جمهوری اسلامی ایران

ریاست جمهوری

مرکز مدیریت راهبردی افتا

راهنمای پیشگیری و مقابله با بدافزارهای باج گیر

اردیبهشت ۱۳۹۶

فهرست مطالب

۱. مقدمه

بدافزارهای باج‌گیر یا باج‌افزارها (Ransomware) بدافزارهایی هستند که جلوی دسترسی کاربران به سیستم یا اطلاعات خود را گرفته و برای برقرار کردن مجدد دسترسی درخواست پول می‌کنند.

به علت استفاده از قوی‌ترین الگوریتم‌های رمزنگاری در این نوع بدافزارها، پس از آلوده شدن سیستم بازیابی با مشکلات و هزینه فراوانی انجام خواهد شد. لذا بهترین راه مقابله، جلوگیری از آلوده شدن به آن‌ها است.

با توجه به مسائل مطرح شده، ضرورت برقراری و حفظ امنیت سایبری در مواجه با باجگیرها در کشور بیش از هر زمان دیگری احساس می‌شود. مستند پیشرو به عنوان راهکاری جامع به‌منظور پیشگیری و مقابله با این تهدید ارائه شده است.

۲. پیشگیری

مهم‌ترین مساله در رویارویی با بدافزارهای باجگیر آگاهی افراد از این تهدید و پیشگیری از آن می‌باشد.

آلوده شدن به بدافزارهای باج‌گیر از روش‌های مختلفی رخ می‌دهد. برخی از رایج‌ترین این روش‌ها شامل موارد ذیل است:

- باز کردن پیوست ایمیل‌های اسپم یا لینک‌های درون آنها
- باز کردن فایل‌های دانلود شده آلوده از سایت‌های نامعتبر یا کلیک روی لینک‌های مخرب
- استفاده از روش های مهندسی اجتماعی برای هدایت کاربران به صفحات فیشینگ
- آلودگی از طریق سایت‌های هک شده و یا شبکه‌های توزیع تبلیغات آلوده
- آلودگی از طریق هک و نفوذ به سیستم‌ها؛ به خصوص سیستم هایی که آسیب‌پذیری آن‌ها وصله نشده است.

حداقل اقدامات موثر در پیشگیری از آلودگی به بدافزارهای باج‌گیر یا کاهش اثر ریسک آنها را می‌توان به بخش‌هایی که در ادامه می‌آید تقسیم نمود.

۲-۱ اطلاع‌رسانی و آموزش کاربران برای پرهیز از رفتار خطرناک

می‌بایست آموزش‌های کافی به کاربران از طریق ویدئوها و بروشورهای آموزشی برای پرهیز از رفتارهای خطرناک نظیر باز کردن فایل‌های پیوست ایمیل، مراجعه به سایت‌های ناشناس یا کلیک روی لینک‌های مشکوک و غیره ارائه شود.

۲-۱-۱ عدم بازگشایی ایمیل‌های مشکوک

بایستی پیوست‌های ایمیل‌های دریافتی قبل از باز شدن با ابزارهای مناسب پویش شوند.

مشخصه‌های ایمیل‌های مشکوک به مخرب بودن به قرار زیر است:

- ایمیل موردنظر در لیست اسپم قرار گرفته باشد.
- فرستنده ایمیل ناشناس باشد.
- آدرس پست الکترونیکی فرستنده، مربوط به یک وبسایت ایمیل رایگان باشد.
- آدرس ایمیل فرستنده با آدرس ایمیل سازمان مورد اعتماد کاملاً متفاوت باشد و یا حتی تفاوت‌های جزئی داشته باشد(وجود تفاوت‌های جزئی در آدرس ایمیل فرستنده و سازمان مورد اعتماد نشان دهنده نوعی مهندسی اجتماعی است).
- در محتوای ایمیل، نام دقیق کاربر ذکر نشده و از نام‌های کلی استفاده شده باشد. برای مثال گیرنده با عبارت‌هایی مانند "مشتری عزیز" ، "کارشناس محترم" خطاب قرار گیرد.
- نوعی احساس فوریت در ایمیل بیان گردد. برای مثال فرستنده تهدید کند که در صورت عدم انجام عمل خواسته شده، حساب شما سریعاً بسته می‌شود.
- ایمیل دارای محتوای ترغیب کننده باشد، در حالی که فرستنده آن معتبر نیست. برای مثال وعده پول، شرکت در قرعه کشی، برنده شدن در لاتاری، تخفیف فروشگاه‌های بزرگ، درخواست برای کمک به یک سازمان خیریه، و یا درخواست کمک به بازماندگان یک حادثه .
- ایمیل حاوی درخواست برای ارسال اطلاعات شخصی مانند نام کاربری، پسورد و یا جزئیات حساب بانکی باشد.
- ایمیل دارای اشتباهات املایی و دستوری باشد.
- ایمیل درحالی از سازمان مورد اعتماد دریافت شود که انتظار نمی‌رود سازمان در آن زمان ایمیلی ارسال کرده باشد.
- کل متن ایمیل در واقع یک عکس از محتوا باشد که در قالب متن قرار گرفته است.
- تصویر موجود در ایمیل حاوی لینک تعبیه شده به یک سایت جعلی باشد.
- ایمیل حاوی لینک و یا پیوست‌هایی باشد که مورد انتظار نیست. به عبارت دیگر نام و فرمت پیوست‌ها متفاوت از نام و فرمت پیوست‌های مورد انتظار باشد.
- پیوست‌ها دارای دو یا چند پسوند برای فرمت خود باشند.

پس از شناسایی ایمیل مشکوک، بایستی نکات زیر رعایت شود:

- بر روی لینک‌های موجود در ایمیل کلیک نشود.
- پیوست‌های ایمیل به هیچ‌وجه باز نشود.
- نباید هیچ‌گونه پاسخی به ایمیل داده شود و با ارسال کننده ایمیل نیز نباید تماس گرفته شود.
- درصورت کلیک بر روی لینکی در ایمیل مشکوک، هیچ اطلاعاتی در وب‌سایت باز شده وارد نشود.
- در نهایت، گزارش ایمیل مشکوک به نهاد مسئول رسیدگی این دسته از ایمیل‌ها ارسال شود.

۲-۱-۲ عدم دریافت فایل از منابع نامعتبر

عدم دریافت فایل از منابع نامعتبر یکی دیگر از اقدامات پیشگیرانه محسوب می‌شود. دانلود فایل‌های کرک نرم‌افزارها و بازی‌ها، نسخه‌های بروزرسانی و غیره، از منابع نامعتبر می‌تواند موجب آلودگی سیستم به باج‌افزارها شود.

۲-۲ پشتیبان‌گیری منظم(Backup Operation)

مهمترین و موثرترین رکن در مقابله با بدافزارهای باج‌گیر داشتن پشتیبان‌های منظم دوره‌ای و غیرمتصل است. مقصود از پشتیبان غیرمتصل، این است که رسانه‌ای که اطلاعات روی آن پشتیبان گرفته می‌شود، باید پس از انجام عملیات پشتیبان-گیری از سیستم جدا شود، تا در صورت آلوده شدن به بدافزارهای باج‌گیر، خود اطلاعات پشتیبان رمزگذاری نشوند. مهمترین داده‌ها عبارتند از:

- سیستم‌عامل ها و سرویس‌های فعال
- داده‌های عملیاتی و حساس

بسیاری از باج‌گیرها علاوه بر رمز کردن فایل‌ها و اطلاعات معمول، اطلاعات پشتیبان و حتی پوشه‌های اشتراکی شبکه و مانند آن را نیز رمز می‌کنند تا همه اطلاعات در دسترس رمز شده و قربانی مجبور به پرداخت باج گردد.

بدیهی است تنها پشتیبان‌گیری منظم کافی نیست و حتما باید با انجام بازیابی‌های دوره‌ای از امکان انجام بازیابی صحیح و بدون مشکل در صورت وقوع حوادث اطمینان حاصل نمود. پشتیبان‌گیری تنها روش تضمینی جلوگیری از تهدید بدافزارهای باج‌گیر به شمار می‌رود.

نکته مهم: همچنین باید نسبت به صحت و سلامت کامل نسخه‌های پشتیبان اطمینان حاصل کرد.

۲-۳ امن سازی سامانه ها

۲-۳-۱ نصب و به روز کردن ضدویروس

اگر چه باج‌گیرهای اینترنتی از بهترین و به روزترین ضدویروس‌ها نیز عبور می‌کنند، اما داشتن یک ضدویروس معتبر و به روز به منظور کاهش خطر این تهدیدات بسیار موثر است. البته باید همواره در نظر داشت که در حال حاضر ضدویروس تاثیر کمی در جلوگیری از این خطر دارد، چرا که اگر بدافزار باج‌گیر یک بار موفق به عبور از سد ضدویروس شود، قربانی مجبور به پرداخت باج خواهد شد.

در عین حال به علت همه‌گیر بودن و در دسترس بودن ضدویروس‌ها، نویسندگان بدافزارهای باج‌گیر تمرکز خاصی روی این ابزارهای امنیتی دارند و قبل از انتشار نسخه‌های جدید خود (که برخی اوقات در یک روز هزاران نسخه جدید و یکتا است) حتما آن را با ضدویروس‌های موجود تست کرده و از عدم شناسایی باج‌افزار خود مطمئن می‌شوند.

لازم به ذکر است سامانه‌های ضدویروس باید تنها از عرضه کنندگان معتبر تهیه شوند تا از اصالت این سامانه‌ها اطمینان حاصل شود.

۲-۳-۲ نصب و استفاده از ابزار خاص ضدباج‌گیر

استفاده از ابزاری موسوم به ضدباج‌گیر که قابل نصب در کنار ضدویروس بوده و بدافزارهای باج‌گیر را به صورت رفتاری شناسایی و خنثی کند در مقابله با این تهدید می‌تواند موثر باشد. در تهیه این ابزارها باید حتما دقت شود که :

۱- از اصالت سامانه ضدباج افزار اطمینان حاصل شود؛

۲- از عرضه کنندگان معتبر تهیه شود؛

۳- به صورت سرویس رایانش ابری نباشد.

۲-۳-۳ پیکربندی امن سیستم‌عامل و نرم‌افزارها

به‌روز کردن سیستم‌عامل و نرم‌افزارهای مورد استفاده بخصوص مرورگرها و نرم‌افزارهای ارتباطی یا رایج مانند کلاینت ایمیل و مجموعه آفیس و غیره تاثیر بالایی در کاهش ریسک آلودگی به تهدیدات بدافزاری دارد. امروزه بسیاری از تهدیدات بدافزاری از طریق روش‌ها و آسیب‌پذیری‌های شناخته شده انجام می‌شوند و در نتیجه امن‌سازی و به‌روز بودن می‌تواند حداقل این اطمینان را بدهد که آلوده کردن سیستم، کار ساده‌ای نبوده است. بخصوص در مورد بدافزارهای باج‌گیر به علت رواج استفاده از کیت‌های حمله[۱] در آلوده‌سازی، این مساله بسیار مهم است.

از جمله این امن‌سازی‌ها در بحث باج‌افزارها شامل موارد زیر است:

- در صورت امکان سرویس(RDP(Remote Desktop Protocol غیرفعال شود و یا از سایر روش‌های دسترسی در این خصوص استفاده شود.
- به کاربران سازمان حداقل مجوزهای لازم و کنترل دسترسی را بدهید به اندازه‌ای که نیاز سازمانی آنها را مرتفع کنند.
- از پسوردهای قوی استفاده کنید، به طوریکه با روش‌های کشف رمز عبور مانند حملات دیکشنری به راحتی قابل شناسایی نباشد
- از لیست سفید برنامه‌های کاربردی که تنها به برنامه‌های شناس و مورد تایید، براساس سیاست‌های امنیتی اجازه‌ی اجرا می‌دهند، استفاده کنید.
- برای انجام کارهای روزانه و غیر ضروری به عنوان کاربر نرمال و یا کاربری غیر از Admin در سیستم وارد شوید.
- سرویس‌ها و پورت های غیرضروری را غیرفعال کنید.
- پنجره‌های popupها را بر روی مرورگر بلوکه کنید.

[۱] Exploit Kit

- درصورت وجود قابلیت ضد اسپم در سرور پست الکترونیکی، آن را فعال نموده یا از نرم افزار های مخصوص این کار استفاده کنید.
- امکان Autoplay را برای جلوگیری از راه اندازی خودکار هارد اکسترنال یا فلش USB در هنگام اتصال به رایانه غیرفعال کنید

۲-۳-٤ غیرفعال کردن و محدود کردن اجرای اسکریپت‌های غیرضروری

یکی از روندهای رو به رشد در بدافزارهای باج‌گیر استفاده از اسکریپت‌های SCR, JS, VBS, WSF و مانند آن به عنوان اولین مرحله آلودگی است. با توجه به محدودیت‌های سرویس‌دهنده‌های ایمیل در ارسال فایل‌های اجرایی، تمرکز و نرخ تشخیص بالاتر این فایل‌ها، و نیز راحتتر بودن درهم‌سازی اسکریپت‌ها، نویسندگان باج‌افزار به سوی این ابزارها رغبت بیشتری پیدا کرده‌اند.

از طریق :

- ۱- غیرفعال کردن برنامه اجرایی wscript ویندوز مانند Windows script host و Windows power shell

۲- غیرفعال کردن ماکروهای مجموعه آفیس به نحوی که بدون پرسش از کاربر این ماکروها محدود شوند

می‌توان فریب دادن کاربران نامطلع و آلوده کردن سیستم را تا حد خوبی مهار کرده و به حداقل رساند.

۲-۳-٥ پیشگیری از اجرای برنامه‌ها از مسیرهای خاص

از اجرای فایل در فولدرهای خاص مانند %TEMP% ، Downloads یا %AppData% جلوگیری شود. همچنین می‌توان قوانینی اعمال کرد که هر برنامه‌ای که خارج از فولدرهای ProgramFiles می باشد اجرا نشود یا اینکه فقط برنامه های امضا شده اجرا شوند. برای این کار می‌توان از نرم‌افزار Microsoft AppLocker استفاده نمود. این ابزار در ویندوز ۷ و ویندوز سرور ۲۰۰۸ برای جلوگیری از اجرای برنامه‌های ناخواسته طراحی شده است.

۲-۳-٦ بستن ارتباط با کانال‌های کنترل و فرماندهی باج‌افزار

می‌توان در هنگام شیوع باج‌افزار جدید از لیست‌های سیاه معتبر و بروز به‌منظور قطع ارتباط کاربران سازمان با سرورهای C&C باج‌افزارها استفاده کرد زیرا اغلب باج‌افزارها پس از نصب نیاز به ارتباط با سرورهای خود برای دریافت کلید و شروع فرآیند رمزنگاری دارند. اگرچه این راهکار به عنوان یک رویکرد جامع در مقابله با باج‌افزارها محسوب نمی‌شود اما یک گام مهم و سریع در غیر فعال کردن موقت آنها محسوب می‌شود. با قطع کردن موقت ارتباط با آدرس‌های منتشر کننده بدافزارهای باج‌گیر می‌توان از آلوده شدن سیستم‌های بیشتر در سازمان جلوگیری کرد. برای نمونه می توان با استفاده از فایروال سازمان، دسترسی به C&C را فیلتر کرد.

به دلیل استفاده از الگوریتم‌های تولید نام دامنه در کد برخی از باج‌افزارها، توصیه می‌شود از روش‌های شناسایی این گونه از نام‌های دامنه نیز در ترافیک سازمان استفاده شود. برخی از این نام‌های دامنه عبارتند از:

- yslkvbbummq.work
- vinbjwjfuq.su
- rbjuwkqhktemxvk.xyz
- aushewagwr.pw
- ymvbuagowoaucpbc.su
- yjhhhgtp.pw
- csdbxklkbfmljiomg.click
- ksbnorjlt.click

۴-۲ رصد اخبار امنیتی

با رصد مداوم اخبار امنیتی می‌توان مشخصات باج‌افزارهایی که به‌تازگی شناسایی شده‌اند را استخراج و از این اطلاعات برای اقدامات پیشگیرانه استفاده نمود.

۳. اقدامات ضروری حین مواجه شدن با سیستم آلوده

معمولاً آلودگی به باج‌گیر بسیار پر سرو صدا است و بلافاصله با نمایش یک پیغام بزرگ، تغییر تصویر پس‌زمینه ویندوز، فایل‌های راهنمای پرداخت باج، یا نهایتا باز نشدن فایل‌های اطلاعاتی مشخص می‌شود.

در صورت آلودگی به بدافزارهای باج‌گیر انجام اقدامات زیر ضروری است:

۱. قطع کردن سیستم آلوده از تمامی شبکه‌ها و خاموش کردن تمامی امکانات wireless از جمله Wi-Fi یا بلوتوث. تمامی دستگاه‌های ذخیره‌سازی مانند USB یا هارد درایوها را از سیستم جدا کنید.
۲. رایانه آلوده را در صورت امکان خاموش کرده و از روشن کردن مجدد آن خودداری شود. چرا که احتمال رمزگذاری چندباره روی فایل‌ها یا تکمیل عملیات رمزگذاری روی فایل‌هایی که به هر دلیلی مصون مانده‌اند، وجود دارد.
۳. اطلاع‌رسانی به سلسله مراتب درون سازمانی و مراجع ذی‌صلاح نظیر مرکز مدیریت راهبردی افتا جهت جلوگیری از انتشار بدافزار در سازمان و سایر سازمان‌ها
۴. از دستکاری سیستم آلوده تا حد امکان خودداری شود. اگر از داده‌ها پشتیبان وجود دارد بهتر است تا زمانیکه بدافزار پاکسازی نشده و روش آلودگی و روش جلوگیری از تکرار اتفاق پیدا نشده است، از بازیابی خودداری شود. چرا که وجود بدافزار ممکن است منجر به آلودگی مجدد (بلافاصله، یا با فاصله زمانی) شده و در بدترین حالت پشتیبان‌ها نیز از دست بروند.

در مورد سرویس‌های حیاتی که وقفه در ارائه آنها خسارات زیادی به بار می آورد، بهتر است سرویس روی سیستم دیگری مجدداً راه‌اندازی شود و سیستم اصلی برای بررسی نگهداری شود.

٤. اقدامات پس از حادثه

عملیات پس از حادثه اقداماتی را شامل می‌شود که باعث می‌شود که سیستم به حالت نرمال بازگردد و بتواند سرویس‌دهی کند. مراحل کاری متخصصان در برخورد با سیستم آلوده به قرار زیر است:

۱. شناسایی بدافزار عامل حادثه و حذف آن از سیستم جاری و سایر سیستم‌های مرتبط و پشتیبان توسط افراد متخصص
۲. بررسی شبکه برای یافتن تاثیر بدافزار در سایر نقاط شبکه (پوشه‌های اشتراکی در دسترس و غیره)
۳. مشخص شدن راه آلودگی به باج‌افزار و انجام اقدامات امن‌سازی بخش پیشگیری برای جلوگیری از تکرار آن
۴. سیستم پشتیبان را بروزرسانی کرده و ابتدا به صورت آزمایشی در مقابل عامل حادثه تست و ارزیابی کنید. در صورتی که سیستم پشتیبان درست کار کرد، آن را راه‌اندازی کرده و سپس در شبکه قرار دهید.
۵. رفتار سیستم و عامل حادثه را تا زمان پایداری سیستم و رفع بحران به صورت مناسب و شبانه‌روزی رصد کنید.

به‌منظور بازیابی اطلاعات روش‌های زیر توصیه می‌شوند که توسط افراد متخصص قابل استفاده است:

۱. بازیابی اطلاعات پشتیبان گرفته شده در صورت وجود و تست سیستم
۲. در صورت عدم وجود پشتیبان: بررسی ابزارها و راهکارهای موجود برای بازگردانی اطلاعات بدون پرداخت باج
   - برخی باج‌گیرها در صورت نگهداری ترافیک شبکه قابل بازیابی هستند و کلید در لاگ شبکه موجود است؛ لذا در حفظ لاگ‌ها کوشا باشید.
   - بخشی از اطلاعات شما می تواند توسط ابزارهای بازیابی (Data Recovery) بازیابی شود؛ لذا از دستکاری یا تغییر محتوای سیستم اجتناب گردد.
۳. جهت پرداخت باج به تنهایی تصمیم نگرفته و با سلسله مراتب خود مشورت نمایید؛ لازم به ذکر است که پرداخت باج لزوماً منجر به رمزگشایی نخواهد شد.
۴. در صورتیکه دستیابی به اطلاعات فوریت ندارد، می‌توان فایل‌های رمزشده را استخراج و نگهداری نمود، چرا که در آینده ممکن است روش رمزگشایی پیدا شده یا کلیدهای آن آزاد شود. (اتفاقی که برای بسیاری از باج‌گیرها با گذر زمان افتاده است.)