SOPHOS
Cybersecurity evolved.

بهترین تجربیات فایروال
برای مقابله با باج‌افزارها

شبکه گستر
امنیت شما | وظیفه ما

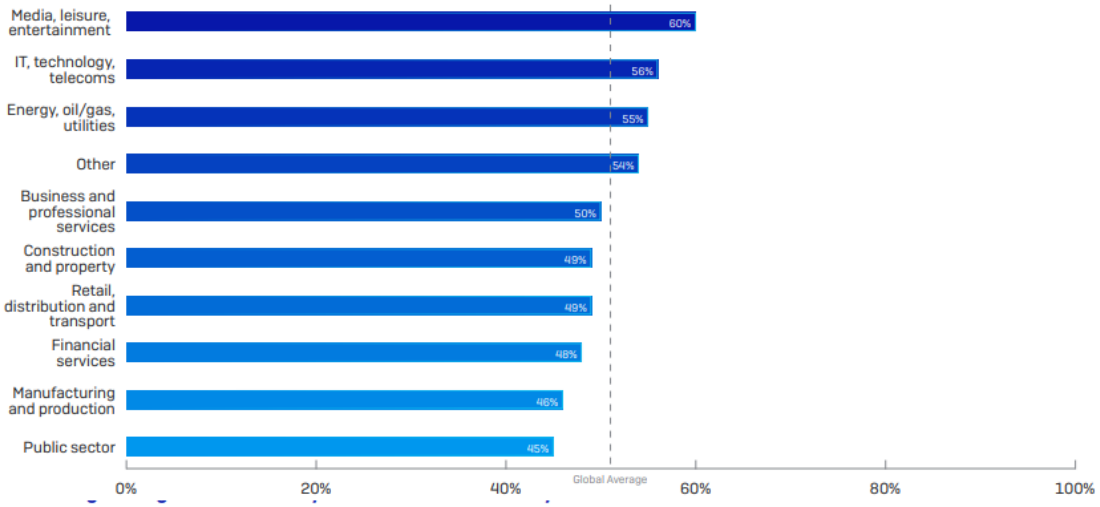
فهرست مطالب

هکرها چه کسانی را هدف قرار می‌دهند؟

هکرها چه کسانی را هدف قرار می دهند؟

پاسخ کوتاه: در یک نظرسنجی اخیر، ۵۱٪ از پاسخ‌دهندگان گفتند که در سال گذشته مورد حمله باج‌افزار قرار گرفتند و به نظر می‌رسد که بزرگی سازمان عامل مهمی نیست.

۴۷ درصد سازمان‌ها کمتر از ۱۰۰۰ کارمند داشتند در حالی‌که ۵۳ درصد بیش از ۱۰۰۰ کارمند داشتند. هیچ کشور، منطقه یا بخش بازار از مصونیت برخوردار نیستد.



اگر در اخبار "حمله باج‌افزار" را جستجو کنید، چندین حمله موفقیت‌آمیز جدید را در هر هفته مشاهده خواهید کرد. اثرات مخرب هستند: خواسته‌های بزرگ باج‌افزار، از دست دادن چشمگیر زمان و بروز اختلال در کسب‌وکار، آسیب رساندن به شهرت، از دست دادن داده‌ها و در موارد فزاینده‌ای، اطلاعات حساس شرکت توسط مهاجمان در حراج قرار می‌گیرد.

چگونه باج‌افزار به شبکه وارد می‌شود؟

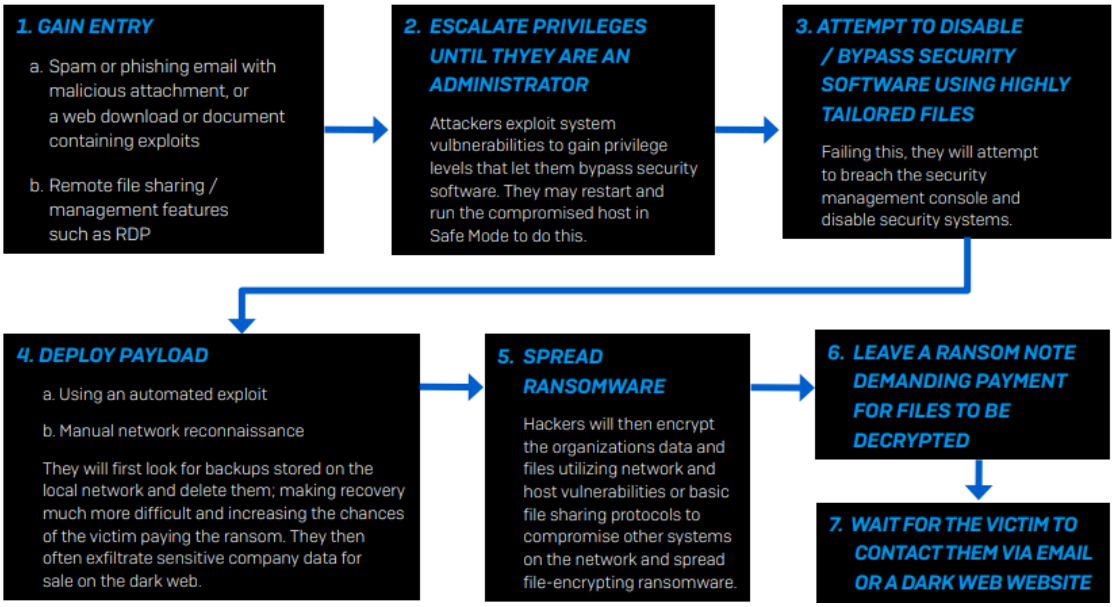
در سال ۲۰۲۰، حملات مبتنی بر سرور روند فزاینده‌ای داشت. این حملات کاملاً هدفمند و پیچیده هستند و برای استقرار آنها تلاش بیشتری لازم است. با این حال، به دلیل ارزش بالاتر دارایی‌هایی که رمزگذاری می‌شوند، به‌طور معمول آسیب‌زننده‌تر هستند و می‌توانند با اخاذی چندمیلیون دلاری سازمان‌ها را فلج کنند.

HOW THE RANSOMWARE GOT INTO THE ORGANIZATION	% INCIDENTS
Via a file download/email with malicious link	29%
Via remote attack on server	21%
Via email with malicious attachment	16%
Misconfigured public cloud instances	9%
Via our Remote Desktop Protocol (RDP)	9%
Via a supplier who works with our organization	9%
Via a USB/removable media device	7%
Other	0%
Don't know	0%
Total	100%

با این حال، همانطور که از پاسخ‌های نظرسنجی در جدول بالا مشاهده می‌کنید، مهمترین نقطه ورود باج افزار از طریق فایل‌های دانلود شده یا ارسال شده به کاربران در حملات هرزنامه‌ای یا فیشینگ است. امنیت را به دست کاربران خود ندهید. برای این نوع حملات، بهتر است از سازمان خود را با استفاده از فایروال قوی محافظت کنید.

حمله باج‌افزار چگونه کار می‌کند؟

تصویر زیر مراحل اجرای حملات هدفمند باج‌افزاری را نشان می‌دهد.



RDP یا پودمان استقرار باج افزار؟

Remote Desktop Protocol – به اختصار RDP – و سایر ابزارهای اشتراک صفحه کار نقطه پایانی مانند Virtual Network Computing – به اختصار VNC – از ویژگی های بی‌ضرر و بسیار مفید اکثر سیستم‌های عامل است که به کارکنان اجازه می‌دهد از راه دور به سیستم‌ها دسترسی پیدا کرده و آنها را مدیریت کنند.

RDP و سایر پودمان‌های مدیریت از راه دور به درستی ایمن نیستند؛ حداقل محدود کردن نشانی‌های IP که می‌توانند از طریق ابزارهای از راه دور متصل شوند، می‌تواند شما را در برابر مهاجمان امن‌تر نگه دارد. مهاجمان اغلب از تکنیک "سعی و خطا" (Brute-force) استفاده می‌کنند؛ در این تکنیک صدها هزار ترکیب نام کاربری و رمز عبور تا رسیدن به مورد مناسب امتحان می‌شود.

چگونه می‌توان از سازمان در مقابل باج افزار محافظت کرد؟

برای محافظت صحیح از سازمان خود در برابر باج‌افزار، سه اقدام اساسی وجود دارد که باید انجام دهید.

۱- امنیت فناوری اطلاعات خود را ارتقا دهید

فایروال و امنیت نقاط پایانی (ضدویروس) شما می‌توانند از حملاتی که به شبکه وارد می‌شوند محافظت کنند و اگر به هر طریقی به شبکه شما نفوذ شود، می‌توانند از گسترش و آلوده شدن سیستم‌های دیگر جلوگیری کنند. اما همه فایروال‌ها و راهکارهای امنیت نقاط پایانی نمی‌توانند این کار را به طور موثر انجام دهند؛ بنابراین مطمئن شوید که یک سامانه امنیت فناوری اطلاعات دارید.

اطمینان حاصل کنید که موارد زیر را دارید:

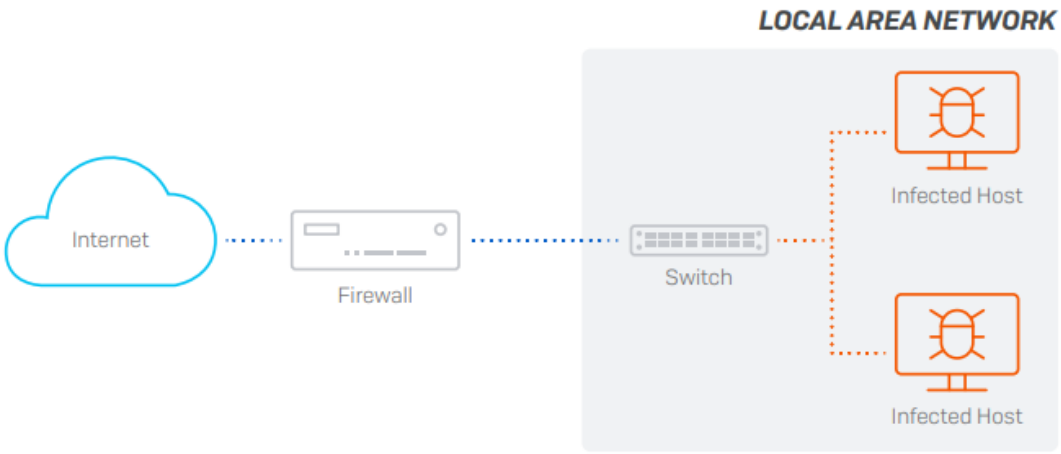
- Affordable Sandboxing (جعبه شنی با قیمت مناسب) برای تجزیه و تحلیل رفتار فایل قبل از ورود به شبکه شما.
- Machine learning technology (فناوری یادگیری ماشینی) برای شناسایی انواع جدید تهدیدات روز-صفر در هر فایلی که از طریق فایروال وارد می‌شود.
- Firewall IPS با امکان Live Signature Updating برای جلوگیری از سو استفاده از شبکه.
- دسترسی از راه دور VPN رایگان و آسان برای مدیریت شبکه از راه دور بدون ایجاد مخاطرات امنیتی.
- Endpoint Protection (ضدویروس) با قابلیت‌های ضدباج‌افزار.

۲- دسترسی و مدیریت از راه دور را ببندید

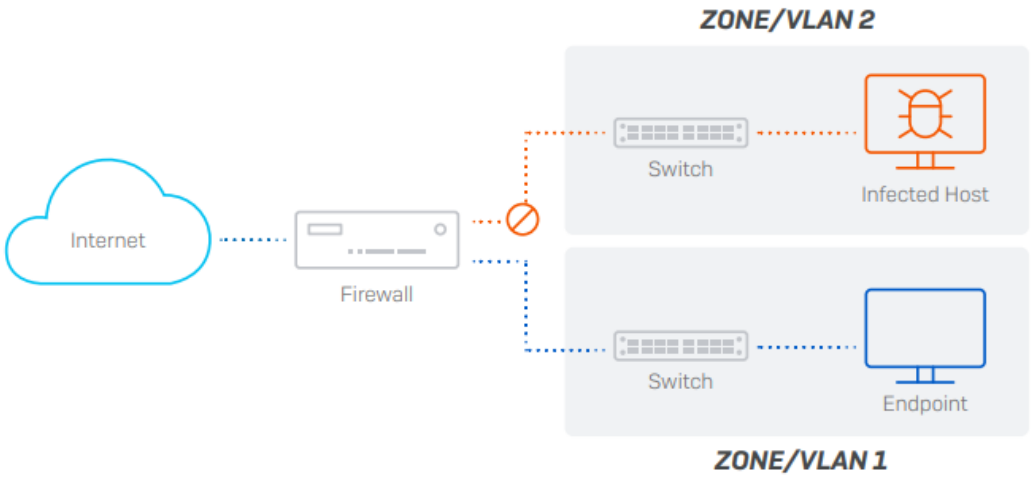
وقتی صحبت از شبکه‌ها می‌شود، هر دریچه به دنیای خارج یک آسیب‌پذیری بالقوه است که باید منتظر سوءاستفاده از آن به وسیله حمله باج‌افزار بود. بستن دسترسی پودمان RDP، پورت‌های باز و سایر پودمان‌های مدیریتی یکی از موثرترین اقداماتی است که می‌توانید برای ایمن‌سازی شبکه خود در برابر حملات هدفمند باج‌افزار انجام دهید. روش‌های مختلفی برای انجام این کار وجود دارد. یک روش محبوب محدود کردن دسترسی به نشانی‌های IP شناخته شده است. روش دیگر این که قبل از دسترسی به منابعی مانند RDP، لازم است همه کاربران از اتصال VPN استفاده کنند. همچنین، سرورهای خود را به‌درستی ایمن و دسترسی به آنها را سخت کنید، از رمزهای عبور پیچیده‌ای که مرتباً تغییر می‌کنند استفاده کنید و از احراز هویت چندعاملی استفاده کنید.

۳ - شبکه خود را تقسیم‌بندی کنید

متأسفانه، بسیاری از سازمان‌ها با یک توپولوژی شبکه مسطح فعالیت می‌کنند و تمامی نقاط پایانی آنها به یک سوئیچ مشترک متصل می‌شوند. این توپولوژی با امکان ایجاد Lateral Movement (حرکت جانبی) آسان یا گسترش حملات در شبکه محلی، حفاظت را به خطر می اندازد زیرا فایروال هیچگونه دید یا کنترلی بر ترافیکی که از طریق سوئیچ عبور می‌کند ندارد.



بهترین روش این است که LAN را به زیرشبکه‌های کوچکتر با استفاده از Zone یا VLAN تقسیم کنید و سپس آنها را از طریق فایروال به هم متصل کنید تا بتواند از ضدبدافزار و محافظت IPS بین بخش‌ها استفاده کند. این کار می تواند تلاش برای Lateral Movement (حرکت جانبی) در شبکه را شناسایی و مسدود کند.



این‌که شما از Zone یا VLAN استفاده می‌کنید به استراتژی تقسیم‌بندی شبکه و دامنه شما بستگی دارد؛ اما هر دو با ارائه گزینه‌ای برای اعمال امنیت و کنترل مناسب بر حرکت ترافیک بین بخش‌ها، قابلیت‌های امنیتی یکسانی را ارائه می‌دهند. Zoneها برای استراتژی‌های تقسیم‌بندی کوچکتر یا شبکه‌هایی با سوئیچ غیرمدیریتی ایده‌آل هستند. ایجاد VLAN ها در اکثر موارد روش ارجح برای تقسیم‌بندی شبکه‌های داخلی است و نهایت انعطاف‌پذیری و مقیاس‌پذیری را ارائه می‌دهد. با این حال، آنها نیاز به استفاده (و پیکربندی) سوئیچ‌های لایه ۳ مدیریت شده دارند.

گرچه ایجاد VLAN ها بهترین روش برای تقسیم‌بندی شبکه شماست، اما "بهترین روش" برای تقسیم‌بندی شبکه وجود ندارد. شما می‌توانید شبکه خود را بر اساس نوع کاربر (داخلی، پیمانکار و میهمان)، بر اساس بخش (فروش، بازاریابی و مهندسی)، بر اساس سرویس، دستگاه یا نوع نقش (WiFi، IoT،VoIP، ایستگاه‌کاری و سرور)، یا هر ترکیبی که برای معماری شبکه شما منطقی است، تقسیم‌بندی کنید. اما به‌طور کلی، شما می‌خواهید قسمت‌های کمتر قابل اعتماد و آسیب پذیر شبکه خود را از بقیه جدا کنید. همچنین می‌خواهید شبکه‌های بزرگ را به بخش‌های کوچکتر تقسیم کنید. همه اینها با هدف کاهش خطر نفوذ تهدید و انتشار آن است.

بهترین تنظیمات فایروال و پیکربندی شبکه

اطمینان حاصل کنید که بهترین محافظت را دارید. شامل یک فایروال مدرن نسل جدید با قابلیت IPS، TLS Inspection، Zero-day Sandboxing، و Machine learning محافظت در برابر باج‌افزار.

RDP و سایر سرویس‌ها را با فایروال خود ببندید. فایروال شما باید بتواند دسترسی کاربران VPN و نشانی‌های IP مجاز نشده در فهرست سفید را محدود کند.

با مرور و بازنگری کامل در کلیه قوانین Port-forwarding، سطح حمله را تا حد ممکن کاهش دهید و درگاه‌های باز غیرضروری را ببندید. هر پورت باز نشان‌دهنده یک حفره در شبکه شما است. در صورت امکان، از VPN برای دسترسی از خارج به منابع موجود در شبکه داخلی استفاده کنید تا اینکه از Port forwarding استفاده کنید.

مطمئن شوید که هر پورت به درستی باز شده. با اعمال حفاظت مناسب IPS در قواعد فایروال مربوط به آن ترافیک.

TLS Inspection را فعال کنید. با پشتیبانی از آخرین استانداردهای TLS 1.3 در ترافیک وب برای اطمینان از اینکه تهدیدات از طریق جریان ترافیک رمزگذاری شده وارد شبکه شما نمی شوند.

خطر lateral movement حرکت جانبی را به حداقل برسانید. با تقسیم LAN ها به مناطق کوچکتر جدا شده یا VLAN ها در داخل شبکه که توسط فایروال محافظت و بهم متصل می شوند. برای جلوگیری از گسترش سوء استفاده ها، کرم ها و ربات ها بین بخش های LAN، حتماً از قواعد IPS مناسب استفاده کنید.

سیستم های آلوده را به طور خودکار جدا کنید. هنگام بروز infection، مهم است که راه حل امنیت IT شما بتواند به سرعت سیستم های آسیب دیده را شناسایی کرده و به طور خودکار آنها را جدا کند تا زمانی که پاک شوند. (مانند Sophos Synchronized Security)

از رمزهای عبور قوی و احراز هویت چند عاملی استفاده کنید. برای مدیریت remote و ابزارهای به اشتراک گذاری فایل، به طوری که به راحتی توسط ابزار هک مهاجمان آسیب نبینید.

سوفوس چگونه می‌تواند کمک کند؟

Sophos به‌روزترین راهکارهای امنیت فناوری اطلاعات را برای دفاع در برابر جدیدترین باج‌افزارها ارائه می‌دهد.

شما نه تنها در هر نقطه از بهترین حفاظت برخوردار هستید، بلکه از تجربه سالها ادغام بین فایروال و نقطه پایانی نیز بهره‌مند می‌شوید که مزایای فوق‌العاده‌ای را از لحاظ نظارت بر سلامت شبکه و توانایی پاسخگویی خودکار به حوادث امنیتی ارائه می‌دهد.

با Award-winning XG Firewall، تمرکز قبل از هر چیز بر جلوگیری از حمله به شبکه است. در صورتی که باج‌افزار شبکه شما را مورد حمله قرار می‌دهد، شما دو برابر تحت پوشش هستید. XG Firewall به لطف ادغام با Intercept X (سامانه محافظت از نقاط پایانی سوفوس)، می‌تواند به‌طور خودکار باج‌افزار را در مسیر خود متوقف کند. مانند این است که شبکه خود را روی خلبان خودکار قرار دهید؛ یک نیروی بسیار مؤثر در کنار تیم شما.

ما این فناوری را Sophos Synchronized Security می‌نامیم. Synchronized Security ویژگی‌های محافظت از شبکه و نقاط پایانی ما را در یک سیستم امنیت سایبری قدرتمند و کاملاً یکپارچه ادغام می‌کند و بهترین قسمت اینکه مدیریت همه اینها آسان است. همراه با تمام محصولات دیگر Sophos از کنسول مدیریت Sophos Central.

فناوری‌های کلیدی XG Firewall و Intercept X که به‌طور خاص برای مقابله با باج‌افزار طراحی شده‌اند به شرح زیر است:

Sandstorm Sandboxing فایروال XG و تجزیه و تحلیل Machine Learning از فایل‌های وارد شده در شبکه به شما اطمینان می‌دهد که حتی انواع مختلف باج‌افزارها، بهره‌جوها و بدافزارهای قبلاً دیده نشده از طریق هرزنامه، فیشینگ یا بارگیری در وب گسترش نیابد.

سامانه پیشگیری از نفوذ (IPS) در XG Firewall آخرین سوءاستفاده‌های از شبکه و حملاتی را که ممکن است هکرها برای یافتن نقاط ضعف دفاعی شما استفاده کنند، مسدود می‌کند.

گزینه‌های گسترده اما ساده VPN XG Firewall به شما امکان می‌دهد تمام حفره‌های شبکه خود را ببندید و وابستگی خود را به اتصالات آسیب‌پذیر RDP از بین ببرید؛ در حالی که کاربران نیز به‌طور کامل به شبکه خود دسترسی دارند.

XG Firewall بازرسی کارامد از ترافیک TLS 1.3 را با کنترل سیاست انعطاف‌پذیر ارائه می‌دهد و به شما اطمینان می‌دهد که می‌توانید تعادل کامل بین حریم خصوصی، محافظت و عملکرد را برقرار کنید و اطمینان حاصل کنید که تهدیدات از طریق جریان‌های رمزگذاری شده به شبکه شما وارد نمی‌شوند.

Sophos Synchronized Security فایروال XG را با حفاظت Endpoint و Intercept X ادغام کرده و با شناسایی اولین علائم، متوقف کردن آنها و اطلاع رسانی به شما، به طور خودکار به حملات باج‌افزاری پاسخ می‌دهد.

Sophos Intercept X با محافظت از نقطه پایانی به همراه CryptoGuard می‌تواند حمله فزار را که در حال انجام است تشخیص داده، متوقف کرده و به‌صورت خودکار هر گونه اقدام انجام شده توسط آن را به حالت قبل باز گرداند. XG Firewall نیز شامل فناوری CryptoGuard در بستر Sandbox برای جلوگیری از باج افزار قبل از ورود به شبکه شما است.

نتیجه

باج‌افزار یک پدیده سایبری دائمی است و به تکامل خود ادامه خواهد داد. گرچه ممکن است هرگز نتوانیم باج‌افزار را به‌طور کامل ریشه‌کن کنیم، پیروی از بهترین تجارب فایروال که در این متن ذکر شده است، بهترین شانس محافظت در برابر آخرین باج افزارها و سایر تهدیدات مخرب را به سازمان شما خواهد داد.

خلاصه

- اطمینان حاصل کنید که بهترین محافظت را دارید.
- RDP و دیگر سرویسهای دسترسی ریموت را با فایروال ببندید.
- سطح گسترش حمله را تا آنجا که ممکن است کاهش دهید.
- با استفاده از محافظت مناسب IPS، هر پورت باز را ایمن کنید.
- برای دانلودها و پیوست‌ها، از Sandbox و Machine Learning Analysis استفاده کنید.
- با تقسیم‌بندی LAN، خطر Lateral Movement (حرکت جانبی) درون شبکه را به حداقل برسانید.
- سازوکار جداسازی خودکار سیستم‌های آلوده را فعال کنید.
- برای مدیریت ریموت و ابزارهای اشتراک فایل از رمزهای عبور قوی و احراز هویت چندعاملی استفاده کنید.

اتـــاق خـبـــر

newsroom.shabakeh.net

خدمات پس از فروش و پشتیبانی

my.shabakeh.net

مـرکـز آمـــوزش

events.shabakeh.net

تـارنـمـای شـرکـت

WWW.shabakeh.net

شبکه گستر

شـرکت مـهـنـدسی شـبـکـه گسـتر

تهران خیابان شـهید دستگردی (ظفر) شماره ۲۷۳

تلفن / دورنگار ۴۲۰۵۲ - ۰۲۱

www.shabakeh.net info@shabakeh.net