خطر یو.اس.بی درایوها

این مقاله نشان می دهد که کاربران معمولی خطر اتصال لوازم جانبی ناشناخته را به رایانه خود نمی دانند، که بر اهمیت ریسک پیاپی پدید آمده از جانب یو.اس.بی درایوها تاکید دارند. سازمان ها می توانند اقداماتی برای محافظت در برابر حملات ناشی از یو.اس.بی بحث شده بردارند.

جامعه فنی از مدت ها قبل تردید داشته اند که افراد درایوهای فلش یو.اس.بی را که از زمین پیدا می کنند، وارد رایانه خود می کنند. متاسفانه این کار به خاطر انگیزه های از خود گذشتگی یا کنجکاوی انسانی، انجام ناآگاهانه این کار سازمان را در برابر حمله داخلی-اسب تروجان واقعی، آسیب پذیر می کند. جامعه ما پر از وقایع این حملات است. هکرها اغلب ادعا می کنند که آنها می توانند با ابداع نمودن برچسب های فریبنده و جلب توجه حس کنجکاوی انسان ها را هک کنند.

هنگامی که به حمام می روم، پاکتی را در جایگاه ویژه قرار می دهیم. در روکش پاکت برچسبی میگذارم که نشان می دهد:خصوصی. درون پاکت خصوصی کلید یو.اس.بی با بازدهی مخرب می باشد. این کار را در یک جایگاه انجام می دهم همچنین در راهرو کنار دستشویی تا فرصت و شانس را افزایش دهم امید به اینکه یک نفر یکی از انها را یافته و به اندازه کافی کنجکاو باشد تا آن را به رایانه خود متصل کند. با اطمیان کافی، این روش همیشه جواب می دهد. به هر حال، علی رغم این شایعه ها، تحلیل رسمی درباره اثرگذاری این حملات وجود نداشته اند که چه چیزی کاربران را انگیزه می بخشد که درایوها را متصل کنند. در این اثر، به بررسی این مطلب می پردازیم که آیا یواس بی درایوها ریسک به بار می آورند و به ارزیابی داستن قدیمی می پردازیم که کاربران هر درایو یو اس بی را که از روی زمین پیدا کنند، به رایانه متصل می کنند.

آزمایش ما: مرور کلی

برای اطمینان یابی از اینکه کاربران درایوهایی که روی زمین پیدا می کنند به ابزار متصل می کنند، آزمویش سطح کلان انجام دادیم که در آن حدود 300 فلش درایو در محوطه دانشگاه ایلینویس در فضای اربانا-چمپین انداختیم. در این هجوم، فایل های مورد انتظار را در درایو با فایل های اچ.تی.ام.ال جایگزین نمودیم که حاوی تصویر نهادینه

در سرور مرکزی بود که به ما اجازه می داد پیگیری کنیم که درایو به کجا متصل شده است. پی بردیم که کاربران تا 98 درصد درایوها را برداشتند و 45 درصد درایوها به رایانه متصل شدند. به علاوه حمله بسیار آنی بود به طوری که اولین درایو یافت شده ظرف شش دقیقه پس از زمان انداختن به ابزار متصل گردید. مغایر با عقیده عمومی، ظاهر درایو این احتمال را افزایش نداد که فرد آن را به رایانه خود متصل سازد. در عوض، کاربران همه انواع درایو ها را به ابزار متصل نمودند مگر اینکه روش تعیین محل صاحب آن وجود نداشت که نشان می داد بسیاری از شرکت کنندگان انگیزه از خود گذشتگی داشتند. به هر حال، هر چند برخی کاربران ابتدا درایو را با انگیزه از خود گذشتگی متصل نمودند، حدود نیمی از انها تحت تثیر کنجکاوی واقع شده و ابتدا فیل های فریبنده را از جمله عکس های مسافرت، را باز کردند قبل از اینکه سعی کنند صاحب درایو را بیابیند. برای درک بهتر انگیزه کاربران، این انتخاب را برای کاربران پیشنهاد دادیم که نظرسنجی کوتاهی را کامل کنند هنگامی که درایو را متصل نمودند. اکثر انها بیان داشتند که درایو را متصل نمودند تا صاحب آن را بیابند یا اینکه از سر کنجکاوی بوده است هر چند عده کمی اقرار نمودند که برنامه ریزی کرده بودند که درایو را نزد خود نگه دارند. دانشجویان و کارکنان که درایو را متصل کرده بودند، چندان سواد رایانه ای نداشتند و تفاوت عمده ای با هم نظیران خود نداشتند. هنگامی که تحریک شدند، 68 درصد از شرکت کنندگان بیان نمودند که آنها هنگام اتصال درایو هیچ گونه احتیاطی به خرج ندادند. از افرادی که این کار را کردند، 16 درصد درایو را با نرم افزار انتی ویروس خود اسکن کردند و 8 درصد معتقد بودند که سیستم عامل یا نرم افزار امنیت از آنها محافظت خواهد نمود. در پایان، چند نفر از شرکت کنندگان که احتیاط کردند این کار را به طور ناکارامد انجام دادند و اکثر آنها به هیچ وجه احتیاط نکردند.

ما از هیئت بازبینی موسسه ای دانشگاه ایلینیوس تاییدیه را دریافت نموده و صحه گذاشتیم و با سهامداران عمده (واحدهای فناوری اطلاعات، قانونی و ایمنی عمومی) ضمن طراحی آزمایش رو به رو شدیم. ما به طور خودکار هر نوع کد را روی سیستم شرکت کنندگان اجرا نکردیم و فقط توانستیم داده ها را جمع آوری کنیم اگر شرکت کنندگان روی فایل های فلش درایو دو بار کلیک می کردند. از شرکت کنندگان اطلاعاتی کسب گردید و فرصت کشیدن درایو را به آنها دادیم.

آیا درایوهای یو.اس.بی هنوز تهدید آفرین اند؟

بسیاری از ویندوزهای مایکروسافت دیگر به طور خودکار کدهای دلخواه را اجرا نمی کنند، هنگامی که درایو یو.اس.بی متصل می گردد که بسیاری از حملات سنتی مبتنی بر یو.اس.بی را از بین می برد. به هر حال، اتصال یو .اس.بی درایو هنوز خطر عمده ای به بار می آورد. سه گروه جامع حملات موثر یو.اس.بی وجود دارد :مهندسی اجتماعی، کلاه برداری و تخریب اطلاعات.

ساده ترین نوع حمله مهندسی اجتماعی بوده که در ان درایو هر نوع کد اتصالی را اجرا نمی کند اما در عوض کاربر نهایی را فریب می دهد که فایل درایو یو .اس.بی را باز کند. فایل های روی درایو می توانند حاوی اسب تروجان یا محتوی اچ.تی.ام.ال بوده که تلاش دارند به اسناد محرمانه دست یابند. ساده ترین نوع حمله از جانب درایورها به دو دلیل اتفاق می افتد: مهاجم می تواند از درایو های خریداری شده از فروشگاه استفاده کند و حمله متکی بر یافتن آسیب پذیری های سیستم عامل نباشد. به هر حال، اعتبار آنها نیز در حد مینیمم بوده و بسیار به چشم می آیند چون متکی بر کاربر نهایی اند که فایل ها را باز کند بدون اینکه شک و تردیدی داشته باشد. متاسفانه همانطور که در زیر توصیف می کنیم، بسیاری از کاربران فایل ها را در درایو بدون هر نوع عکس العمل باز می کنند.

شکل 1- یو اس.بی درایو عادی و درایو حمله مبتنی بر ابزار رابط انسان. دفاع سیستم های عامل سنتی را می توان با کنترل گر خرد طراحی شده به عنوان درایو یو.اس.بی از کار انداخت که ابزار رابط انسان را جلوه نمایی کرده و ضربه های کلیدی مخرب وارد می سازند.

حمله پیچیده تر نوع متفاوتی از ابزار یو.اس.بی به نام فلش درایو طراحی می کند. در حالی که درایو یو.اس.بی نمی توانند به طور خودکار کد را اجرا کنند، ابزارهای رابط انسانی یو.اس.بی از جمله صفحه کلید و مووس نیاز به تایید و صحه گذاری کاربر ندارند. این بدان معناست که اگر ابزار یو.اس.بی خود را به عنوان صفحه کلید شناسایی کند، آن می تواند بلافاصله ضربات کلیدی مخربی القا کند که دستگاه را به مخاطره می افکند. این حمله دشوارتر از حمله مهندسی اجتماعی ساده پیاده سازی می شود چون نیاز به

پیکربندی ابزار سطح پایین برای جوله نمایی ابزار رابط انسان دارد تا به طور فیزیکی ابزار را به عنوان درایو یو.اس.بی درست کند و نوسانات سیستم عامل را کنترل کند.

به هر حال این مسئله به طور قابل ملاحظه با دسترسی اخیر خرده کنترل گرهای مبتنی بر آردونیو راحت تر شده است که توسعه سطح پایین را میسر می گردانند. شکل 1 خرده کنترل گر طراحی شده تینزی را نشان می دهد که پوسته وارون در ویندوز و سیستم عامل مک دارند و دستورات باش یا پاورشل مورد نیاز را در پس زمینه «تایپ می کند». ابزارهای خارج از قفسه این نوع همچنین در دسترس هستند، هر چند آنها به طور عمده هزینه آنها بیش از درایوهای یو.اس.بی خریداری شده در فروشگاه است. هنوز شدت این روش بیشتر از حمله مهندسی اجتماعی است اما می تواند به راحتی از سوی هکر حرفه ای انجام گردد.

پیچیده ترین نوع حمله یو.اس.بی موردی است که در آن ابزار یو.اس.بی آسیب پذیری معروف در سیستم عامل میزبان یا سخت افزار را هدف قرار می دهد. این هجوم های «سرسخت» به دشوار قابل تشخیص بوده و اغلب نیاز به اجراء وقت گیر دارند که آنها را در اکثر محیط ها قابل استفاده می گرداند. به هر حال، اگر مهاجم بتواند به هجوم سرسخت دست یابد، محافظت دربرابر این هجوم به طور باورنکردنی دشوار است. خط مشی های سیستم عامل را می توان از کار انداخت و محافظت کمی وجود دارد که مدیران می توانند فراتر از اختلال در بخش های یو.اس.بی در پیش گیرند.

هر یک از سه هجوم دارای معایب و مزایای خود اند. اجرای حملات مهندسی اجتماعی جزئی بوده اما متکی بر کنجاوی کاربر اند. از طرفی دیگر، حملات شدید، به دشوار قابل تشخیص بوده اما محافظت عمده در برابر آنها تقریبا غیر ممکن است. ابزارهای کلاهبرداری رابط انسان به مخاطره منطقی دست می یابند؛ آنها را می توان با مواد در دسترس راحت درست کرد و نیاز به تعامل کاربر ندارند پس از اینکه ابزار متصل گردید.

شکل 2- نمای دو درایو مطالعه شده. پنج درایو مختلف رو روی زمین انداختیم:الف- کنترل بدون برچسب ب) و ج) دو درایو برای انگیزه بخشی به از خود گذشتگی و یک مورد با کلید متصل و یک مورد با برچسب بـازگردانی و د) و ه) دو درایو برای انگیزه بخشی به منافع خود: یک مورد با آرم محرمانه و دیگری با «جواب امتحانات نهایی.»

آیا کاربران درایو ها را برمی دارند؟

برای تعیین کردن اینکه کاربران درایوهای یافت شـده روی زمـین را متصـل خواهنـد کـرد، تقریبـا 300 درایـو در محوطه دانشگاه ایلینویس در پردیس اربانا-چمپین آوریل 2015 انداختیم، و سنجیدیم که چه تعداد از انها برداشته شدند و متصل شدند. برای ردیابی ایمن مبتنی اینکه چه زمانی درایوها متصل می شوند، هر درایو را با فایـل هـایی پر نمودیم که متناسب با ظاهر درایو بودند اما فایل های اچ تی ام ال حاوی برچسـب آی ام جـی مرجـع بـه سـرور

مدیریت مرکزی بودند. این روش محدود بود چون نمی توانستیم موقعیت هایی را شناسایی کنیم که در آن کاربران فایلی را روی درایو باز نکنند. به هر حال، باور دارمی که این تعادل ایمنی را فراهم می کند، با توجه به اینکه نمی خواهیم کدی را روی دستگاه های کاربران اجرا کنید.

هنگامی که درایوها را می انداختیم، عوامل متغییر زیر را بررسی کردیم تا ببینیم که آیا آنها این احتمال را افزایش می دادند درایو متصل خواهد شد:

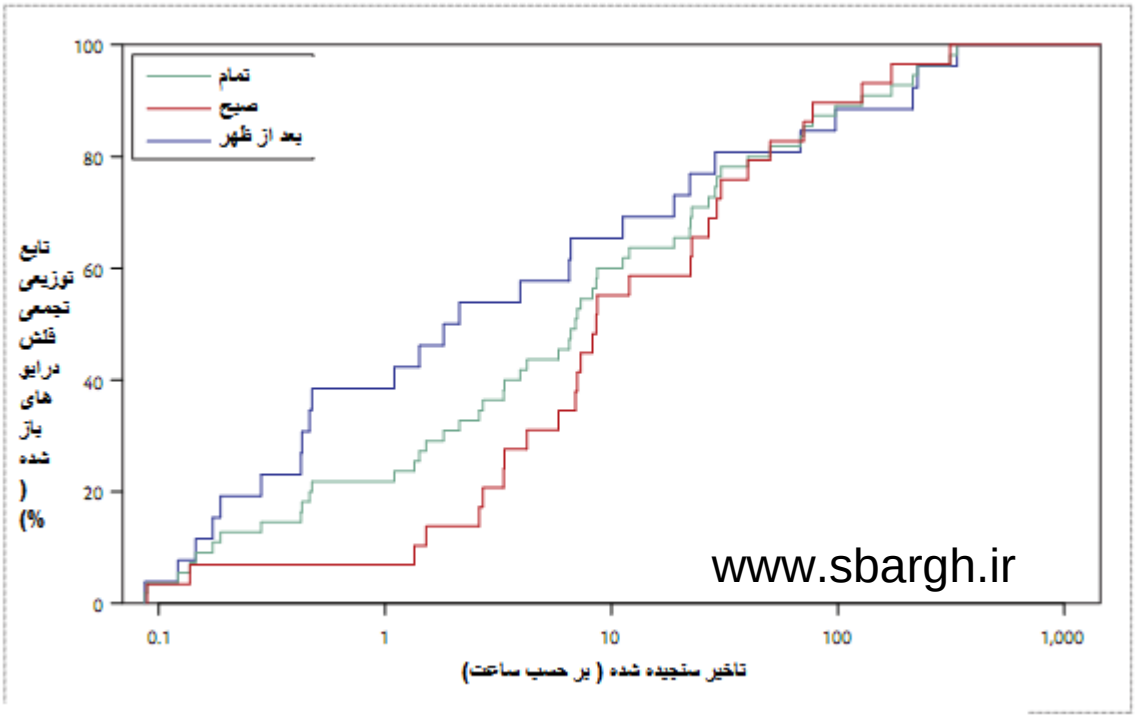
- ظاهر درایو: نوع درایوهایی را متغیر نمودیم که در هر نقطه محوطه انداختیم تا ببینیم آیا کاربران به واسطه از خود گذشتگی یا منافع شخصی انگیزه یافتند. درایو هایی با برچسب سود یا با کلیدهای متصل مهندسی شدند تا گرایشات از خود گذشتگی را تحریک کنند، درایوهایی با بر چسب «محرمانه» یا «جواب امتحانات نهایی» به منظور تحریک گرایشات خودخواهانه بودند و درایوهایی فاقد برچسب گروه کنترل ما بودند. شکل 2 نشان دهنده مثالی از هر کدام می باشد.
- محل جغرافیایی. فلش درایوها را در 30محل منحصر به فرد در محوطه در بین 5 محیط مختلف قرار دادیم: محل پارک، راهروها، نواحی علمی (کلاس درس، کتابخانه)، نواحی عمومی (راهرو ساختمان، کافی تریا) و نواحی خارجی (از جمله پیاده رو ها).
- زمان روز. درایوها را طی صبح (6 صبح الی 10 صبح) و بعد از ظهر (1 عصر الی 5 عصر) انداختیم.

به طور شگفت انگیز، پی بردیم که کاربران یک یا چند فایل را در 135 الی 197 فلش درایو (45 درصد) باز کردند و 290 درایوها (98 درصد) از محل انداختن خود برداشته شدند. چون هر نوع کدی را هنگام اتصال درایو اجرا نکردیم، معلوم نیست که آیا کاربران باقی 155 درایو را متصل نمودند. به هر حال، دو رقم نخست به ما این اجازه را می دانند که میزان موفقیت هجوم را بین 45 و 98 درصد بسنجیم.

ظاهر درایو

در حالی که درایوها نشانه «محرمانه» یا «پاسخ های سوالات نهایی» یا حاوی کلیدهای بودند، اما میزان موفقیت متفاوتی نسبن درایوهای بدون برچسب نداشتند، درایوهای با برچسب بازگردانی میزان موفقیت کمتری به ازای حمله داشتند. تردید داریم که این مسئله به خاطر شرکت کنندگان از خود گذشته باشد که روش های تعیین محل صاحب درایو در اختیار آنها نهاده شده بود:آدرس ایمیل روی بر چسب. برخی شرکت کنندگان به طور بارز بر این

اتفاق نظر بودند که برای ما داده های مفصل درباره کاربرد خود فراهم سازند که شامل این بود که چه فایل هایی را باز کردند و چه زمانی این کار را انجام دادند. ما بررسی کردیم که چه فایل هایی را شرکت کنندگان ابتدا باز کردند تا ببینیم که آیا اسامی فایل ها هر نوع اطلاعاتی درباره انگیزه های خود فراهم می سازند.



شکل 3- زمان تاثیر بین زمانی که فلش ها را انداختیم و زمانی که آنها متصل هب دستگاه شدند.

هر چند این واقعیت وجود دارد که شرکت کنندگان کمتری درایوهای را با برچسب های بازگردانی متصل نمودند حاکی از اینکه به طور از خود گذشته عمل نمودند، ترتیب عملیات فایل تصویر اندکی مختلف را نشان می دهد. درایوهای بدون برچسب و نیز درایوهای دارای کلید و یا برچسب بازگردانی حاوی فایلی بودند که به عنوان رزومه صاحب عمل می نمود که می تواند به عنوان محل منطقی برای یافتن اطلاعات تماس صاحب فلش درایو به کار رود. به هر حال، تقریبا نیمی از شرکت کنندگان که داده ها را فراهم نمودند ابتدا یکی از عکس های تعطیلات را باز کردند که به طور منطقی کمکی به پیدا کردن صاحب درایو نمی نمود. تردید داشتیم که شرکت کنندگانی که درایوها را برداشتند این کار را با نیت از خود گذشتگی انجام داده باشند اما گاهی کنجکاوی انها بر از خود گذشتگی انها غلبه نمود.

بهنگام بودن

پی بردیم که 87.5 درصد از درایوها در سری اول که بازگشتیم آنها را بررسی کنیم برداشته شده بودند، عصر همان روزی که درایوها صبح آن روز افتاده بودندو صبح روز بعد انداختن درایوها در عصر دیروز. همچنین به اندازه گیری

زمان بین انداختن درایوها و زمان متصل شدن آنها پرداختیم. درایوها متوسط زمان 6.9 ساعت به رایانه متصل شدند طوری که در شکل 3 توصیف شده است. درایوهایی که در عصر انداختیم به طور عمده سریع تر متصل شدند. به هر حال در هر دو حالت حمله موثر بوده و شرکت کنندگان بلافاصله درایو را کشیده بودند. جالب تر انکه بیش از 20 درصد از درایوها ظرف یک ساعت پس از افتادن وصل شده بودند. چون مهاجم ممکن بود برای شروع حمله به تک اتصال نیاز داشته باشد این حمله می توانست طی زمان کوتاه باعث آسیب گردد.

Reason	Respondents (n = 62)	
	No.	%
To return drive to owner	42	68
Curiosity	11	18
Listed a location instead of why he or she picked up the drive	5	8
To keep drive	2	3
Was given drive by someone else	2	3

جدول1

چرا کاربران درایوها را متصل می کنند؟

برای درک اینکه چرا کاربران درایوها را برداشته و احتیاط هایی می کنند، این فرصت را به افرادی دادیم که فلش ها را برداشته بودن تا نظرسنجی بی نام را پر کنند به طوری که ارتباطی با نظرسنجی در فایل های اچ تی ام ال روی درایو بیابیم. برای جمع آوری مقادیر نظرسنجی پایه ای دانشگاه ایلینیوس، همچنین 600 عضو تصادفی دانشگاه ایلینیوس در محوصله اورابانا-چمپین در دسمایر 2015 ایمیل کردیم. از کاربران درباره مورد زیر سوالاتی پرسیدیم

- جمعیت شناسی. سوالات جمعیت شناسی از بانک سوالات سروی-مانکی (از جمله سن، جنسیت و سطح تحصیلات) به همراه نسبت شرکت کننده با دانشگاه ایلینیوس (هیئت علمی، کارکنان یا دانشجویان) پرسیدیم.
- -دانش قبلی. پرسیدیم که آیا شرکت کنندگان از قبل درباره مطالعه شنیده بودند. بعدها پاسخ هایی را رد نمودیم که کاربر دارای دانش قبلی بود.
- انگیزه. از شرکت کنندگان علت برداشتن فلش درایو را پرسیدیم و اینکه آیا ظاهر بیرونی یا هر نوع عامل دیگر بر تصمیم آنها در انجام این کار تاثیر گذاشته است.

- رفتارها و مهارت رایانه. سوالاتی از مقیاس اهداف رفتار امنیتی پرسیدیم تا رفتارهای رایانه ای و امنیت رایانه شرکت کنندگان را بسنجیم و نیز سه سوال از سه مطالعه دیگر انجام دادیم تا مهارت رایانه ای آنها را بسنجیم.

- طرز تلقی به ریسک. سوالاتی از مقیاس ریسک پذیری زمینه خاص مطرح نمودیم کـه نظرسـنجی استانداردسـازی شده بود تا بسنجیم که فرد چگونه در رفتار پرخطر شرکت می کند.

62 پاسخ معتبر به نظرسنجی دریافت نمودیم که با 31 پاسخ معتبر جمـع آوری شـده از نظرسـنجی ایمیـل خـود مقایسه شدند و به اعضا تصادفی جامعه دانشگاهی ارسال گردیدند.

انگیزه

هنگامی که ازپاسخ دهندگان پرسیده می شود چرا در درایو قرار می دهند، اکثر انها پاسخ می دهند که می خواهند درایو را برگردانند (68 درصد) یا اینکه کنجکاو بودند (18 درصد). چند شـرکت کننـده خـاطر نشـان نمودنـد کـه کلیدهای متصل آنها را تشویق نمود تا مالک را بیابند. برای مثال: « آن اضطراری بود کـه بـه صـاحبش بازگردانـده شود. فرد ممکن است بیرون از آپارتمان/منزل خود مانـده باشـد، لـذا مـایلم آن را سـریع برگـردانم.» تعـداد کمـی کنجکاوی را مطرح نمودند که بر حس تردید غلبه داشت. « تعجب می کنم چرا تصویر جی.پی.ایی.چی دارای آدرس اچ.تی.ام.ال بود.» در دو حالت، شرکت کنندگان اقرار نمودند که درایو را برمی دارند چون نیاز به فلش درایو دارند به هر حال باید خاطر نشان نمود که کاربران احتمالا تمایل دارند گرایشات از خود گذشتگی را بسیار گـزارش دهنـد و موارد منافع شخصی را کمتر گزارش دهند. جدول 1 این نتایج را گزارش می دهد.

احتیاط

اکثر کاربران (68 درصد) به وضوح بیان نمودند که آنها هنگام متصل نمودن درایو احتیاط نمی کنند. برای کسـانی که احتیاط می کنند، ده نفر فایل ها را با نرم افزار آنتی ویروس اسکن می کنند، پنج نفر معتقدند کـه اُ.اس از آنهـا محافظت خواهد کرد، پنج نفر رایانه را قربانی نموده و نه نفر شکل دیگر محافظت را بیان نمودند. ما روندهای زیر را خاطر نشان می سازیم:

- شرکت کنندگان خطر بازدید از وب سایت های مخرب را نادیده گرفتند. چندین مورد از انها حتی فایل های موجود در فلش درایو را ایمن تر از نوع بسط یافته اچ.تی.ام.ال دانستند.
- شرکت کنندگان به طور عمدی از منابع موسساتی برای فعالیت غیر ایمن استفاده کردند تا از آلوده شدن رایانه خود اجتناب ورزند. برای مثال، هنگامی که از یکی از پاسخ دهندگان درباره مسائل ایمنی پرسیده شد، در پاسخ گفت، « من یک رایانه دانشگاه را قربانی این نوع آلودگی کردم»

- شرکت کنندگان به سیستم عامل خود و نرم افزار امنیت اعتماد داشتند تا از آنها محافظت به عمل آورد، برای مثال، « من به مک بوک خود اعتماد می کنم تا عامل دفاع خوبی در برابر ویروس ها باشد.»
- چند شرکت کننده احتیاط های منطقی در پیش گرفتند از جمله باز کردن فایل اچ.تی.ام.ال در ویراستار متن و اتصال درایو به رایانه آفلاین.

جمعیت سنجی

از بین 62 پاسخ دهنده به نظرسنجی یو.اس.بی، 41 مورد به عنوان دانشجو کارشناسی تعیین شدند، 13 مورد دانشجوی فارغ التحصیل ، هفت مورد کارکنان بودند که با جمعیت دانشکده چندان تفاوتی نداشتند؛ به هر حال، خاطر نشان می کنیم که هیچ کدام از پاسخ دهندگان عضو هیئت علمی نبودند. شرکت کنندگان 65٪ مرد و 35٪ زن بودند که تفاوت عمده ای با جمعیت دانشگاهی کلی نداشت. به طور مشابه، توزیع سنی دانشجو به طور عمده با جمعیت بزرگتر دانشگاه فرقی نداشت. هیچ اختلاف مردم شناسی عمده ای بین نظرسنجی ایمیل شده به فضای دانشکده (خط مبنا) و آمار چاپ شده دانشگاه ایلینیوس نیافتیم که نشان داد نظرسنجی خط مبنا به سمت هر نوع جمعیت سنجی ویژه یک سو نگری نداشت.

طرز تلقی به ریسک

نظرسنجی ما شامل سوالاتی از بخش ریسک پذیری داسپرت بود که می سنجید شرکت کنندگان چگونه در رفتارهای پرخطیر در پنج زمینه مختلف شرکت می کنند. پاسخ های شرکت کنندگانی را که درایو های یافت شده ا متصل نمودند با افراد مطالعه اولیه داسپرت مقایسه نموه و نظرسنجی را به نمونه دانشگاه ایلینیوس ایمیل کردیم. شرکت کنندگانی که درایو یو.اس.بی را متصل نموده بودند تمایل بیشتری داشتند تا در بخش سلامت/ایمنی، تفریحی و زمینه اجتماعی نسبت به جمعیت دانشگاه ایلینویس ریسک بپذیرند ؛ اشتیاق آنها به ریسک تفریحی حتی بیشتر از جمعیت داسپرت پرخطیرتر به لحاظ سنجش مردمی بود (جدول 3 را ببینید). این امر نشان می دهد که ریسک تفریحی می تواند برای تشخیص آسیب پذیری در برابر حملات فلش درایو به کار رود.

دانش رایانه و امنیت

برای سنجش مهارت رایانه ای کلی، از سه سوال مطالعه دیگر استفاده کردیم که از شرکت کنندگان می پرسید آیا آنها سیستم عاملی را روی رایانه نصب نموده اند یا اینکه مجدد نصب کرده اند، آیا شبکه خانگی را پیکربندی نموده

اند یا اینکه آیا صفحه وب ایجاد کرده اند. شرکت کنندگان به عنوان کارشناس دسته بندی شدند اگر پاسخ آنها به تمامی سوالات آری بود. تفاوت عمده ای بین میزان کارشناسان بین شرکت کنندگان ما و مطالعه دیگر وجود نداشت.

همچنین سوالاتی از اس.ایی.بی.آی.اس شامل ساختیم که نشان می دهد کاربران نهایی چگونه به خوبی توصیه های امنیتی معروف را دنبال می کنند از جمله اینکه من از گذرواژه های مختلف برای حساب های گوناگون خود استفاده می کنم که صاحب آنها هستم، اگر مسئله امنیت را بیابم، به کار خود ادامه می دهم چون فرض می کنم فرد دیگر آن را اصلاح خواهد کرد. شرکت کنندگان نظرسنجی ما با جمعیت ترک مکانیکی آمازون در ایگلمن و پیر در اکثر آیتم ها متفاوت عمل نمودند اما با گروه دانشگاه ایلینویس با دو آیتم فرق داشتند: من صفحه رایانه خود را تنظیم می کنم تا به طور خودکار قفل گردد اگر از آن در دوره طولانی مدت زمانی استفاده نکنم. و وقتی درباره به روز رسانی نرم افزار انگیزه می یابم، بلافاصله آن را نصب می کنم. این نتایج نشان می دهد شرکت کنندگانی که فلش درایور را انتخاب نمودند دارای رفتارهای امنیتی مشابهی همانند هم نظیران خود بوده و حمله علیه جمعیت دانشگاه ایلینویس موثر بوده به جای اینکه گروه فرعی متمایل به غیر فنی باشد.

	Respondents (n = 62)	
Precaution	**No.**	**%**
Scanned files with antivirus	10	16
Mentioned OS security features	5	8
Sacrificed a computer	5	8
Opened a file in a text editor	4	6
Sandboxed a file	3	5
Contacted or searched for a member of the research group to verify that the experiment was legitimate	2	3
The following specific words were used in participants' responses in the shown proportions:		
No	42	68
Yes	8	13

جدول2

بازگردانی ها و واکنش ها

همچنین تلاش های شرکت کنندگان را برای بازگردانی درایوهای یافت شده طبق زیر بررسی نمودیم.

درایوهای بازگردانی شده

هر چند به شرکت کنندگان این آموزش را دادیم که آنها می توانند فلش درایوهایی را نگه دارند که پیدا می کننـد، 54 (18 درصد)دایوها را بازگرداندند. از میان درایوهای بازگردانده شده، 36 (67 درصد) هرگـز بـه رایانـه متصـل نشدند. بخش عمده (17 مورد از 54، 32 درصد) از درایوهای بازگردانده شده دارای کلیدهای متصل بودند. یـازده مورد از درایوهای باقی مانده دارای برچسب های بازگردانی بودند ، نه مورد از این درایوها به رایانه متصل نبوده انـد. اکثر شرکت کنندگان که درایوها را به ما بازگرداندند کارکنان آی.تی یا اجرایی بودند.

ایمیل

درایوهایی با برچسب های بازگردانی حاوی 10 نام ساختگی تولید از شده 100 اسم معروف در بین سرشماری های 1993 و2000 آمریکـا بودنـد. سـپس حسـاب هـای منحصـر بـه فـرد جـی میـل را از شـکل نـام کوچک.فامیلی.ان.@جی.میل.دات کام یافتیم که در آن، حرف ان نشان دهنده شماره چهار رقمی تصادفی بود. هـر نام و ایمیل متناظر با آن را روی شش درایو نوشتیم. به طور متوسط، هر گیرنده 4.8 ایمیل از 4.4 فرستنده پس از یک هفته دریافت نمودند. اختلاف برجسته ای به لحاظ تعداد ایمیل ها یا تعداد آدرس های ایمیل منحصر بـه فـرد برای اسامی مرد و زن وجود نداشت.

رسانه اجتماعی

سایت های رسانه اجتماعی را به ازای هر نوع توصیفات آزمایش نظارت نمـودیم. سـاعت 11 صـبح روز دوم، دانـش آموزی تصویری را در فیس بوک یکی از فلش درایوها با کلیدهای وصل شده قرار داد. روز بعد ساعت 1 عصر شرکت کننده ای در ساب دریت دانشگاه درباره یافتن چند درایو در فضای دانشگاه نظر گذاشت و بیان کرد که آنها گزارش این رخداد را به گروه آی.تی دادند. نظردهندگان حضور (و آلوده نبودن) فلش درایوها را تایید نموده و درباره هدف مطالعه فکر کردند. دو نظر دهنده خوانندگان را هشدار دادند که از متصل نمدن ابزارها به رایانه های خـود اجتنـاب ورزند. روز بعد، یکی از کارکنان آی تی درباره پاسخ های امتحان نهایی نظری گذاشت و خوانندگان را تشویق نمـود که درایوها را به ابزاری متصل نکنند. علی رغم اخبار آزمایش و توصیه کارکنان آی تی درباره اتصال درایوها، حملـه عمدتا موفق بودند. شرکت کنندگان در طی آزمایش دوبار فلش درایوها را به محققانی بازگردانند که سعی داشـتند انها را بیندازند. این رویدادها را نمایش موثر از خود گذشتگی می دانیم که مبنای نتایج ما می باشد.

توصیه ها

سازمان ها می توانند مراحل گوناگونی را برای محافظت از خود در برابر این نوع حمله در پیش گیرند.

آموزش به کاربران

اختلاف جمعیت شناختی عمده ای بین جمعیت کلی در دانشگاه ایلینویس و شرکت کنندگانی نیافتیم که فلش درایو ها را برداشتند. شرکت کنندگان همچنین دارای ظرفیت ریسک مشابه و رفتارهای امنیتی بودند. انجمن های اموزشی باید هر فرد را در سازمان شامل سازد نه فقط شرکت کنندگانی که به طور یکنواخت در برابر این نوع حمله آسیب پذیر اند . هر چند رابطه بالقوه بین ظرفیت ریسک تفریحی یافتیم و از طریق یو اس بی به مخاطره افکندیم، اتکا بر این تناسب را پیشنهاد نمی کنیم.

هوشیار باشید

در طی آزمایش، یکی از واحدهای فناوری اطلاعات دانشگاه ایلینویس از سوی کارکنان بخش اطلاع رسانی شد پس از اینکه چند درایو در ساختمان خود یافتند. به طور مشابه نماینده های اجرایی با ما تماس گرفتند که از واحدهای مختلف بودند که سرانجام تعداد عمده ای از درایوها را جمع آورده کرده بودند که نزدیکی آنها جامانده بود. کسانی که درایوها را انداخته بودند همجنین به محل ها در چند وقت از روز بازگشتند و شرکت کنندگان آنها را از انداختن درایوها اطلاع رسانی نمودند.

به هر حال شرکت کنندگان درایوها را به آنها به جای پی بردن به رفتار مشکوک خود بازگرداندند. سازمان ها باید کارکنان را توصیه کنند که متوجه رفتار مشکوک و علائم هجوم بوده و کانال هایی برای کارکنان برای گزارش سریع مسائل فراهم سازند.

Our participants versus ...	Risk attitude				
	Ethical	Financial	Health/safety	Recreational	Social
DOSPERT study	Less	Less	Less	More	Less
University of Illinois	Not significant	Not significant	More	More	More

جدول 3

استحکام بخشی به منابع محاسبه

هر موقع که شرکت کنندگان احتیاط می کنند، آنها به پیکربندی موجود رایانه متکی می شوند .شرکت کنندگان استفاده از اسکنرهای ویروس را ذکر کردند و بر ویژگی های امنیت سیستم عامل تاکید داشتند و حتی رایانه های

مشترک را قربانی نمودند قبل از اینکه روش هایی از جمله بازکردن فایل ها را در ویرایش گر متن تحت نظارت قرار دهند.

ما توصیه می کنیم دستگاه ها تقویت شوند تا پیامدهای بالقوه در کنش های غافلانه کاربر کاهش یابد.

داشتن برنامه

شرکت کنندگان درایوها را سریع وصل نمدودن که بیش از 20 درصد ظرف یک ساعت پس از جا انـداختن متصـل نمودند. بدین لحاظ کشف حمله ممکن است به زودی قبل از مخاطره افکنی (و حتی پس از آن) رخ دهـد. هشـدار دهی ها باید متمرکز گردند تا اطمینان حاصل گردد که کارکنان متوجه حملات هستند.

مطالعه نشان می دهد که این روش حمله باید در برابر کاربران موثر بوده و فرد معمولی خطر متصـل نمـودن ابـزار جانبی ناشناخته را به رایانه خود نمی داند. دریافتیم که حمله و هجوم هنگامی که با ریسک های مربوط بـه اتصـال درایو ترکیب می گردد، هنوز می تواند برای بسیاری از سازمان ها خطر آفرین باشد. امیدواریم که بـا مطـرح کـردن این جزئیات مدیران را یادآور شویم که گاهی ساده ترین حملات واقع بینانه ترین تهدیدات اند. بـرای بررسـی ایـن خطر، سازمان ها باید کاربران را آموزش دهند، منابع محاسباتی را دربرابر حملات مبتنی بـر یـو اس بـی مسـتحکم سازند و برنامه پاسخ در حالت حمله فراهم سازند.