برای جلوگیری از آلوده شدن به باج‌افزارها چه باید کرد؟

در این نوشتار قصد داریم که مروری مختصر روی مهمان‌های ناخوانده امروزی که به سرورها نفوذ می‌کنند داشته باشیم. در دنیای فناوری این مهمان ناخوانده به باج‌افزارها معروفند.

خوب است بدانید در باج‌افزارهای مدرن که از سال ۲۰۱۷ که در کشورهای مختلفی منتشر شده‌اند مانند NotPetya، Petya، WannaCry و Locky از مدل‌های رمزنگاری دوگانه استفاده شده است. این باج‌افزارها از رمزنگاری AES و RSA برای قفل کردن فایل‌های قربانیان استفاده می‌کند. این سوءاستفاده از تکنولوژی تقریبا دی‌کُد کردن فایل‌ها توسط محققین امنیت را غیر ممکن می‌کند.

اگر قرار باشد به موضوع امنیت و نگهداری داده‌ها از زاویه دید باج‌افزارها نگاه کنیم باید به این سئوال جواب دهیم که چطور فایل‌ها را قفل کنیم که کسی جز خود باج‌افزار نتواند آنها را مجدد بازگشایی کند؟ برای رسیدن به جواب این پرسش باید مجموعه‌ای از مقدمات در مورد الگورتیم‌های رمزنگاری را بررسی کنیم و بفهمیم که استفاده از هر یک از مدل‌های رایج برخورد با باج‌افزارها دارای چه نقاط قوت و ضعفی هستند.

باج‌افزارهایی فقط با رمزنگاری متقارن

الگورتیم‌های رمزنگاری متقارن مانند AES می‌توانند برای رمزنگاری فایل‌هایی با سرعت بسیار بالا، استفاده شوند. این دست باج‌افزارها که فقط از این مدل الگورتیم‌ها استفاده می‌کنند همه فایل‌های کاربر را سریعا رمزنگاری کرده و روی دیسک به همراه کلید رمزنگاری، ذخیره می‌کنند. زمانی که قربانی مورد هدف، باج را پرداخت می‌کند باج‌افزار به بازگشایی همه فایل‌ها با کلیدهای متناظر با آنها که روی دیسک ذخیره شده‌اند، اقدام می‌کند. این روش به محققین این اجازه را می‌دهد که بعد از جستجوی دیسک و یافتن کلیدها، ابزاری را تولید کنند که فرآیند بازگشایی همه فایل‌های کاربر را یک به یک و با استفاده از این کلیدهای یافت شده، طی کند.

رمزنگاری غیرمتقارن سمت کاربر

در این مدل باج‌افزار یک جفت کلید RSA تولید و همه فایل‌ها را با استفاده از کلید عمومی رمزنگاری و کلید خصوصی آن را در سرور مرکزی، ذخیره و نگهداری می‌کند. این مدل رمزنگاری که معمولا در دسته الگورتیم‌های کُند قرار می‌گیرد برای فایل‌های بزرگ بسیار زمان‌بر است. مشکل دیگری که این الگورتیم به همراه دارد این است که باید کلید خصوصی در سرور قربانی تولید و سپس برای نگهداری به سرور مرکزی باج‌افزار ارسال شود. برای تحقق این هدف که کلید خصوصی به سرور مرکزی منتقل شود می‌بایست سرور قربانی دسترسی به اینترنت داشته و سرور مرکزی نیز آنلاین باشد. به همین دلیل اگر ارتباط هر یک از این دو عامل قطع باشد این ریسک وجود دارد که باج‌افزار نتواند کلید خصوصی را به سمت سرور مرکزی ارسال کند و همه اطلاعات قربانی برای همیشه به صورت رمزنگاری شده باقی بمانند.

رمزنگاری غیرمتقارن سمت سرور

در این روش، سرور مرکزی باج‌افزار یک جفت کلید تولید می‌کند که توسط باج‌افزار در سرور قربانی، دانلود می‌شود. با این روش پس از اینکه قربانی باج را پرداخت کرد باید فایل‌های کاربر رمزگشایی شوند؛ به همین دلیل باید کلید خصوصی مورد نظر برای قربانی ارسال شود تا فرآیند لازم برای بازگشایی رقم بخورد. تا اینجا از نظر منطقی مشکلی وجود ندارد؛ اما این ریسک وجود دارد که بعد از ارائه کلید خصوصی، قربانی این فایل برای دیگر قربانیان به اشتراک بگذارد. به عبارت دیگر کلید خصوصی برای همه افشاء شود.

راه حل دیگر این است که باج‌گیر از قربانی بخواهد که همه فایل‌های آلوده خود را بر روی سرور مرکزی، آپلود کند تا فرآیند رمزگشایی توسط خود باج‌گیر با رمز خصوصی که در اختیار دارد، انجام شود. در این روش از کلید خصوصی محافظت می‌شود؛ اما برای فایل‌های حجیم روی بستر اینترنت این امکان به هیچ‌وجه وجود ندارد.

رمزنگاری غیرمتقارن سمت سرور و کاربر + رمزنگاری متقارن

این مدل از رمزنگاری یعنی الگوریتم‌های دوگانه در اکثر باج‌افزارهای مدرن امروزه استفاده می‌شود. یعنی هم رمزنگاری متقارن و هم رمزنگاری نامتقارن در این مدل استفاده می‌شود؛ به طوریکه برای رمزنگاری نیازی به اینترنت و ارتباط با سرور مرکزی باج‌افزار وجود ندارد. برای بازگشایی فقط باید کلیدی از سرور مرکزی باج‌افزار دریافت شود که این امر منطقا از طریق اینترنت انجام می‌شود. در این مدل هم سرور مرکزی و هم باج‌افزار در سرور قربانی نصب می‌شوند و 2 کلید RSA مربوط به خود را تولید می‌کنند.

در این نوشته ما کلیدها را به نحو زیر نامگذاری می‌کنیم:

• gPub.key برای کلید عمومی ساخته شده در سیستم قربانی.
• gPriv.key برای کلید خصوصی ساخته شده در سیستم قربانی.
• Spub.key برای کلید عمومی ساخته شده در سرور مرکزی باج‌افزار.
• Spriv.key برای کلید خصوصی ساخته شده در سرور مرکزی باج‌افزار.

در ادامه نحوه کار این باج‌افزارهای مدرن را با یک مثال، بررسی می‌کنیم:
برای هر سیستمی که آلوده می‌شود باج‌افزار، فایل‌های Cpub.key و Cpriv.key را در لحظه به صورت آفلاین تولید می‌کند. کلید Spub.key را هم که درون خود به صورت Hardcode شده به همراه دارد. در مرحله بعدی کلید Cpriv.key را به وسیله Spub.key رمزنگاری و سپس رمزنگاری همه‌ی فایل‌ها را با استفاده کلید AES آغاز می‌کند. در آخر، همه کلیدهای AES را توسط Cpub.key رمزنگاری می‌کند.
برای اینکه قربانی بتواند فایل‌های خود را رمزگشایی کند نیاز به کلیدهای AES دارد که متاسفانه این کلیدها توسط gPub.key رمزنگاری شده‌اند. برای بازگشایی کلیدهای AES وجود کلید gPriv.key الزامی است که مجددا متاسفانه gPriv.key توسط کلید Spub.key رمزنگاری شده است. برای بازگشایی کلید gPriv.key وجود Spub.key الزامی است و این تنها سرور مرکزی باج‌افزار است که می‌تواند این کلید را ارائه دهد.

ضعف های منطقی رایج در باج‌افزارهای مشهور

WannaCry : علیرغم اینکه این باج‌افزار از روش اشاره شده در بالا برای آلوده کردن سیستم‌های قربانیان استفاده کرده است؛ اما محققین امنیتی موفق شده‌اند که اعداد اولی که در تولید جفت کلیدهای RSA استفاده شده‌اند را با توجه به اطلاعات موجود در

RAM سیستم کامپیوتر به شرطی که خاموش نشده باشد را استخراج و کلید خصوصی را بازسازی کنند.

Bad Rabbit: محققین کشف کرده‌اند که کلیدهای لازم برای بازگشایی به طور کامل از روی RAM و حتی فایل‌های Windows Shadow Copy حذف نمی‌شوند که همین امر به قربانی اجازه می‌دهد که از مکانیزم Restore موجود در خود ویندوز به منظور بازیابی اطلاعات استفاده کند.

Harasom: این باج‌افزار از آن دسته باج‌افزارهای ساده‌ای است که یک کلید را به صورت مشترک برای همه قربانیان استفاده می‌کند به همین دلیل محققین به راحتی می‌توانند این کلید را کشف و استفاده کنند.

راه‌های جلوگیری از آلوده شدن به باج‌افزارها

می‌توان از یک استراتژی سه لایه برای جلوگیری از مهمان‌های ناخوانده استفاده کرد که آنها را با هم مرور کنیم:

آموزش: اولین و اصلی‌ترین لایه به نظر تعداد زیادی از مختصیص، بخش آموزش است. در این بخش باید به کاربران خود آموزش دهید که چه برخوردی در مواجه با فایل‌های ناشناس ایمیل‌های مشکوک، سایت‌های عجیب داشته باشند. باج‌افزارها در عین پیچیدگی عملیاتی بعد از آلودگی و حمله به سیستم قربانی، شرایط انتشارهای بسیار ساده‌ای را در دسترس دارند.

آنتی‌ویروس: دومین لایه برای جلوگیری از نفوذ این مهمان‌های ناخوانده به قلعه شما در صورتی که کاربر آموزش دیده عمدا یا سهوا روی لینک عجیبی یا فایل مخربی کلیک کند، استفاده از آنتی‌ویروس Endpoint برای سیستم‌های کاربران است. این آنتی‌ویروس

با توجه به آنالیزی از ترافیک شبکه‌ای، همه فایل‌های سیستم و فایل‌های ورودی و خروجی سیستم را پایش می‌کند و بر اساس رفتار نرم‌افزار و Signature باج‌افزارها را تشخیص و حذف می‌کند. به همین دلیل، توصیه می‌شود که این دست ابزارها در سازمان خودتان حتما استفاده کنید.

نسخ پیشتیبان: می‌توان از این لایه به عنوان قوی‌ترین دیوار دفاعی نام برد. یادتان باشد همیشه از فایل‌های سیستم‌های حیاتی به اندازه نیاز **نسخ پشتیبان** تهیه کنید. درباره سرورهایی که نقش پایگاه داده در شبکه شما را ایفا می‌کنند نگرانی جدی وجود ندارد؛ چون معمولا نرم‌افزارهای سروری پایگاه داده که در سطح سازمانی استفاده می‌شوند مانند SQL Server یا Oracle و یا MySQL خودشان مکانیزم‌های تهیه نسخ پشتیبان را به حد نیاز دارند. این ابزارها فقط به تنظیم و نگهداری دقیق نیاز دارند تا مشخص شود هرکدام را باید چه زمانی و با چه مدل پشتیانی می‌توان تهیه کرد و هریک از نسخ پیشتیبان تا چه بازه زمانی قابلیت حفاظت دارند.

در مورد دیگر سرور و سیستم‌های کاربران باید از فرآیند بکاپ‌گیری مانند VSS Shadow Copy برای سیستم‌های ویندوزی و یا LVM و تهیه کپی از فایل‌ها به صورت سریع و مخفی، استفاده کرد.