۶ گام برای مقابله با باج افزارها

مقدمه

باج افزارها یکی از سه تهدید مهم حال حاضر دنیای فناوری اطلاعات هستند که باتوجه به نقاط ضعف و سهل انگاری ها در زمینه ملاحظات امنیتی، نحوه مقابله با این قبیل حوادث جزء ابهامات و دغدغه‌های اصلی کارشناسان ذیربط است. فرض کنید اکنون در سیستم یکی از کاربران علایم باج افزار مشاهده شده و کلیه اطلاعات محلی و شبکه شما رمز شده است. شما بعنوان کارشناس امنیت، اولین اقدامی که انجام خواهید داد، چه خواهدبود؟ با چه مرجعی تماس می گیرید؟ اطلاع رسانی به کارکنان و مشتریان کسب و کارتان چگونه خواهدبود؟ و سوالاتی از این دست که وقتی در بطن ماجرا قرار بگیرید، اهمیت آمادگی و اقدام صحیح و به موقع روشن خواهدشد. در این محتوی سعی شده است، اقدامات عملی و استاندارد مواجهه با این رویداد و اتخاذ تدابیر لازم در زمان وقوع حادثه معرفی شود.

- آمادگی اولیه
  - دانش خود را در زمینه خط مشی های(۱) امنیتی سیستم عاملهای رایج افزایش دهید.
  - دانش خود را در زمینه خط مشی های رایج نمایه(۲)کاربران افزایش دهید.
  - از به‌روزبودن محصولات امنیتی داخل و لبه شبکه اطمینان حاصل نمایید.
  - از آنجاکه این تهدید اغلب ازطریق کاربران نهایی درک و گزارش می شود، سعی کنید آگاهی نیروهای پشتیبان فناوری اطلاعات را از این حیث ارتقاء بخشید.
  - نسبت به وجود پشتیبان های جامع، به‌روز و در دسترس از داده‌های شبکه و محلی کاربران اطمینان حاصل کنید.

- شناسایی تهدید:

علایم عمومی ظهور باج افزار

۲-۱)دریافت ایمیل‌های شغلی عجیب (عموماً در ظاهر مبدل صورتحساب) که دارای پیوست هستند.

۲-۲)ظهور یک پیام باج‌خواهی روی دسکتاپ کاربر با مضمون رمزشدن اطلاعات و مطالبه وجه برای رفع مشکل (شکل ۱)

شکل ۱) پیام باج افزار واناکریپت در دسکتاپ کاربر

۲-۳)شکایت کاربران از حذف یا خراب‌شدن فایلهای محلی یا شبکه یا تغییر عجیب پسوند فایلها نظیر(aaa. , xyz. , abc.)

۲-۴)تغییر تعداد بیشماری از فایل‌های شبکه در مدت زمان بسیار کوتاه

علایم مبتنی بر میزبان(۳)

۲-۵)جستجو کنید آیا کدهای باینری اجرایی در پروفایل کاربران (%APPDATA% , %ALLUSERSPROFILE%) و نیز %SystemDrive%وجود دارد؟

۲-۶) مضمون پیامهای باج‌افزاری و وجود پسوندهای عجیب نظیر بند ۲-۳ را بررسی کنید.

۲-۷) درصورت امکان از حافظه رایانه یک تصویر تهیه کنید (۴)

۲-۸) در خصوص وقوع فرآیندهای غیرمعمول، جستجو و بررسی انجام دهید.

۲-۹) در زمینه وجود الگوهای غیرعادی پیوست ایمیل‌ها، بررسی انجام دهید.

۲-۱۰) فعالیتهای غیرعادی مرورگر وب یا شبکه‌تان خصوصاً تلاش برای ارتباط با آی‌پی‌های Tor , I2Pو وب‌سایتهای پرداخت بیت کوین را بررسی کنید.

علایم مبتنی بر شبکه

۲-۱۱) الگوهای ارتباطی با منابع مخرب (۵) را جستجو و درصورت وجود، بررسی کنید.

۲-۱۲) الگوهای ارتباطی با منابع باج‌افزاری (۶) را جستجو و درصورت وجود، بررسی کنید.

۲-۱۳) در این قسمت نیز موارد ۲-۹ و ۲-۱۰ را انجام دهید.

- **مهار**

۳-۱) ارتباط تمام رایانه‌هایی که در معرض خطر هستند، از شبکه قطع کنید.

۳-۲) درصورتی‌که امکان ایزوله‌سازی رایانه‌ها وجود ندارد، ارتباط شبکه درایوهای اشتراکی(۷) را قطع نمایید.

۳-۳) ترافیک به سمت سرورهای فرمانی-کنترلی باج‌افزارها(۸) را بررسی و مسدود نمایید.

۳-۴) الگوهای ناشناخته مشاهده‌شده را برای پشتیبان امنیت نهایی(مشاور امنیت شبکه برون‌سازمانی) خود ارسال نمایید.

۳-۵) آدرسهای آی‌پی، نامهای دامنه و آدرسهای وب ناشناس مخرب را برای مسئول امنیت داخلی سازمان ارسال کنید.

- **ترمیم**

۴-۱) تمامی کدهای باینری را از پروفایلهای آسیب‌دیده (%APPDATA% , %ALLUSERSPROFILE%) و همچنین %SystemDrive% بیابید و حذف کنید.

۴-۲) اگر مورد فوق مقدور نبود، به ناچار بایستی یک ایمیج پاک از ویندوز برگردانید.

- **بازیابی**

هدف :بازگشت سیستم به حالت عادی پیش از حمله

۵-۱) آنتی ویروس‌تان را به نحوی بروزرسانی نمایید که کدهای باینری مخرب را دفع نماید.

۵-۲) اطمینان حاصل نمایید قبل از برقراری ارتباط بین سیستمها هیچ کد باینری مخربی درون آنها موجود نباشد.

۵-۳) مطمئن شوید ترافیک شبکه به حالت عادی اولیه بازگشته باشد.

۵-۴) مستندات و داده های کاربران را از آرشیوها بازگردانید.

تمامی مراحل فوق بایستی گام به گام و همراه با مانیتورینگ فنی انجام شوند.

- **مستندسازی**

تهیه گزارش

بایستی پس از رفع آسیبها و بازگشت فعالیتها به روند عادی، یک گزارش از حادثه تهیه شود به‌طوری‌که در دسترس همه دست‌اندرکاران قرار گیرد.

گزارش بهتر است شامل مضامین زیر باشد:

- نحوه شناسایی اولیه حادثه
- اقدامات و جداول زمانی عملکردها
- اقداماتی که بدرستی انجام شدند.
- اقداماتی که به اشتباه انجام شدند.
- هزینه حادثه برای سازمان

- **سرمایه‌گذاری:**
- لازم است اقدامات مربوط به بهبود فرآیندهای شناسایی تهدیدات شبکه و بدافزارها تعریف شود تا در راستای این تجربه، سرمایه‌گذاری لازم صورت گیرد.

منبع:

- IRM #۱۷

Web: https://cert.societegenerale.com

IRM Author: CERT SG / Jean-Philippe Teissier

IRM version: ۱.۰

E-Mail: cert.sg@socgen.c

(۱) Policy

(۲) Profile

(۳) Host

(۴) Capture a memory Image

(۵) Exploit Kits

(۶) Ransomware C&C

(۷) Shared Drives

(۸) Ransomeware’s C&C