امنیت اطلاعات ۲۰۱۲

زیر میکروسکوپ

دیده‌بان ۵
امنیت فناوری اطلاعات

بسم الله الرحمن الرحیم

دیده بان ۵
امنیت فناوری اطلاعات

گزارش امنیت فناوری اطلاعات در سال ۲۰۱۲

ویژه نامه بهار ۱۳۹۲ - افتانا

با استفاده از منابع شرکت های: Kaspersky و Trustwave

سردبیر: علیرضا صالحی
ترجمه‌ها: واحد ترجمه افتانا
گرافیک: نیلوفر فروغی، عاطفه محمدی
باسپاس از: محمد مبصری، شرکت تجارت امن خاورمیانه

info@aftana.ir تلفن: ۸۸۵۱۹۱۸۲

بـازرسی‌هـای انجـام شده در ۲۰۱۱

تحقیقاتی که از سوی Trust Ware در مورد پاسخگویی در مقابل حوادث سایبری انجام شده است که اطلاعات به دست آمده از سوس یازمان‌های قربانـی و یا اشخاص ثـالث حاکی از نتایج نگران کننده ای است که در ادامه به آنهـا می‌پردازیم. اما ذکر این نکته بسیار حائز اهمیت است که اطلاعاتی که ما بر اساس آن‌هـا تحلیل‌هـای خود را انجام داده‌ایـم بر اساس پیش بینی‌هـا و ارزیابی‌ها صورت نگرفته‌اند بلکـه بر اسـاس داده‌هـای واقعـی که توسط Trustware Spiderlabs به دست آمده ارائه شده است.

کشورهـا و متولـوژی استفـاده

در سـال ۲۰۱۱ Trustware Spiderlabs مطالعـات زیـادی را روی بیش از ۳۰۰ مورد از افشای اطلاعات که در ۱۸ کشور دنیا دارد انجام داد. بیشتر تحقیقات به نسبت سال گذشته در بخش آسیـا و اقیانوسیه (APAC) انجام شد چرا که در این مدت تغییرات زیادی در جهت قدرتمند کردن قوانین ضد افشای اطلاعات رخ داده است. برای مثـال کشورهای بیشتری در حوزه APAC در حال تطبیق خود با اسانداردهای کارت‌های پرداخت Payment Card Industry Datasecurity Standard(PCI PSS)
با این انطباقی که در کشورهای این حوزه در حال انجام است طبیعتا سازمان‌های بیشتری متعهد به ارائه گزارش از میزان افشای اطلاعـات در دوره های زمانی مشخص هستند. به طور مشابه اتفاقـات جدیدی نیز در حوزه آمریکای لاتین و دریای کارائیب نیـز به وقوع پیوسته است و سازمان‌هـای بی‌شماری تحت قوانین PCI PSS در حال فعالیت هستند.

18 تعـداد کشورهـا

>300 رخنـه در داده‌هـا

داده‌هـای مـورد بررسـی:

در ادامه روندهایی که در سالهای گذشته دیده می‌شد، ۸۹% از تحقیقات ما شامل سرقت داده های مشتریان که شامل اطلاعات کارت‌های پرداخت، اطلاعات شناسایی شخصی و سایر اطلاعات مثل آدرس‌های ایمیل است. ایمیل‌های فعال از مشتریان بسیار مقاصد ارزشمندی برای حمله هستند و می‌توان از آن‌ها برای حملاتی چون فیشینگ های مرسوم استفاده کرد.

تبهکاران سایبری همچنان در تلاشند تا با استفـاده از بازارهای سیاهی که به تازگـی در این حوزه ایجاد شده است و به سـادگی امکـان تبـدیل اطلاعات کارت‌هـای اعتبـاری به پول نقـد را می‌دهـد به پول‌هـای زیـادی دست‌یابنـد.

در موارد زیـادی در سـال ۲۰۱۱ وجود دارنـد که حاکـی از آن است کـه تبهکـاران سایبـری با استفـاده از مقاصد جذابـی چون شماره حساب‌هـای مالـی تجاری (مثل کدهای رهگیـری، و یا شماره‌های شناسایی تاجر و ...) توانسته‌اند فعالیت‌هـای چشمگیـری را در حـوزه جعـل کارت‌هـای بانکـی صورت دهند.

زمانی که شمـاره شناسایی یک تاجر به دست می‌آید، تبهکاران سعی می‌کنند تا این اطلاعـات را بایک کارت پرداخت منطبق کنند و با یک سیستم تراکنش جعلی می‌تواننـد از این کارت پول برداشته و در نهایت این تراکنش‌های حیله گرانه به عنـوان تراکنش‌هـای صحیح و مناسب توسط سیستم‌های اصلی در نظر گرفته می‌شوند.

از همین فرآیند برای پول‌شویی نیز استفاده می‌شود. به عبارت دیگر پول‌های کثیف با استفاده از شماره شناسایی یک تاجر که هیچ سیستم مالی به آن مظنون نبوده جابجا می‌شود و تبدیل به پول تمیز می‌شود.

برای مثال هکرها می‌تواننـد از یک دسته از کارت‌های بانکی برای خرید استفاده کنند و در نهایت از هر کدام از این کارت‌های برای پرداخت بخش کوچکی از هزینـه خرید استفـاده کنند.

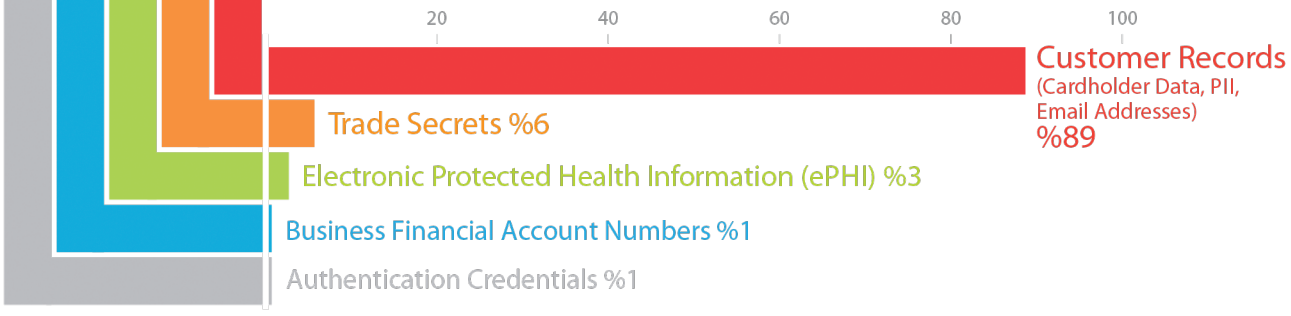
لذا سرقت اسـرار تجاری یکـی از جذاب‌تـرین و در عین حال پیشرفتـه‌ترین روش‌هـایی است که هکرهـا از آن برای دستیابی به مقاصد خود استفـاده می‌کننـد.

از دیگر اتفاقـات مهمی که در سال می‌توان به آن اشـاره نمـود سرقت اطلاعـات بهداشتی و درمـانی افـراد بود که البته ۳% از کل افشـای اطلاعـاتی که در این سال توسط Trust Ware بررسی شده بود را شامل می‌شود و شاید دلیل اصلی آن ارتقـاء آگاهی‌ها در خصوص حفظ اطلاعات و ارتقاء سیستم‌های حفاظتی که به واسطه وضع قوانین جدید و همچنین ارتقاء آگاهی عمومی باشد.

وضعیـت امنیـت در صنـایـع

صنـایع:

به طور ثابت و طی روندی که در از سال‌هـای قبل نیز ادامـه داشتـه است بخش‌های صنـایع غذایی و نوشیدنـی، خـرده فروشی‌هـا و صنایع گردشگـری حدود ۸۵% افشای اطلاعات را به خود اختصـاص داده‌انـد و همانطور که قابل حدس زدن است اطلاعات کارت‌های پرداخت، عمده‌ترین هدف حملات سایبری بوده‌اند؛ و این در حالی است که افراد شاغل کسب و کارهای کوچکی که در این حوزه مشغول فعالیت هستند دارای اطلاعاتی به مراتب کمتر از کارمندان یک بانک بزرگ در خصوص حفظ اطلاعات حیاتی و ارتقاء سامانه‌های امنیتی در محیط مجازی هستنـد و همین امر مهم‌تـرین مسئله‌ای است که هکرهـا از آن بهترین استفاده را می‌کنند و لذا استاندارد کردن سامانه‌هـای رایانـه‌ای به خصوص در حـوزه فرانچایز می‌تواند تاثیر عمده‌ای در ارتقاء امنیت اطلاعات و در نتیجه کاهش حجم افشای اطلاعـات داشته باشند چرا که بر اساس اطلاعات به دست آمده بیش از یک سوم از افشای اطلاعاتی که در بخش صنایع غذایی و نوشیدنی، خرده فروشی و توریسم انجام شده است مربوط به صنایعی است که عمدتا به شیوه فرانچایز اقدام به پیشبرد اهداف تجاری خود می‌کنند.



ارزیـابی هـدف‌هـا:

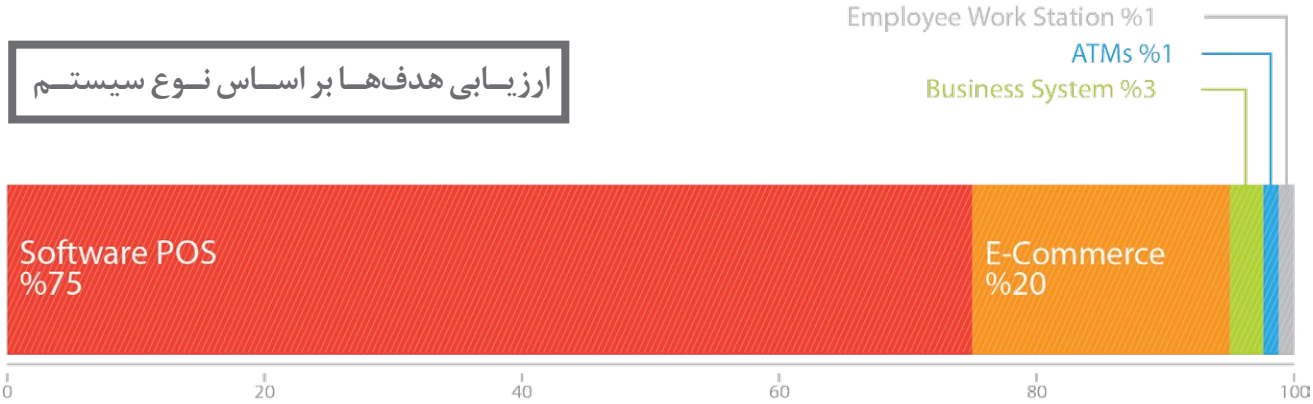
سیستم‌های اطلاعاتی که دارای فرآیندهای پرداخت هستند همواره به عنوان یکی از جذاب‌ترین هدف‌های هکرها مد نظر بوده است. زمانی که هکرها اطلاعات این کارت‌های پرداخت مبتنی بر این سامانه‌ها را بدست می‌آورند می‌توانند به راحتی با استفاده از این اطلاعات یک کارت تقلبی ایجاد نمایند و متعاقبا با استفاده از آن اقدام به خرید کالاها و خدمات مورد نیاز خود با استفاده از این کارت‌ها کنند.

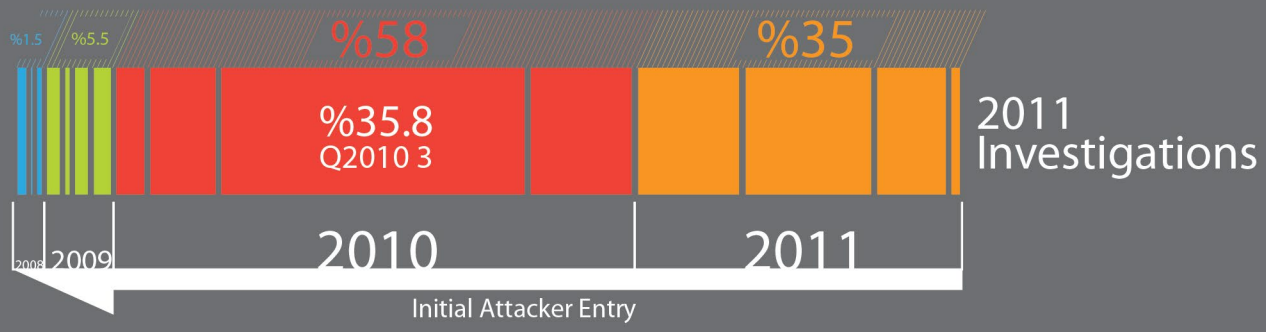
راهکاری به نام رمز نگاری Point to Point (P2PE) عرضه شده است که می‌تواند تا حد زیادی ریسک سوء استفاده از سامانه‌ها و دستگاههای POS را به شدت کاهش دهد البته برای اینکه این فناوری بتواند به خوبی مفید واقع شود می‌بایست تنظیمات و پیکربندی آن با متناسب با شرایط به کارگیری به درستی انجام شود و در صورت دستیابی به این مهم آمار سوء استفاده از حوزه های امنیتی این سیستم که هنگام تبادل اطلاعات از دستگاه POs بین بانک مبدا و مرجع انجام می‌شود به شدت کاهش می‌یابد.

در سال ۲۰۱۱ آمار افشای اطلاعات از طریق زیر ساخت‌های تجارت الکترونیک از ۹% به ۲۰% افزایش یافته است که عمده دلیل آن گسترش استفاده از ین زیر ساخت در ناحیه APAC است چرا که در این ناحیه تمایل زیادی برای استفاده از این زیر ساخت برای تراکنش‌های مالی به نسبت استفاده از سامانه های مبتنی بر POS وجود دارند. اما ATM ها نیز اگرچه به صورت نامنظم، اما در مقاطعی مورد حمله هکرها قرار گرفته‌اند و این در حالی است که اگر هکر بتواند PIN های موجود در کارت‌های نوار مغناطیسی را روی جعل کند به راحتی می‌تواند از طریق این دستگاه‌ها به مقدار نامتناهی پول تقد دسترسی پیدا کند. یکی از رایج‌ترین روش‌ها برای دستیابی به این اطلاعات استفاده از ابزارهای سخت‌افزاری است اما روندی که در طول سال گذشته دیده شده است باز هم تاکید بر نفوذ سیستم‌های نرم‌افزاری از طریق نصب بدافزارها در ATM است.

اما در این میان کارمندان نیز خود به عنوان اهدافی جذاب برای به دست آوردن اطلاعات محرمانه و اعتباری مد نظر برای هکرها و تبهکاران سایبری قرار گرفته‌اند. در این بین ایمیل‌هایی با اهداف خرابکارانه به برخی از کارمندان خاص که بعضا از مدت‌ها قبل نیز در نظر گرفته شده‌اند ارسال می‌شود. این ایمیل معمولا یک فایل و PDF یا یک فایل اجرایی و یا یک URL را به همراه خود دارد و به مجرد اینکه کاربر از هر کدام از موارد فوق استفاده نماید بلافاصله بدافزار مورد نظر هکرها روی رایانه آن‌ها نصب می‌شود و به سرعت در سایر رایانه‌ها نیز از طریق شبکه گسترش می‌یابد.

معمولا نخستین کاری که این بدافزارها انجام می‌دهند این است که به هکری که آن‌ها را منتشر کرده است این اجازه را می‌دهند تا دسترسی بی‌حد و حصری به اطلاعات موجود در سامانه‌های رایانه‌ای که بدافزار روی آن نصیب شده است را فراهم نماید.





مسئولیت پذیری مدیران سیستم

بخش عمده‌ای از تحلیل‌هایی که ما روی گزارشات مربوط به افشای اطلاعات انجام دادیم (حدود ۷۶%) بیانگر این مسئله بود که یکی از مهم‌ترین مواردی که منجر به افشای اطلاعات شده است مربوط به واکنش‌های دیرهنگام یا نامناسب شخص ثالث بوده است. مسئله‌ای که هکرها نیز به خوبی از آن مطلع هستند و تا حد ممکن نیز از این ضعف به نفع خود استفاده کرده‌اند.

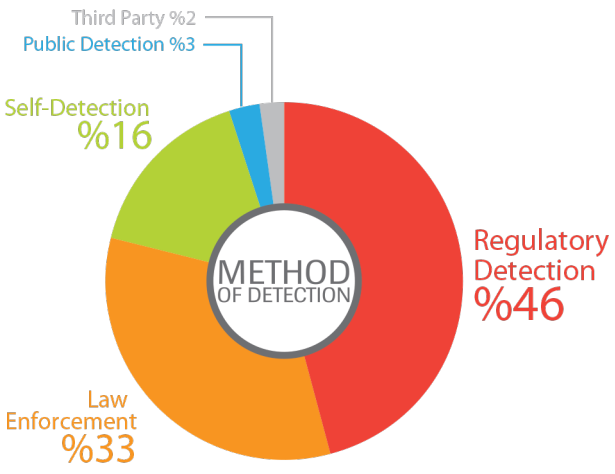
همانطور که گفته شد اغلب این سوء استفاده‌ها نیز امروزه در صنایع غذایی، نوشیدنی، خرده فروشی‌ها صورت می‌گیرد چرا که معمولا این صنایع کلیه موارد مربوط به توسعه زیر ساخت‌های رایانه‌ای خود را برون سپاری می‌کنند.

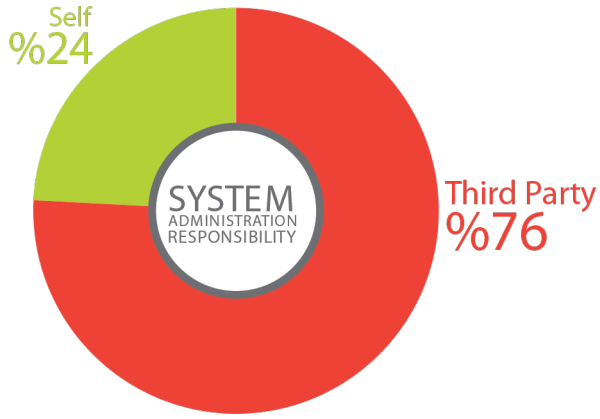
در مثالی دیگر قربانیان از اینکه افراد شخص ثالث تنها برای مجموعه محدودی از زیر سیستم‌های امنیتی مسئولیت داشته‌اند و در بسیاری دیگر از موارد خدمات خاصی ارائه نمی‌کنند و بنابراین سیستم‌های رایانه‌ای آن‌ها در این بخش‌ها دارای آسیب‌پذیری زیادی هستند.

در خصوص ۸۴% باقی مانده از سازمان‌ها آن‌ها به گزارشاتی که به آن‌ها توسط نهادهای خارجی اطلاعاتی داده می‌شود اتکا می‌کنند. اما این اتکا ضررهای فراوانی را متوجه این سازمانها می‌کنند. به طور مثال در یکی از این موارد یک شخص سوم به طور میانگین بعد از اینکه بدافزار مورد نظر ۱۳۷,۵ روز را در محیط سایبری سازمان مشغول انجام فعالیت‌های مخرب خود بوده است را کشف کرده‌اند.

ولی سازمان‌هایی که در این مورد به خود اتکا داشته‌اند دارای بخش‌های داخلی امنیت اطلاع بوده‌اند با میانگین زمانی تنها ۴۳ روز بعد از آلودگی اولیه توانسته‌اند بدافزارهایی که به سامانه رایانه‌ای آن‌ها نفوذ کنند را شناسایی کنند.

در این میان اما به خصوص در ایالت متحده با تغییر قوانین و وضع قوانین موجود، کشف بد افزارها به خصوص در مورد اعضای سازمانی تحت عنوان U.S. Secret Service and Electronic Crime Task Force از عدد ۷% در سال ۲۰۱۰ به عدد ۳۳% در سال ۲۰۱۱ افزایش پیدا کرده است و این مسئله بیانگر تاثیر بسزای قانون‌گذاری صحیح و توجه دقیق به قوانین است.





آمـار بدافزارهـا:

انـواع و اقسام بدافزارهـا در انـواع اشکـال و انواع اندازه‌هـا به قصد سرقت اطلاعـات حساس، ایجـاد امکان کنتـرل از راه دور برای صاحب بدافـزار و یا استفاده از رایانـه به عنوان یک ابزار باتنتی و حتی برای ایجاد خسارت‌های فیزیکی ایجاد شده‌اند.

Trustware Spiderlabs از سالیان گذشته مشغول تحلیل بدافزارها به منظـور پایش روند توسعه بدافزارهـا بوده است و در حال حاضر بانک اطلاعاتی از این بدافزارهـا را گـردآوری کـرده است.
در حال حاضر این بانک اطلاعاتی شگرفی را در خصوص مراحل پیشرفت شگرفی را که امـروزه در تولید بدافزارهـا رخ داده است را در اختیـار کارشناسان قرارداده است.

بدافزارهـای هدفمنـد در مقابل بدافزارهـای عمومی

بدافزارهـایی که تا به حال در مقیاس‌هـای گسترده‌ای توانسته اند خود را توزیع کنند اغلب از استراتژی خود تکثیر شوندگی استفاده می‌کنند. اما برخی دیگر از بدافزارها تنها از ویژگی خود تکثیرشوندگی استفاده نمی‌کنند بلکه از آسیب‌پذیری‌های رایجی که در سایـر نرم‌افزارهـا وجود دارند نیز استفاده نمی‌کنند لرا بدون این نشانه‌هـای مشخص پیـدا کـردن و تشخیص این بدافزارها برای نرم‌افزارهـای ضدبدافزار بسیـار دشـوار است و البتـه در حالی که بهتـرین نرم‌افـزارهای ضدبدافـزار توانستنـد حداکثـر ۶۰% از بدافزارهـایی کـه درون بـانک اطلاعـاتی ما قرار دارنـد را کشف کننـد.

بدافزارهایی که به طور رایج دیده و یافت می‌شوند اغلب شامل اجزایی برای آلوده کردن رایانه، بخش دستور و کنترل (C&C) و... می‌باشد و نکته قابل توجه این است که با ترکیب و کم و زیاد کردن هر یک از این مولفه ها به راحتی یک بدافزار جدید بوجود می‌آید که در حدود ۸۹% از بدافزارهایی که در بانک اطلاعاتی Trust ware spiderlabs وجود دارند به همین ترتیب ایجاد شده‌اند.

بدافزارها البته هر روز پیچیده تر می‌شوند، به طور تخمینی ۱۳% از بدافزارهای بانک اطلاعاتی که در اختیار آزمایشگاههای Trustware است نشان می‌دهد که این بدافزارها دارای فناوری منحصر به فرد خود هستند و برای تحلیل نحوه عملکرد و زبان برنامه نویسی آن‌ها نیاز به دانش عمیقی وجود دارد.

تاکتیک‌هایی چون ثبت DLL ها، دستکاری در تنظیم‌های AppInit- DLL و DLL Hijaclaing بیشترین تکنیک‌هـایی هستند که توسط Trust ware spiderlabs به ثبت رسیده‌اند.

Packers:

فشرده‌سازها، نرم‌افزارهای کاربردی هستند که به کاربر این امکان را می‌دهند تا فایل‌های اجرایی خود را فشرده کنند تا حجم کمتری داشته باشند؛ و در بسیاری موارد دارای ویژگی و رمزنگاری نیز می‌باشند و همین ویژگی به یکی از بهترین و مرسوم‌ترین راه‌ها برای بدافزارها بدل شده است تا با استفاده از آن بتواند خود را درون کدهای باینری مخفی کنند و به راحتی تکثیر شوند و البته این روش می‌تواند از بدافزارها در مقابل یافت شدن توسط ضد بدافزارها نیز حمایت کند.

باید گفت که در میان نمونه‌ها بدافزارهایی که ما در بانک اطلاعاتی خود جمع‌آوری کرده‌ایم بسیاری از آن‌ها از همین روش برای دستیابی به مقاصد پلید خود استفاده می‌کنند به عبارتی در حدود بیش از ۳۶% از کل نمونه‌ها.

انواع بدافزارها

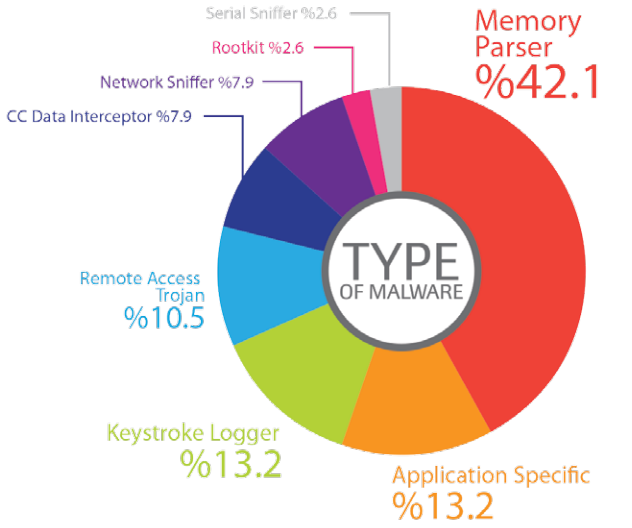
همانطور که در شکل زیر نیز دیده می‌شود بدافزارهای نوع Memory Parser در حدود ۴۲ % از کل بدافزارهایی که در بانک اطلاعاتی ما وجود داشتند را تشکیل می‌دهند.

پس از آن بدافزارهای Application Specific را می‌توان به عنوان روندی نوظهور در نظر گرفت و بررسی نحوه عملکرد آنها به اطلاعات فنی و دانش زیادی نیاز دارد. این نوع بدافزارها بیشتر روی سامانه های POS و ATM متمرکز هستند.

بدافزارهای Application Specific به طور مستقیم به اطلاعات حساس در حافظه و یا با استفاده از کاربر و حتی نرم‌افزار ثالث برای اینکه به طور مستقیم اطلاعات مورد نیاز را به بدافزارها ارسال کنند. تحقیقات ما نشان می‌دهد که بسیاری از هکرها در حال به روز رسانی بدافزارهای خود به نسخه‌های جدیدتری هستند که بتوانند از روش‌های جدید تری وبه دور از چشم نرم افزارهای ضدبدافزار به مقاصد خرابکارانه خود دست یابند باید گفت که هنوز زبان‌های برنامه نویسی چون C++ و Delphi و Net. به عنوان محبوب‌ترین زبان‌های خارجی برنامه‌نویسی برای کدنویس های بدافزارها مطرح هستند. البته همچنان هکرها از قطعه کدهایی بسیار قیمتی نیز استفاده می‌کنند. قطعه کدهایی که با کمترین تغییر در آن‌ها می‌توان اقدامات بسیار زیادی را توسط آن‌ها صورت داد.

انجام مهندسی معکوس در نمونه بدافزارهایی که در بانک اطلاعاتی ما وجود داشت اغلب حاکی از یک سرقت از کدهای متن بازی که برای مقاصدی دیگر نوشته شده بودند حکایت داشت. هکرها با ایجاد تغییراتی کوچک در این کدها به کلی توانسته بودند کاربری آن‌ها را تغییر دهند.

نکته جالب توجه دیگری که در نمونه‌هایی که به طور خاص در سال ۲۰۱۱ به بانک اطلاعاتی اضافه شدند دیده‌می‌شوند گسترش

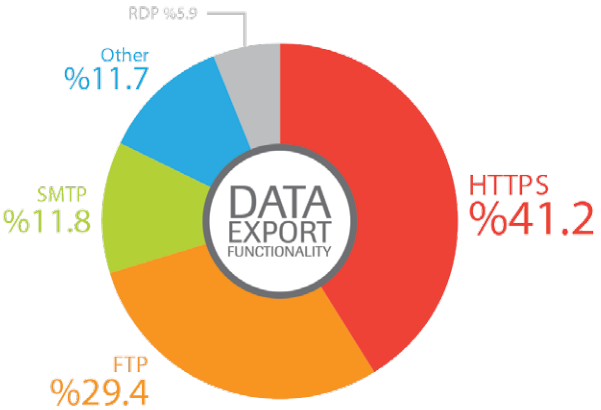


روند استفاده از PerlZExe که برای اینکه نسخه قابل حمل Perl را بتوانند درون بدافزارها به صورت توکار استفاده کنند می‌باشد.

Perl اصولا به سبب ویژگی‌های خاصی که دارد بسیار مورد توجه بدافزار نویس‌ها قرار گرفته است.

داده‌های خروجی

استفاده از ضعف‌های پروتکل HTTP برای دستیابی اهداف خرابکارانه روندی بود که در سال ۲۰۱۰ آغاز شد و اکنون با تحقیقات به عمل آمده می‌توان گفت که در سال ۲۰۱۱ گسترش بی‌اندازه‌ای یافته است. در نمونه‌هایی بررسی شد ۴۱٫۲% از بدافزارها از HTTp یا CTP و ترافیک پورت ۸۰ و ۴۴۳ برای نفوذ یا سرقت اطلاعات استفاده کرده‌اند. البته باید گفت که روند نوظهوری برای استفاده از HTTPS نیز آغاز شده است که لازم است مدیران شرکت‌ها و سازمان‌ها و همچنین کارشناسان امنیت اطلاعات تدابیر جدیدی را برای جلوگیری از سوء استفاده از این پروتکل اتخاذ کنند.



اما پروتکل FTP:File Transfer Protocol به طور سنتی یکی از جذاب‌ترین پروتکل‌ها برای سرقت اطلاعات و یا نفوذ به سیستم‌ها بوده است.

پروتکل SMTP:Simple Mail Transfer Protocol نیز از دیگر پروتکل‌هایی است که از لحاظ جذابیت برای هکرها در رده سوم قرار دارد چرا که سهم ۱۱٫۸% را به خود اختصاص داده است.

ضعف امنیت سیستم‌ها زیر میکروسکوپ

بنگاه‌ها و شرکت‌های تجاری به طور مداوم به دنبال حفاظت از دارایی‌های خود هستند که این دارایی‌ها هم شامل دارایی‌های فیزیکی و هم دارایی‌های فکری می‌شود. در ادامه به ۴ روش بنیادین که برای ارتقاء امنیت بنگاه‌ها و شرکت‌های تجاری به کار می‌روند خواهیم پرداخت.

در محیط کاری:
چهار منبع آسیب پذیری

در هر روز کاری کارمندان به شبکه کاری دسترسی پیدا می‌کنند، ایمیل‌های زیادی ارسال و دریافت می‌کنند، به وب دسترسی دارند و از ابزارهای موبایل استفاده می‌کنند. هکرها و تبهکاران سایبری همواره از محل کار به عنوان محلی که دارای فرصت‌های زیادی است یاد می‌کنند و تا به حال نیز از همین فرصت‌ها استفاده‌های فراوانی برای دست یافتن به مقاصد پلید خود استفاده کرده‌اند.

اما Trustware Spiderlabs بیش از ۲۰۱۱ در محیط‌های کاری انجام داد تا متوجه شود که مهم‌ترین بخش‌هایی که شرکت‌ها از آن‌ها آسیب می‌بینند چه بخش‌هایی هستند. نتایج این تحقیقات منجر به شناسایی ۴ نقطه آسیب‌پذیر شد که عبارتند از : شبکه، ایمیل، وب و ابزارهای موبایل؛ و در حالی که بسیاری از کارشناسان حوزه امنیت فناوری اطلاعات تمرکز خود را روی کشف تهدیدات جدید متمرکز کرده‌اند حال آنکه هنوز هم بسیاری از حملات خرابکارانه با روش‌های قدیمی و بعضا ساده صورت می‌گیرد.

شبکه ها- مسئله سیستم های قدیمی هنوز پابرجاست

مسائلی چون امنیت کلمات عبور، ابزارهای قدیمی، پروتوکل‌های نرم‌افزاری و سخت‌افزاری و مدیریت ناکارآمد همچنان یکی از عمده‌ترین مواردی هستند که نه تنها در حال حاضر بلکه سالیان پیش نیز امنیت شبکه‌های رایانه‌ای را تهدید می‌کرده‌اند.

احراز هویت در شبکه

تعین هویت در شبکه یکی از فراگیرترین آسیب‌پذیری‌هایی تحت شبکه در سال ۲۰۱۱ بوده است. می‌توان این نوع آسیب‌پذیری را به ۴ گروه که خودطیف گسترده‌ای را شامل می‌شوند تقسیم کرد:

موضوع شبکـه/دامنـه

این آسیب‌پذیری به طور مستقیمی با Network Domain Microsoft Active Directory و هر نوع ابزاری که به مدیریت فایل‌ها یا به اشتراک‌گذاری پرینتر در شبکه می‌پردازد در ارتباط است. آسیب پذیری‌ها می‌تواند به سبب فقدان سیاست‌هایی خاص در خصوص ایجاد کلمات عبور در دامین که منجر به ایجاد کلمات عبور ضعیف و یا حتی نبود کلمه عبور می‌شود به وجود آمده باشند.

از دیگر مواردی که در این خصوص می‌توان به آن‌ها اشاره کرد ایجاد حساب‌های کاربری موقتی است که از نوع Admin است که در بسیاری از شبکه‌ها و به دلایل متعدد ایجاد می‌شوند اما هیچگاه این حساب‌ها پاک نمی‌شوند و بسیاری از هکرها و بدافزارها اتفا قا با استفاده از همین حساب‌های کاربری که به حال خود رها شده‌اند می‌توانند به درون شبکه نفوذ کنند.

موضوع ابزار/سرویس

از مهم‌ترین مواردی که می‌توان در خصوص این دسته از آسیب‌پذیری‌ها به آن‌ها اشاره کرد، به کارگیری ابزارها و خدمات در شبکه با داشتن تنظیمات پیش فرض و حتی نداشتن کلمه عبور مناسب برای ورود به بخش تنظیمات آن‌هاست.

در خصوص ابزارها و خدمات می‌توان به موارد زیر اشاره کرد :

*روترها، سوییچ‌های شبکه، دیواره‌های آتش و سایر ابزارهای امنیتی که با کلمات عبور پیش فرض، ضعیف و حتی بدون کلمه عبور در حال کار در شبکه هستند.

*خدمات بانک اطلاعاتی مثل اوراکل یا Microsoft SQL

*رابط‌های کاربری مدیریتی برای VOIP و سایر ابزارهای PBX

موضوع ایستگـاه کاری/دستـرسی از دور

حساب‌های کاربری که اطلاعات آن یا تکمیل نشده و یا به راحتی قابل حدس زدن است و یا Workstation های با خدمات ad-hoc مثل VNC و PCAnywhere و یا سایر نرم‌افزارهایی که امکان دسترسی از راه دور را فراهم می‌کنند می‌توانند هریک به عنوان نقطه ضعف اساسی برای سازمان‌ها محسوب شوند.

البته مثل قسمت قبلی درجه تاکید این آسیب‌پذیری‌ها بسته به نوع ابزارها یا نرم‌افزارهای موجود و نوع محله بسیار متفاوت است و البته استفاده از کلمات عبور که مجددا بین دامین و سیستم Local استفاده شده و همچنین کلمات عبور تکراری که در چندین سیستم به کار گرفته شده‌اند نیز خود مزید بر علت هستند.

موضوع شبکـه/انتقـال

گواهینامه های اعتبار سنجی که در شبکه به صورت متن‌هایی آشکار هستند و یا از الگوهایی منسوخ و ضعیف برای رمز نگاری استفاده می‌کنند نیز یکی دیگر ازموارد معضلاتی هستند که به شدت در کاهش امنیت محیط تبادل اطلاعات اثر گذار است.

حمـلات قدیمـی

متاسفانه با وجود هشدارهـای فـراوان امنیتـی هنـوز هم تعـداد زیـادی از شبکه‌هـا و سیستم‌هـای رایانـه‌ای وجود دارند که در مقابل حملاتی که بـه شیوه‌هـای قدیمی و بعضا منسوخ صورت می‌گیـرند بسیار آسیب‌پذیـر هستند. روش‌هـایی که حتی نخستیـن کاربردهای آنهـا به بیش از ۱۰ سال قبل باز می‌گـردد. سازمان‌ها معمولا از فناوری‌های جدیـد استفـاده می‌کنند اما زیـر ساخت‌هـای قبلی را نامنـاسب با آن‌ها بازآرایـی نمی‌کنند. در ایـن حالت معمولا حملاتی که صورت می‌گیرد را می‌توان در بخش‌هـای زیـر دسته‌بندی کرد:

پروتکل‌های رمزنگاری نشده

به پروتوکل‌هایی که از طریق آن‌ها اطلاعات حساس شرکت و یا سازمان و کار بر جا به جا می‌شود و عدم رمز نگاری در بسیاری از آن‌ها موجب شده است که اطلاعات بسیار زیادی از طریق آن‌ها افشا شود و می‌توان افشا و یا سرقت اطلاعات از این طریق را به عنوان یکی از معضلات جدی سازمان‌ها و شرکت‌ها در نظر گرفت این چنین پروتکل‌هایی به خوبی برای هکرها و نفوذ گران شناخته شده‌اند و لذا فقط ضعف مناسبی برای انجام حملات اکتیو و پسیو هستند.

پروتکل‌های قدیمی

به طور غیر قابل باوری پروتکل‌هایی چون «r» Unix همچنان به فزونی در بسیاری از محیط‌های رایانه ای دیده می‌شوند و البته تستفاده هم می‌شوند. اسناد آمو زشی زیادی برای گذر از این پروتوکل‌ها برای سالیان متمادی است که تولید شده‌اند و به وفور در اینترنت یافت می‌شوند و متاسفانه اغلب وجود چنین ابزارهایی در نظر گرفته نمی‌شوند و سازمانهایی که همچنان از این ابزارها استفاده می‌کنند می‌بایست تجدید نظر جدی به سیاست‌های ارتقا امنیت رایانه ای خود داشته باشند.

قواعد شبکه که به اشتباه تنظیم شده‌اند

ابزارهای مدیریت دسترسی در شبکه مثل روترها و دیواره‌های آتش معمولا هم به طور ناصحیح به کار گرفته می‌شوند و به طور ناصحیح تنظیم می‌شوند. حتی در گاهی مواقع بسیاری از سازمان‌ها به خاطر صرفه جویی در هزینه‌ها عمدتا از ابزار های نا مناسبی در شبکه‌های خود استفاده می‌کنند که گاهی اوقات نبود این چنین ابزارهایی بهتر از بودن آن‌هاست چرا که هکرها به خوبی از نقطه ضعف این نوع ابزارها مطلع‌اند و مسئله زمانی بحرانی‌تر می‌شود که بسیاری از سازمان‌ها همین ابزارها را نیز با تنظیمات پیش فرض و حتی در غلط در شبکه و زیر ساخت‌های رایانه ای خود به کار می‌گیرند که این نکته نیز به شدت در ضعف امنیتی آن‌ها تاثیر گذار است.

مسئله انجام تنظیمات صحیح به خصوص تعیین قوانین دسترسی در این نوع ابزارها به حدی با اهمیت است که در صورت انجام ندادن آن‌ها عملا این ابزارها به ابزارهایی بی‌مصرف بدل خواهند شد و در واقع وجود آن‌ها دروازه ورود و امنی را برای حملات ویروس‌ها، کرم‌ها و سایر بدافزارها فراهم می‌کند.

ببرهای کاغذی

مسئله بعدی که در مورد به کارگیری ابزارهای امنیتی بسیار حائز اهمیت است این است که ابزارهای سخت‌افزار و نرم‌افزاری که در سازمان‌ها به قصد ارتقاء وضعیت امنیتی نصب می‌شوند معمولا متناسب نوع تهدید و یا نقطه ضعفی که سازمان دارد تنظیم نمی‌شوند و به صورت معمول یک سری تنظیمات که در همه شبکه‌ها صورت می‌گیرد در نهایت در آن‌ها نیز اعمال می‌شود. به این پدیده اصطلاحا Paper Tiger می‌گویند.

مثال‌های زیادی از این دست را می‌توان به عنوان نمونه‌های بارز مد نظر Paper Tiger در سال ۲۰۱۱ در نظر گرفت که یکی از آن‌ها استفاده از فایروال‌های Host – Based به جای تفکیک شبکه به صورت واقعی است. مسئله مواردی شبکه نیز از دیگر مواردی است که اغلب به آن کم توجه می‌شود، بسیاری از سازمان‌ها از یک معماری تخت و بزرگ به سبب ارزان بودن آن‌ها استفاده می‌کنند در صورتی که نوع معماری شبکه بستگی زیادی به ساختار فیزیکی و موضوعی سازمان دارد.

آمار اسکن آسیب پذیری‌ها

در این بخش نتایج حاصله از تحلیل‌های صورت گرفته روی ۲ میلیون اسکن انجام شده را بررسی خواهیم کرد.

گواهی‌هـای پیش فـرض

بسیاری از دستگاه‌ها و ابزارها با همان کلمات عبور و نام کاربری پیش فرض و معمولا با کلیه امکانات دسترسی به بخش‌های مختلف به کار گرفته می‌شوند. این کلمات عبور پیش فرض هم معمولا تغییر نمی‌کنند و برای سال‌ها به همان حال باقی می‌مانند و همین مسئله به هکرها و تبهکاران سایبری این اجازه را می‌دهند تا بتوانند تنها با سواستفاده از این ضعف امنیتی به خود ابزار مورد نظر دسترسی داشته باشند بلکه از طریق آن بتوانند به سایر ابزارها و سیستم‌هایی که به یک شبکه متصل هستند نیز دسترسی پیدا کنند.

۲۸% درصد Apache Tomcat نصب شده با گواهینامه‌های پیش فرض

۱۰% درصد JBoss نصب شده با گواهینامه‌های پیش فرض

۹% درصد phpMyAdmin نصب شده با گواهینامه‌های پیش فرض که دو درصد از آن‌ها کلا هیچ احراز هویتی نیاز ندارند

۲% درصد ابزارهای سیسکوی نصب شده با گواهینامه‌های پیش فرض

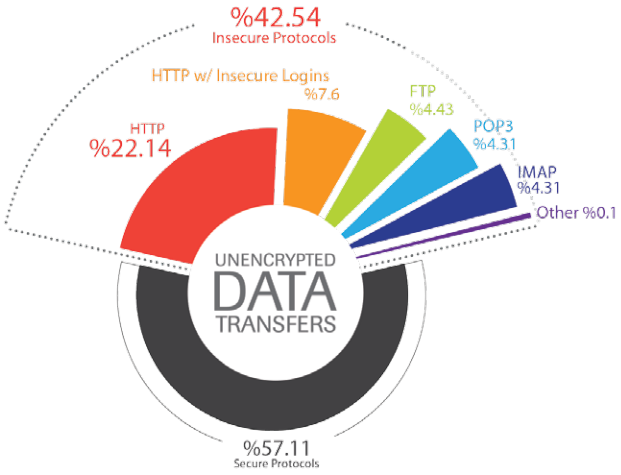
متاسفانه در بسیاری از موارد در بررسی‌هایی که ما روی ابزارها و دستگاه‌هایی که به طور معمول در تمام شبکه‌های بزرگ به کار برده می‌شوند به این نتیجه رسیده‌ایم که واقعا تعداد کثیری از این دستگاه‌ها با همان تنظیمات پیش فرض به حال خود رها شده‌اند.

به طور خاص در مورد PHPmy Admiy مواردی از این دست بسیار دیده می‌شوند. مواردی که به راحتی این امکان را به هکر داده است تا از طریق آن به اطلاعات موجود در سرور دسترسی پیدا کند.

انتقال داده‌ها به صورت رمزنگاری نشده

اگر چه پروتکل‌های رمزنگاری برای انتقال صفحات وب، ایمیل‌ها و صوت و تصویر و حتی انواع فایل‌ها بیش از یک دهه است که وجود دارند اما آنچنان که باید نتوانسته‌اند بر روند ارتقاء امنیت در این دوره در این موارد تاثیرگذار باشند. می‌توان گفت که هنوز بیشتر کاربران از پروتکل‌های غیر ایمن برای انتقال اطلاعات خود در شبکه اینترنت استفاده می‌کنند.

بیش از یک چهارم خدمات مبتنی بر HTTP توسط Trust ware Spider labs بررسی شده‌اند و متاسفانه حتی بسیاری از صفحات وب که در آن‌ها باید کاربر لاگین کند یعنی کلمه عبور و نام کاربری را وارد کند از پروتکل‌های غیر ایمن برای انتقال اطلاعات استفاده می‌کنند.



دسترسی به شبکه‌ها

۱۰%

بررسی‌های TrustKeeper نشان می‌دهد که ده درصد از ارتباطات اینترنتی می توانند به پایگاه داده داخلی دسترسی داشته باشند و ۵درصد از آن‌ها از MySQL استفاده می‌کنند

۳%

بررسی‌های TrustKeeper نشان می‌دهد که سه درصد سیستم‌ها

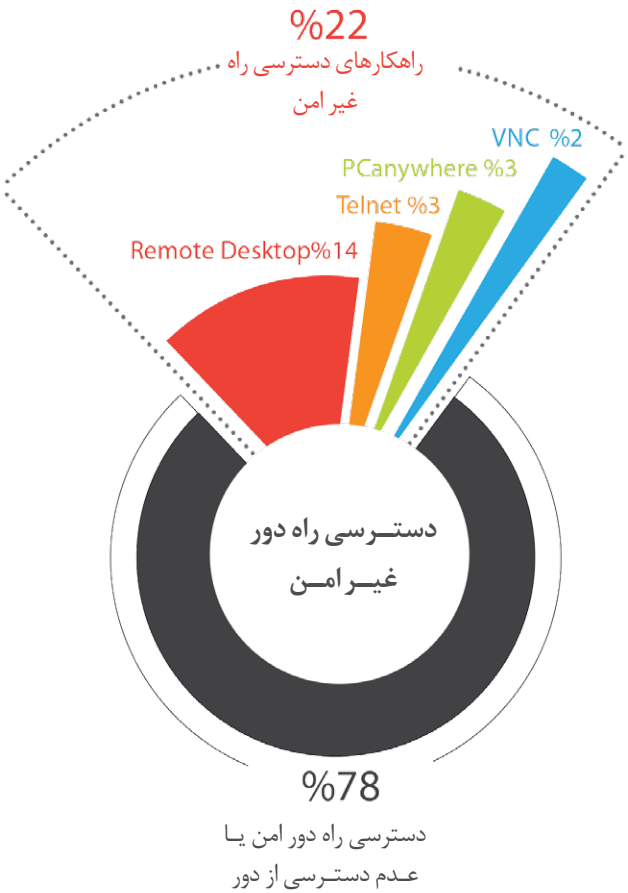
بررسی‌های دیگری که توسط Trust Keepe صورت گرفته است بیانگر این مطلب است که تعداد قابل توجهی از سازمان‌ها از خدمات شبکه ایمنی استفاده نمی‌کنند. این خدمات، خدماتی چون سرورهای دیتا به یس و خدمات شبکه ویندوز را شامل می‌شوند. عموما، اما این ضعف امنیت به سبب کمبود دانش فنی در سازمان‌ها و یا راهنمایی‌های نادرست و گمراه کننده برای انجام تنظیمات دیواره آتش خود مزید علت بر افشای اطلاعات سازمان‌ها توسط هکرها شده است.

دیتابیس سرورها به خصوص My SQL یکی از بزرگ‌ترین قربانیان حملات هکری بوده است و بسیاری از اطلاعات سرقت شده از وبسایت‌ها و سرورهایی صورت گرفته است که بانک اطلاعاتی آن‌ها My SQL بوده است.

و البته توجه نکردن به مسئله ضعف امنیتی این چنین سیستم‌هایی می‌تواند حتی باعث شود که هکرها بتوانند به سیستم‌هایی که دارای رمزهای عبور پیش فرض هم نیستند به راحتی نفوذ کنند چرا که راهکارهای دیگری جهت نفوذ پیش پای آنان قرار می‌گیرد.

دسترسی از راه دور غیر امن

علیرغم وجود گسترده ارتباطات امن در بستر VPN همچنان ۲۲% از سازمان‌ها از بسترهای غیر امن برای دسترسی از راه دور استفاده می‌کنند و طبیعتا این حجم گسترده از ارتباطات که در بسترهای غیر ایمن استفاده می‌شوند می‌توانند مشکلاتی را به طور بالقوه ایجاد کنند که از جمله مهم‌ترین آن‌ها لورفتن کاکات عبور و نام‌های کاربری و سایر اطلاعات بعلاوه نرم‌افزارها و سخت‌افزارهایی که امکان دسترسی مستقیم به یک رایانه یا دستگاه را فراهم می‌کنند به هکرها این امکان را می‌دهند تا بتوانند حملاتی بهتر و موفق‌تر را صورت دهند و به شدت ریسک عدم موفقیت حملات را کاهش می‌دهند.



۱۰ ریســک مهـــم

۱.کلمه عبور ضعیف و حتی نبــود کلمه عبور برای حساب‌های کاربــری ادمین

بسیاری اوقات برای سیستم‌های یونیکس و ویندوز از کلمات عبور قابل حدس استفاده می‌شوند و البته در بسیاری دیگر از مواقع حتی کلمه عبوری هم تنظیم نمی‌شود.

۲.انتقــال اطلاعــات حســاس

انتقال اطلاعات حساس در بستر بدون رمزنگاری مثل CHD و PII یا SSN در سیستم‌های فاقد رمزنگاری در شبکه‌های داخلی جابجا می‌شوند.

۳.کلمــه عبــور ضعیــف

کلمه عبور ضعیف و حتی نبود کلمه عبور برای MS SQL Server تنظیم کلمه عبور ضعیف و حتی گاهی مواقع نبود کلمه عبور یکی از مهم‌ترین راه‌های نفوذ در SQL است.

۴.ARP: Adress Resolution Protocol Cache Poison

حمله به ARP یک نوع OSI Layer۲ طبقه بندی می‌شوند.
یک پیام بی‌جهت ARP به یک یا چند رایانه در یک شبکه ارسال می‌شوند که در حالی از تغییر آدرس‌های Mac است و این پیام عموما شامل بدافزارها و یا تشویق به انجام فرآیندی است که هکر منتظر است تا شما آن را انجام دهید.

۵.Wireless Clients Probe for ESSID from stored Profile when not connected

یک حمله Karma زمانی اتفاق می‌افتد که یک نفوذگر یک AP بی سیم را آغاز کند و...

۶.Continued Use of Wired Equivalent Privacy (WEP) Encryption

Wep پروتکلی که برای رمزنگاری انتقال دیتا در بستر JEI 802.11 است. بسته‌هـای اطلاعـات در این پروتکـل به صـورت RC4 و تحت یـک کلید اصلی مشتـرک بین کلیه ایستگاه‌هـای رادیویی رمزنگاری می‌شوند. اما این تحلیل‌های مختلف روی این پروتکل مشخص کرد که این پروتکل به طور کلی دارای نقص است و می‌توان از آن سوء استفاده‌های فراوانی کرد.

۷- Client Sends LAN Manager (LM)

Response for NTLM Authentication
مکانیزم‌های مختلفی وجود دارند که با استفاده از آن‌ها می‌توان یک Client را فریب داد تا اطلاعات تایید هویت خود را به جهت دسترسی یک بدافزار به سرور یا سایر ابزارهای موجود در شبکه لوداد.

حملات DNS یا DHCP که توسط لینک‌های توکار در صفحات وب صورت می‌گیرند می‌توانند بسیار موثر باشند. چرا که اگر کاربری که به آن حمله شده است از قضا خود ادمین شبکه باشد اتفاقاتی خواهد افتاد که هیچ به مذاق مدیر شرکت خوش نخواهد آمد چرا که دسترسی‌های بی حد و حصری برای حمله کننده ایجاد می‌شود که دسترسی به رایانه و ابزارهای داخلی شبکه و دامنه‌ها و اعتبارنامه‌ها و گواهینامه‌های امنیتی ادمین تنها بخشی از آن چیزی خواهد بود که هکر به آن‌ها دست خواهد یافت.

۸.Misconfigured Firewall Rules Permit Access to Internet Resources

بر اساس پیچیدگی که در نحوه کنترل و دسترسی‌ها در دیواره آتش وجود داشته باشد انجام تنظیمات ناصحیح و حتی رها کردن تنظیمات پیش فرض به حال خود می‌تواند راه ورود هکرها به شبکه را آسان کند.

۹.Storage of sensitive Information Outside the Designated secured Zone

اطلاعات حساسی که در محل‌هایی غیر امن و بدتر از آن رمزنگاری نشده نگهداری می‌شوند بسیار در خطر هستند.

۱۰.Sensitive Information Transmitted over Bluetooth

در سال ۲۰۱۱ رشد بی سابقه ای در تولید و فروش ابزارهای دارای سیستم‌های بلوتوث رخ داد که متعاقب آن بسیاری از افراد بسیاری از اطلاعات حساس خود را از طریق آن جابجا کردند که در این میان هکرهای زیادی از این فرصت سوء استفاده کردند.

تهدیدهای جدید و حملاتی که در هر روز ظهور می‌کنند همچنان یکی از مهم‌ترین دغدغه‌های کارشناسان بخش‌های امنیتی شرکت‌ها و سازمان‌ها است در حالیکه همچنان توجه کافی به تهدیدات و حملات قبلی و قدیمی‌تر ندارند.

موارد زیادی در تست‌های نفوذ و اسکن‌های آسیب‌پذیری هستند که به خوبی شناخته شده‌اند و از ۱۰ سال پیش تا الآن و حتی قبل‌تر از آن از زمانیکه نخستین شبکه‌های رایانه‌ای بوجود آمدند همچنان به عنوان معضل وجود دارند به خوبی مسئله آن‌ها رفع نشده است و هکرها و نفوذگران نیز به خوبی از این مسئله مطلع هستند. گاه حملات خوبی را با استفاده از همین ضعف‌های امنیتی ساده انجام می‌دهد:

بدیهی است که آسیب پذیری‌هایی که در گذشته تا حال وجود داشته‌اند به راحتی و بدون نیاز به ابزارهای سخت‌افزاری و نرم‌افزاری پیچیده قابل استفاده هستند و همه این‌ها در حالی است که همین ابزارهای

سخت‌افزاری و نرم‌افزاری که آن‌ها برای انجام حملات سوء استفاده از آسیب پذیری ها استفاده می‌شوند.

همزمان با پیشرفت فناوری بسیار پیشرفت کرده‌اند.
لذا توجه به آسیب پذیری ها و تهدیدات امنیتی قدیمی بسیار مهم است.

چه چیزی در صندوق ایمیل‌های ما هست؟
روند ایمیل‌ها در سال ۲۰۱۱

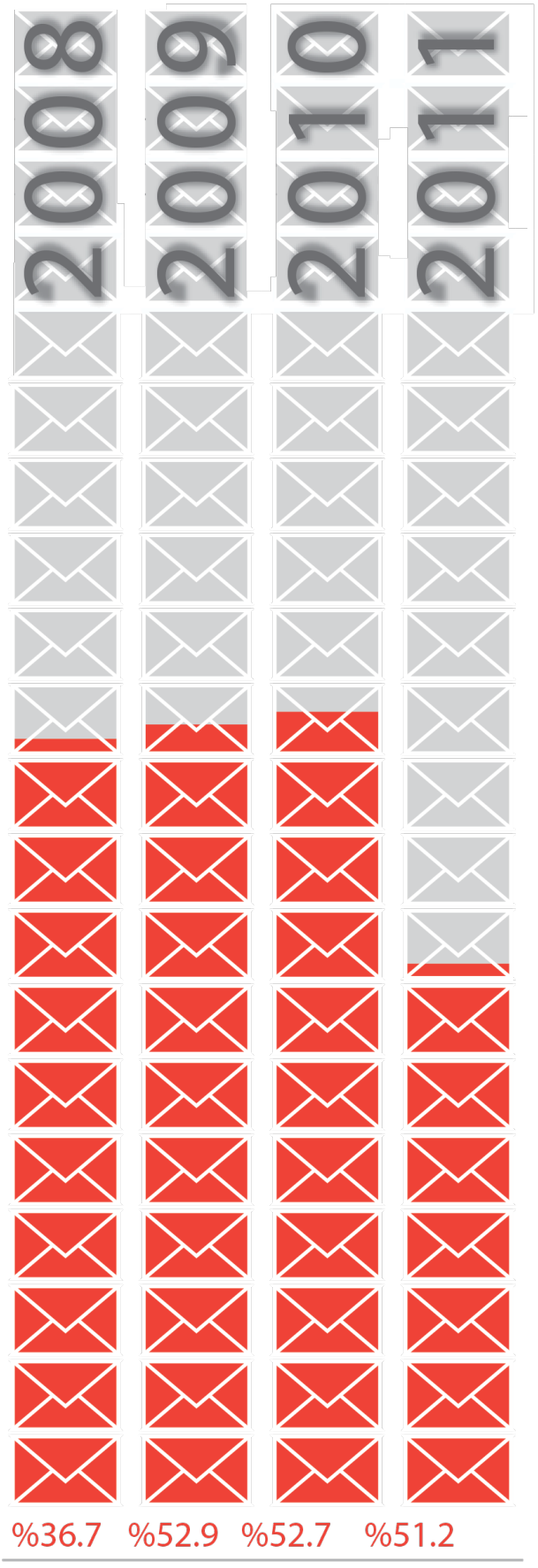
می‌توان اوج ارسال هرزنامه و اسپم را سال ۲۰۰۸ دانست و بعد از آن بود که در صد ارسال ایمیل‌های صحیح و مناسب به آرامی رو به رشد گذاشت اگرچه ارسال اسپم و هرزنامه روندی کاهشی را دنبال کرد اما روند ارسال ایمیل‌هایی که حاوی ویروس و بدافزار بودند هرسال نسبت به سال گذشته دوبرابر شدند. اگر جه در حال حاضر تعداد کل ایمیل‌هایی از این دست تنها حدود ۱% از کل ایمیل‌های ارسالی را شامل می‌شود.

همچنین نکته جالب اینکه هکر و نفوذگران تمایل زیادی به ارسال این دست ایمیل‌ها در بین ساعت ۸ تا ۹ صبح دارند. با توجه به روندی که در سال ۲۰۱۰ مشاهده کردیم در سال این دست ایمیل‌ها به جای اینکه به صورت انبوه صورت بگیرد به صورت محدود و مختص کاربرانی خاص ارائه می‌شود.

آمار ایمیل‌ها:

آمارهایی که از بررسی بیش از ۴ میلیارد ایمیل به دست آمده است، بسیار قابل توجه است. در صد ایمیل‌هایی که به عنوان اسپم و هرزنامه توسط نرم افزارهای امنیتی در نظر گرفته می‌شدند به طور قابل توجهی از ۵۰% به عدد ۳۷,۷ % در سال ۲۰۱۱ کنترل پیدا کرده است.

می‌توان گفت که یکی از مهم‌ترین دلایلی که موجب این کاهش چشمگیر در مقدار ارسال هرزنامه ها بود بکارگیری روش‌های مبتنی بر متدولوژی Real Time Black list (RBL) بود که از اواخر سال ۲۰۱۰ اجرایی شد. این لیست به طور پیش فرض دارای لیست بی شماری از آدرس سرورهای ارسال کننده ایمیل‌های اسپم و هرز است. به طور مرتب نیز به روز می‌شود.



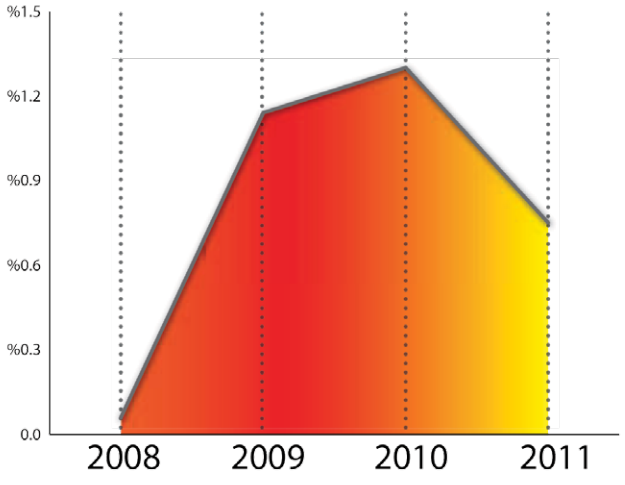
موضوع در هرزنامه‌ها

می‌توان به طور کلی عمده ایمیل‌های هرزنامه را (حدود ۸۳% کل) را به ۲ قسمت عمده طبقه بندی کرد: قرص‌های دارویی و هرزه نگاری
اما باقی این ایمیل‌ها را می‌توان به گروه های متعددی تقسیم کرد که به طور مثال Fake Watch(۴%)، Datiny (۱%)و ... از جمله آن‌ها هستند.
لیست کامل آن‌ها را در نمودار زیر می‌بینید.

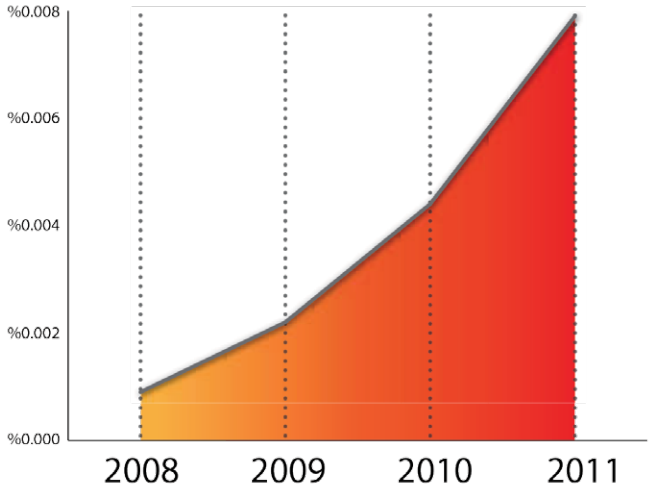
دسته‌بندی موضوع هرزنامه‌ها

فایل‌های خطرناک

جلوگیری از ارسال فایل‌های اجرایی توسط ایمیل مسئله ای بوده که در سال ۲۰۰۸ اجرایی شد. جلوگیری از ارسال فایل‌های مخرب که طبیعتا بیشترین طیف آن فایل‌های اجرایی (.exe) بودند توانست کمک شایانی به ارتقاء سطح امنیت ایمیل‌ها کند چرا که بسیاری از تروجان‌ها و کرم‌ها از این طریق اقدام به تکثیر خود می‌کردند و نهایت پس از ۳ سال از انجام این کار تعداد کل ایمیل‌هایی که به این صورت آلوده می‌شدند به یک چهارم مقدار اولیه کاهش پیدا کرد و پس از پیش بینی‌های آتی نیز از روند نزولی این امر در سال‌های حکایت دارد.



درصد ویروس‌های کشف شده



درصد ضمایم اجرا شدنی

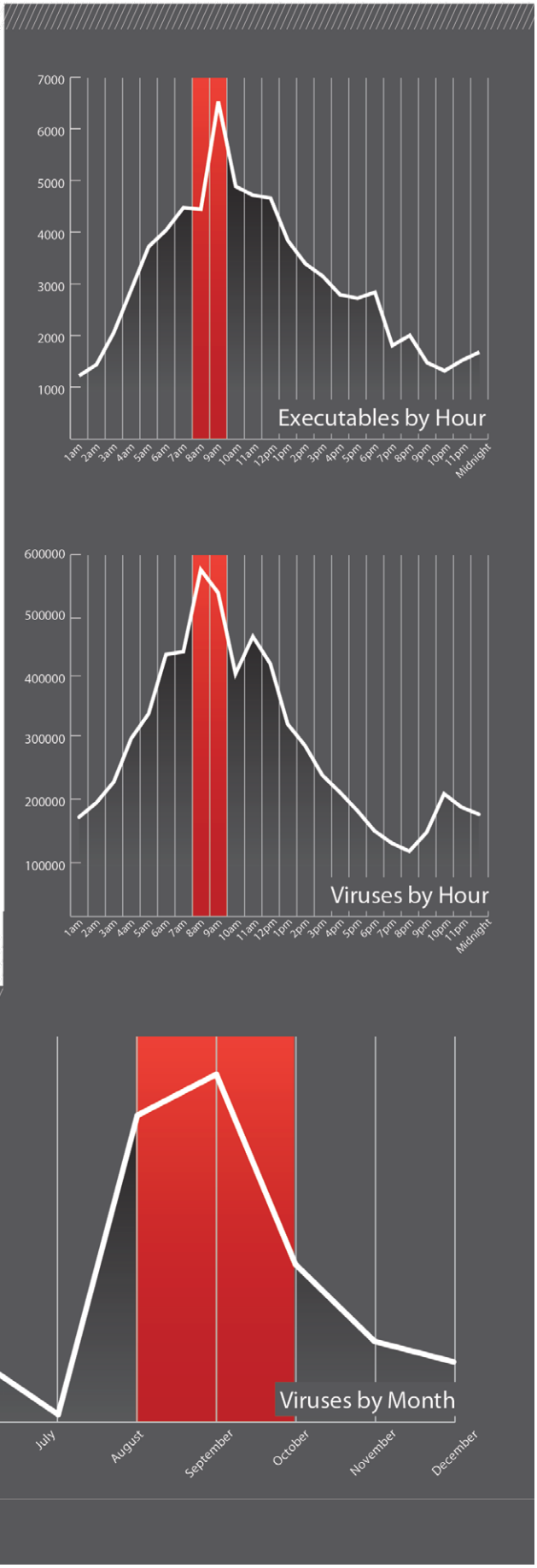
تحلیـل زمـانی

تحلیل‌هایی که به صورت ساعتی، ماهیانه و سالانه در نمودارهای زیر ارائه شده است نتایج بسیار جالبی را به دست می‌دهد.

تعداد فایل‌های اجرایی مخرب و ویروس‌هایی که در ابتدای صبح ارسال می‌شوند رشد زیادی یافته است و اوج این ارسال بین ساعت ۸ تا ۹ صبح صورت می‌گیرد؛ و این بدان منزله استا که هکرها و نفوذ گرها در تلاشند تا کار برانی که بلافاصله و در اول وقت اداری ایمیل‌های خود را چک می‌کنند را آلوده کنند. در فاصله بین ماههای آگوست تا ابتدای اکتبر چیزی در حدود ۳% از کل ایمیل‌ها حاوی فایل‌های مخرب و اجرایی و یا ویروس بوده‌اند.

به طور کلی بر اساس روندهای گذشته چیزی در حدود شش ماه طول می‌کشد تا بتوان ابزارهای شناسایی این فایل‌ها را به طور کلی در همه محیط‌های نرم افزاری نصب و به کار برد که اگر این روند همچنان پابرجا باشد باید منتظر اعلام کشف شدن تعداد بیشماری بدافزار جدید در مارس ۲۰۱۲ باشیم.
امروزه البته ایمیل‌ها همچنان جذاب‌ترین ابزار نشر بدافزارها هستند و هکرهای بسیاری از ایمیل برای انتشار ابزارهای خود استفاده می‌کنند.

با توجه به ارزیابی های PEW Internet در سال ۲۰۱۱ حدود ۹۳% از افرادی که از جستجوی اینترنتی به عنوان یک ابزار جذاب و پر طرفدار استفاده می‌کنند به همان میزان نیز از ایمیل‌ها و خدمات مربوط به آن استفاده می‌کنند و همین مسئله نیز سبب شده تا هکرها از محبوبیت این سرویس اینترنتی کمال سوء استفاده را انجام دهند و نه تنها محب. وبیت آن بلکه طبیعت دینامیک آن نیز مسئله دیگری است که هکرها را به آن بسیار علاقمند کرده است.



وب- تحلیل چند عامل از تکنیک‌های حمله مدرن

چه چیزی هکرها را تحریک می‌کند تا ابزارهای وبی را هک کنند؟ از چه روش‌هایی استفاده می‌کنند؟ از چه نوع آسیب‌پذیری‌هایی استفاده می‌کنند؟

سازمان‌ها به شدت مشغول پیدا کردن پاسخ این سوالات حیاتی هستند پروژه‌های متعددی در حفره امنیت ابزارهای وبی در حال اجرا ست که در حال یافتن آسیب‌پذیری‌های رایجی هستند که هکرها از آن‌ها برای حمله به بسیاری از ابزارهای وبی استفاده می‌کنند که از جمله آن‌ها می‌توان به برنامه CRE و Buy Trag اشاره کرد.

اما به طور کلی می‌توان در خصوص عوامل موثر بر افزایش ریسک هک شدن به معادله زیر دست یافت :

ریسک - تهدیـد ❋ آسیب‌پذیـری ❋ Impact

به هر صورت تحقیقات ادامه دارد، تحقیقاتی که سعی دارد با بدست آوردن انواع اطلاعات به کارشناسان کمک کند تا متوجه شوند که عموما سازمان‌هایی که مورد حمله قرار می‌گیرند به چه فعالیتی مشغول هستند، عوامل محرک اصلی که در پشت ماجرای هک کردن و حمله سایبری به سازمان‌هاست چیست؟

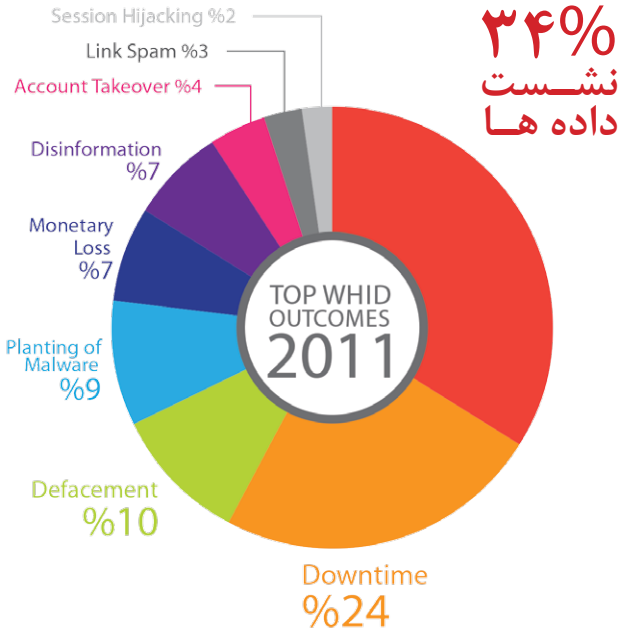
به طور مثال WHID : Web hacking Incidents Database پروژه‌ای است که بدست آوردن لیستی از آسیب‌پذیری ابزارهای وبی که به نحوی مورد توجه هکرها بوده است می‌پردازد. پروژه WHID در وهله اول به عنوان ابزاری برای ارتقاء آگاهی کاربران و برنامه نویسان در خصوص آسیب‌پذیری ابزارهای وبی و در مرحله بعدی با استفاده از آمار و ارقامی که جمع آوری می‌کند و تحمیل آن‌ها به ارائه ابزارها و خدماتی در خصوص ارتقاء امنیت ابزارهای وبی خواهد پرداخت. این برنامه بر خلاف سایر برنامه‌های پایش امنیت ابزارهای وب که تمرکز ویژه‌ای روی موارد فنی دارند بیشتر به تاثیر حملات و سوء استفاده‌ها از این ابزارها که منجر به خسارت‌های فراوانی شده‌اند می‌پردازد.

آمارهای WHID در سال ۲۰۱۱

به طور کلی با توجه به اطلاعات بدست آمده از سوی آمار و ارقام که توسط این برنامه ارائه شده است می‌توان کل حملاتی که به بدافزارهای وبی صورت گرفته است را به دو گروه تقسیم کرد: گروه اول که با هدف کسب سود صورت گرفته و گروه دوم که با هدف‌های ایدئولوژی و اعتقادی انجام گرفته است.

نفوذ به قصد درآمدزایی

هکرهای حرفه‌ای به شدت به دنبال توسعه روش‌های جدید و پیچیده‌تری برای کسب درآمد از طریق سوءاستفاده از صنف‌های امنیتی ابزارهـای وبی هستند و آمار بالای افشای اطلاعات حساس کاربران از طریق سایت‌هـای تجارت الکترونیک خود مزید این مطلب است و ماجرا زمانی حساس‌تـر می‌شـود که هکرهـا این اطلاعـات را در بازارهـای سیـاه به سـایرینی کـه



می‌توانند سوءاستفاده‌های فراوانی از آن‌ها کنند به فروش می‌رسانند. سرقت پولی که در ۷% از کل حملات رخ داده است نتیجه عمده روش‌های بهینه شده برای انجام تراکنش‌های مالی فریبنده است که کاربر در واقع فکر می‌کند که به درستی در حال انجام آن‌هاست. در صورتی که نمی‌داند در زمین هک بازی می‌کنند و به راحتی اطلاعات حساس بانکی خود را به هکر می‌دهند از جمله مهم‌ترین بدافزارهایی که همچنان می‌توان بدان‌ها اشاره کرد SPY eye و Zeus هستند که مشغول پایش کاربر می‌مانند و به محض اینکه کاربر وارد سایتی برای انجام عملیات بانکی و یا پرداخت اینترنتی شد اطلاعات حساس وی را به سرقت می‌برند.

نفـوذ بـا اهـداف ایدئولـوژیک

هکتیویست‌های ایدئولوژیک از اینترنت برای رساندن پیامهای خویش استفاده می‌کنند و به طور کلی از ۲ روش عمل می‌کنند که اولی عبارتند از، از دسترس خارج کردن سایت‌ها (۲۴%) و تغییر شکل صفحات (۱۰%) درست مشابه نافرمانی‌های اجتماعی که در دنیای واقعی صورت می‌گیرد، مثل جنبش اشغال وال استریت، گروه‌های هکری آنلاین نیز با هدفهای اعتقادی به ایجاد اخلال در فرآیندهای تجاری می‌پردازند. اما همانطور که از نظر گذشت در کنار از دسترس خارج کردن وبسایت‌ها مسئله مهم دیگری که هکتیویست‌ها به دنبال آن هستند ایجاد تغییر شکل در وبسایت است.

مسئله انجام تغییر شکل مسئله‌ای بسیار جدی در خصوص استفاده از آسیب‌پذیری‌های ابزارهای وبی است.

البته الازم به ذکر است که تغییر شکل در رابط کاربری وبسایت‌ها، مسئله‌ای بود که تا همین اواخر چندان به آن توجهی نمی‌شد. اما مسئله نگران کننده اینجاست که در واقع همچنان حفره‌های امنیتی و آسیب‌پذیری‌هایی که از مدت‌ها قبل هکرها برای انجام تغییر شکل در وبسایت‌ها از آن استفاده می‌کردند همچنان وجود دارند و در واقع

عمده روش‌هایی که نفوذگران از آن‌ها برای هک و تغییر شکل وبسایت‌ها استفاده می‌کنند روش‌هایی بسیار ساده هستند که از سال‌ها پیش نیز مورد استفاده قرار می‌گرفتند و همچنان نیز جذابیت خود را از دست نداده‌اند. چرا که اصلاحات زیر ساختی در بخش توسعه ابزارهای وب صورت نگرفته بود، اما مسئله آنجا اهمیت پیدا می‌کند که شاید هکرها اقدامی به تغییر شکل وبسایتها نکنند و ظاهر اولیه آن را حفظ کنند ولی درون کدهای آن بدافزارها و لینک‌های مخرب خود را قرار دهند. اینجاست که بدون آنکه صاحب سایت و کاربر قربانی از چیزی خبر داشته باشند بسیاری از اعمال خرابکارانه صورت می‌گیرد.

جالب است بدانید عمدتا سایت‌هایی با مضامین سیاسی و خبری هدف اینچنین حملاتی قرار می‌گیرند.

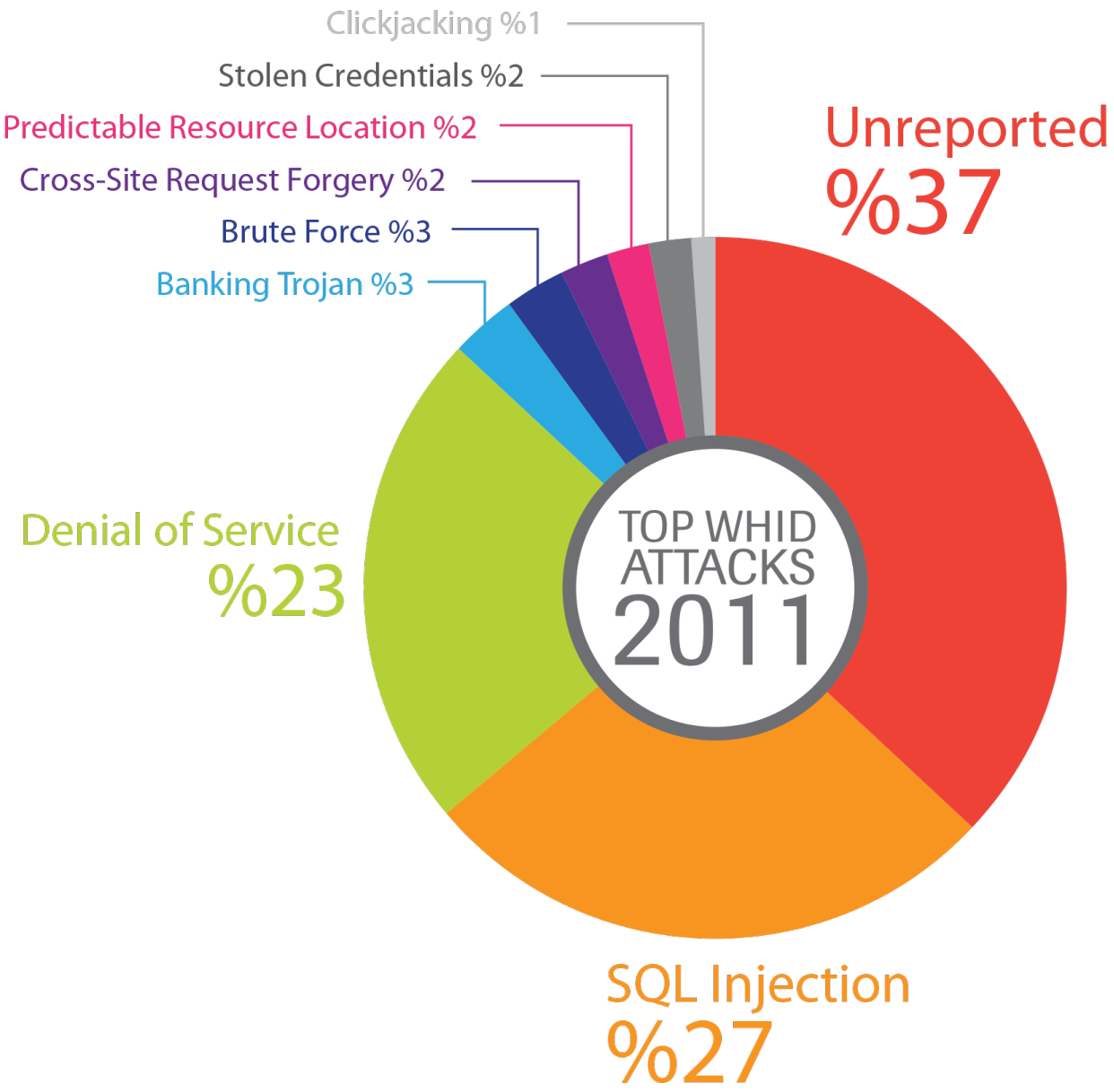
تحلیل روش‌های حمله

یکی از پرخطرترین اتفاقاتی که در زمینه هک وبسایت‌ها می‌تواند رخ دهد این است که وبسایت به نحوی هک شود اما صاحب آن متوجه این اتفاق نشده باشد.

باید گفت که ۳۷% از کل وبسایت‌های هک شده‌ای که ما آن‌ها را مطالعه کرده‌ایم چنین وضعی داشته‌اند.

Insufficient logging

سازمان‌هایی که به درستی اقدام به انجام تنظیمات امنیتی لازم در خصوص زیر ساخت‌های وبی خود نکرده‌اند و سامانه‌ها پایش و ردیابی قابل اطمینانی به جهت نظارت دقیق از نحوه ورود و خروج کاربران ندارند عمدتا هدف شماره یک اینچنین حملاتی هستند.



بررسی دقیق‌تر اینک HTTP و توسعه صحیح و به هنگام دیواره آتش می‌تواند یکی از بهترین راه‌ها در مقابله با اینچنین حملاتی باشند.

Public Disclosure Resistance

بسیاری از سازمان‌هایی که به نحوی هدف حمله سایبـری قرار می‌گیرند از اینکه این مسئله عمومی شود بسیار هراس دارند و شـاید یکی از دلایلی که اطلاعات کمی بعد از افشـای حملات سایبری به برخی از سازمان‌هـا منتشر می‌شود نیز موید این مطلب باشد چرا که به زعم آن‌ها نیز افشـای این چنین حملاتی می‌توان به شدت بر اعتمـاد مشتریان نسبت به کارآیـی سازمان آن‌هـا تاثیر گذار باشد و در بسیـاری از موارد همین مسئله مـانع بدست آوردن اطلاعـات صحیح و در نتیجه ایجاد راه‌حل‌هـایی مناسب می‌شوند و این‌هـا همه در حالـی است که در اغلـی این اتفاقـات همه تلاش‌ها متوجه چگونگی حذف و پاک کردن بدافـزار زیر ساخت‌هـای وبی می‌شوند و تقریبا در همه موارد هیچ تلاشی در جهت شناسـایی راه نفوذ این بدافزارها به این زیر ساخت‌هـا و رفع حفره امنیتی که هکـر با استفـاده از آن توانسته است بدافـزار خود را در این زیر ساخت‌هـا قرار دهد صورت می‌پذیرد و بنابـراین بدیهی است که مدتی بعد سازمان مجددا از همـان حفره امنیتی برطرف نشده مورد حمله قرار می‌گیرد.

Bypass Network Security

روش‌هـای زیادی برای خـارج از دسترس کردن ابزارهـای وبی از طـریق اشباع پهنـای بانـد سرور وجـود دارد که معمولا از طریق ارسال‌هـای انبوه برای دسترسی به وب صورت می‌گیـرد که موجب افـزایش بی‌انـدازه استفـاده از پهنای بانـد و همچنین استفـاده از ظرفیت پردازشـی سرور می‌شوند و پس از آنکـه مقـدار این درخواست‌هـا از حد معینی فراتـر رفت سرور قـادر به پاسخگـویی به حملات نخواهد بود و طبیعتـا وبسـایت از دسترس خـارج می‌شود و همیـن مسئله ساده نیز عمدتـا برای ارتقـای امنیت زیـرسـاخت‌هـای وبی در نظـر گرفتـه نمی‌شوند و با تنظیمـات خـاص دفـاعی در مقـابل این حملات در سامانه‌هـای امنیتی سرورهـا نمی‌بینیم.

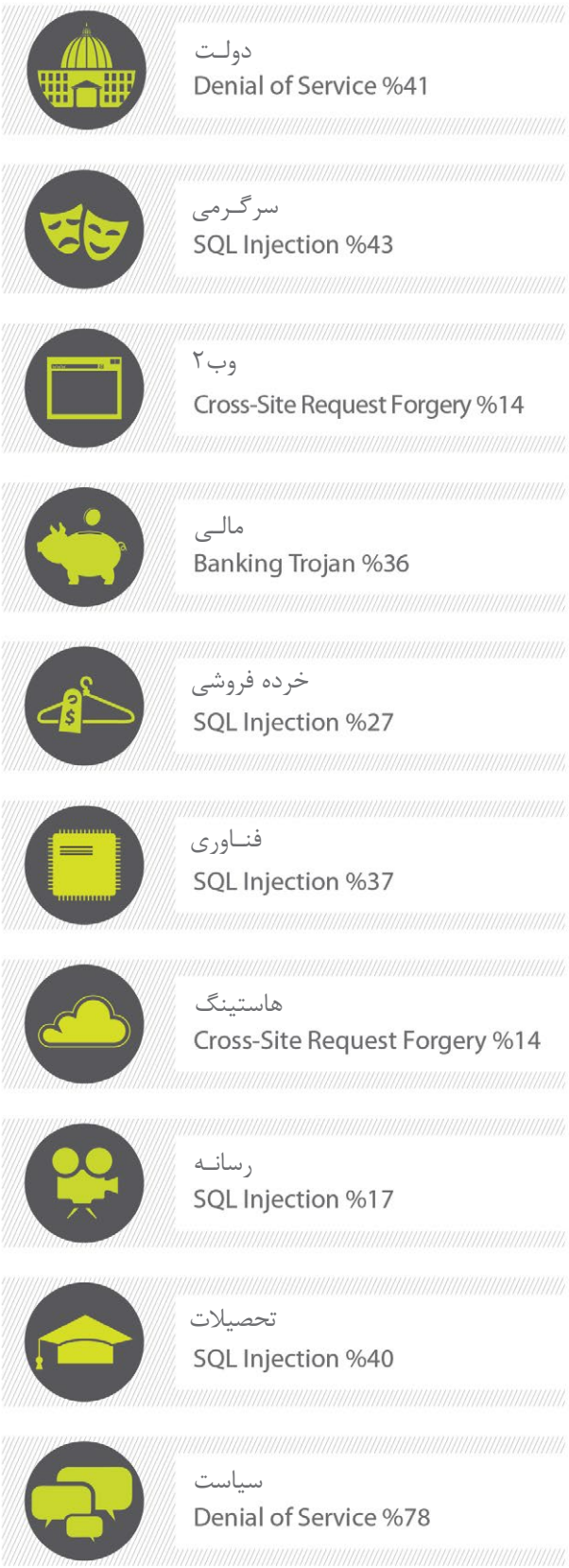
Often Excluded From Application Penetration Testing

به سبب بسیاری از دلایل نظر آگاهی کم مدیران عالـی و میـانی و همچنین هزینه بر بودن و حتی نبود ابزارهای لازم عمدتـا تستهـای نفـوذ به صورت اثر بخشی در مورد ابزارهـا و زیرساخت‌هـای وبی سازمان‌هـا صورت نمی‌گیـرد مسئلـه‌ای که می‌توانـد تا حـد بسیار زیـادی در ارتقـاء سطح این سازمان‌ها در مقابلـه با حملات سایبری اثـرگذار باشد.

تحلیل روش‌هـای حمله بر اساس حوزه‌هـای کاری

اما جمع بندی و نتیجه گیـری نهـایی که می‌توان از اطلاعـات بدست آمـده صورت داد این است که در حال حاضر بیشتر روش‌هـای هک و نفوذ به وبسایت‌هـا از طریق از دسترس خارج کردن وبسایت‌ها و همچنین نفوذ به SQL صورت می‌گیرد.

حملات مهـم به تفکیک حوزه‌هـای کاری



در دنیـای موبـایل

متاسفانه اغلب مدیران ابزارهایی چون گوشی‌های هوشمند و تبلت‌ها را به عنوان یک پی سی کوچک در نظر می‌گیرند و کتاسفانه این پیش فرض غلط باعث بروز مشکلات امنیتی فراوانی در طول سالیان گذشته در سازمان‌ها شده است اگر نگوییم همه این ابزارها ولی بیشتر آن‌ها محصولاتی در درجه مصرف کننده هستند منظور از ابزارهایی در درجه مصرف کننده ابزارهایی هست که عمدتا با ۳ رویکرد عمده تولید شده‌اند:

۱- جذب بیشترین طیف کاربران
۲- راحتی در کاربری
۳- قابلیت اجرای برنامه های سرگرمی و چند رسانه ای

و متاسفانه با رشد سرسام آور این ابزارها، مسئله امنیت آن‌ها از رشد چندانی برخوردار نبوده است و روند حملات به این ابزارها مدتی است که آغاز شده و روند پیش بینی‌ها از سرعت رشد این حملات حکایت دارد و یک رویکرد پیش فعال در خصوص ارتقاء امنیت سخت‌افزاری و نرم‌افزاری این ابزارها می‌تواند از بسیاری از آسیب‌هایی که در آینده می‌توانند بسیار دردو ساز باشند جلوگیری کنند.

ذکر این نکته ضروری است که نفوذ بدافزارهای همراه نه تنها می‌تواند خرابکاری‌های معمولی که در پی سی‌ها انجام می‌شود را صورت دهد بلکه به عدد ابزارهای جدید و پیشرفته ای نظیر دوربین‌ها، GPS و... می‌توانند اطلاعاتی بسیار با ارزشمندتر و جذاب‌تر از ابزار همراه کاربر به سرقت ببرند. سیستم عامل آندرویید به سبب گسترش روزافزون خود امروزه به یکی از محبوب‌ترین پلتفرم‌ها برای تولید و انتشار بدافزار تبدیل شده است و متاسفانه امنیت آن نیز به موازات توسعه استفاده و به کارگیری از آن چندان توسعه نیافته است.

همگرایی موبایل برای تروجان‌هـای بانکی

در سال ۲۰۱۱ نسخه موبایل بدافزارهای مخصوص سرقت اطلاعات بانکی رشد روزافزونی پیدا کرد. در همین سال بود که سورس کد اصلی بدافزار مشهور Zeus منتشر شد و احتمالا ترکیب این کدها با کدهای بدافزار مشهور دیگری به نام SPY Ware توانست منجر به پدیده‌ای مخرب شود که روی هر دو پلتفرم Android و ZiPhone نصب شود و اطلاعات مربوط به تراکنش‌های مالی TAN:Mobile Transaction Authentication صدها هزار کاربر در سر تا سر دنیا به راحتی سرقت کنند. خدمات و ابزارهای جدیدی نیز که در حوزه پرداخت الکترونیک از طریق ابزارهای همراه ایجاد شده‌اند (مثل کیف پول مجازی، NFC و...) هم حوزه های جذابی را برای کاربران و البته هکرها و نفوذ گران فراهم کرده‌اند.

باید گفت که اتفاقات و حملاتی که در سال ۲۰۱۱ در حوزه پرداخت الکترونیک از طریق ابزارهای موبایل انجام شد با رویکرد مهندسی اجتماعی پی گرفته شده در این رویکرد دو خبری از اجبار کاربر به دانلود برنامه خاص و یا ارسال کرم به ابزار همراه او نیست و کاربر خود با اختیار خود اطلاعات را در اختیار بدافزار قرار می‌دهد.

بدافزارهـای مستقل از مکـان

اپراتورهای تلفن همراه از این پس در رهگیری ابزارهای همراهی که هریک از کاربران به طور رند از آن‌ها استفاده می‌کنند تنها نیستند چرا که بدافزارها در ردیابی کاربران از طریق سامانه های GPS و جمع‌آوری اطلاعات مکانی کاربران با آن‌ها همراه شده‌اند. البته با وجود اینکه قصد اصلی هکرها و نفوذگران از جمع‌آوری اطلاعات مکانی افراد مشخص نیست اما می‌توان تصور کرد که آن‌ها سرانجام می‌توانند راهی را پیدا کنند که این اطلاعات را ارزشمند کنند.

برای مثال اطلاعات به سرقت رفته کارت‌های پرداخت در یک حوزه محلی می‌توانند به شدت برای فریب سامانه‌های کشف تقلب فر آیند پرداخت کاربرد داشته باشند. در ماه‌های گذشته هر دو سیستم عامل آندرویید و IOS از لحاظ سوءاستفاده به لحاظ جمع آوری اطلاعات مکانی افراد آسیب پذیری‌های جدی از خود بروز داده‌اند.

بدافزارهـای جدید و تمرکـز بر اندرویـد

البته روند رو به توسعه‌ای که در حال حاضر برای تولید بدافزارها تحت پلتفرم آندروید در حال اتفاق است چندان هم دور از انتظار و عجیب نیست. آندروید بیش از ۵۷% بازار تلفن‌های همراه را به خود اختصاص داده است همچنین قابلیت نصب App از طریق فروشنده‌های دیگر در سیستم عامل اندروید نیز از دیگر ویژگی‌هایی است که آن را برای هکرها جذاب کرده است.

اپل اما در این میان با داشتن سیستم بسته خود توانست تا حدی امن‌تر جلوه کند اما به عدد جیل برک (Jail Break) امروزه به راحتی هر نوع App که تحت سیستم‌های عامل اپل قابلیت اجرا داشته باشند در انواع ابزارهای اپل قابل نصب است و تنها پیزی که باید انتظار برآورده شدن آن را داشت رشد چشمگیر بدافزارهای مبتنی بر سیستم عامل اپل است و با اینکه IOS خود سهم کوچک ۱۸% خود از بازار را حفظ کرده است اما باز هم تعداد زیادی از ابزارها در همین بازار ۱۸% وجود دارند که می‌توانند جذابیت‌های بی‌اندازه‌ای برای هکرها داشته باشند.

اما امنیت بازارهای همراه با چالش‌های دیگری در جبهه های دیگر نیز روبروست. در حالی که تطبیق پذیری و هماهنگ شدن این ابزارها با سایر ابزارها هر روز سریع‌تر و راحت‌تر انجام می‌شود، هکرها نیز نقشه‌های فراوانی برای استفاده از این فعل و انفعالات در سر می‌پرورانند.

همچنین رشد ذخیره اطلاعات حساس در ابزارهای موبایل نیز چالش دیگری است که امنیت این دستگاه‌ها با آن روبروست.

همزمان بدافزارهای قدیمی نیز برای استفاده بهینه از ابزارهای موبایل بروزرسانی شده‌اند تا بتوانند حداکثر استفاده را از ابزارها و امکانات جدید انجام دهند و به نظر می‌رسد در حال حاضر تولید کنندگان ابزارهای سخت‌افزاری و نرم‌افزاری بهتر است به جای رقابت صرف برای کسب درصد بیشتری از بازار بر سر توسعه امنیت و ابزارهای کاربردی‌تر به رقابت بپردازند. با توجه به جوان بودن این حوزه پیش بینی‌ها از آینده آن بسیار دشوار است اما آنچه که مسلم است سال پیش رو سالی بسیار پر چالش و خبر ساز در حوزه امنیت ابزارهای موبایل خواهد بود.

دفـاع مـا:
چهـار کنتـرل پایـه‌ای

یک سامانه حفاظتی تمام عیار هیچگاه وجود ندارد و نخواهد داشت و نهایت هر چیزی نقص و کاستی‌های مخصوص به خود را خواهد داشت. در جریان شناسایی و تحلیل این نقصان‌ها و به اشتراک گذاری آن‌ها با سایر متخصصین حوزه امنیت خواهد بود که منجر خواهد شد تا بتوان با سرعت بهتری این نقیصه‌ها را برطرف کرد. در این قسمت ۴ نوع مختلف از فرآیندهایی را که می‌توانند از شما در مقابل این نقصان‌ها حفاظت کنند را بررسی خواهیم کرد.

این ۴ مورد عبارتند از کلمات عبور تجاری، رمزنگاری در فرآیند انتقال اطلاعات ضد ویروس‌ها و دیواره‌های آتش.
باید گفت که بر اساس یافته‌های ما این ۴ مورد به ظاهر ساده یا اصلا در زیرساخت‌های سایبری سازمان‌ها وجود ندارد و یا اگر دارد از اساس به درستی به کار گرفته نشده اند.
و این مورد دوم حتی به مراتب خطرناک‌تر از مورد اول است چرا که مدیران با به کارگیری غلط این ابزارها دچار نوعی حس امنیت کاذب می‌شوند و با این فرض بسیاری از موارد امنیتی دیگری را در نظر نخواهند گرفت.

تحلیل رمز عبور تجاری

مسئله کلمه عبور مسئله بسیار مهم و ابتدایی در ارتقاء سطح امنیت است، در این بخش به تحلیل داده‌هایی که از مشتریان Trustware بدست آمده است می‌پردازیم :

خطرات رمز عبور بدون توجه به انتخاب رمز عبور

حتی انتخاب قوی‌ترین کلمات عبور نیز کارساز خواهند بود اگر زیر ساختهای سایبری سازمان نظیر رمز نگاری و مولفه‌های نرم‌افزاری و سخت‌افزاری به درستی ایجاد و اعمال نشده باشد.
این مسئله بسیار مهمی به خصوص توجه به این مسئله است که حتی اگر زیر ساخت‌های فنی سایبری سازمان نیز به بهترین حالت ایجاد و اعمال شده باشند باز هم خطای انسانی و ضعف آگاهی کارمندان و حتی فرهنگ سازمانی می‌تواند به راحتی همه این موارد را پشت سر بگذارد و باعث افشای اطلاعات شود. یکی از رایج‌ترین آسیب‌پذیری‌ها، آسیب پذیری SMBnv 067-MS08 در Microsoft Word 2000 , XP Server2003 , و بعدا در Server2008 / Vista است که به طور ممتد در طول چهار سال باعث می‌شد که هکرها بدونت داشتن کلمه عبور بتوانند به اطلاعات این فایل‌ها دسترسی داشته باشند.

به روز رسانی نرم‌افزارها و نصب وصله‌هایی که برای آن‌ها عرضه می‌شود نیز از اهمیت بالایی برخوردار است. به طور مثال نصب نشدن یک وصله بروز رسانی در سرورهای آپاچی زمینه بروز حملات سایبری به وبسایت‌هایی که روی این سرورها میزبانی می‌شدند صورت گرفت.

مسئله دیگری که انتخاب و وجود کلمات عبور در آن‌ها بسیار با اهمیت است نرم‌افزارهایی هستند که امکان ایجاد دسترسی از راه دور را برای کاربران فراهم می‌کنند. به طور مثال VNC حتی در دو مرحله اقدام به گرفتن کلمه عبور می‌کند اما باز هم وجود یک حفره امنیتی در آن باعث می‌شد تا هکرها به راحتی از وجود و مرحله گرفتن کلمه عبور، عبور کنند و به مقاصد خود دست یابند. چرا که به طور معمول VNC اطلاعات بین دو پی سی را که به هم وصل کرده بود را به صورت رمز نگاری شده منتقل نمی‌کرد و چه بسیار هکرهایی که از این مسئله سوء استفاده کردند.

ضعف در روش‌های رمزنگاری

یکی دیگر از مواردی که به ارتقاء سطح امنیت یک سامانه می‌انجامد نوع رمز نگاری است که توسط آن کلمه عبور رمز نگاری می‌شود. اگر ضعفی در الگوریتم رمز نگاری کلمه عبور وجود داشته باشد در واقع هدیه‌ای را به هکر اهدا کرده‌اید تا به راحتی به واسطه آن بتواند به سیستم حمله کند و در واقع هکر به جای اینکه از کلمه عبور استفاده کند برای دسترسی به متابع سیستم از ضعف موجود در سیستم رمزنگاری استفاده می‌کند.

یکی دیگر از این مثال‌ها استفاده از LM: LAN Manager است که کلمه عبور را مدیریت می‌کند این برنامه به عنوان یکی دیگر از برنامه های بسیار مطرح که از یک الگوریتم افسانه‌ای برای رمزنگاری استفاده می‌کند مطرح بوده و هست و هنوز هم کاربردهای زیادی دارد.

می‌توان گفت که این برنامه در نسخه‌های بعد از Windows NT به طور پیش فرض فعال بود. اما بعدها معلوم شد که این برنامه در کمتر از یک دقیقه هک می‌شود چرا که این برنامه کلیه کلمات عبور را در یک طول ثابت ۱۴ بایتی که خود به ۲ قسمت ۷ بایتی تقسیم می‌شود تبدیل می‌کند و هریک را از طریق الگوریتم DES رمز نگاری می‌کند و در واقع همین دو تکه کردن کلمه عبور که برای ارتقاء امنیت و بهبود فرآیند رمزنگاری انجام می‌شود باعث کاهش بی اندازه رمزنگاری بر آن شد و مسئله تا جایی پیش رفت که مایکروسافت در نهایت این برنامه را در پروژه ویندوز Vista و Server ۲۰۰۸ آن را غیر فعال کند. اما هنوز این برنامه در ویندئزهای XP و ۲۰۰۳ به طور گسترده به کار برده می‌شود. و به طور گسترده نیز این سیستم‌ها مورد سوء استفاده قرار می‌گیرند.

روش‌هـای قدیمـی

نوشتن کلمات عبور در اسناد ادله‌ای ما کاغذهایی که در دسترس همگان است نیز همچنان به شدت شایع است و جالب است بدانید که این مسئله در سازمان‌هایی که قوانین سخت‌گیرانه‌تری در مورد وضع کلمات عبور دارند و کلمات عبور را در بازه های زمانی مشخص می‌بایست تغییر دهند رایج‌تر است. چرا که کلمات عبور کمتر قابل یادآوری است و لـذا کاربران مجبور به یادداشت کـردن آنهـا می‌شوند و به طور میانگین در حدود ۱۵% از سازمان‌ها و بخش‌هـایی که تحت بررسی موارد مربوط به امنیت فیزیکی قرار گرفتند در یک بخشی از محل کار توانستیم کلمـات عبور دست نویس را پیدا کنیم. اما یکی از روش‌های امتحان شده و رایج برای سرقت کلمات عبور نصب Key Logger هـا است. نصب موفقیت‌آمیـز

یک Key Logger حتی می‌تواند از راه دور نیز صورت پذیرد اگر پی سی کاربر به حدی آسیب پریر باشد که به راحتی و از راه دور قابل کنترل باشد.
اما در حال حاضر یکی از روش‌هایی که به شدت مورد توجه هکرهاست استفاده از روش‌های مبتنی بر مهندسی اجتماعی است تا از این طریق بتوانند اطلاعات حساب کاربری افراد را به سرقت ببرند.

در این روش هکرها تمام تلاش خود را برای جلب اطمینان کاربران به صورت کاملا طبیعی متمرکز می‌کنند و به نحوی آن‌ها را قانع می‌کنند تا حساب کاربری و سایر اطلاعات حساس خود را به نحوی پشتیبانی کنند. یکی از رایج‌ترین این موارد حملات فیشینگ است که امروز به عدد وجود شبکه‌های اجتماعی موفقیت‌های بسیار زیادی کسب کرده است.

دام‌های رمز عبور

در پاسخ به اعمال سیاست‌های سخت‌گیرانه که در برخی از سازمان‌ها و شرکت‌ها در خصوص کلمات عبور صورت می‌پذیرد کاربران نیز به راه‌های نو آورانه‌ای برای بی اثر کردن این سیاست‌ها روی آورده‌اند که از آن جمله می‌توان به موارد زیر اشاره کرد:

رمز عبورهای اشتراکی

استفاده از فرم ساده و دم دستی قوانین ایجاد کلمه عبور مثل بزرگ کردن حروف اول آن و یا قراردادن یک علامت تعجب در آن.
مسئله دیگر آن است که معمولا در سازمان‌ها برای کارمندان تازه وارد خود از کلمات عبور ساده مثل Wellcome یا Changeme استفاده می‌کنند و از آنها می‌خواهند که خود آن را تغییر دهند که معمولا مدت زیادی این کلمات عبور بدون تغییر باقی می‌مانند.

Service Account هایی که به طور خودکار ایجاد می‌شوند نیز به طور کلی دارای کلمات عبور ضعیفی هستند که معمولا مدیران IT نیز فراموش می‌کنند آن‌ها را تغییر دهند.

یک مثال بسیار معمول در این رابطه سرورهای مبتنی بر Microsoft SQL هستند که با توجه به ضعف‌های عمده‌ای که در محیط Active Directory سوءاستفاده‌های فراوانی از آن صورت گرفت.

Shared Password

کلمات عبور اشتراکی که به واقع می‌توانند محیط سایبری یک سازمان را فلج کنند این وضعیت بین خدمات و ابزارها بسیار رایج است متاسفانه به طور مثال مدیر IT یک سازمان که با صدها دستگاه کوچک و بزرگ رایانه‌ای سرو کار دارد از یک کلمه عبور یکسان برای نوع خاصی از همه دستگاه‌ها استفاده می‌کند و با این کار زیرساخت سایبری سازمان را در مقابل تهدیدات زیادی قرار می‌دهد. مثال دیگری که در آن معمولا این پدیده دیده می‌شود رمزهای عبوری است که توسط نرم‌افزارهایی که کار آن‌ها بک‌آپ‌گیری است تعیین می‌شوند. از آنجاییکه معمولا تعداد فایل‌های بک‌آپ گرفته شده رو به فزونی می‌رود لذا معمول است که از یک کلمه عبور برای آن‌ها استفاده شود.

نه تنها کلمات عبور اشتراکی که پدیده دیگری به نام حساب‌های اشتراکی نیز می‌توانند به یک باره ضربات جبران ناپذیری را به زیرساخت سایبری سازمان وارد کنند چرا که اگر هکری بتواند تنها یکی از این حساب‌ها را هک کند به ناگاه به کلیه حساب‌های اشتراکی نیز دسترسی خواهند داشت و پس از آن نیز ماجرا معلوم است و جالب‌تر آن است که ابزارهای آماده‌ای برای این کار نیز در دسترس هکرها قرار دارد که از آن جمله می‌توان به Medusu اشاره کرد.

انتخاب رمز عبور ضعیف

معمولا کاربران در انتخاب کلمات عبور چنان خلاقانه عمل نمی‌کنند. به طور مثال انتخاب نام یک تیم محلی ورزشی و یا نام یک فعالیت مهم که در نزدیکی محل زندگی آن‌ها وجود دارد از جمله موارد بسیار شایع است و حتی بسیاری از کلمات عبور بر پایه نام شرکتی که کاربر در آن کار می‌کند ایجاد می‌شوند.

همچنین ایجاد کلمه عبور بسیار با بازه زمانی که کلمه عبور در آن ایجاد شده است مرتبط است و به طور مثال بسیاری از کاربرانی که حتی کلمه عبور خود را به طور منظم تغییر می‌دهند چون در بازه های زمانی ماهانه، فصلی و حتی سالیانه این کار را انجام می‌دهند بنابراین رفتار آن‌ها بسیار قابل پیش بینی خواهد بود و با این پیش‌بینی پذیر بودن چنین رویدادهایی دست هکرها برای هک کردن و بدست آوردن کلمات عبور بسیار بالا خواهد بود.

روش دیگری که کاربران از آن برای ایجاد کلمات عبور متعدد خود استفاده می‌کنند ایجاد کلمات عبور افزایشی است به این صورت که یک کلمه عبور را به عنوان مبنا در نظر می‌گیرند و برای هر حساب کاربری کاراکتری را به آن اضافه می‌کنند که معمولا به صورت اضافه کردن یک عدد در انتهای آن است و با اینکه این روش بسیار هوشمندانه به نظر می‌رسد اما به راحتی توسط هکرها قابل پیش بینی است. مسئله دیگری که مدیران IT باید به آن توجه کنند این است که واقعا منظور از ایجاد یک کلمه عبور قدرتمند و پیچیده چیست؟

این مسئله به خصوص در محیط Active Directory بسیار مورد توجه است چرا که به طور مثال کاربران در این محیط می‌توانند کلمات عبوری را با شرایط گفته شده توسط Active Directory ایجاد کنند. که باید طول آن حداقل ۸ کاراکتر باشد و حداقل شامل ۳ تا از ۵ نوع کاراکتر (حروف کوچک/ حروف بزرگ/ اعداد/ کاراکترهای خاص و Unicode) باشد.
اما با این سیاست‌های به ظاهر سخت‌گیرانه عبارت «Password1» می‌تواند با تطابق کامل با این قوانین به عنوان یک کلمه عبور پیچیده مد نظر باشد.
اما آیا این کلمه عبور یک کلمه عبور پیچیده است؟

پیچیدگی رمز عبور در مقابل طول رمز عبور

کاربران و مدیران آیتی اغلب بر این باورند که پیچیده کردن یک کلمه عبور در ایمن‌تر کردن آن بسیار موثر است. اما ممکن است زمانی که فردی بخواهد یک کلمه عبور خاص را پیدا کند اعمال این سیاست‌ها مانع حدس زدن کلمه عبور شود اما این سیاست در مورد هکرهایی که مسلح به انواع بدافزارهای هک کلمات عبور هستند چندان مناسب نیست.

به طور مثال به برخی موارد از جایگزینی کاراکترها به عنوان عاملی برای ارتقاء امنیت کلمه عبور استفاده می‌شود که در جدول زیر می‌توانید برخی از آن‌ها را ببینید.

کاراکتر جایگزین	کاراکتر اصلی
@ or 4	A
3	E
!	I
5	S

طول رمز عبور

	رمزهای ممکنه
10	5.98737×10^{19}
9	6.30249×10^{17}
8	6.6342×10^{15}
7	69,833,729,609,375
6	735,091,890,625
5	7,737,809,375
4	81,450,625
3	857,375
2	9025
1	95

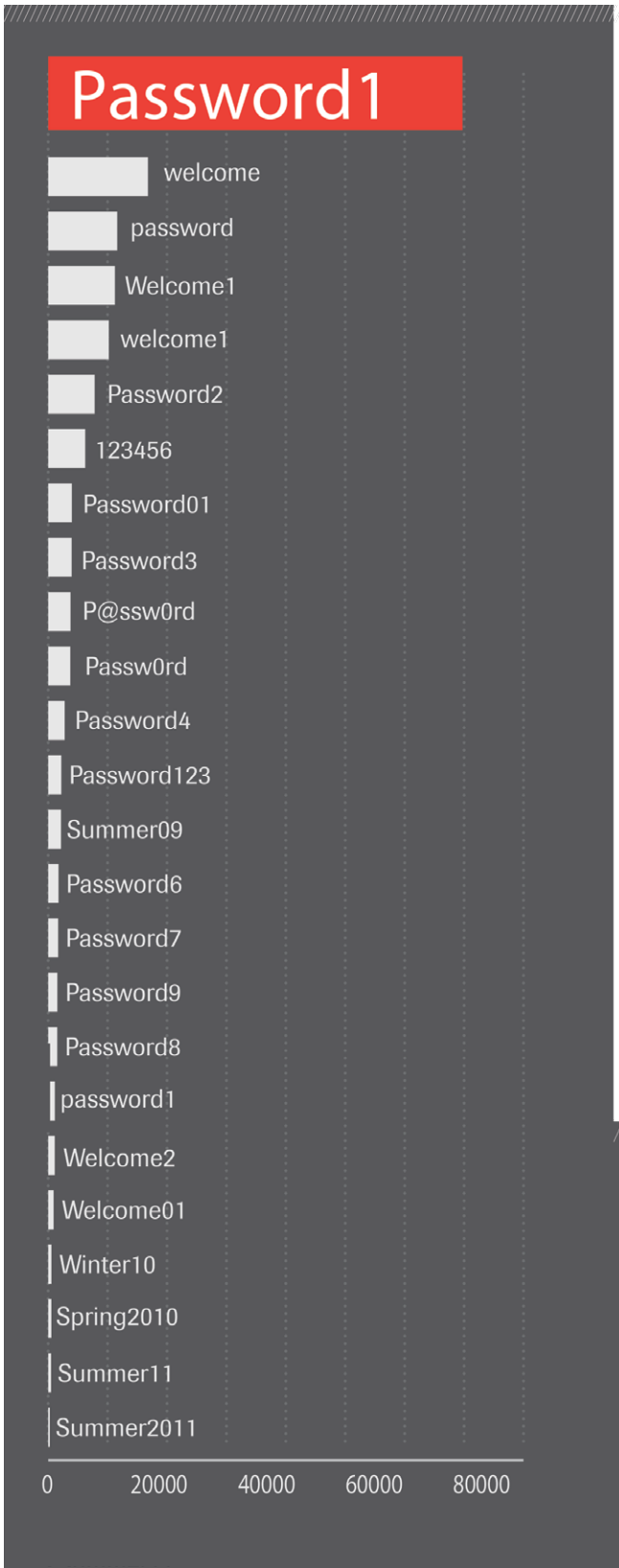
این روش البته شاید تا چندی پیش روش مناسبی بوده است اما در حال حاضر در فرهنگ لغت کلمات عبور قابل حدس بسیاری از هکرها این موارد لحاظ شده است و شاید بتوان گفت که به سادگی با افزایش طول کلمه عبور بتوان به طور موثری امنیت آن را ارتقا داد. چرا که هر کارکتری که طول کلمه عبور اضافه می‌شود سختی حدس زدن آن را چنانچه در جدول زیر می‌بینید به طور نمایی افزایش خواهد داد.

اما با روش‌های هک کلمه عبور آشنا شوید:

۱. فرآیند هک کلمه عبور با حمله LM ها صورت می‌گیرد.

۲. استفاده ازویژگی بازیابی کلمات عبور در Crypt haze Multiforc وی با استفاده از لیست کاملی از کلمات عبور رایج.

۳. استفاده از ابزار رایگان دیگری به نام act Hash cat-Plus که از محبوبیت فراوانی هم برخوردار است و توسط Hashcat Suite عرضه شده است



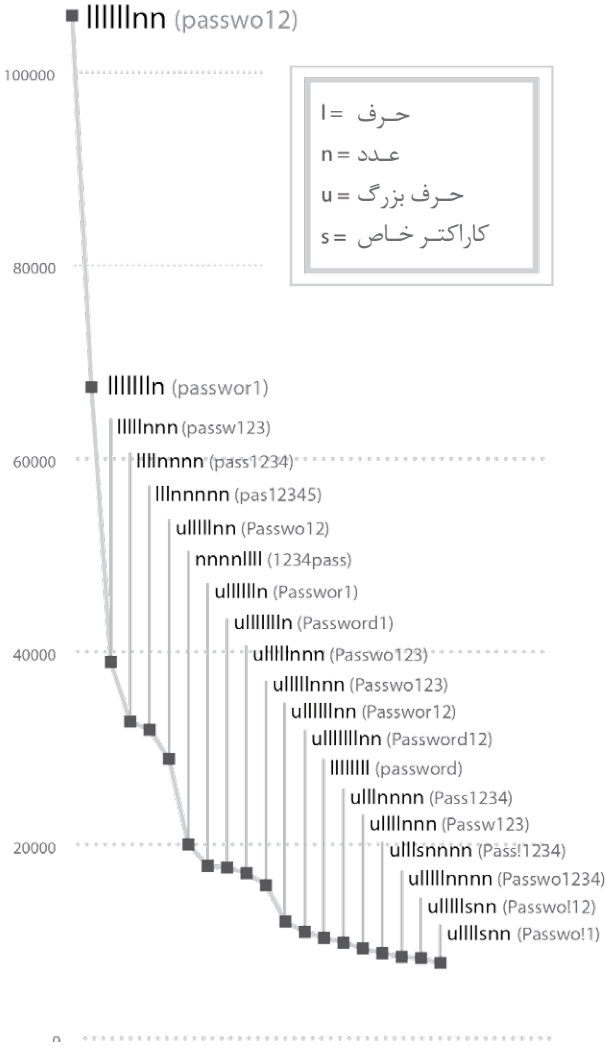
۲۵ رمزعبـور متـداول

این فهرست بر اساس داده‌های جمع‌آوری شده از صنایع مختلف تنظیم شده است.

۵درصد افراد از حالت‌هـای مختلف Password استفـاده می‌کننـد و ۱/۳ درصد هم از welcome در برخـی نرم‌افزارهـا استفـاده می‌کنند.

۲۰ توالی مورد استفاده

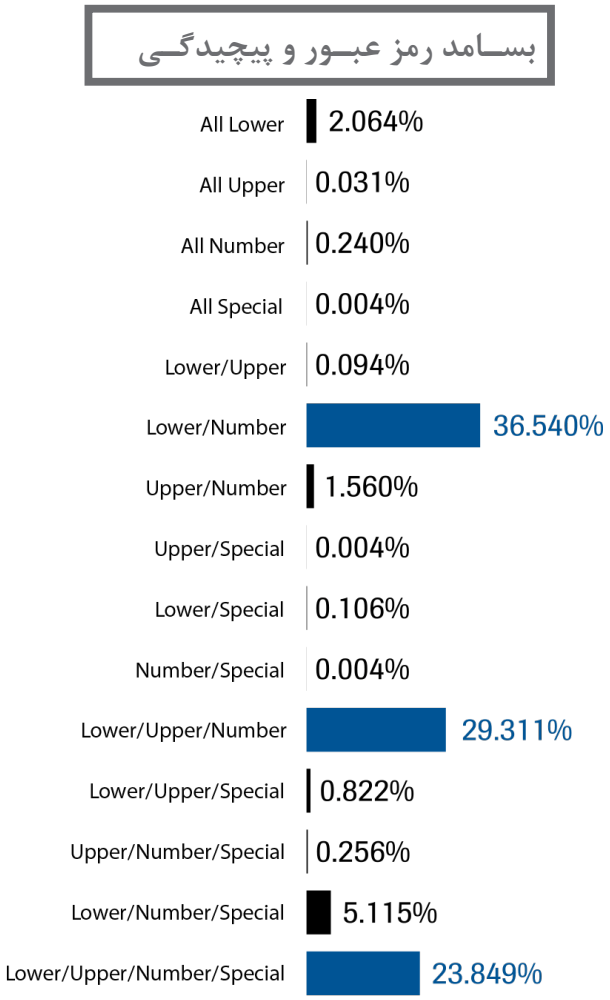
کلمات عبور را می‌توان با شیوه دیگری که به نام تکرار حروف مشهور است پیچیده تر کرد. در مثال زیر عمده تکرارهایی که در کلمات عبور تحلیل شده‌اند را بر حسب L (حروف الفبا)، N(عدد) و کاراکترهای خاص می‌توانید ببینید.



طبق آنچه که در نمودار بالا دیده می‌شود بیشترین حالت تکرار در ترکیب ۶ حرف و ۲ عدد خود را نشان می‌دهد و در مرحله بعدی ترکیب ۷ حرف و ۱ عدد جزء رایج‌ترین ترکیبات است و به طور کلی این یکی از نتایج قابل انتظاری است که مربوط به ایجاد کلمات عبور در محیط Active Directory است چرا که سیاست‌های ایجاد کلمه عبور در این محیط و همچنین ساده بودن کلمات عبور به جهت یادآوری باعث شده است که این چنین کلمات عبوری ایجاد شود و نکته قابل توجه این است که کلیه این ترکیب‌ها توسط روال‌های پایه ای پیش بینی کلمه عبور قابل حدس زدن هستند و همچنین نکته دیگری مه در این نمودار می‌توان به آن اشاره کرد این است که تنها از مرحله شانزدهم به پایین است که در ترکیب‌های تحلیل شده می‌توان اثری از به کارگیری کاراکترهای خاص را پیدا کرد و این مسئله بیانگر آن است که کاربران چندان از این کاراکترها در کلمات عبور خود استفاده نمی‌کنند.

پیچیدگی رمز عبور

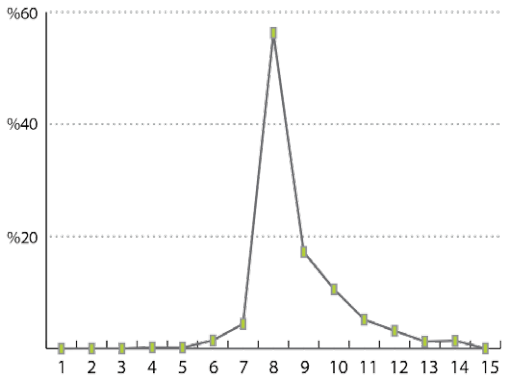
در این بخش هم از جنبه دیگری به ترکیب‌های به کار گرفته شده در کلمات عبور پرداخت شده است که نتایج آن جالب توجه است.



طول رمز عبور

در مثال زیر طول رایج کلمه عبوررا می‌توانید ببینید

و همانطور هم که در نموداردیده می‌شود یکی از رایج‌ترین طول‌ها، طول هشت کاراکتری است که باز هم دلیل آن تاثیرات سیاست‌های انتخاب کلمه عبور در Active Directory است.



استفاده در کلمات کلیدی

در جدول زیر می‌توانید برخی از کلیدواژه‌های جدول معروف را بیابید. با

ماه‌ها	27,191 passwords used English spelling of months (January – December)
ایالت‌های آمریکا	72,389 passwords used U.S. States (Illinois, California)
فصل‌ها	74,368 passwords used seasons (spring, fall)
اسامی کودکان	170,013 passwords used names in the “top 100 male and female baby names of 2011” list.

این توضیح که این طبقه بندی گاهی اوقات شامل نام تیم‌های ورزشی محلی، اسامی مشهور در یک شهر و اطلاعات مرتبط با نوع سازمانی که در یک شهر خاص است، می‌گردد.

معانی

معمولا زمانی که قوانین برای تامین امنیت اعمال می‌شود کاربران از پایین‌ترین رده آن‌ها برای رهایی از تکلیف‌هایی که به آن‌ها اعمال می‌شود استفاده می‌کنند. برای مثال تنظیمات پیش فرض در محیط Active Directory موارد زیر را پیشنهاد می‌دهند:

- کلمه عبور باید حتما حداقل ۶ کاراکتر باشد.
- کاراکترهای کلمه عبور باید ۳ تا از ۵ ویژگی زیر را داشته باشد:
  - حروف بزرگ انگلیسی A – Z
  - حروف کوچک انگلیسی (a-z)
  - رقم‌های ۰ تا ۹
  - کاراکترهای خاص مثل (!,@,#,%)
  - یونی کدها
- کلمه عبور نباید شامل ۳ یا تعداد بیشتری از کاراکترهایی که در نام کاربری وجود دارند، باشد.

و همانطور که قبلا گفته شد در نهایت با اعمال همه این سیاست‌ها کلمه عبور«Password1» به عنوان یک انتخاب وحشتناک از سوی سیستم به عنوان یک کلمه عبور پیچیده و مناسب در نظر گرفته می‌شود.

اما نکته دیگری که باید به آن توجه کرد این است که حتی در برخی دیگر از سازمان‌ها برای اینکه امنیت کلمه عبور بالاتر هم باشد سیاست‌های مالی برای تغییر منظم این کلمات در بازه‌های زمانی اعمال می‌شود که از آنجاییکه کاربران تمایل زیادی به استفاده از همان کلمات عبور قبلی دارند چرا که یادآوری آن اساسا راحت‌تر است نهایتا کلمه عبور فوق را به «Password2» تغییر می‌دهند.

توصیه‌ها

نخستین راهکارهایی که می‌توان برای ارتقاء امنیت کلمات عبور در نظر گرفت پایان دادن به ضعف‌های امنیتی فناوری قدیمی است که هنوز بر مبنای آن‌ها این کلمات تولید می‌شوند.

در خصوص Windows AD به نظر می‌رسد استفاده از برنامه‌هایی چون LAN Manager برای ذخیره کردن کلمات عبور لازم باشد و همچنین در راس همه موارد استفاده از روش‌های رمزنگاری برای جلوگیری از جملات امتحان کلمه عبور می‌تواند بسیار راهگشا باشد. باید گفت که این موارد بسیاری از سیستم‌های مبتنی بر Unix رعایت شده است اما در مورد ویندوز به یک برنامه ثالثی برای آن‌ها نیاز خواهید داشت.

اما هیچ راهکاری بدون آموزش کارمندان و ارتقاء سطح آگاهی آن‌ها اثر بخش نخواهد بود. باید کارمندان و کاربران را تشویق کرد تا آنجا که می‌توانند موارد امنیتی و سیاست‌های مرتبط با آنان را نادیده بگیرند.
و این مهم در مورد آن دسته از کاربرانی که در سطح مدیریت فعالیت می‌کنند بسیار مهم‌تر است.

کاربران باید به چه مواردی در هنگام انتخاب کلمه عبور توجه کنند؟

در حال حاضر باید در پاسخ به این سوال گفت که امروزه باید کلمه عبور را به عنوان یک عبارت در نظر گرفت نه کلمه عبور مثلا «This is my password No really is» یک نمونه مناسب از یک عبارت است که حدس زدن آن به مراتب دشوارتر از یک کلمه است.

مسئله دیگر در انتخاب عبارت عبور به جای کلمه عبور این است که حتی یادآوری آن نیز به مراتب راحت‌تر از یادآوری یک کلمه است و با وجود پیچیدگی اما در ذهن جا می‌گیرند. البته باید گفت که ایجاد یک سامانه امنیتی مناسب که دارای حداقل‌هایی از سیاست‌های درست انتخاب کلمه عبور و تنظیمات صحیح زیر ساخت‌های نرم‌افزاری و سخت‌افزاری باشد همچنان راه زیادی در پیش دارد.

ضد ویــروس:
فیــل در اتـــاق

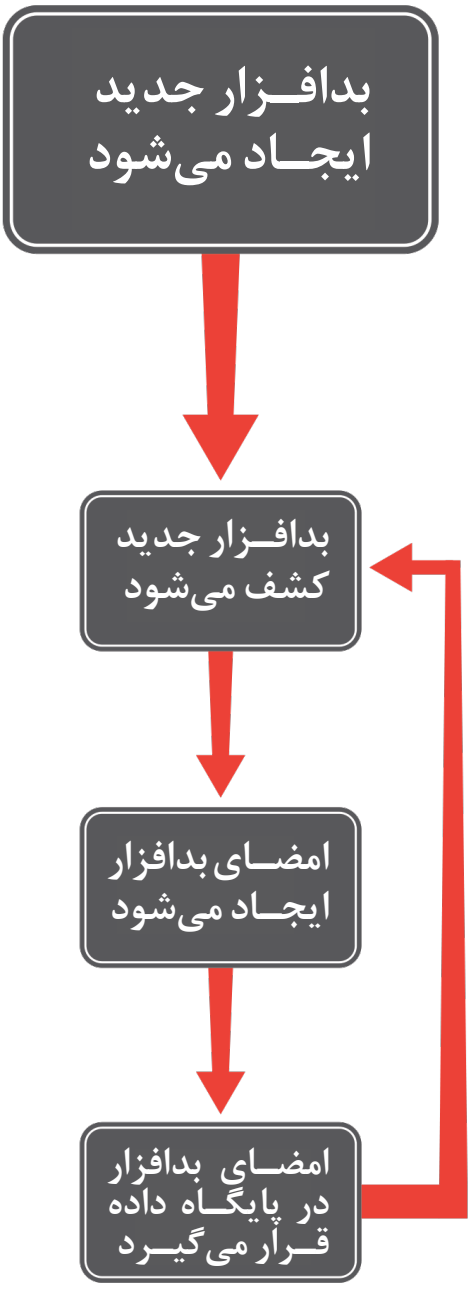
جمله‌ای که قبول آن سخت است ولی واقعیت دارد: ما از آنتی‌ویروس استفاده می‌کنیم، اما هنوز امنیت نداریم. باید گفت که برداشت‌های منسوخ از واژه آنتی ویروس و گاهی مواقع عدم آگاهی از همه قابلیت‌های آن در موارد پیداکردن و از بین بردن بدافزارها موجب شده است که هکرهای زیادی حتی روی سامانه‌هایی که آنتی‌ویروس روی آن‌ها نصب شده است به همه مقاصد پلید خود دست یابند. رویکرد پذیرفته شده‌ای که در حال حاضر در این صنعت وجود دارد که زمانی که یک بدافزار کشف می‌شود یک شانه برای آن در بانک اطلاعاتی این نرم‌افزارها ایجاد شود تا با کمک آن بتوانند در آینده و در سایر سیستم‌ها به راحتی این بدافزارها را کشف کنند.

فرآیند ایجاد نشانه با مشخص کردن یک بدافزار جدید که اطلاعات آن از طرق مختلفی چون تحقیقات سازنده آنتی‌ویروس، گزارش‌های کاربران و... به دست سازندگان آنتی‌ویروس رسیده است شروع می‌شود. بعد از آن شانه ایجاد می‌شود و از همه مشتریان خواسته می‌شود تا بلافاصله نرم‌افزار خود را بروز کنند.

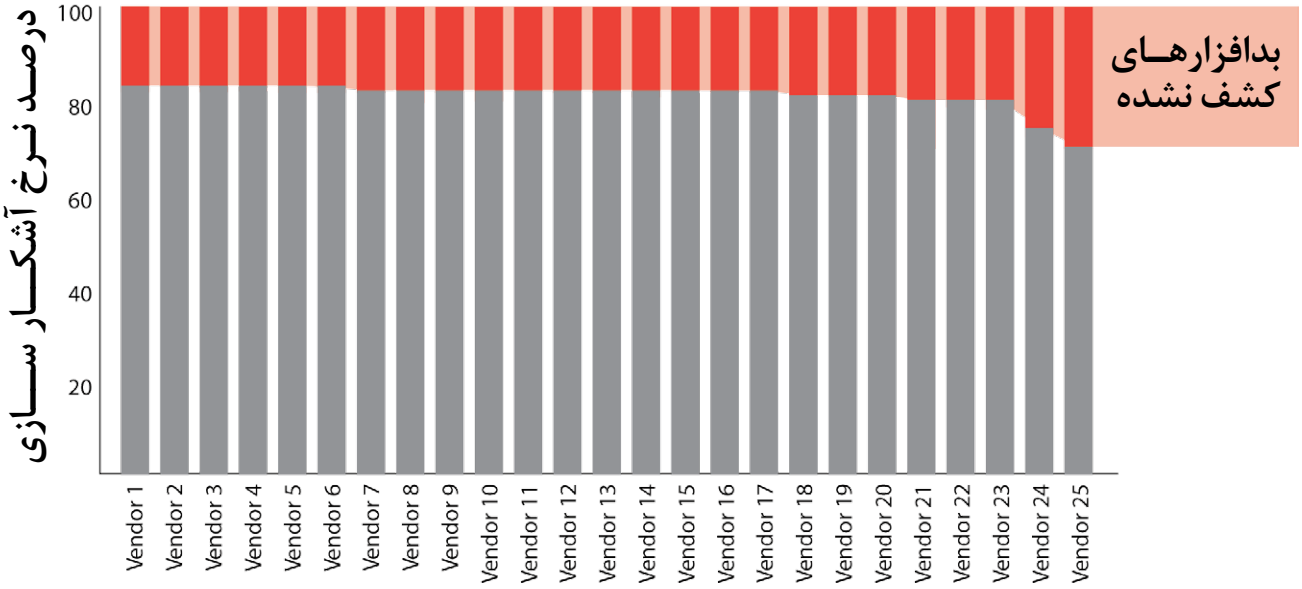
اما برای اینکه این شانه‌ها همواره و در هر حالتـی بتواننـد اطلاعات صحیح را به آنتی‌ویروس منتقل کنند می‌بـایست دارای حداقلـی از استانداردهـا باشنـد و به طور مثال اگر به شـانه‌ای که بسیـار رایج و عمومی است استفاده شود آنگاه قطعا کشف بدافـزار با اطمینان مورد قبولی صورت نخواهد گرفت و یا اینکه ممکن است به اشتباه یک بدافـزار دیگر تلقی شود. از سوی دیگر اگر به شانه‌ای استفاده شود که بیش از اندازه خاص باشد ممکن است که باز هم این بدافزار در همه ابزارها کشف نشود.

بعد از ایجاد شانه، کلیه شانه‌ها از طریق یک فرآیند GAS یا Asuality Assurance مورد ارزیابی قرار می‌گیرند تا این اطمینان حاصل شود که هنگام به روزرسانی هیچ صدمه ای متوجه مشتریان نباشد و این فرآیند به طور معمول بسیار حائز اهمیت است چرا که در موارد بسیاری بروز رسانی یک آنتی‌ویروس منجر به ایجاد آسیب‌های حیاتی جبران ناپذیری به رایانه‌های کاربران می‌شود که در یکی از بارزترین خطاها می‌توان به خطای نرم‌افزار Microsoft Security Essential اشاره کرد که نرم‌افزار محبوب Google Chrome را به عنوان یک تروجان بانکی شناسایی کرد چرا که در مرحله CSA به درستی ارزیابی‌های لازم در آن انجام شده بود.

در واقع بعد از مرحله CSA از مشتریان به انحاء مختلف خواسته شد تا نرم‌افزار خود را به روز کنند و بعد از بروزرسانی است که محافظت از کاربر در مقابل آن بدافزار آغاز خواهد شد.
البته بدیهی است که این روش ایرادهای بسیار زیادی دارد که از جمله آنها می‌توان به فاصله نسبتا طولانی تا ایجاد و انتشار یک بدافزار، کشف آن و تولید شانه‌های مختص آن و در نهایت بروز رسانی توسط کاربر اشاره کرد.
مسئله دیگری که در این خصوص می‌توان به آن اشاره کرد این است که حتی بعد از این فرآیند نسبتا طولانی کاربر تنها در مقابل نسخه‌های قدیمی‌تر یک بدافزار محافظت می‌شود و برای اینکه کاربر در مقابل نسخه‌های جدید این بدافزار حفاظت به عمل آید طی مراحل فوق باید تکرار شود.



رونـد ایجـاد امضـا



نتـایج

Trust Spider بیش از ۷۰۰۰۰ بدافزار را در سال ۲۰۰ مورد ارزیابی قرارداده است. در این میان از رایج‌ترین و معروف‌ترین آنتی ویروس‌ها نیز برای تست نحوه تشخیص آن‌ها استفاده کردیم. به طور میانگین آنتی‌ویروس‌ها توانستند در حدود ۸۱% از کل نمونه بدافزارهایی که در بانک اطلاعاتی ما بودند را شناسایی کنند (چهار تا از هر پنج بدافزار).

بهترین آمار شناسایی عدد ۸۳% و کمترین آن‌ها ۷۰% است. بدیهی است که شاید این آمارها برای حفاظت از یک دانش آموز آمار قابل قبولی باشد اما برای حفاظت از زیر ساخت‌های سایبری یک سازمان به هیچ وجه قابل قبول نیست و لذا حتی بسیاری از این سازمان‌ها که اقدام به نصب این آنتی ویروس‌ها هم کرده‌اند آسیب‌پذیری زیادی در هنگام حمله بدافزارها دارند.

با توجه به این اطلاعات باید گفت که با اینکه معمولا هزینه خرید آنتی ویروس یکی از کلیدی‌ترین موارد در تامین هزینه‌های امنیت اطلاعات هر سازمان است اما نباید این مسئله باعث شود که کاملا متکی به این نرم‌افزارها باشیم به عبارت دیگر آنتی ویروس‌ها همواره باید با ترکیب با سایر ابزارها و تکنیک‌ها که برای آشکارسازی و کشف بدافزارها بکار می‌روند، به کار رود که از آن جمله می‌توان به ابزارهایی نظیر تحلیل فایل‌های Log، تست‌های نفوذ، استفاده از دیواره‌های آتش اشاره کرد.

فـایـروال

فایروال در حالت عادی یک فناوری ساده است. چرا که جموعه‌ای از دستورالعمل‌ها را که توسط مدیر شبکه اعمال می‌شود را اجرا می‌کند. قریب ۲۵ سال بعد از معرفی چنین ویژگی و علیرغم ظهور تکنولوژی‌های نوظهور این سامانه همچنان به عنوان یکی از کلیدی‌ترین موارد برای حفظ امنیت کاربرد دارد.

فایروال‌های امروزی اما مجموعه گوناگونی از امکانات جدید فراوانی را برای مدیر شبکه فراهم می‌کند که می‌توانند به مراتب تنظیمات بیشتری را برای ارتقاء سطح امنیت شبکه سازمان اعمال کنند.

NAT: Network Address Translation یکی از فناوری‌های دیواره‌های آتش است که در اوایل دهه ۹۰ معرفی شد. این فناوری برای ایجاد یک ارتباط ایمن بین ابزارهای درونی یک سازمان که از بسته اینترنت برای ارتباط استفاده می‌کردند بوجود آمد تا اطلاعات را به صورتی منتقل کند که در بین راه نه قابل ردیابی باشند نه قابل استفاده در حال حاضر از دو نوع NAT استفاده می‌شود :

SNAT: Source Network Address Translation

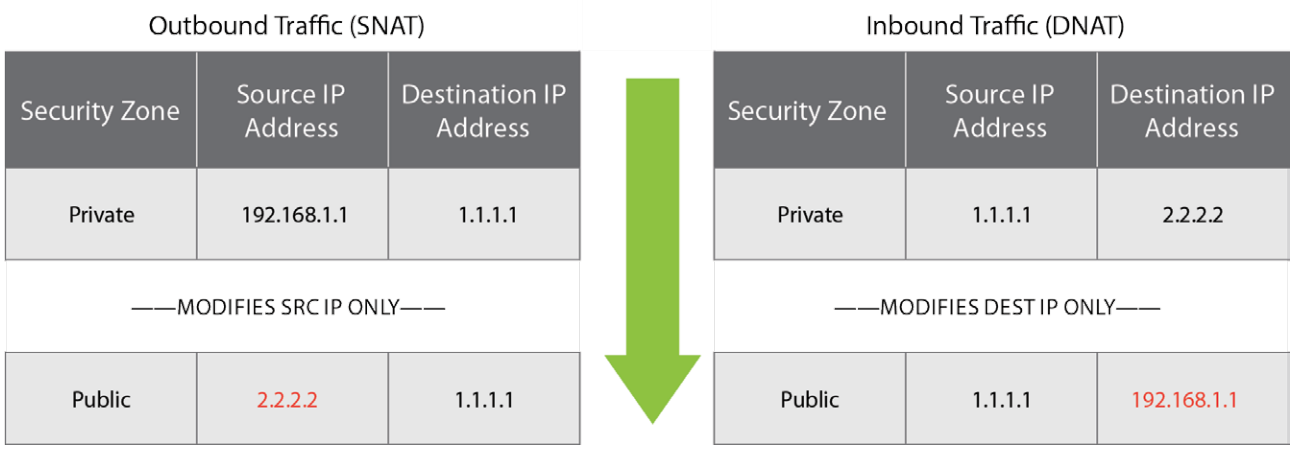
DNAT: Destination Network Address Translation

زمانی که یک سرور میزبان با استفاده از یک آدرس Private قصد ایجاد یک ارتباط با یک آدرس Public را دارد می‌بایست از NAT استفاده کند که بنا بر کاربرد از هریک از انواع بالا استفاده می‌شود به طور مثال علی رغم بلوغ فایر وال‌ها اقدامات کمی در خصوص تامین امنیت

RFC1918 Private Address Space

Start IP Address	Destination IP Address	Prefix
10.0.0.0	10.255.255.255	10/8
172.16.0.0	172.31.255.255	172.16/12
192.168.0.0	192.168.255.255	192.168/16

لایه‌های اصلی آن صورت گرفته است. آسیب‌پذیری‌هایی که امتروزه در لایه‌های سطح پایین این ابزارها قرار دارد و به شدت روی لایه‌های سطح بالا تاثیر گذار است و در واقع بسیاری از شرکت‌های تولید کننده



بهتر است به جای اضافه کردن امکانات و مزایای متعدد تیمی روی هسته اصلی این ابزارها کار کنند تا آسیب‌پذیری‌های سطح پایین این ابزارها برطرف شود.

در واقع پیچیدگی روزافزونی که در شبکه‌های رایانه‌ای بوجود آمده است موجب ایجاد آرام گپ‌هایی در لایه‌های دفاعی آن‌ها شده است.

گپ‌هایی که گرچه به خودی خود تهدید تلقی نمی‌شوند اما در واقع هریک حفره‌ای امنیتی تلقی می‌شوند که بسیاری از هکرها می‌توانند از آن‌ها سوءاستفاده‌های فراوانی بکنند. یکی از این گپ‌ها که در بسیاری از سازمان‌های تحن مطالعه Trustware دیده شد فاصله زیادی است که از لحاظ سازمانی بین مدیر شبکه و کارشناس منیت شبکه وجود دارد. و در واقع بسیاری از سازمان‌ها به این دو به عنوان دو بخش جداگانه نگاه می‌شود در حالی که تنها در صورتی می‌توان به ارتقاء سطح امنیت شبکه امید داشت که این دو بخش با همدیگر کار کنند.

Trustware: آزمایش‌های زیادی را انجام داده است تا متوجه شویم که هکرها چگونه از این گپ‌ها بهره‌برداری می‌کنند. در طول انجام این آزمایشات ما توانستیم به جدیدترین حفره‌هایی که هکرها از آن‌ها استفاده می‌کنند دست یابیم حفره‌های OBNAT و Broken NAT.

BNAT در حالت ابتدایی در طول جلسات TCP مشاهده می‌شود. زمانی که یک Client بخواهد یک جلسه عادی TCP را آغاز کند می‌بایست که ۳ مرحله زیر را صورت دهند :

زمانی که یک سناریوی BNAT دیده می‌شود تغییرات زیادی دیده می‌شود.

درصـد سرویس‌هـای مـورد استفـاده

درصـد	سـرویس	پـورت
9%	FTP	21
9%	SSH	22
10%	SMTP	25
34%	HTTP	80
34%	HTTPS	443
1%	Microsoft-DS	445
2%	MS-SQL	1433
0%	Oracle DB	1521
1%	MySQL	3306
2%	RDF	3389

رفتار شرکت‌ها نسبت به امنیت فناوری اطلاعات چگونه بوده است

چه کسانی مورد پرسش قرار گرفتند؟
متخصصانی در بیش از ۳۳۰۰ شرکت

مستقر در ۲۲ کشور در سراسر جهان

- کسب و کارهای کوچک (دارای ۱۰ تا ۹۹ شغل مرتبط با کامپیوتر) 30%
- کسب و کارهای متوسط (دارای ۱۰۰ تا ۹۹۹ شغل) 41%
- کسب و کارهای بزرگ (بیش از ۱۰۰۰ شغل) 29%

سرمایه گذاری سالانه در امنیت اطلاعات

€7,682 €27
کسب و کارهای کوچک

€69,231 €38
کسب و کارهای متوسط

€2,859,375 €110
کسب و کارهای بزرگ

مهم‌ترین نگرانی‌های متخصصان آی تی

- جلوگیری از رخنه‌های امنیتی 31%
- حفاظت از داده‌ها 27%
- نرخ بازگشت سرمایه گذاری 23%
- آشنایی با فناوری‌های جدید 23%
- سرمایه گذاری‌های آتی 22%

مهم‌ترین ریسک‌های کسب و کار

- ناپایداری اقتصادی 55%
- تهدیدات سایبری 50%
- صدمه به برند و خوشنامی 37%
- مشکلات مرتبط با امنیت سایبری
- سرقت سرمایه‌های فکری 31%
- تقلب 26%

مهم‌ترین سنجه‌های امنیتی

- حفاظت دربرابر بدافزارها 67%
- مدیریت وصله‌های امنیتی 62%
- کنترل سطح دسترسی 45%
- جداسازی زیر ساخت‌های حیاتی 45%
- رمزگذاری داده‌های حساس 44%

تهدیدات درونی

- نرم افزارهای خطرناک 40%
- گم کردن ابزارهای همراه توسط کارکنان 29%
- نشت تصادفی داده ها توسط کارکنان 31%
- نشت جهانی داده‌ها 21%
- از دست دادن تجهیزات 25%
- از دست دادن داده‌های تجاری از طریق حفره‌های امنیتی نرم‌افزارها 35%

تهدیدات بیرونی

- کلاهبرداری 35%
- هرزنامه‌ها 56%
- حملات بد افزاری 61%
- سرقت ابزارهای همراه 20%
- نفوذ به شبکه 23%
- 35%

نابودی داده ها در اثر حملات بد افزاری

چگونه می توانیم به نحو موثرتری با هرزنامه مبارزه کنیم؟

در حملات هرزنامه‌ای به طور کلی، ۴۳ درصد از ایمیل‌های ناخواسته طی ده دقیقه ابتدایی حمله، ارسال می‌شوند.
(بر اساس گزارش آزمایشگاه کسپرسکی)

پالایش چند لایه‌ای هرزنامه‌ها

بر اساس ویژگی‌های پیام

- متن پیام به طور معمول خوانده می شود
- فرستنده در لیست سیاه قرار می گیرد
- پیام در یکی از گروه بندی‌های هرزنامه ها طبقه بندی می شود
- محتوای هرزنامه ثبت می شود

بر اساس تحلیل‌های ضد هرزنامه‌ای

- پایگاه داده‌ای ضد هرزنامه‌ای
  به کمک سرویس روزآمد سازی، این کار فقط چند ثانیه به طول می انجامد

استفاده از فناوری ابری

- جزئیات پیام هرزنامه‌ای مشخص می گردد
- داده ها به کلاینت نرم افزاری داده شود و از طریق آن درخواستی به ابر داده می‌شود
- محتوای پیام تحلیل شده ولی محرمانه باقی می ماند

توجه به ویژگی تکرار شوندگی

- فناوری پالایش پیام های تکراری، با توجه به محتوا، هرزنامه های جدید را مشخص می‌کند.
- ایمیل‌های مشکوک یک بار دیگر بررسی می شوند
- پیام‌هایی که تکرار شوندگی زیادی دارند، به طور خودکار قفل می گردند.

در ازای هر ۱۰۰۰ پیام که دریافت می کنید

- ۲۵۷ – ایمیل واقعی
- ۷۱۳ – هرزنامه و ایمیل ناخواسته

۳۰ – هرزنامه به همراه خود، پیوست‌های خطرناک یا آلوده دارند.

ایمیل‌های خطرناک توسط موتور ضد هرزنامه شناسایی و مسدود می شوند.

حفره‌های امنیتی جدید و خطرناک نیز مسدود می شوند.

البته حفره‌ها و آسیب پذیری‌ها به طور مستمر برای حملات هدفمند مورد استفاده قرار می گیرند.

موتور ضد هرزنامه می تواند تا ۹۹/۷٪ از ایمیل‌های ناخواسته و هرزنامه‌ها را مسدود نماید :

بیشترین
جلوگیری از ورود هرزنامه‌ها

کمترین
خطا در شناسایی بدافزارها

با استفاده از منابع آزمایشگاه کسپرسکی

TM HOST
Quality Web Hosting Services

ایمن و پایدار

سرویس‌های میزبانی TM HOST

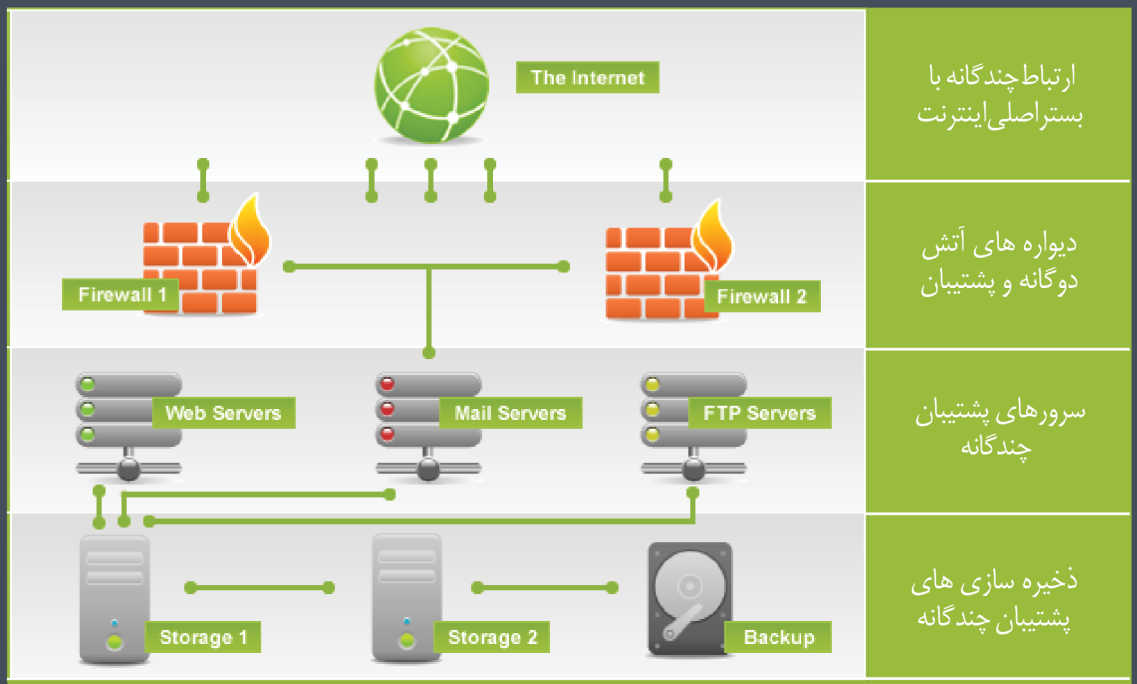
سرورهای DELL

شبکه گیگابیتی

پلتفرم ویندوزی

پلتفرم لینوکس

زیرساخت‌های فنی TM HOST



به همراه امکان ارائه: سرورهای اختصاصی، سرورهای هایبریدی، سرورهای خصوصی مجازی

جهت کسب اطلاعات بیشتر و یا کسب نمایندگی با TM HOST تماس بگیرید.

www.tmhost.net

info@tmhost.net