SOPHOS
Cybersecurity delivered.

تاثیر تخریب نسخه‌های پشتیبان در حملات باج‌افزاری

بر اساس نظرسنجی شرکت امنیتی سوفوس از ۲،۹۷۴ سازمانی که طی سال ۲۰۲۳ هدف حمله باج‌افزاری قرار گرفتند

شبکه گستر
امنیت شما | وظیفه ما

مقدمه

دو راه برای بازیابی داده‌های رمزگذاری‌شده در یک حمله باج‌افزار (Ransomware Attack) وجود دارد؛ برگرداندن فایل‌ها از طریق نسخه‌های پشتیبان (Backup) و یا پرداخت باج به مهاجمان. تخریب نسخه‌های پشتیبان توسط مهاجمان، آنها را قادر می‌سازد تا توانایی قربانی را در بازیابی داده‌های رمزگذاری‌شده محدود کرده و با این کار، راهی جز پرداخت باج برای سازمان باقی نگذارند.

این گزارش تجزیه و تحلیل عمیقی از میزان تأثیر تخریب نسخه پشتیبان در جریان یک حمله باج‌افزاری ارائه می‌دهد. همچنین میزان فراوانی این تکنیک مهاجمان را به روشنی نمایش می‌دهد.

مروری بر این بررسی

یافته‌های این گزارش، بر اساس نظرسنجی از ۲،۹۷۴ متخصص فناوری اطلاعات/امنیت سایبری که سازمان‌هایشان در سال گذشته میلادی مورد حمله باج‌افزار قرار گرفته ارائه شده است. نظرسنجی مذکور به سفارش شرکت Sophos و توسط آژانس تحقیقاتی مستقل Vanson Bourne در ژانویه و فوریه ۲۰۲۴ انجام شده است. شرکت‌کنندگان در این نظرسنجی، متخصصان شاغل در سازمان‌های کوچک و متوسط با ۱۰۰ تا ۵،۰۰۰ کارمند در کشورهای استرالیا، اتریش، برزیل، فرانسه، آلمان، هند، ایتالیا، ژاپن، سنگاپور، آفریقای جنوبی، اسپانیا، سوئیس، بریتانیا و ایالات متحده بوده‌اند.

خلاصه مدیریتی

پیامدهای مالی و عملیاتی تخریب نسخه‌های پشتیبان در حملات باج‌افزاری بسیار زیاد است. هنگامی که مهاجمان، موفق به تخریب نسخه‌های پشتیبان می‌شوند، سازمان تقریباً دو برابر بیشتر احتمال دارد که باج را بپردازد و هزینه‌ای را از بابت بازیابی متحمل می‌شود که هشت برابر بیشتر از کسانی است که نسخه‌های پشتیبان آنها تحت تأثیر قرار نگرفته است.

شناسایی و متوقف کردن عوامل مخرب، قبل از به خطر افتادن نسخه‌های پشتیبان، شما را قادر می‌سازد تا تأثیر حمله باج‌افزار بر سازمانتان را به میزان قابل‌توجهی کاهش دهید. سرمایه‌گذاری در حفاظت از نسخه‌های پشتیبان، انعطاف‌پذیری و میزان مقاومت در برابر حملات باج‌افزاری را افزایش داده و هزینه کل مالکیت (TCO) امنیت سایبری سازمان را کاهش می‌دهد.

درس اول:

گردانندگان حمله باج‌افزاری، تقریباً، همیشه برای تخریب نسخه‌های پشتیبان شما تلاش می‌کنند

۹۴ درصد از سازمان‌هایی که در سال میلادی گذشته مورد حمله باج‌افزار قرار گرفتند، گفته‌اند که مجرمان سایبری سعی کرده بودند تا در طول حمله، به نسخه‌های پشتیبان، دست‌درازی و آنها را تخریب کنند.

نمودار زیر، درصد حملات باج‌افزاری که در جریان آنها مهاجمان برای تخریب نسخه‌های پشتیبان، تلاش کرده‌اند را به تفکیک هر حوزه نمایش می‌دهد.

درصد حملات باج‌افزاری که در جریان آنها مهاجمان برای تخریب نسخه‌های پشتیبان، تلاش کرده‌اند

درس دوم:

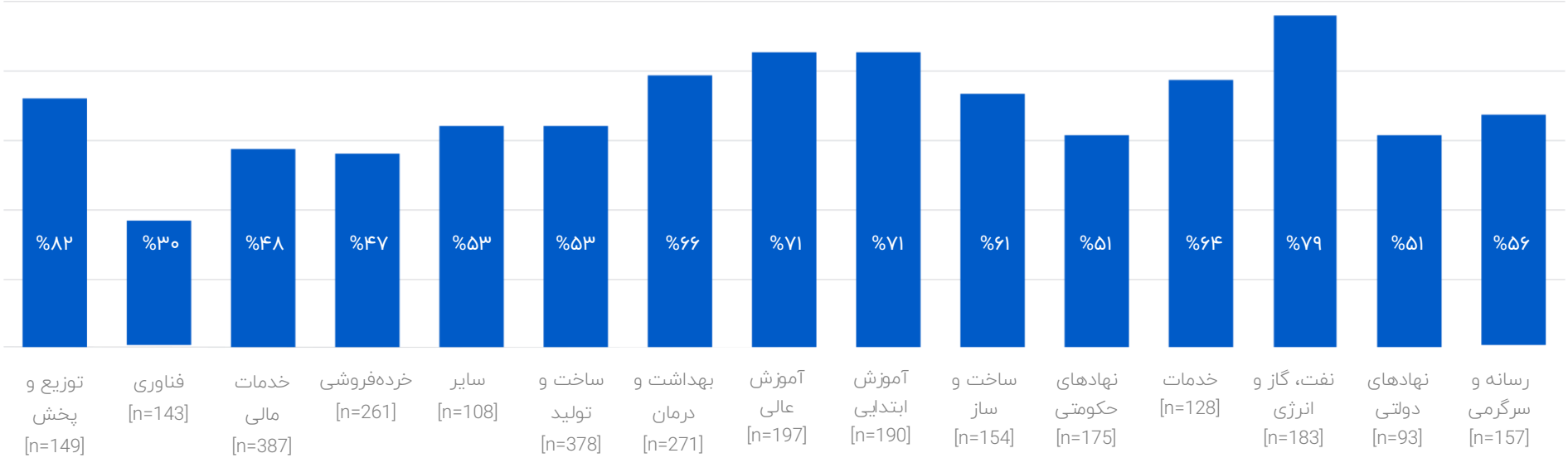
نرخ موفقیت در تخریب، در صنایع مختلف به‌شدت متفاوت است

در تمام حوزه‌ها، ۵۷ درصد از تلاش‌ها برای تخریب نسخه‌های پشتیبان، موفقیت‌آمیز بوده است. به این معنی که مهاجمان توانستند بر عملیات بازیابی اطلاعات بیش از نیمی از قربانیان خود تأثیر بگذارند. آمار موفقیت مهاجمان، بسته به حوزه‌ای که سازمان قربانی در آن فعال است بسیار متفاوت بوده است:

- تخریب موفق نسخه پشتیبان سازمان‌هایی که در بخش‌های نفت، گاز و انرژی و آموزش فعال بوده‌اند در مقایسه با سایرین بالا بوده است.
- در مقابل، مهاجمان در سازمان‌های فعال در حوزه فناوری و خرده‌فروشی، کمترین نرخ موفقیت را در دست‌درازی به نسخه‌های پشتیبان داشته‌اند.

چندین دلیل احتمالی در پشت پرده این تفاوت‌ها وجود دارد. ممکن است شرکت‌های فعال در حوزه فناوری از سازوکارهای قوی‌تری برای حفاظت از نسخه‌های پشتیبان خود برخوردار باشند. آنها همچنین ممکن است در شناسایی و توقف اجرای حمله، پیش از اثرگذاری مهاجمان بر روی نسخه‌های پشتیبان، بهتر عمل کرده باشند.

از سویی دیگر، سازمان‌های فعال در حوزه نفت، گاز و انرژی ممکن است درصد بالاتری از حملات پیشرفته و پیچیده را تجربه کرده باشد. علت، هر چه باشد، تأثیر آن قابل توجه بوده است.



میزان موفقیت در تخریب نسخه‌های پشتیبان توسط مهاجمان

درس سوم:

اخاذی دو برابری در صورت تخریب نسخه‌های پشتیبان

رمزگذاری داده‌ها

۸۵ درصد از سازمان‌هایی که نسخه‌های پشتیبان آنها معدوم شده، گفته‌اند که مهاجمان قادر به رمزگذاری داده‌های آنها بودند؛ در مقایسه با ۵۲ درصد از سازمان‌هایی که نسخه‌های پشتیبان آنها در امن باقی مانده بوده.

باج‌گیری

مبلغ اخاذی‌شده از سازمان‌هایی که نسخه‌های پشتیبان آنها مورد دست‌درازی قرار گرفته بود، به‌طور متوسط بیش از دو برابر سازمان‌هایی است که نسخه‌های پشتیبان‌شان از گزند مهاجمان در امان مانده. به نظر می‌رسد مهاجمان احساس می‌کنند در صورت موفقیت در تخریب نسخه‌های پشتیبان، در موقعیت برتری قرار دارند و می‌توانند مبلغ بیشتری را مطالبه کنند.

نرخ پرداخت باج

سازمان‌هایی که نسخه‌های پشتیبان آنها تخریب شده بود، تقریباً دو برابر بیشتر از سازمان‌هایی که پشتیبان‌هایشان تحت تأثیر قرار نگرفته بود، مبلغ اخاذی‌شده را برای بازیابی داده‌های رمزگذاری‌شده پرداخت کرده‌اند.

مبلغ پرداختی باج

میانگین پرداخت باج توسط سازمان‌هایی که نسخه‌های پشتیبان آنها به خطر افتاده بود، ۲ میلیون دلار بود؛ تقریباً دو برابر سازمان‌هایی که نسخه‌های پشتیبان‌شان دست نخورده باقی مانده بود (۱/۰۶۲ میلیون دلار). آنها همچنین کمتر قادر به مذاکره در مورد پرداخت باج بودند. به‌طوری که کسانی که پشتیبان آنها به خطر افتاده بود، به‌طور متوسط ۹۸٪ از مبلغ درخواستی را پرداخت کردند. کسانی که نسخه‌های پشتیبان آنها امن مانده بود، توانستند پرداخت را به ۸۲ درصد از مبلغ اخاذی‌شده اولیه کاهش دهند.

نرخ رمزگذاری داده‌ها

%۸۵
زمانی که نسخه‌های پشتیبان توسط مهاجمان تخریب شده‌اند

%۵۲
زمانی که مهاجمان موفق به تخریب نسخه‌های پشتیبان نشده‌اند

باج درخواستی [میانه]

۲/۳ میلیون دلار — در صورت تخریب نسخه‌های پشتیبان

۱ میلیون دلار — در صورت عدم تخریب نسخه‌های پشتیبان

پرداخت باج از سوی قربانی برای بازیابی داده‌ها

%۶۷
زمانی که نسخه‌های پشتیبان توسط مهاجمان تخریب شده‌اند

%۳۶
زمانی که مهاجمان موفق به تخریب نسخه‌های پشتیبان نشده‌اند

باج پرداختی [میانه]

۲ میلیون دلار — در صورت تخریب نسخه‌های پشتیبان

۱/۰۶۲ میلیون دلار — در صورت عدم تخریب نسخه‌های پشتیبان

درس چهارم:

۸ برابر هزینه بیشتر در بازیابی اطلاعات در صورت تخریب نسخه پشتیبان

هر حمله باج‌افزاری منجر به پرداخت باج نمی‌شود. حتی در صورت پرداخت، مبلغ باج، تنها بخشی از هزینه‌های بازیابی است که سازمان بر اثر اجرای حمله متحمل آنها می‌شود. اختلالات ناشی از باج‌افزار اغلب تأثیر قابل‌توجهی بر تراکنش‌های تجاری روزانه دارند. ضمن آن که فرایند بازیابی سیستم‌های فناوری اطلاعات، اغلب پیچیده و پرهزینه است.

میانگین هزینه بازیابی حادثه ناشی از حمله باج‌افزار برای سازمان‌هایی که نسخه‌های پشتیبان آنها به خطر افتاده هشت برابر سازمان‌هایی بوده که نسخه‌های پشتیبان آنها تحت تأثیر قرار نگرفته است. احتمالاً دلایل متعددی در پشت پرده این تفاوت‌ها وجود دارد؛ از جمله کارهای اضافی که معمولاً برای بازگردانی داده‌های رمزگشایی‌شده - در مقایسه با فرایند بازگردانی اطلاعات از طریق نسخه پشتیبان - مورد نیاز است. همچنین ممکن است موفقیت مهاجمان در تخریب نسخه پشتیبان، نشان‌دهنده ضعیف‌تر بودن امنیت و سایر سازوکارهای فناوری اطلاعات سازمان قربانی باشد.

کسانی که نسخه‌های پشتیبان‌شان مورد دست‌درازی قرار گرفته، زمان بازیابی بسیار طولانی‌تری را تجربه کرده‌اند و تنها ۲۶٪ آنها موفق شده‌اند که در عرض یک هفته فرایند بازیابی را انجام دهند؛ در مقایسه با ۴۶٪ از کسانی که نسخه‌های پشتیبان آنها امن مانده.

هزینه بازیابی اطلاعات در نتیجه حمله باج‌افزاری [میانه]

۳ میلیون دلار	زمانی که نسخه‌های پشتیبان توسط مهاجمان تخریب شده‌اند
۰/۳۷۵ میلیون دلار	زمانی که مهاجمان موفق به تخریب نسخه‌های پشتیبان نشده‌اند

توصیه‌ها

پشتیبان‌گیری، بخش مهمی از یک استراتژی جامع کاهش ریسک سایبری است. اگر نسخه‌های پشتیبان شما به‌صورت برخط در دسترس هستند، باید فرض برای آن بگذارید که مهاجمان هم قادر به دستیابی به آنها خواهند بود. توصیه می‌شود که:

- به‌طور منظم نسخه پشتیبان تهیه کرده و آنها در مکان‌های مختلف ذخیره کنید. حتماً MFA (تأیید هویت چندعاملی) را برای حساب‌های پشتیبان ابری خود فعال کنید تا شانس مهاجمان در دسترسی به آنها کمتر شود.
- در بازه‌های زمانی مناسب، بازیابی اطلاعات از طریق نسخه‌های پشتیبان را امتحان کنید تا در صورت وقوع یک حمله واقعی، به‌سرعت و به‌سادگی بتوانید وضعیت را به قبل از حمله باز گردانید.
- ضمن امن نگاه داشتن نسخه‌های پشتیبان، رخدادهای مشکوک مرتبط با آنها را بررسی کنید و در صورت نیاز، نسبت به آنها واکنش نشان دهید. در نظر داشته باشید که هر کدام از این رخدادها می‌توانند نشانه‌ای از تلاش مهاجمان برای دستیابی به آنها و در ادامه تخریبشان باشد.

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶ خیابان شهید دستگردی (ظفر) شماره ۲۷۳

تلفن / دورنگار	۰۲۱ – ۴۲۰۵۲
رایانامه	info@shabakeh.net
تارنمای شرکت	www.shabakeh.net
خدمات پس از فروش و پشتیبانی	my.shabakeh.net
مرکز آموزش	shabakeh.net/events
اتاق خبر	newsroom.shabakeh.net