به‌روزرسانی جدید باج‌افزار Sam Sam

فهرست مطالب

۱ مقدمه

شرکت Sophos[۱] دریکی از جدیدترین فعالیت‌های خود, یک آنالیز دقیقی از گروه بسیار خطرناک باج‌افزار، که تحت عنوان SamSam نام‌گذاری شده، ارائه کرده است. آزمایشگاه FortiGuard به‌عنوان عضوی از Fortinet[2] با اتحادیه تهدید سایبری (CTA), کلیه شاخص‌های مرتبط با این تسخیر (IoCs[3]) را قبل از انتشار، برای اطمینان از اینکه مشتریان FortiGuard از آخرین افشا، محافظت می‌شوند, دریافت کرده است. باج‌افزار SamSam، برای اولین بار در اواخر سال ۲۰۱۵ به‌عنوان یک خطر با مشخصه ریسک پایین، ظاهر شد. ولی از آن موقع به‌شدت گسترش‌یافته است و طیف وسیعی از سازمان‌ها، مؤسسات بهداشت و درمان و آموزش‌وپرورش و دولت‌های محلی را مورد هدف قرار داده است. Sophos برآورد کرده است که تا به امروز، گروه مسئول SamSam تقریباً شش میلیون دلار از قربانیان خود اخاذی کرده است. SamSam با کمک یک استراتژی متمرکز جهت بهره‌برداری از آسیب‌پذیری‌ها و سپس به‌صورت انتقال جانبی در طول شبکه به‌سمت هدف شناسایی‌شده، ماشین‌های قفل‌شده را مورد هدف قرار می‌دهد. جهت جلوگیری از تشخیص، این حملات معمولاً در زمان حساب‌شده، بعد از ساعات کاری، انجام می‌شود. مهاجمان پس از انجام شناسایی، نفوذ به دستگاه‌های هدف را تا زمانی که شرایط محیطی برای حمله مناسب نباشد، انجام نمی‌دهند. در زمان مناسب SamSam، به‌طور هم‌زمان به تمام دستگاه‌های شناسایی‌شده، حمله می‌کند و این باعث می‌شود که محافظت دستگاه‌ها مشکل شود. مهاجمان SamSam ترکیبی از ابزارهای متداول مانند pen testing و ابزار post-exploitation

[۱] https://www.sophos.com/en-us.aspx

[۲] https://www.fortinet.com

[۳] https://searchsecurity.techtarget.com/definition/Indicators-of-Compromise-IOC

(Mimikatz) جهت به‌دست‌آوردن اعتبار و از ابزار PSexec جهت انتقال در طول سازمانی که در آن، SamSam به صورت دستی نصب شده است، استفاده می‌کنند. این روش معمولاً موثر است چون هیچ هشداری را فعال نمی‌کند و دستگاه‌های امنیتی به‌طور معمول چنین ترافیکی را به‌عنوان فرمان‌های قانونی از شخصی داخل سازمان، در نظر می‌گیرند. و ازآنجایی‌که مهاجمان بدافزار SamSam را به‌طور دستی نصب می‌کنند، اغلب این فرآیند توسط مدیران سیستم یا شبکه یا بسیاری از ابزارهای دفاعی (محافظتی) AV و IPS، قابل‌تشخیص نیست. نگرانی فقط مربوط به فایل‌های ارزشمند مورد هدف (اسناد، داده‌ها و غیره) نیست، بلکه فایل‌های پیکربندی مانند فایل‌هایی که در مایکروسافت آفیس هستند نیز برای ایجاد اخلال، موردحمله قرار می‌گیرند.

۲ حفاظت از سازمان در مقابل SamSam و باج‌افزارهای دیگر

باج‌افزار به‌شدت در تخریب سازمان مؤثر است و اغلب کسب‌وکارهای کاملاً دیجیتال، ازجمله مؤسسات مالی و مراکز بهداشتی، را مجبور به انجام معاملات پیچیده و بزرگ با استفاده از مداد و کاغذ (غیرمکانیزه) می‌کند. ازآنجایی‌که بسیاری از سازمان‌ها، مدت زمان خرابی را معادل ده‌ها، صدها یا هزارها دلار ارزیابی می‌کنند لذا نیاز به بازگرداندن عملیات سیستم دارند و این موضوع، سازمان را به پرداخت هزینه‌های باج جهت بازکردن دستگاه‌ها و شبکه‌ها، هدایت می‌کند. بااین‌حال، هیچ تضمینی وجود ندارد که پرداخت باج، کلیدهای ضروری جهت بازکردن دستگاه‌ها را فراهم کند و یا اینکه سیستم‌های به خطرافتاده دوباره به خطر انداخته نشوند چون مجرمان می‌توانند چنین حمله‌ای را تکرار کنند.

بهترین پاسخ به باج‌افزار SamSam این است که مجهز و آماده‌باشیم.

۳ به‌روزرسانی دستگاه‌ها، نرم‌افزارها و برنامه‌های کاربردی

اغلب رخنه‌های باج‌افزاری با بهره‌برداری از آسیب‌های وصله‌نشده، آغاز می‌شود. و اغلب اوقات، این آسیب‌پذیری‌هایی برای هفته‌ها، ماه‌ها و حتی سال‌ها در دسترس بوده‌اند. سازمان‌ها باید سخت‌افزارها، نرم‌افزارها و برنامه‌های کاربردی، آسیب‌پذیری‌ها و خطرات خود را اولویت‌بندی کرده و سپس یک فرآیند منظم برای مدیریت تمام بخش‌های لازم و به‌روزرسانی‌ها، پیاده‌سازی کنند.

نادیده گرفتن این روش امنیتی، سازمان‌ها را به حملات ازجمله SamSam حساس می‌کند، حتی زمانی که از حملات ساده و پایه‌ای شبکه استفاده می‌شود تا در شبکه رخنه ایجاد شود.

۴ مدیریت دسترسی و اعمال راه‌حل‌های Segmentation داخلی

جهت محدودکردن و همچنین گسترش تهدیدات، سازمان‌ها باید از مدیریت دسترسی قوی همراه با بخش‌بندی شبکه امن، جهت جداسازی دستگاه‌ها و داده‌ها، استفاده کنند تا اطمینان حاصل شود که حتی کسانی که دارای دسترسی ممتاز به کل شبکه دارند، نمی‌توانند دستگاه‌های تسخیرشده را ببینند.

مدیریت دسترسی نیاز به احراز هویت کاربران و برنامه‌های کاربردی که به دنبال دسترسی به اطلاعات حساس و به‌روزرسانی نرم‌افزار هستند، دارد و روش‌هایی مانند احراز هویت دو عامله، تک نشانه و حتی بیومتریک قابل استفاده است. بخش‌بندی شبکه همچنین می‌تواند کانال‌های دسترسی جداگانه و امن برای مواردی مانند دستگاه و مدیر سیستم، فراهم کند.

۵ مدیریت ترافیک پایه

به دلیل روند رو به رشد نرم‌افزارهای مخرب در استفاده از pen testing و ابزارهای مدیریت، به‌منظور بارگیری بر روی سیستم‌های هدف، بسیار مهم است که تمام فعالیت‌های ترافیکی و فعالیت‌های مدیریتی

برنامه‌ریزی شود. این مورد به سیستم آنالیز رفتاری اجازه می‌دهد تا سریعاً در مورد رویدادهای غیرمنتظره یا غیرمعمول مدیریتی، نظیر پیکربندی دستگاه، هشدار دهد.

۶ پشتیبان‌گیری از داده‌ها

به‌جای پرداخت باج، یک واکنش مؤثر، جایگزینی سیستم‌عامل، نرم‌افزار و برنامه‌های تسخیرشده با نسخه پشتیبان سالم تهیه‌شده، است. این راه‌حل نیاز به چند مرحله دارد. اول، پشتیبان‌گیری باید به‌صورت مرتب انجام شود تا رخنه ایجادشده بین زمانی که یک حمله شناسایی‌شده تا آخرین پشتیبان سالم را برطرف کند. پشتیبان‌گیری باید به دنبال نرم‌افزارهای مخرب و سایر ناهنجاری‌ها باشد. چون نمی‌خواهید با استفاده از یک پشتیبان که شامل همان نرم‌افزارهای مخرب است یک دستگاه به خطر بیافتد. درنهایت، مدیران باید این پشتیبان‌گیری را خارج از شبکه ذخیره کنند، بنابراین آن‌ها در طول حمله یا پس از آن خراب نمی‌شوند و همیشه در دسترس هستند.

۷ راه‌حل‌ها و محافظت‌ها

آزمایشگاه FortiGuard تمامی IOCs را برای SamSam که در وبلاگ Sophos نوشته‌شده است را مورد آنالیز قرارداده است و گزارش داده که حافظت‌های AV در همه نمونه‌های شناخته‌شده، وجود دارد:

W۳۲/Samas.C!tr

MSIL/Kryptik.BV!tr

MSIL/Filecoder_Samas.B!tr

W۳۲/Generik.BV!tr

W۳۲/Samas.F!tr

W۳۲/Kryptik.BV

W۳۲/Agent.PCS!tr.spy

W۳۲/MSIL.LGG!tr

W۳۲/MSIL.LGF!tr

BAT/RansRun.A!tr

W۳۲/Generik.BW!tr

MSIL/Kryptik.BW!tr

W۳۲/Ransom.EWU!tr

MSIL/Filecoder.AR!tr

W۳۲/STUBDCRYP.A!tr

W۳۲/RUNNER.GBB!tr

PossibleThreat

MSIL/Generic.AP.٦٤٣٧٠!tr

MSIL/Injector.JAX!tr

MSIL/Generic.AP.١١FED٦!tr

MSIL/Generic.AP.FC٧CE!tr

Trojan.FNEY!tr

MSIL/Generic.AP.A٨٦٤٢!tr

W۳۲/Samas.A!tr

Trojan.FLLL!tr

W۳۲/Generic.A!tr

MSIL/Generic.AP.٧٠DAA!tr

MSIL/KillFiles.Y!tr

Generik.DHAHMQP!tr

MSIL/Generic.AP.٥AC٨٠!tr

Trojan.FLAI!tr

Ransomware.SAMAS!tr

W۳۲/Agent.SFI!tr

MSIL/Samas.B!tr

W۳۲/Samas.AB!tr

W۳۲/DELETER.SEA!tr

W۳۲/Agent.B!tr

Ransom.A!tr

Ransom!tr

W۳۲/Agent.XN!tr

W۳۲/Ransom.DSR!tr

MSIL/Filecoder_Samas.A!tr

Trojan.O!tr

W۳۲/MSIL.GWZ!tr

W۳۲/Tpyn.A!tr

Generik.FIXATIN!tr

W۳۲/MSIL.GJR!tr

W۳۲/Tpyn.SAMAS!tr

Trojan.SAMAS!tr

W۳۲/Tpyn.CHU!tr

MSIL/Ransomware.FHD!tr

Ransomware.FHD!tr

W۳۲/MSIL.FZL!tr

W۳۲/RansmSam.A!tr

W۳۲/MSIL.FZK!tr

BAT/Starter.B!tr

MSIL/Agent!tr

Trojan.I!tr

Ransomware.FDL!tr

W۳۲/Samas.AR!tr

W۳۲/Deshacop.BMV!tr

W۳۲/Mimikatz.A!tr

W۳۲/Kryptik.BV

همچنین تمامی URIهای مربوط به این حمله، توسط فیلتر وب‌سایت آزمایشگاه FortiGuard، به لیست‌سیاه اضافه‌شده است.

۸ منابع

https://www.fortinet.com/blog/threat-research/critical-samsam-ransomware-update.html