمن می توان از تکنیک های مورد استفاده توسط بدافزارهایی همچون Agent.Btz بهره برد. در این روش حمله، کامپیوتری که باید آلوده شود حتماً باید به یک پردازنده داخلی یا فنی که روی کیس نصب شده، تجهیز شده باشد. امروزه بسیاری از سیستم‌های کامپیوتری از چنین ساز و کاری استفاده می کنند. آلوده سازی یک تلفن همراه با چالش کمتری روبرو است. بطوریکه می توان از بردارهای مختلف حمله همچون ارسال ایمیل ها، پیام کوتاه متنی یا ویدئویی، برنامه های مخرب و... برای آلوده سازی تلفن همراه استفاده کرد. در ادامه اطلاعات حساس کامپیوتر (کلیدهای رمزنگاری و...) جمع آوری شده، تعدیل شده و از طریق امواج مافوق صوت و با استفاده از فن های داخلی کامپیوتر به بیرون از آن فرستاده می شود. یک تلفن همراه که نقش یک دریافت کننده (گیرنده) را بازی کرده و مجهز به یک میکروفون است این داده های انتقال یافته را شناسایی و دریافت کرده، در ادامه این داده ها را دمدوله و رمزگشایی کرده و آنها را برای یک هکر از طریق داده های موبایلی همچون SMS یا WiFi ارسال می‌کند. البته به این نکته توجه داشته باشید، در مدل ارائه شده توسط این گروه از پژوهشگران از یک تلفن همراه به عنوان یک دریافت کننده استفاده شده است. دستگاهی که بطور معمول در مجاورت سیستم های کامپیوتری قرار دارد. اما از انواع دیگری از گیرنده ها همچون کامپیوتری با یک میکروفون، لپ تاپ و... می‌توان استفاده کرد. تصویر زیر نشان می‌دهد چگونه یک کامپیوتر شخصی که در مجاورت یک تلفن همراه قرار دارد، به سادگی قربانی این حمله می شود.

این بدافزار که احتمالضا از طریق عامل هایی همچون درگاه USB یک ماشین را آلوده می کند، رفتاری شبیه به کدهای مورس دارد. زمانی که نصب می شود، مکان داده ها روی یک ماشین را پیدا کرده و با کنترل سرعت فن پردازنده ماشین و فن خنک کننده سیستم شکلی از یک موج صوتی را تولید کرده و این امواج را برای دستگاهی که در آن نزدیکی قرار دارد، برای رمزگشایی ارسال می‌کند. البته در این روش سرعت انتقال نسبتاً کند است. محققان اعلام کرده اند در این روش نرخ دریافت داده‌ها ۹۰۰ بیت بر ساعت است که برای گوش کردن به دستگاهی که در فاصله هشت متری از ماشین قرار دارد، ارسال می شود. در حالیکه این مکانیزم برای دانلود یک آلبوم موسیقی ایده آل نیست، اما برای سرقت گذرواژه‌ها و کلیدهای رمزنگاری ایده آل است. به نظر می رسد این تحقیق تکمیل کننده تحقیقاتی است که در ارتباط با badBIOS انجام شده است. یک قطعه بدافزاری مخرب و افسانه ای که با هدف باز کردن حفره ای در قلب سیستم عامل یک سامانه کامپیوتری به منظور به وجود آوردن نشتی داده ها از طریق امواج مافوق صوت ساطع شده توسط سیستم مورد استفاده قرار می گیرد.

تحقیق مشابه دیگری نشان می دهد چگونه می توان بطور محرمانه کلیدهای تایپ شده توسط کاربر را در قالب یک گزارش محرمانه و به صورت یک فایل صوتی عادی که از طریق اسپیکرهای کامپیوتر پخش می شود، به سرقت برد.

ویدئو مربوط به اثبات تکنیک Fansmitter:

https://www.youtube.com/watch?v=v2_sZIfZkDQ

در صورت تمایل جهت کسب اطلاعات بیشتر در خصوص تکنیک Fansmitter می تواند به مقاله ارائه شده آن در لینک زیر مراجعه نمایید:

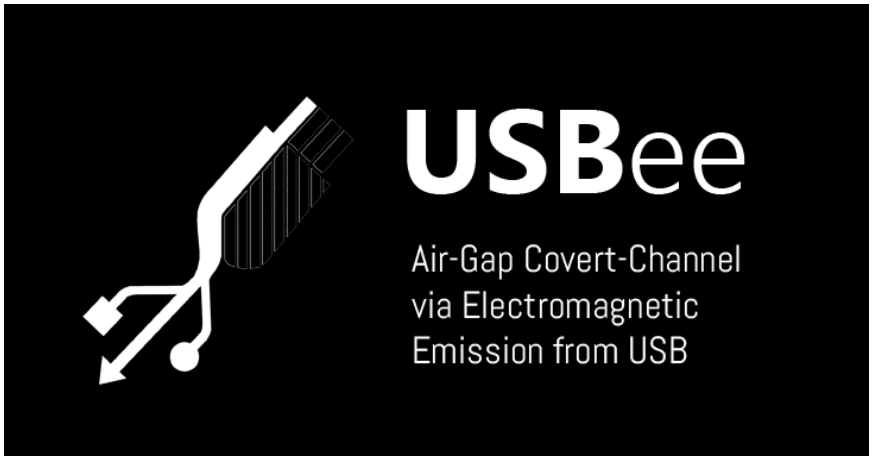
https://arxiv.org/ftp/arxiv/papers/1606/1606.05915.pdf

تکنیک USBee

تیمی از محققان دانشگاه بن گوریون در کشور اسرائیل راهی برای استخراج اطلاعات حساس از رایانه های دارای شکاف هوا - این بار با استفاده از انتقال فرکانس رادیویی از کانکتورهای USB بدون نیاز به سخت افزار تخصصی نصب شده بر روی USB، کشف کرده اند.

این حمله که USBee نامیده می‌شود، پیشرفت قابل توجهی نسبت به حذف کننده USB ساخته شده توسط NSA به نام CottonMuth است که در سندی که توسط ادوارد اسنودن، کارمند سابق NSA به بیرون درز کرده بود، اشاره شد.

در این روش سیستمی که در محیط Air-Gap قرار دارد با اتصال یک حافظه قابل حمل آلوده می شود و همین حافظه قابل حمل (که از طریق کابل USB به سیستم متصل است) داده ها را که همان کلمات کلیدی می باشند به سیستمی دیگر خارج از محیط Air-Gap ارسال می کند. این سیستم نیز مجهز به یک گیرنده با آنتن معمولی است که از طریق درگاه USB به سیستم متصل شده است. داده ها در این سیستم با تبدیل فرکانس به محتوای باینری تبدیل به همان داده ارسالی خواهند شد.



برخلاف CottonMuth، USBee به مهاجم نیازی ندارد که یک دستگاه USB تغییر یافته را به محل قرارگیری رایانه دارای شکاف هوا که هدف قرار گرفته است، منتقل کند. در عوض، این تکنیک دستگاه های USB را که قبلاً در داخل تأسیسات قرار دارند، به یک فرستنده RF بدون تغییر سخت‌افزار تبدیل می‌کند.

علاوه بر این، USBee هیچ ایمپلنتی در سیستم عامل و درایورهای USB برای اجرای حمله ندارد. محققان در یک مقاله تحقیقاتی خود نوشته اند: «ما یک روش نرم افزاری را برای استخراج داده های کوتاه برد با استفاده از انتشارات الکترومغناطیسی از یک دانگل USB معرفی می کنیم. برخلاف روش‌های دیگر، روش ما به سخت افزار انتقال [RF] نیاز ندارد زیرا از گذرگاه داده داخلی USB استفاده می‌کند. محققان تأکید می‌کنند که روش حمله USBee صرفاً مبتنی بر نرم افزار است، اگرچه برای اجرا باید شرایط خاصی را داشته باشد. آنها همچنین اشاره کرده اند: کامپیوتر محافظت شده باید به بدافزار آلوده شود، به احتمال زیاد، با کمک یک خودی. هر دستگاه USB باید به آن رایانه آلوده وصل شود. مهاجم باید در نزدیکی دستگاه در معرض خطر قرار گیرد، معمولاً حداکثر در فاصله ۳-۵ متری. USBee با تعدیل داده‌هایی که با سرعت بالا به دستگاه‌های متصل شده تغذیه می‌شوند، درگاه‌های USB رایانه مورد نظر را به فرستنده‌های فرکانس رادیویی کوچک (RF) تبدیل می‌کند."

در صورتی که نیازمند اطلاعات و جزئیات بیشتر هستید، می‌توانید ویدیوی مربوطه و سند روش پیاده‌سازی این روش را از لینک زیر دانلود کنید.

https://youtu.be/E28V1t-k8Hk

در صورت تمایل جهت کسب اطلاعات بیشتر در خصوص تکنیک BitWhisper می تواند به مقاله ارائه شده آن در لینک زیر مراجعه نمایید:

https://cyber.bgu.ac.il/t/USBee.pdf

تکنیک BitWhisper

در سال ۲۰۱۵ خبر آمد که محقیق دانشگاه Ben-Gurion کشور اسرائیل (اسامی محققین: Mordechai Guri، Matan Monitz، Yisorel Mirski و Yuval Elovici) موفق به معرفی تکنیکی جهت استخراج اطلاعات توسط گرما و حرارت ایجاد شده توسط CPU و GPU سیستم های کامپیوتری شده اند. این تکنیک که متکی بر تبادل حرارت بین دو سیستم کامپیوتری است تا رمزهای عبور یا کلیدهای امنیتی را به صورت مخفیانه ذخیره کند. معمولاً برای رایانه ها گرما یک موضوع دردسر ساز و اساساً یک مشکل است. اما اکنون به غیر از بلند شدن دود از CPU یا GPU رایانه باید نگران یک موضوع مهم دیگر در خصوص گرما نیز بود.

وب سایت Net-Security گزارش داد که یک تیم تحقیقاتی در دانشگاه «بن گوریون» در کشور اسرائل، اقدام به طراحی و تولید بد افزاری کرده اند با نام BitWhisper که به هیچ وجه شبیه به بد افزارهایی که معمولاً کاربران با آنها سر و کار دارند نیست. این بد افزار یکی از عجیب ترین بد افزارهایی است که به عنوان ابزار هک از آن استفاده می شود.

کار این بد افزار به این ترتیب است که دستگاه های آلوده به آن می توانند داده ها را با استفاده از گرمایی که تولید می کنند منتقل سازند. برای مثال فرامین و دستورات می توانند با ایجاد مدولاسیون یا نوسان حرارتی از یک سیستم به سیستم دیگر منتقل شوند. به این ترتیب دستگاه یا سیستم هدف، با استفاده از سنسورهای حرارتی خود این فرامین را دریافت کرده و واکنش تعریف شده را نشان می دهد. از طریق این مکانیزم همچنین می توان میزان داده های کوچک همچون گذرواژه ها را نیز منتقل ساخت:

شاید در ابتدا این سیستم و مکانیزم چندان برای هک رایانه ها کاربردی به نظر نرسد، اما زمانیکه به اهداف اصلی این بد افزار یعنی BitWhisperواقف شویم میزان جدیت کار آن را درک می کنیم. این بد افزار بیش از هر چیز مخصوص به سیستم های شکاف هوایی یا Air-Gappedطراحی شده است. یعنی رایانه هایی که برای حفظ امنیت آنها، هیچگونه ارتباط وایرلس یا کابل با شبکه وجود ندارد.

حدس زدن اینکه چه سیستم هایی به یک چنین ساز و کار امنیتی مجهز هستند کار چندان سختی نیست: سیستم های حساس دولتی، تجهیزات نظامی – همچون موشک ها – و رایانه های کنترل تجهیزات رآکتورهای هسته ای. سیستم هایی که تنها از طریق پروژه های پیچیده می توانند به بد افزار آلوده شوند.

اکنون بد افزار BitWhisper مخصوص به آلوده ساختن این سیستم ها طراحی شده است و اینکه با کندی قادر به رد و بدل کردن اطلاعات است، هیچ اهمیتی ندارد، زیرا جایگزینی برای آنکه به سادگی بتواند همین میزان اطلاعات را نیز تبادل کند، وجود ندارد.

اما در این مورد که این بد افزار از ابتدا چگونه قادر به ورود به رایانه هدف است، می توان سناریوهای مختلفی در نظر آورد. یکی از این راه هاPre-Load کردن این بد افزار در حافظه رایانه است و راه دیگر آن مسیر همیشگی یعنی Flash USB است. اگر بخاطر آوریم که چگونه بد افزار Stuxnet در تجهیزات

اتمی ایران جای گذاری شد، می توان حدس زد که برای ورود این بد افزار به رایانه ها می توان راه های مختلفی را در نظر آورد.

ویدئو مربوط به اثبات حمله توسط تکنیک BitWhisper:

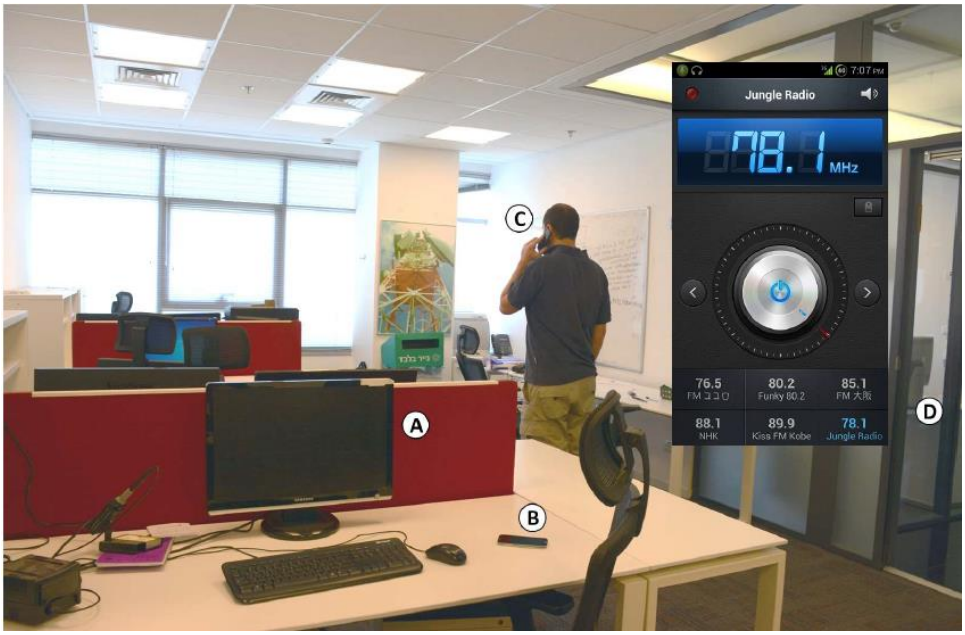
https://youtu.be/EWRk51oB-1Y

در صورت تمایل جهت کسب اطلاعات بیشتر در خصوص تکنیک BitWhisper می تواند به مقاله ارائه شده آن در لینک زیر مراجعه نمایید:

https://arxiv.org/ftp/arxiv/papers/1503/1503.07919.pdf

تکنیک AirHopper

در سال ۲۰۱۴ تکنیک جدید به نام AirHopper معرفی شد. این تکنیک می تواند کارت گرافیک کامپیوتر را به فرستنده FM تبدیل می کند تا ضربات کلید روی کیبورد یا اصطلاحاً را Capture کند. محققان امنیتی در آزمایشگاه امنیت سایبری در دانشگاه بن گوریون در اسرائیل راهی برای ردیابی رایانه شخصی حتی بدون اتصال به شبکه پیدا کردند. این تکنیک مبتنی بر سرقت داده ها با استفاده از سیگنال های رادیویی اصطلاحاً تکنیک AirHopper نامیده می شود.



محققان بدافزار یک اثبات مفهومی یا PoC را توسعه داده اند که می تواند به یک شبکه بسته نفوذ کند تا با استفاده از سیگنال های رادیویی FM تلفن همراه، داده‌های دستگاهی را که به طور کامل از اینترنت یا هر اتصال Wi-Fi جدا شده است، استخراج کند.
آقای Mordechai Gurl که از محققین و مدیر مرکز امنیت سایبری دانشگاه بن گوریون است به همراه پروفسور Yuval Elovici، در نهمین کنفرانس بین المللی IEEE در مورد ارائه ای درباره نرم افزارهای مخرب و ناخواسته (MALCON 2014) که در شهر دنور آمریکا برگزار شد، ارائه کردند. این فناوری جدید به عنوان "AirHopper" شناخته می شود - اساساً یک برنامه keylogger برای ردیابی آنچه در رایانه یا تلفن همراه تایپ می شود است.

ویدئویی که تکنیک AirHopper را اثبات می کند:
https://youtu.be/2OzTWiGl1rM

در صورت تمایل جهت کسب اطلاعات بیشتر در خصوص تکنیک AirHopper به مقاله ارائه شده آن در لینک زیر مراجعه نمایید:
http://www.enggjournals.com/ijcse/doc/IJCSE17-09-05-026.pdf

تکنیک DiskFiltration

در تاریخ جولای ۲۰۱۶ خبر آمد که هکرها می توانند کامپیوترها را به کمک چراغ های چشمک زن LED هارد دیسک ها هک کنند. محققان دانشگاه بن گوریون، به کمک چشمک های چراغ LED، راهی برای هک هارد دیسک کامپیوترها و سرورها یافتند.

در ۲۲ فوریه ۲۰۱۶ این تیم، یک ویدئو از عملکرد این هک در YouTube منتشر کردند. در این ویدئو هواپیمایی بدون سرنشین یا پهباد با یک دوربین به نام Air-gapped Camera، در بیرون یک ساختمان اداری در حال پرواز است و مشغول اسکن کردن چراغ های هارد دیسک یک کامپیوتر و ضبط اطلاعات به وسیله چراغ های LED داخل ساختمان است. این دوربین قادر است بدون نیاز به شبکه، اینترنت و هیچگونه ارتباط فیزیکی هک را انجام دهد. با چشمک زدن چراغ های LED هارد، سیگنالی حاوی اطلاعات به Air-gapped ارسال می شود و کافیست که دوربین، چشمک زدن این چراغ ها را دریافت کند. حتی اطلاعات حساس و کدگذاری شده نیز به کمک این دستگاه قابل دسترسی خواهد بود. علاوه بر این دستگاه، نرم افزار های مخرب هم قادر به کنترل وضعیت چراغ LED و دریافت اطلاعات از هارد دیسک هستند.

در نتیجه تا زمانیکه LED در حال چشمک زدن باشد امکان روی دادن اتفاقات مشکوک وجود دارد. به گفته محققان، این داده ها با سرعت ۴۰۰۰ بیت در ثانیه به کمک یک سنسور فتودیود به Air-gapped منتقل می شود. لازم به ذکر است که این دوربین قادر به دریافت ۶۰۰۰ چشمک LED در ثانیه است که چشم انسان قادر به انجام این کار نیست و همچنین قادر است این کار را تا فاصله ۲۰ متری بیرون ساختمان انجام دهد. پس از ثبت چشمک زدن LED، کار رمزگشایی آغاز می شود و هکر به کمک سیگنال های دریافت شده، اطلاعات را رمزگشایی و بازسازی می کند. علاوه بر این، محققان این کار را با دوربین های دیگری چون دوربین های امنیتی، دوربین های موبایل، سنسورهای نوری و غیره آزمایش کردند؛ همه این دوربین ها قادر به ضبط چشمک های LED بودند. برای جلوگیری فعلی از این نوع هک، می توان به سادگی با چسب های سیاه و سفید این LEDها را پوشاند و همچنین می توانید کامپیوترهایتان را از دید دوربین های اطرافتان حفظ کنید.

ویدئو مربوط به هک و استخراج اطلاعات به کمک تکنیک DiskFiltration:

https://www.youtube.com/watch?v=4vIu8ld68fc
https://youtu.be/H7lQXmSLiP8

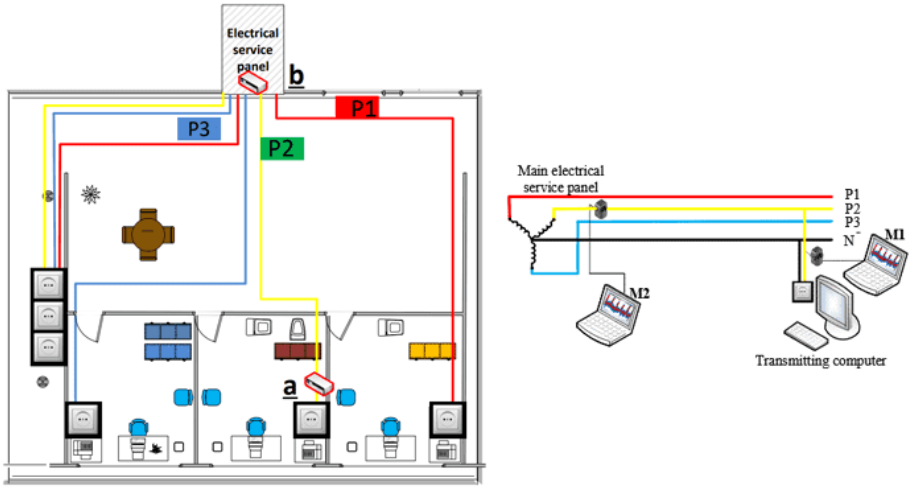
در صورت تمایل جهت کسب اطلاعات بیشتر در خصوص تکنیک DiskFiltration به مقاله ارائه شده آن در لینک زیر مراجعه نمایید:

https://arxiv.org/ftp/arxiv/papers/1608/1608.03431.pdf

تکنیک PowerHammer

در ۳۱ فروردین ۱۳۹۷ خبر آمد که هکرها از طریق خطوط برق نیز موفق به استخراج اطلاعات حساس شده اند. این تکنیک یا PowerHammer در واقع یک بدافزار است که جهت استخراج اطلاعات از کامپیوترهای Air-Gapped از خطوط برق استفاده می کند.

این حمله زمانی انجام می شود که شخصی بدافزار «Power Hammer» را بر روی سیستم air-gapبارگذاری کند. این برنامه درایوها را برای یافتن فایلی که می خواهد منتقل شود، اسکن می کند و سپس مصرف برق CPU را با تغییر میزان جریانی که کامپیوتر می کشد، دستکاری می کند. با این کار می توان سیگنالی را بر روی خطوط برق شامل مصرف برق بالا و پایین ۱ و ۰ باینری فرستاد.



برای دریافت این سیگنال هکر باید به پنل برق بیرون ساختمان دسترسی داشته باشد. از این پنل می توان اطلاعات را با نرخ کمتر از ۱۰ بیت در ثانیه از کامپیوتر دریافت کرد. محققان این روش را«Phase-level power hammering» نامند. اگر هکر داخل ساختمان باشد نسخه ای قدرتمندتر از حمله به نام «Line-level power hammering» امکان پذیر خواهد بود. زیرا با کاهش سیگنال های غیرمرتبط بر روی خط، بدافزار می تواند سریعتر مصرف برق CPU را مدوله کند. این کار موجب می شود تا نرخ دریافت اطلاعات به ۱۰ تا ۱۰۰۰ بیت بر ثانیه برسد. به عنوان یک اثبات مفهومی، تیمی توانستند اطلاعاتی را با نرخ ۱۰۰۰ بیت در ثانیه از سیستمی با CPU نوع Intel Haswell و همچنین با نرخ ۱۰۰ بیت بر ثانیه از سرور متصل Intel Xenon E5-2620 انتقال دهند. اگرچه نرخ های فوق بسیار سریع نیستند، اما محققان توانستند نرخ خطای صفر درصد را مدیریت کنند. استفاده از Phase-level power hammering از خارج از ساختمان همراه با نویز پس زمینه، منجر به انتقال اطلاعات تا سرعت سه بیت بر ثانیه و نرخ خطای ۴,۲ درصد شد. در این نرخ می‌توان یک فایل PDF صد کیلوبایتی را در طی حدود ۳ روز سرقت کرد. در هر حال اکنون هیچ نشانه ای مبنی بر استفاده از این تکنیک برای سرقت اطلاعات از کامپیوترهای air-gap وجود ندارد. با این حال اثبات مفهومی امکان پذیری آن را هرچند نسبتاً کند، اثبات می کند.

در صورت تمایل جهت کسب اطلاعات بیشتر در خصوص تکنیک PowerHammer به مقاله ارائه شده آن در لینک زیر مراجعه نمایید:

https://arxiv.org/pdf/1804.04014.pdf

تکنیک MAGNETO and ODINI

در تاریخ ۱۳ اسفند ۱۳۹۶ خبر آمد که گروهی از محققان امنیتی که بیشتر بر روی یافتن روش‌های هوشمندانه برای ورود به کامپیوترهای air-gapped توسط بهره برداری از انتشار little-noticed از اجزای یک کامپیوتر مانند نور، صدا و گرما متمرکز هستند یک گزارش تحقیقاتی منتشر کردند که نشان می دهد نه تنها می توانند داده ها را از روی یک کامپیوتر air gap بدزدند بلکه می‌توانند داده ها را از یک کامپیوتر داخل یک قفس فارادی نیز بدزدند.

قفس های فارادی محفظه‌های فلزی هستند که تمام سیگنال‌های الکترومغناطیسی مانند: Wi-Fi، بلوتوث، تلفن همراه و دیگر ارتباطات بیسیم را مسدود می کنند و هر دستگاهی که در این قفس نگهداری می شود از تمامی شبکه های بیرونی ایزوله می شود.

با این حال، یک مرکز تحقیقاتی امنیت سایبری که توسط Mordechai Guri در دانشگاه بن گورین کشور اسرائیل اداره می‌شود، دو تکنیک را توسعه داده است که به آنها کمک می کند داده ها را از رایانه های داخل قفس فارادی نیز در اختیار داشته باشند.

این دو روش که MAGNETO و ODINI نام گذاری شده اند، از یک بدافزار که بر روی یک کامپیوتر air-gappedدر داخل قفس فارادی قرار دارد، استفاده می کنند تا میدان های مغناطیسی ناشی از کامپیوتر را توسط تنظیم حجم کاری بر روی هسته CPU کنترل کرده و از آن برای انتقال اطلاعات به صورت مخفیانه استفاده کنند.

دکتر Guri در این باره می گوید: "همه در مورد شکستن air gap برای ورود صحبت می‌کنند، اما هیچکس در مورد دریافت اطلاعات از آن صحبت نمی کند. این موضوع دروازه را برای این تحقیقات باز کرد تا محافظ غیر قابل نفوذ در اطراف شبکه های air gap را بشکند".

به گفته این محقق، هنگامیکه یک کامپیوتر (بدون توجه به اینکه آیا در air-gapped قرار دارد و یا در داخل قفس فارادی) آلوده شده است، مهاجمان می‌توانند داده های سرقت شده را بدون نیاز به انتظار برای برقراری یک اتصال دیگر به دستگاه آلوده استخراج کنند.

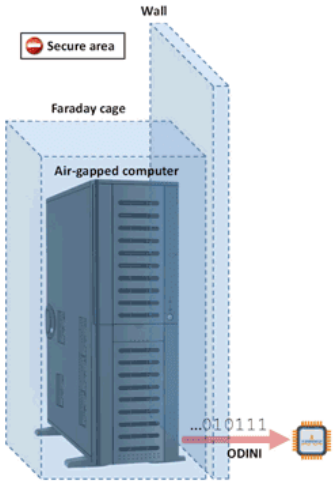
چگونه حملات MAGNETO و ODINI کار می کنند؟

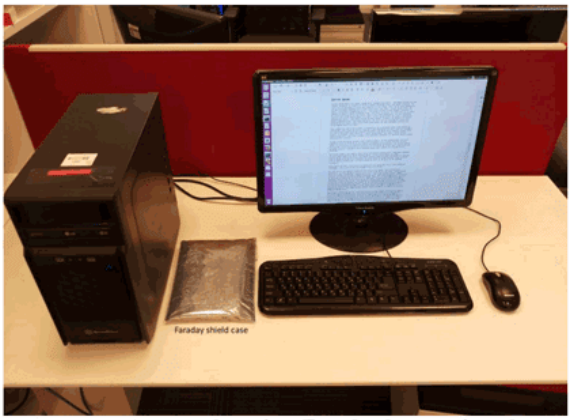
هنگامیکه یک مهاجم دارای انگیزه به نحوی موفق به قراردادن یک بدافزار بر روی یک رایانه air-gapped می‌شود، این بدافزار سپس شروع به جمع آوری بخش های کوچکی از اطلاعات می‌کند؛ مانند داده های Keylogging، کلیدهای رمزگذاری، tokenهای گواهی نامه و رمزهای عبور.

بدافزار PoC که توسط این تیم تحقیقاتی توسعه یافته است، در مرحله بعدی به طرز الکتریکی یک الگوی فرکانس میدان مغناطیسی را با تنظیم میزان بار پردازنده طراحی می کند، که می تواند با اضافه کردن بار CPU با محاسباتی که باعث افزایش مصرف برق و تولید میدان مغناطیسی شدید می شود، تولید شود.

این انتشار الکترومغناطیسی (آکوستیک، نوری و حرارتی) از کامپیوتر آلوده شده به اندازه کافی قدرتمند است تا جریان کوچکی از داده های به سرقت رفته را به یک دستگاه نزدیک، که یک گیرنده است که توسط مهاجم کنترل می‌شود، منتقل کند.

این فرآیند در ابتدا شامل ترجمه داده ها به binary، برای مثال ۰ و ۱، و انتقال آنها به الگوهایی شبیه کد مورس با توجه به انتشار الکترومغناطیسی است.





A smartphone in a Faraday bag receives the magnetic signals from a transmitting computer nearby.

در مقاله مربوطه آمده است: "برنامه انتقال تنها یک رد پای کوچک در حافظه باقی می گذارد و حضور آن را به راحتی از برنامه های ضد ویروس پنهان می کند. در سطح سیستم عامل، برنامه های ارسالی نیازی به امتیازات ویژه یا بالاتری ندارند (مانند root یا admin) و از این رو می توانند از طریق یک فرآیند معمولی در فضای کاربری آغاز شوند. کد انتقالی عمدتاً شامل عملگرهای پایه ای CPU مانند busy loopsمی شود که رفتارهای مخرب را افشا نمی کند و آن را از تشخیص داده شدن توسط ابزارهای آنالیز دور نگه می‌دارد".

در حالیکه هر دو حمله MAGNETO و ODINI طراحی شده اند که اطلاعات داده شده را از یک کامپیوتر ایمن با استفاده از انتشار الکترومغناطیسی تهیه کنند، تنها تفاوت بین این دو از این قرار است:

- حمله MAGNETO یک حمله کوتاه مدت است که در آن یک برنامه اندروید که بر روی گوشی هوشمند مهاجم نصب شده است می تواند داده های سرقت شده را با کمک مغناطیس تلفن دریافت کند، یک سنسور مغناطیسی که می تواند اطلاعات را انتقال دهد حتی اگر گوشی هوشمند در داخل کیف فارادی قرار داشته باشد یا بر روی airplane mode تنظیم شده باشد.
- حمله ODINI حمله کنندگان را قادر می سازد تا سیگنال های الکترومغناطیسی را از محدوده اندکی طولانی تر و با استفاده از یک سنسور مغناطیسی اختصاصی دریافت کنند.

در مورد حمله MAGNETO، این تیم موفق شد تا حداکثر ۵ بیت در ثانیه را در فاصله ۱۲.۵ سانتی متر (۵ اینچی) به دست آورد، در حالیکه حمله ODINI با بیشترین سرعت انتقال ۴۰ بیت در ثانیه در محدوده ۱۰۰ تا ۱۵۰ سانتیمتر (۳-۵ اینچ) بسیار کارآمدتر عمل کرد.

Work	Signal generation	Receiver	Max bit-rate	Max distance
ODINI [24]	CPU cores	magnetic sensor	40 bit/sec	100 to 150 cm
MAGNETO (this paper)	CPU cores	smartphone	5 - 0.2 bit/sec	0 to 12 cm (desktops)
Hard Disk Drive ([23])	Hard Disk Drive (magnetic)	smartphone	2 - 0.06 bit/sec	0 to 12 cm (laptops)

هر دوی حملات ODINI و MAGNETO حتی اگر دستگاه air-gapped مورد هدف در داخل قفس فارادی قرار داشته باشند نیز کار می کنند، که این قفس ها بگونه ای طراحی شده اند که از میدان های الکترومغناطیسی، از جمله بلوتوث، Wi-Fi، تلفن همراه و دیگر ارتباطات بیسیم جلوگیری کنند.
محققان سه رویکرد متفاوت را پیشنهاد می کنند که می توانند مورد استفاده قرار گیرند تا از ایجاد یک کانال مغناطیسی پنهانی جلوگیری کنند؛ که عبارتند از محافظت، مسدود کردن و منطقه بندی.

ویدئوهای مربوط به اثبات تکنیک MAFNETO and ODINI:

https://youtu.be/yz8E5n1Tzlo
https://youtu.be/h07iXD-aSCA

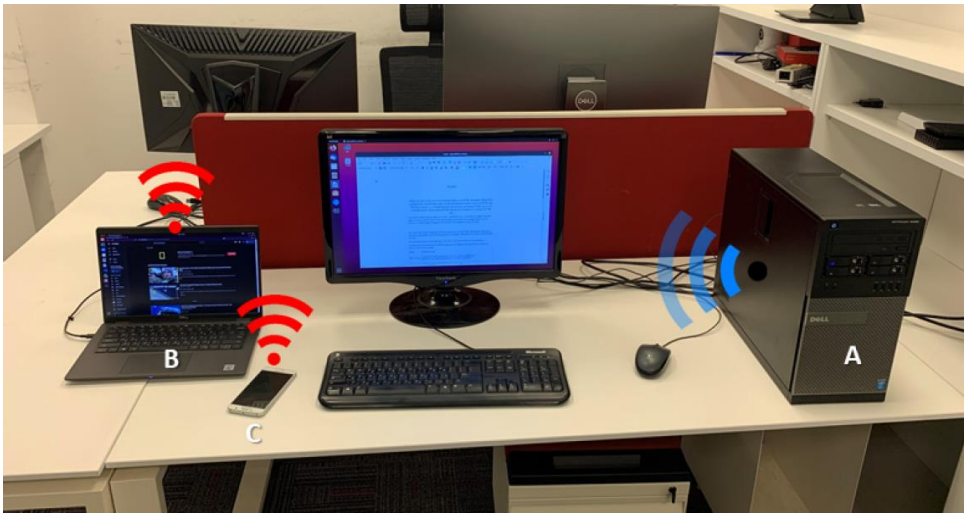
در صورت تمایل جهت کسب اطلاعات بیشتر در خصوص تکنیک MAGNETO and ODINI به مقالات ارائه شده آن در لینک زیر مراجعه نمایید:

MAGNETO article:
https://cyber.bgu.ac.il/advanced-cyber/system/files/MAGNETO_0.pdf

ODINI article:
https://cyber.bgu.ac.il/advanced-cyber/system/files/ODINI_1.pdf

تکنیک Air-Fi

تکنیک Air-Fi در واقع خروج داده ها از رایانه های شبکه Air Gap از طریق سیگنال های Wi-Fi (بدون سخت افزار Wi-Fi) است. یک محقق امنیتی کشور اسرائیل نشان دادند که داده های حساس را می توان از طریق تکنیک جدیدی که از سیگنال های Wi-Fi به عنوان یک کانال مخفی استفاده می کند و بطور شگفت آور، بدون نیاز به وجود سخت افزار Wi-Fi در سیستم های مورد نظر، از رایانه های شبکه Air Gap خارج کرد.



این یافته ها امروز در مقاله ای با عنوان Generating Covert Wi-Fi Signals from Air-Gapped Computers توسط دکتر Mordechai Guri، رئیس تحقیق و توسعه دانشگاه بن گوریون از مرکز تحقیقات امنیت سایبری نگف در اسرائیل، منتشر شد.

وی افزود: "محیط های مدرن IT مجهز به انواع مختلفی دستگاه های قابل استفاده از Wi-Fi هستن: گوشی های هوشمند، لپ تاپ ها، دستگاه های IOT، سنسورها و ساعت های هوشمند و سایر دستگاه ها. مهاجم می تواند چنین تجهیزاتی را هک کرده تا انتقالات Air-Fi را دریافت کند".

دکتر Guri گفت: "حمله Air Fi به سخت افزار مربوط به Wi-Fi در کامپیوترهای Air Gap نیاز ندارد و این دقیقاً نکته اعجاب انگیز و البته خطرناک این مسئله است".
ویدئو مربوط به اثبات تکنیک Air-Fi:

https://youtu.be/vhNnc0ln63c

در صورت تمایل جهت کسب اطلاعات بیشتر در خصوص تکنیک Air-Fi به مقاله ارائه شده آن در لینک زیر مراجعه نمایید:

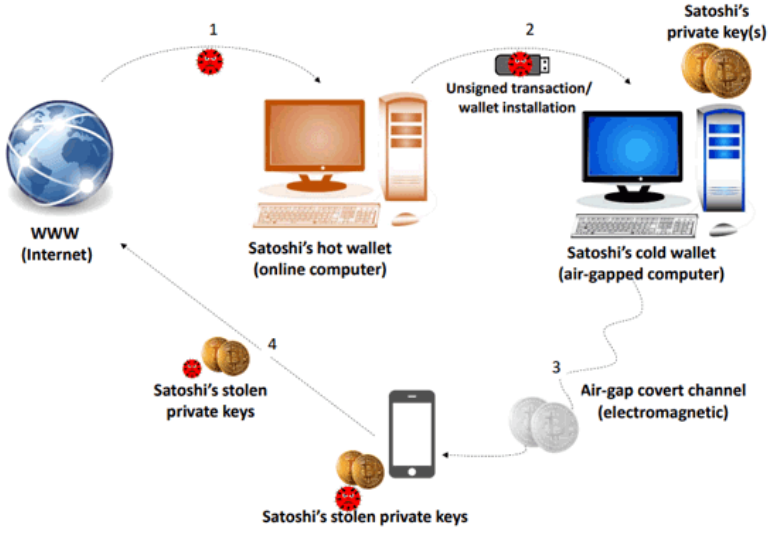
https://arxiv.org/pdf/2012.06884.pdf

تکنیک BeatCoin

دکتر Mordechai Guri، رئیس تیم تحقیق و توسعه در دانشگاه بن گوریون اسرائیل، که قبلاً روش‌های مختلفی را برای سرقت داده ها از یک کامپیوتر Air-Gapped نشان داده بود، اکنون تحقیق جدیدی به نام «بیت کوین» منتشر کرده است.

در واقع BeatCoin یک تکنیک جدید هک نیست. در عوض، این آزمایشی است که در آن این محقق سایبری نشان می دهد که چگونه می توان از تمام روش های ارتباطی خارج از باند کشف شده قبلی برای سرقت کلیدهای خصوصی یک کیف پول رمزنگاری نصب شده در Cold Storage، ترجیحاً یک کامپیوتر Air-Gapped یا Raspberry Pi استفاده کرد.

برای کسانی که نمی دانند، محافظت از ارز دیجیتال خود در کیف پول روی دستگاهی که کاملاً آفلاین است، Cold Storage نامیده می شود. از آنجاییکه کیف پول های دیجیتال آنلاین خطرات امنیتی مختلفی را به همراه دارند، برخی افراد ترجیح می دهند کلیدهای خصوصی خود را آفلاین نگه دارند.



برای آزمایش BeatCoin، دکتر Guri بدافزاری را بر روی یک کامپیوتر Air-Gapped که یک برنامه کیف پول بیت کوین را اجرا می‌کند، مستقر کرد و سپس هر بردار حمله را یک به یک انجام داد تا کلیدهای کیف پول را از طریق کانال های مخفی به دستگاه مجاور منتقل کند.
در این مقاله آمده است: "در مدل حمله خصمانه، مهاجم به کیف پول آفلاین نفوذ کرده و آن را با کدهای مخرب آلوده می کند." این بدافزار می‌تواند از قبل نصب شده یا در طول نصب اولیه کیف پول وارد شود، یا زمانیکه رسانه های قابل جابجایی (مثلاً درایو USB Flash) به رایانه کیف پول وارد می شود تا یک تراکنش را امضا کند، سیستم را آلوده کند. در دهه گذشته بارها و بارها عملی بودن بردارها ثابت شده است."

Type	Method	Recevier	256-bit key
Physical	Removable and external media (E.g., USB flash drives)	Computer	<0.01 sec
Electromagentic	AirHopper (FM signals emitted from the video cable [49], [48])	Mobile phone	<1 sec
Electromagnetic	GSMem (cellular interferences emitted from the CPU-RAM bus) [50]	Mobile phone	~300 sec
Electromagnetic	RADIoT (radio signals generated by embedded and IoT devices) [51]	Mobile phone/ Dedicated receiver	~1-50 sec
Electric	PowerHammer (data exfiltrated thorough the power lines) [54]	Dedicated receiver	~ 30-300 sec
Magnetic	MAGNETO (magnetic signals generated by the CPU to smartphone) [56] ODINI (magnetic signals generated by the CPU) [55] HDD (Magnetic signals emitted from the HDD) - laptops [57]	Mobile phone	~70-1000 sec
Acoustic	Ultrasonic (generated by loudspeakers) [63]	Computer/ Mobile phone	~1-20 sec
Acoustic	MOSQUITO (speaker-to-speaker ultrasonic communication) [65]	Computer	~2-20 sec
Acoustic	Fansmitter (acoustic signals generated by the CPU/chassis fans) [66]	Computer/ Mobile phone	~1000-2000 sec
Acoustic	Diskfiltraition (acoustic signals generated by the HDD actuator arm) [67]	Computer/ Mobile phone	~100-200 sec
Optical	Keyboard LEDs [58]	Local camera (e.g., webcam)	~50-100 sec
Optical	Hard disk drive LEDs (LED-it-GO) (optical signals by HDD indicator LED) [59]	Local camera (e.g., webcam)	~10-100 sec
Optical	Invisible images on screen [61]	Mobile phone	A snapshot
Optical	QR code steganography [62]	Mobile phone	A snapshot

نتایج نشان داده شده در نمودار بالا نشان می‌دهد که تکنیک های AirHopper، MOSQUITO و Ultrasonic سریعترین راه برای انتقال یک کلید خصوصی ۲۵۶ بیتی به یک گیرنده از راه دور هستند، در حالیکه روش های DiskFiltration و Fansmitter چند دقیقه طول می‌کشد.

https://youtu.be/2WtiHZNeveY
https://youtu.be/ddmHOvT866o

در صورت تمایل جهت کسب اطلاعات بیشتر در خصوص تکنیک BeatCoin به مقاله ارائه شده آن در لینک زیر مراجعه نمایید:
https://cyber.bgu.ac.il/advanced-cyber/system/files/BeatCoin-final.pdf

تکنیک GSMem

در سال ۲۰۱۵ خبر آمد که ویروس مضر GSMem ساخته شده محققان دانشگاه بن گورین کشور اسرائیل می تواند اطلاعات را از کامپیوتری که به اینترنت وصل نیست دریافت کرده و آن را به تلفن موبایل منتقل کند. محققان می گویند می توان از طریق Flash حامل اطلاعات، ویروس را وارد کامپیوتر کرد.

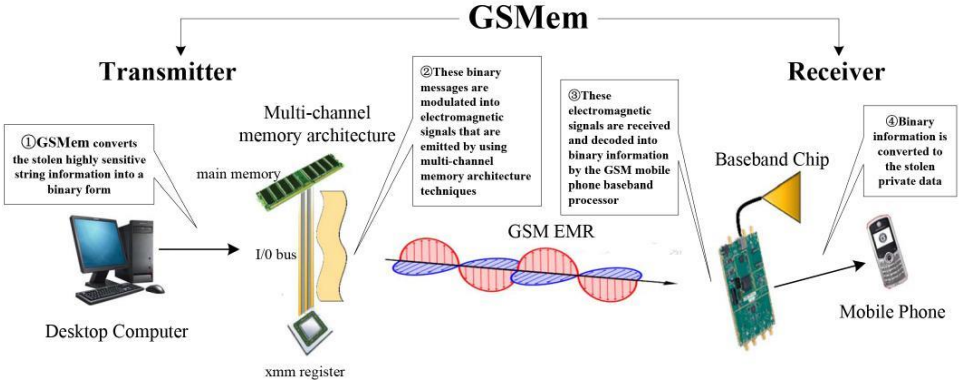
کامپیوتری که مورد حمله ویروس قرار گرفته است به کنترل تبادل سیگنال ها بین پروسسور و حافظه دستگاه می پردازد. در این روش تلفن باید در فاصله ۵ متری از کامپیوتر قرار داشته باشد و سرعت انتقال اطلاعات ۲-۱ بایت در ثانیه خواهد بود. با وجود پایین بودن این سرعت، برای دریافت رمزهای عبور و یا کلید اطلاعات برای دسترسی آتی به اطلاعات کلی تر محرمانه کافی خواهد بود.

در حالیکه محققان اسرائیلی نشان دادند که سرقت اطلاعات از این طریق امکان پذیر است، اما اجرای موفق آمیز برخی از این روش ها مستلزم آن است که کامپیوتر ویژگی‌های سخت افزاری خاصی داشته باشد.

این تحقیق اولین بار در کنفرانس امنیتی USENIX مطرح شد و اولین تحقیقی است که امکان سرقت اطلاعات فقط با استفاده از یک بدافزار و تلفن همراه را نشان می‌دهد.

بدافزاری که توسط محققان اسرائیلی طراحی شده است باید بر روی کامپیوترهایی که هدف این حمله قرار می‌گیرند نصب شود. همانطور که پیشتر نیز اشاره شد، این بدافزار می‌تواند از طریق اتصال یک درایو قابل حمل به کامپیوتر منتقل شود و سیستم را آلوده نماید.

این بدافزار که GSMem نامیده شده بر روی کامپیوتر آلوده به عنوان یک فرستنده عمل می کند. این بدافزار دستورات خاص مبتنی بر حافظه را ایجاد می کند که بین CPU و حافظه ارسال می شوند، امواج رادیویی را در فراکانس‌های GSM، UMTS و LTE تولید می کند که می تواند توسط دستگاه های سیار نزدیک به کامپیوتر دریافت شود.



از آنجاییکه این بدافزار دارای ردپایی بسیار کوچک در حافظه است در نتیجه تشخیص آن (منظور شناسایی از طریق Memory Forensic) بسیار مشکل بوده و به راحتی می تواند از دید برنامه های ضدبدافزاری پنهان بماند.

استفاده از گوشی های هوشمند دارای آنتن ها و پردازنده بسیار قوی می تواند باعث شود تا سرعت ارسال اطلاعات افزایش یابد و همچنین می توان حمله را از فاصله دورتری هدایت کرد.

ویدئو مربوط به حمله GSMem ارائه شده در کنفرانس امنیتی USENIX توسط دکتر Guri:
https://www.youtube.com/watch?v=lQvTckDTUlQ

در صورت تمایل جهت کسب اطلاعات بیشتر در خصوص تکنیک GSMem به مقاله ارائه شده آن در لینک زیر مراجعه نمایید:
https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-guri-update.pdf

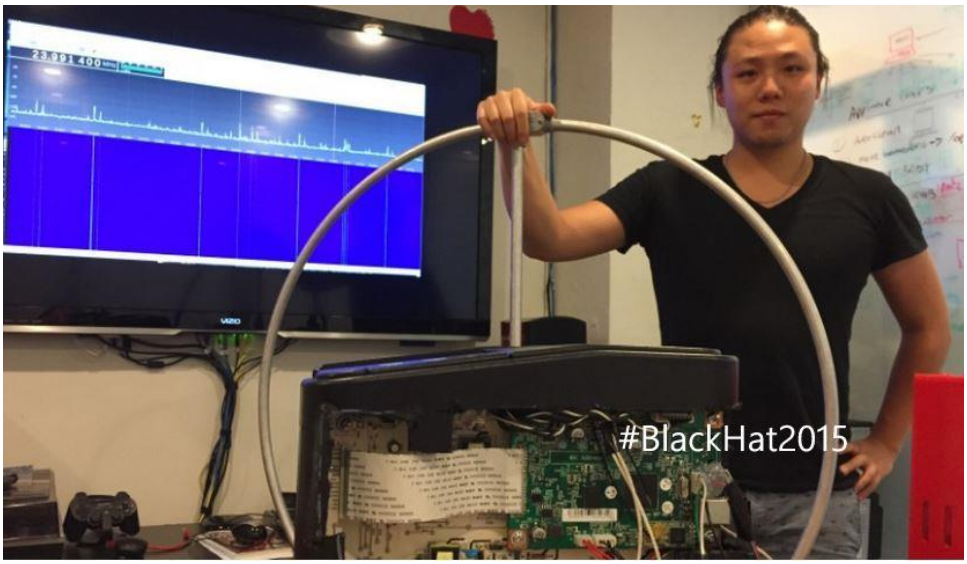
تکنیک Funtenna

تکیک Funtenna، روش دیگری برای ارسال داده ها از رایانه در داخل شبکه ایزوله است که از امواج صوتی استفاده می کند. گروهی از کارشناسان یک تکنیک هک نوآورانه به نام Funtenna را توسعه

دادند که می‌تواند توسط مهاجم برای استخراج داده‌ها از یک رایانه هدف حتی اگر در یک شبکه با شکاف هوا باشد، استفاده کند.

تکنیک Funtenna، یک تکنیک فقط نرم افزاری است که باعث به خطر افتادن عمدی در طیف گسترده ای از سخت افزارهای محاسباتی مدرن به منظور استخراج داده های مخفی و قابل اعتماد از طریق شبکه های ایمن و Air-Gapped استفاده می شود. در متن این مقاله آمده است که: "ما یک تکنیک Funtenna تعمیم یافته را ارائه می‌کنیم که داده های دلخواه را در بخش های وسیعی از طیف الکترومغناطیسی، از زیر آکوستیک گرفته تا RF و فراتر از آن، بطور قابل اعتماد رمزگذاری و منتشر می کند".

«تکنیک Funtenna سخت‌افزاری است که می تواند در تقریباً تمام سیستم های رایانه ای مدرن و دستگاه های تعبیه شده کار کند، و بطور خاص برای کار در سخت افزاری طراحی شده است که به عنوان فرستنده RF عمل نمی کند».
همانطور که توسط محقق Ang Cui از شرکت Red Balloon Security در کنفرانس امنیتی Black-Hat در سال ۲۰۱۵ توضیح داده است، اهمیت این کشف بسیار زیاد است. هک سیگنال رادیویی Funtenna می تواند به مهاجمان اجازه دهد تا از دستگاه های اینترنت اشیاء یا IoT برای جاسوسی از هر هدفی سوء استفاده کنند. کنسول بازی، چاپگر، ماشین لباسشویی و یخچال می توانند اطلاعات رایانه ها را حتی اگر از اینترنت جدا شده باشند، سرقت کنند.



همچنین در این حالت لازم است رایانه مورد نظر در معرض خطر قرار گرفته باشد (Compromised شده باشد)، مهاجمان باید بدافزاری را نصب کنند که برای کنترل مدار الکترونیکی دستگاه (مدارهای ورودی/خروجی همه منظوره) استفاده می شود، داده ها از طریق سیگنال ها به بیرون ارسال می شوند. با ارتعاش آنها در فرکانس های خاص تولید می شود.

ویدئو مربوط به اثبات تکنیک Funtenna:

https://www.youtube.com/watch?v=1H1Lv9DAJPg

حمله Stuxnet

در ژانویه سال ۲۰۱۰ خبر آمد که نیروگاه هسته ای نطنز نیز مورد حمله سایبری قرار گرفته است. بعدها مشخص شد که حمله مربوطه توسط یک Worm کامپیوتری به نام Stuxnet که توسط محقیقین سایبری کشور اسرائیل و آمریکا ساخته شده باعث می شود که دور سانتریفیوژهای نیروگاه را که برای غنی سازی اورانیوم از آنها استفاده می شود را افزایش دهد که با مشاهده افزایش تعداد دورها و رسیدن تا حد آستانه بصورت بی سابقه ای بعدها توسط کشف شد. منشأ ورود این بدافزار نیز یک Flash Memory آلوده به مجموعه نیروگاه هسته ای نطنز اعلام و دلیل کشف نیز اعمال تغییرات در کد این بدافزار توسط محقیقن اسرائیلی بدون هماهنگی با محقیقن آمریکایی مطرح شد. جزئیات بیشتر بعدها در سال ۲۰۱۶ در مستند Zero Day مطرح شد.

نویسنده: میثم ناظمی