palnet
Palnet Group

گروه مهندسی شبکه
پـال نـت

راهکار تخصصی مقابله با باج افزار ها
Solution For Anti Ransomware

info@palnetgroup.ir www.palnetgroup.ir ۰۲۱ - ۸۸۱۷۳۳۱۷

مقدمه

امروزه حملات سایبری جدیدی در دنیا رشد فزاینده ای داشته و بسیاری از شرکت ها و سازمان های خصوصی و دولتی در سرتاسر دنیا هدف این حملات بوده اند. حملاتی که از روش های مختلفی شبکه های سازمانی را آلوده و شروع به رمز گذاری داده ها، دیتابیس ها و فایل های سازمانی میکند. تا به امروز هیچ گونه ابزار رسمی برای کاهش و مقابله با حملات که منسوب به باج افزار ها و malware ها می باشند و در دنیا شناخته شده هستند پیدا نشده و تنها راه کار کاهش و پیشگیری نسبی آن استفاده از موارد ذکر شده در راهکار پیش رو می باشد.

نمونه هایی زیادی از باج افزارها در سراسر اینترنت وجود دارند مانند Cryptowall، JobCrypter، UmbreCrypt، TeslaCrypt که تنها تفاوت آنها در اندازه باج و نوع الگوریتم مورد استفاده برای رمزگذاری فایل ها می باشد. تحقیقات همچنین نشان می دهد که هیچ تضمینی وجود ندارد که فایل های خود را تا به حال حتی پس از پرداخت باج رمزگشایی شود. تنها با پرداخت، به سادگی از کسب و کار مجرمانه حمایت کرده اید بنابراین، شما هرگز نباید باج پرداخت کنید و یا تلاشی برای تماس بگیرید. توجه داشته باشید نرم افزارهای مخربی مانند این باج افزار بطور معمول از طریق به روز رسانی جعلی نرم افزار، شبکه های P2P، پیوست های ایمیل های مخرب و تروجان ها توزیع شده اند.

باج افزار ها می توانند از روش هایی نظیر ایمیل های الوده، سایت های جعلی، فلش های ناقل به باج افزار و دسترسی های راه دور و بسیاری متد های دیگر یک شبکه را تخریب و درخواست بهای نقدی جهت بازگشایی روزها نمایند.

در این مستند سعی داریم تا از بهترین روش های تست شده و معتبر که در حال حاظر در دنیا در حال استفاده می باشند استفاده نماییم تا بتوانیم یک بستری را در شبکه سازمانی پیاده سازی نماییم تا دسترسی و قدرت تخریب داده ها و شبکه ها به حداقل برسد و در کمترین زمان قابل ریکاوری و به روز رسانی باشد.

تاریخچه باج افزار ها

باج‌افزارها **Ransomwar** گونه‌ای از بدافزارها هستند که دسترسی به سیستم را محدود می‌کنند و ایجادکننده آن برای برداشتن محدودیت درخواست باج می‌کند. برخی از انواع آنها روی فایل‌های هارددیسک رمزگذاری انجام می‌دهند و برخی دیگر ممکن است به سادگی سیستم را قفل کنند و پیام‌هایی روی نمایشگر نشان دهند که از کاربر می‌خواهد مبالغی را واریز کنند. باج‌افزارها ابتدا در روسیه مشاهده شدند اما اخیراً تعداد حملات باج‌افزارها به کشورهای دیگر از جمله استرالیا، آلمان و ایالات متحده آمریکا و ایران و بیش از ۹۰ کشور دیگر در سرتا سر جهان افزایش یافته است.

باج افزارها از طرق مختلف مانند کرمها منتشر می‌شوند و پس از نصب و اجرا شروع به اعمالی مانند رمزگذاری هارددیسک می‌کنند. باج افزارهای پیشرفته تر با استفاده از کلید عمومی فایلها را رمز نگاری می‌کنند و کلید خصوصی لازم برای بیرون آوردن فایلها از حالت رمز شده تنها در دستان طراح باج افزار است. کاربر برای باز کردن فایلهایش مجبور به پرداخت وجه به حساب طراح باج افزار می‌شود. برخی دیگر از باج افزارها رمزگذاری انجام نمی‌دهند، بلکه از روش‌های دیگری مثل اختصاص پوسته سیستم عامل به خود و یا تغییر رکوردهای مربوط به بوت استفاده از سیستم را مختل می‌کنند.. اولین باج افزاری که کشف شد تروجان **AIDS** بود که **PC Cyborg**نیز نامیده میشد و در سال ۱۹۸۹ یعنی ۲۷ سال پیش پی سی ها را الوده میکرد.

باج افزارها انواع بسیاری دارند که هر چند نمیتوان همه انها را نام برد اما میتوان انها را به چهار دسته تقسیم کرد : باج افزارهائی که برنامه ها را مسدود میکنند، باج افزارهائی که فایلها را رمزنگاری میکنند، باج افزارهائی از طریق سایتهای وب عمل کرده و محتوا را قفل میکنند، باج افزار هایی که کل سیستم عامل را مسدود می سازند.

انها میتوانند یک فایل پیوست در یک ایمیل بوده و یا از روی سایتهای اشتراک گذاری دانلود شده و یا خود را انتی ویروسی معرفی کنند و از طریق اسیب پذیریهای مرورگر انتشار یابند . در نتیجه روش بخصوصی برای الوده کردن و یا الوده شدن وجود ندارد و تنها راه حل پیشگیری از الودگی است. باج افزارها با اکستنشنهای متفاوتی نیز هستند که از میان میتوان از ".exe" و "scr" نام برد . ایکن انها معمولا بصورتی است که کاربر را دچار خطا میکند چون میتواند شبیه ایکن یک برنامه مشروع باشد.

ارائه تخصصی ترین گام های موثر در خصوص جلوگیری و پیشگیری از حملات باج افزار ها

پنج گام مهم در امن سازی سرورها و کلاینت ها و دیتای سازمان

گام اول: بکاپ و تهیه نسخه پشتیبان

گام دوم: به روز رسانی برنامه ها و سیستم عامل ها

گام سوم: پیاده سازی مکانیزم هوشمند File Server

گام چهارم: مدیریت Firewall

گام پنجم: مدیریت کاربران

استفاده از گام های ذکر شده می تواند تا حد بسیار زیادی از حملات باج افزاری پیشگیری کرده و یا در صورت آلوده شدن شبکه، با کمترین Downtime ممکن شرایط شبکه را به حالتی ایستا و ایده آل بازگردانی کرد.

گام های عنوان شده کاملا بر اساس دانش فنی و متد های معرفی شده روز دنیا می باشد ، روش هایی که پس از پیاده سازی در سازمان ها در سراسر دنیا به عنوان موثر ترین روش برای مقابله با باج افزار ها نام برده شده است.

گام اول: بکاپ و تهیه نسخه پشتیبان

بهترین و موثر ترین روش برای جلوگیری از حملات باج افزار ها دارا بودن یک مکانیزم هایی برای بکاپ گیری و تهیه نسخه پشتیبان از منابع شبکه می باشد.

حال برای تهیه یک سامانه پشتیبان گیری می بایست از راهکار هایی استفاده کرد تا بتوان از تمامی موارد سطوح داده، دیتا بیس و سیستم عامل ها بکاپ های زمان بندی شده گرفته تا بتواند در صورت الودگی موارد عنوان شده در کوتاه ترین زمان ممکن به نزدیک ترین بکاپ سالم رجوع کرده و انرا بازگردانی نمود.

در واقع برای بهبود کیفیت بکاپ ها لازم است تا از دو روز **Online Backup** و **Offline Backup** استفاده نمود.

شبکه هایی که از زیرساخت مجازی سازی سرور ها **Vmware vSphere**، **Xen Server** و **Hyper-V** استفاده می کنند از شرایط بهتر برای بکاپ گیری و ریکاوری بهرهمند هستند. چرا که راهکار پشتیبان گیری از سرور های مجازی دارای سرعتی بهینه تر در ریکاوری می باشد.

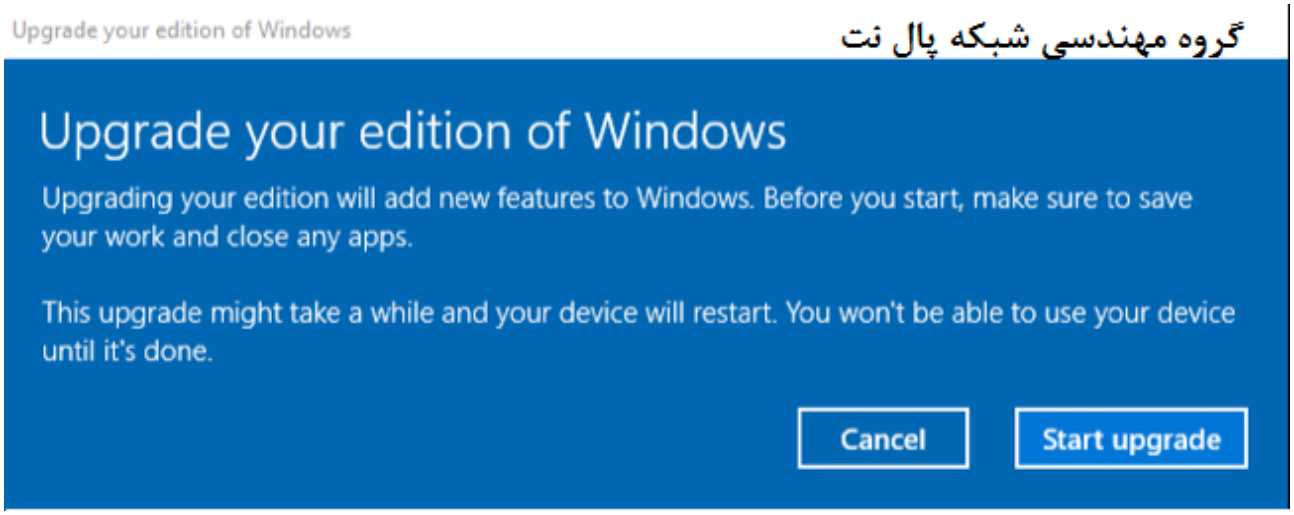
بکاپ گیری از داده ها ، دیتابیس ها و ماشین های مجازی، هر سه به صورت همزمان، مطمئن ترین و بهترین راه برای مقابله با باج افزار ها می باشد و می تواند این اطمینان را حاصل نماید تا در صورت الودگی هرکدام از این عنوان ها، به راحتی ان ها را ریکاوری و بازگردانی نمود.

قابل ذکر است که برای پیاده سازی یک سامانه بکاپ مطمئن ابتدا می بایست شرایط داده ای و رفتاری سازمان سنجیده شود تا بتوان یک برنامه بکاپ گیری زمان بندی شده و با حداقل نیاز به منابع انسانی تهیه نمود و هر انچه که باج افزار ها در اولویت حملات خود قرار می دهند را در نیاز های اصلی تهیه نسخه های پشتیبان قرار داد.

گام دوم: به روز رسانی سیستم عامل ها و نصب Patch های امنیتی حیاتی

مهمترین هدف باج افزار ها سیستم عامل های مایکروسافتی می باشد. سیستم عامل های سروری و کلاینتی که کاربران و سرویس دهنده ها از ان استفاده می نمایند. از مهمترین دلایلی که یک شبکه دچار حملات باج افزاری و رمز نگاری شده می باشد، استفاده از سیستم عامل های میباشد که به روز نشده و از Patch های امنیتی ارائه شده توسط مایکروسافت استفاده نمی کنند.

در این بین به روز رسانی سیستم عامل ها به نسخه های جدید گامی مهم و حیاتی می باشد. زیرا که وجود حفره های امنیت شناسایی شده در ویندوز های قدیمی عامل اصلی ورود و نفوذ ransomware ها می باشد. شرکت مایکروسافت به عنوان متولی اصلی امنیت در ویندوز صریحا اعلام کرده تا ویندوز ها را با استفاده از patch های ارائه داده به اخرین نسخه های امنیتی ارائه شده مانند ویندوز سرور ۲۰۱۲ و ۲۰۱۶ و ویندوز ۱۰ ارتقا داده و از patch های امنیتی اراده شده توسط مایکروسافت برای دیگر نسخه های ویندوز های قدیمی استفاده نمایند تا با استفاده از این بسته ای امنیتی، حفره ای باز و قابل نفوذ بسته شده و راه برای ورود باج افزار ها بسته شود.



حفره های امنیتی مانند SMB، File Services، CIFS که به صورت پیش فرض در ویندوز ها باز بوده و پس از نصب Security Patch ها کنترل شده و پورت های آنها بسته می شود.

همچنین استفاده از آخرین نسخه های نرم افزاری و استفاده از انتی ویروس های معتبر با اخرین به روز رسانی ها و Update های انجام شده می تواند بر این امر کمک بسزایی کند.

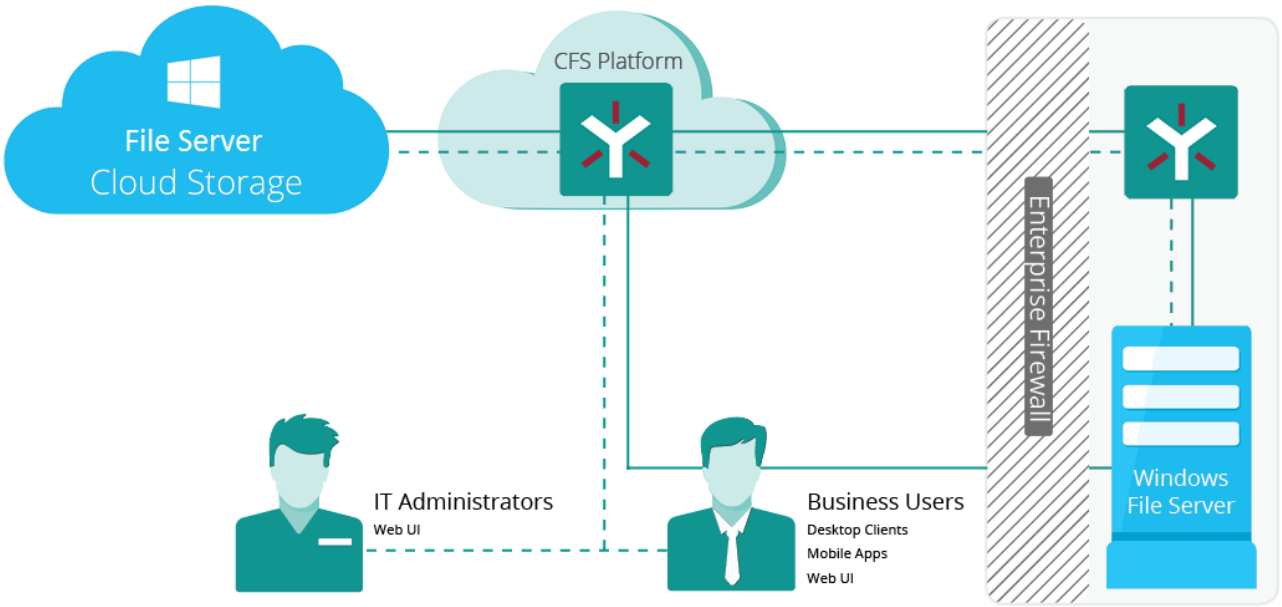
هرچند که انتی ویروس ها قدرت جلوگیری و پاک کردن باج افزار هارا ندارند اما می توانند در قابل پیغامی کاربران را از ورود باج افزار ها بر روی فایل های سیستمی مطلع سازند و LogFile را تهیه نمایند.

گام سوم: پیاده سازی مکانیزم هوشمند File Server

باج افزار ها عمدتا در شبکه هایی که سامانه **File Sharing** وجود دارد نفوذ کرده و فایل هایی که بالاترین سطوح دسترسی را دارند اصلی ترین هدف های رمز گذاری میباشند. بر این منظور، جهت افزایش فایل های به اشتراک گذاشته شده ابتدا واجب است تا تمامی سطوح دسترسی را برای کاربران به حداقل رسانده و در یک مدیریت و مکانیزم رسمی این سطوح دسترسی را کنترل نمود.

پیاده سازی سامانه **File Server** در سازمان ها که می تواند سطوح دسترسی را کنترل کرده و دیگر منابع و سرویس های شبکه را از فایل ها و فولدر های **Share** شده تفکیک کند گامی اساسی و مهم در زیر ساخت شبکه می باشد.

الودگی فایل های **Share** شده اولین هدف برای باج افزار ها می باشد زیرا با وجود دسترسی هلی **Read** و **Write** می تواند به راحتی خود را تکثیر کرده و تمامی شبکه و سیستم هایی را که به **Shared Folder** ها دسترسی دارند آلوده نماید.



در اینجا پیاده سازی **File Server** و تمامی سرویس های وابسته به آن به صورت جدا گانه در شبکه و بهینه سازی سطوح دسترسی کاربران و طبقه بندی کردن تمامی **Shared Permission** ها می تواند تا حد بسیار زیادی از نفوذ باج افزار ها در شبکه جلوگیری نماید و یا در صورت نفوذ امکان تکثیر ان را به دیگر جاهای شبکه ندهد.

گام چهارم: مدیریت Firewall

استفاده از فایروال ها در شبکه و مدیریت تمامی ارتباطات داخلی و خارجی می تواند راه نفوذ باج افزار ها به شبکه را تا حد بسیار زیادی کند و فرسایشی و در بعضی موارد غیر ممکن سازد.

بسیاری از سازمان ها بر این باورند که فایروال ها می توانند خللی در ارتباطات شبکه ای به وجود بیاورد لذا به صورت پیش فرض در شبکه های دامینی، فایروال ویندوزی را برای تمامی سیستم های کاربران مسدود می سازند. اما برای جلوگیری و مقابله با باج افزار ها علاوه برفعال سازی فایروال ویندوزی و پیاده سازی هوشمنانه تنظیمات امنیتی بر روی ان که توسط مایکروسافت اعلام گردیده است می بایست از یک فایروال سخت افازری و یا نرم افزاری دیگر هم استفاده نمود تا با مدیریت وب سایتها، مدیریت پورت ها، مدیریت منابع مصرفی اینترنت کاربران، مدیریت برنامه های کاربردی تحت اینترنت و .... بتوان شبکه های سازمانی را از یک زیرساخت مطئن ترین بهره مند ساخت.

از جمله تنظیمات امنیتی که می توان برای یک فایروال در خصوص مقابله با باج افزار ها اعمال نمود عبارتند از:

توانایی ثبت و اخطار، بازدید حجم بالایی از بسته های اطلاعات، مانیتورینگ ورود و خورج به شبکه از طریق اینترنت، مانیتورینگ و کنترل ارتباطات VPN، امنیت و ایجاد افزونگی مدیریت درگاه های ورودی و خروجی، فیلتر کردن کاربران و ایمیل ها و وب سنایت هاو برنامه های کاربردی و فیلترینگ پورت های مورد نیار و غیر ضروری و ...

فایروال ها می توانند نقشی اساسی در مقابله با باج افزار ها داشته باشند اما نیاز بر این است تا با داشتن یک دانش امنیتی شروع به تنظیمات ان نمود.

گام پنجم: مدیریت کاربران و کنترل دسترسی ها به منابع

کاربران می توانند ناقل و عامل اصلی نفوذ باج افزار ها در شبکه باشند. هرچقدر سطح دسترسی کاربران و اختیارات کاربران به سیستم و شبکه بالا باشد احتمال نفوذ باج افزار ها هم می تواند به شبکه افزایش پیدا کند.

در این خصوص پیاده سازی یک برنامه هوشمند برای تعریف کاربران در ارتباط با کاهش و یا مدیریت بهینه انها به اجرای برنامه ها، نحوه استفاده از ایمیل ها، فایل ها با پسوند های متفاوت، تنظیمات امنیتی بر روی سیستم های کاربران، فرهنگ سازی کاربران برای استفاده صحیح از سیستم ها و شبکه و .... می تواند عاملین اصلی راه های نفوذ باج افزار به شبکه را کاهش داده و سازمان ها را از یک شبکه پاک و عاری از هر گونه آلودگی بهره مند سازد.

تنظیمات و مدیریت کاربران به صورت متمرکز از طریق سرویس های وابسته به اکتیو دایرکتوری، ایجاد پالیسی های متنوع به ازای هر کاربر یا گروهی از کاربران، مانیتور کرده کاربران و تهیه گزارش روزانه جامع از کلربران در خصوص رفتار های نرم افزاری هر کاربر بر روی سیستم های شخصی و منابع شبکه، کاهش سطوح دسترسی رفتاری کاربران به منابع داده ای و اجرای شبکه، اعمال پالیسی های امنیتی در خصوص اجرای فایل ها با پسوند های مشکوک بر روی سیستم کاربران، اعمال تنظیمات امنیتی برای ایمیل کاربران و بسیاری دیگر ازاین قبیل سیاست ها می تواند مهمترین روش را برای بهبود و جلو گیری و مقابله با باج افزار را در اختیار سازمان ها قرار دهد.

از جمله ابزار های که می توانند در خصوص مدیریت کاربران به مدیران و کارشناسان واحد های فناوری اطلاعات کمک نمایند می توان به مواردی نظیر **Microsoft System Center**، **Microsoft Group Policy**، **Script ecurity Policy**، **Domain user Monitoring** و ... اشاره نمود.

خدمات تخصصی گروه پال نت در زمینه مبارزه با نفوذ بدافزارها به داخل شبکه

گروه مهندسی شبکه پال نت تمامی راه کار های عنوان شده را در بسیاری از سایت های متنوعی از مشتریان خود پیاده سازی نموده و توانسته با بکار گیری از دانش تجربی و اجرایی خود مقابله با باج افزار ها و Ransomware ها را در سازمان ها اجرا نماید.

کارشناسان فنی گروه پال نت این نوید را به مدیران، متخصصین و کارشناسان حوزه فناوری اطلاعات و صاحبان کسب و کارهای مختلف می دهد که تا با بهره گیری دقیق و پیاده سازی کامل و تخصصی راه کار های عنوان شده بتواند بخشی قابل توجه از حملات سایبری را کاسته و یا در مواقعی به صورت کامل پیش گیری نماید.

www.palnetgroup.ir