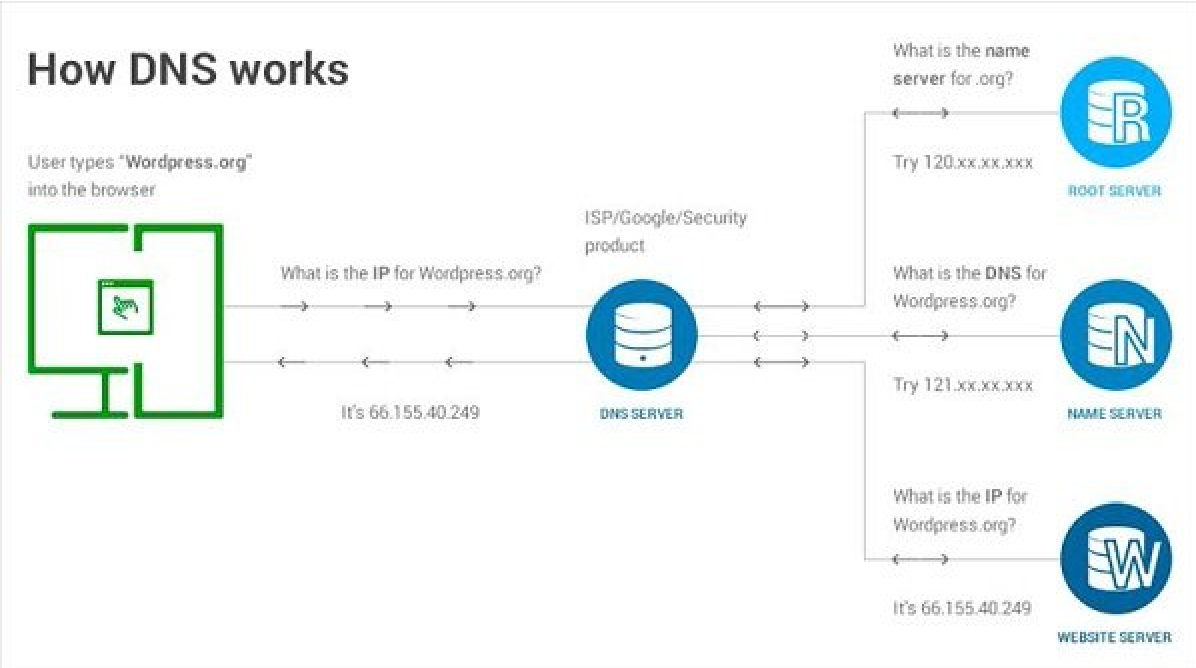
حمله‌ای ناپیدا از دید کاربر

چرا توجه به امنیت سامانه نام دامنه اهمیت دارد؟

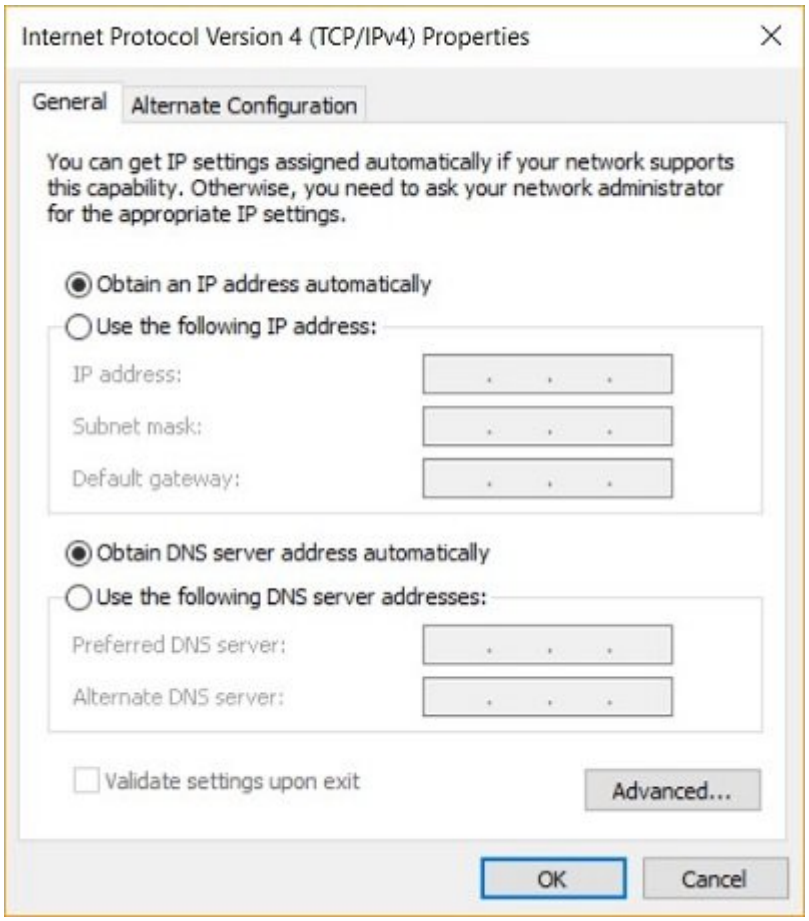
سامانه‌ها و تجهیزات هوشمند به اشکال مختلفی استفاده می‌شوند و برخی مواقع فراموش می‌کنیم این سامانه‌ها چه معماری ظریف و پیچیده‌ای دارند. گاهی اوقات پیچیدگی بیش از اندازه باعث بروز مشکلات امنیتی می‌شود. مشکلاتی که راه نفوذ به سامانه‌ها را برای هکرها هموار می‌کنند. یکی از مهم‌ترین فناوری‌های زیرساختی که تمامی سامانه‌ها و تجهیزات به شکل مستقیم و غیرمستقیم از آن استفاده می‌کنند سامانه نام دامنه (DNS) است. آشنایی با نحوه کار این فناوری و خطراتی که آن‌را تهدید می‌کنند کمک می‌کند در برابر هکرها از مکانیزم دفاعی قدرتمندی استفاده کنیم.

سامانه نام دامنه چگونه کار می‌کند؟

سامانه نام دامنه با هدف ساده کردن دسترسی به سایت‌ها ابداع شد تا کاربران به جای تایپ مقدار عددی یک آدرس (66.155.40.249) که ناملموس است، نام یک آدرس (WordPress.org) را حفظ و تایپ کنند. در مثال فوق، WorPress.org نام دامنه و 66.155.40.249 آدرس پروتکل اینترنت (آی‌پی) است که برای پیدا کردن یا تشخیص دستگاه‌ها یا خدمات کامپیوتری میزبانی شده در اینترنت استفاده می‌شود. سامانه نام دامنه یکی از مولفه‌های کلیدی اینترنت است. DNS نام دامنه‌های مختلفی همچون Microsoft.com، google.com و... را به آدرس آی‌پی ترجمه می‌کند و به کاربران اجازه می‌دهد در کوتاه‌ترین زمان ممکن اطلاعات موردنیاز را پیدا کنند. در دنیای پر مشغله امروز که به‌خاطر سپاری یک شماره ساده کار سختی است، به خاطر سپاری آدرس‌های آی‌پی سایت‌ها غیر ممکن است. به ندرت فردی را پیدا می‌کنید که آدرس آی‌پی سایتی را حفظ کرده باشد، اما در نقطه مقابل هر یک از ما دست کم نام سایت‌های مختلفی را به یاد می‌آوریم. شکل 1 نحوه عملکرد سامانه نام دامنه را نشان می‌دهد.



سامانه نام دامنه نقشی شبیه به موقعیت‌یاب جهانی دارد که درخواست‌های کاربران را از میان مسیرهای متعدد و پیچیده اینترنت عبور می‌دهد تا کاربر به مقصد برسد. به همین دلیل است که سامانه نام دامنه یکی از عناصر مهم و کلیدی زندگی دیجیتالی است. سامانه نام دامنه در هر نقطه و مکانی قرار دارد و همه مردم به شکل مستقیم یا غیر مستقیم از آن استفاده می‌کنند. به عبارت دقیق‌تر ترافیک اینترنتی کاربران از سامانه‌های نام دامنه مختلف عبور می‌کند. سامانه نام دامنه عملکرد معکوسی نیز دارد که ترافیک اینترنت را به سمت مقصد درست هدایت می‌کند، البته به شرطی که هکری سعی نکند این مسیر را تغییر دهد. هکرها می‌توانند سامانه نام دامنه را تحت کنترل بگیرند و به روش‌های مختلف از سامانه کاربران بهره‌برداری کنند، آن‌ها را آلوده کنند و اطلاعات مهم را استخراج کنند.
کاربران عادی به ندرت به سراغ تنظیمات سامانه نام دامنه کامپیوتر خود می‌روند. سامانه‌های عامل به گونه‌ای طراحی شده‌اند که به‌طور خودکار آدرس سرور سامانه نام دامنه را دریافت کنند.
به عبارت دقیق‌تر، گزینه obtain DNS server address automatically در حالت پیش‌فرض انتخاب شده است (شکل 2).



اگر تاکنون به تنظیمات سامانه نام دامنه سیستم‌عامل نرفتید به مسیر Control Panel > Network & Internet > Network Connections بروید، روی ارتباط اینترنتی جاری راست‌کلیک کنید، گزینه Internet Protocol Version 4 (TCP/IPv4)) را انتخاب کنید و سپس دکمه Properties را کلیک کنید. سامانه نام دامنه به روش‌های مختلف زیر پیکربندی و استفاده می‌شود:

- کاربران ممکن است از سامانه نام دامنه شرکت ارائه‌دهنده خدمات اینترنتی استفاده کنند. در این حالت کاربر هیچ کار خاصی انجام نمی‌دهد و فقط به اینترنت متصل می‌شود.
- سامانه نام دامنه عمومی گوگل که به شکل دستی تنظیم می‌شود و سیستم کاربر را به بزرگ‌ترین سرویس سامانه نام دامنه جهان متصل می‌کند.
- راهکارهای امنیتی ویژه سایبری که یک فیلتر ترافیک مبتنی بر سامانه نام دامنه به عنوان بخشی از مجموعه اقدامات دفاعی استفاده می‌شود.

چگونه امنیت سامانه نام دامنه به خطر می‌افتد؟

هکرها به دو روش زیر به تنظیمات سامانه نام دامنه حمله می‌کنند:

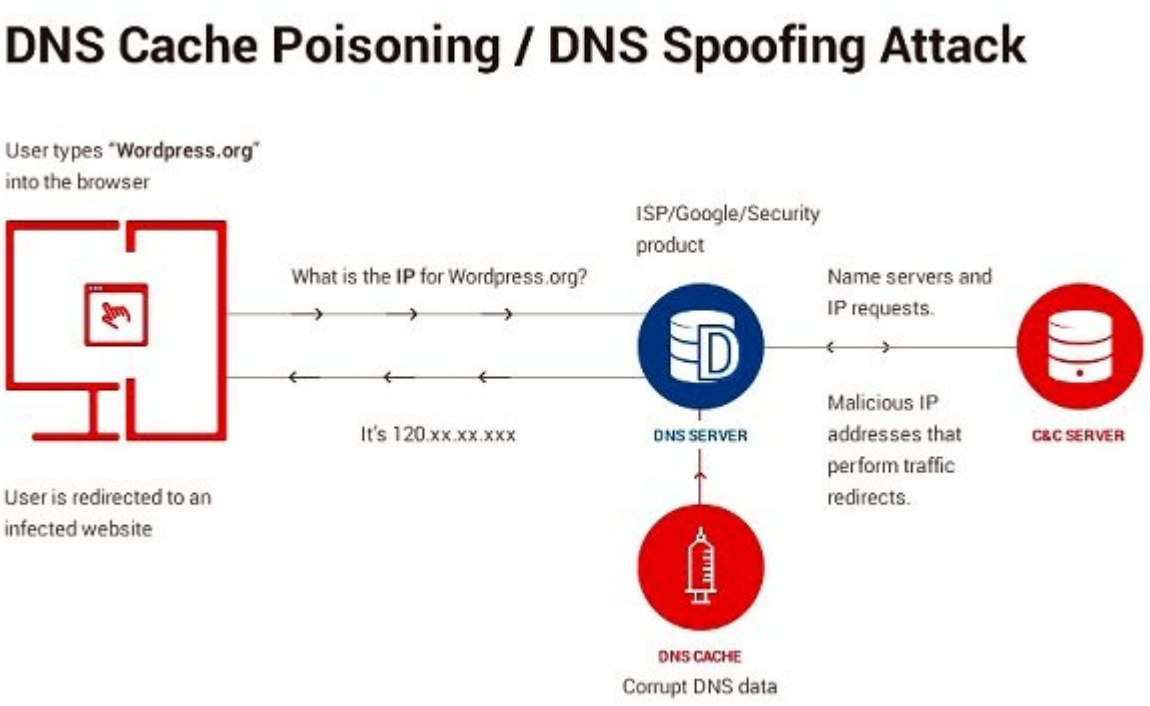
- ایجاد اختلال در عملکرد سامانه نام دامنه
- سوء استفاده از آسیب‌پذیری‌های امنیتی در سرورهایی که خدمات سامانه نام دامنه روی آن‌ها اجرا می‌شوند.

از معروف‌ترین حملات مرتبط با سامانه نام دامنه می‌توان به مسموم‌سازی سامانه نام دامنه (DNS cache poisoning) و ربایش سامانه نام دامنه (DNS hijacking) اشاره کرد. در هر دو حمله، قربانی متحمل ضررهای زیادی می‌شود.

مسموم‌سازی کش سامانه نام دامنه

مسموم‌سازی کش سامانه نام دامنه که به جعل سامانه دامنه معروف است به دستکاری فرآیند پردازش ترجمه (translation) در مکانیزم کاری سامانه نام دامنه اشاره دارد. سرور سامانه نام دامنه همانند مرورگرها کشی دارد که اطلاعات در آن ذخیره می‌شوند. ذخیره‌سازی داده‌ها باعث می‌شود در مراجعه بعدی به سایتی همچون wordpress.org، سامانه نام دامنه سریع‌تر فرآیند ترجمه و تبدیل آدرس‌ها را انجام دهد. حمله مسموم‌سازی سامانه نام دامنه این‌گونه پیاده‌سازی می‌شود که هکرها سعی می‌کنند اطلاعات جعلی و مخرب را درون کش سامانه نام دامنه ذخیره‌سازی کنند. اگر این حمله با موفقیت انجام شود، سرور در زمان پاسخ‌گویی به محاوره‌های قربانیان، یک

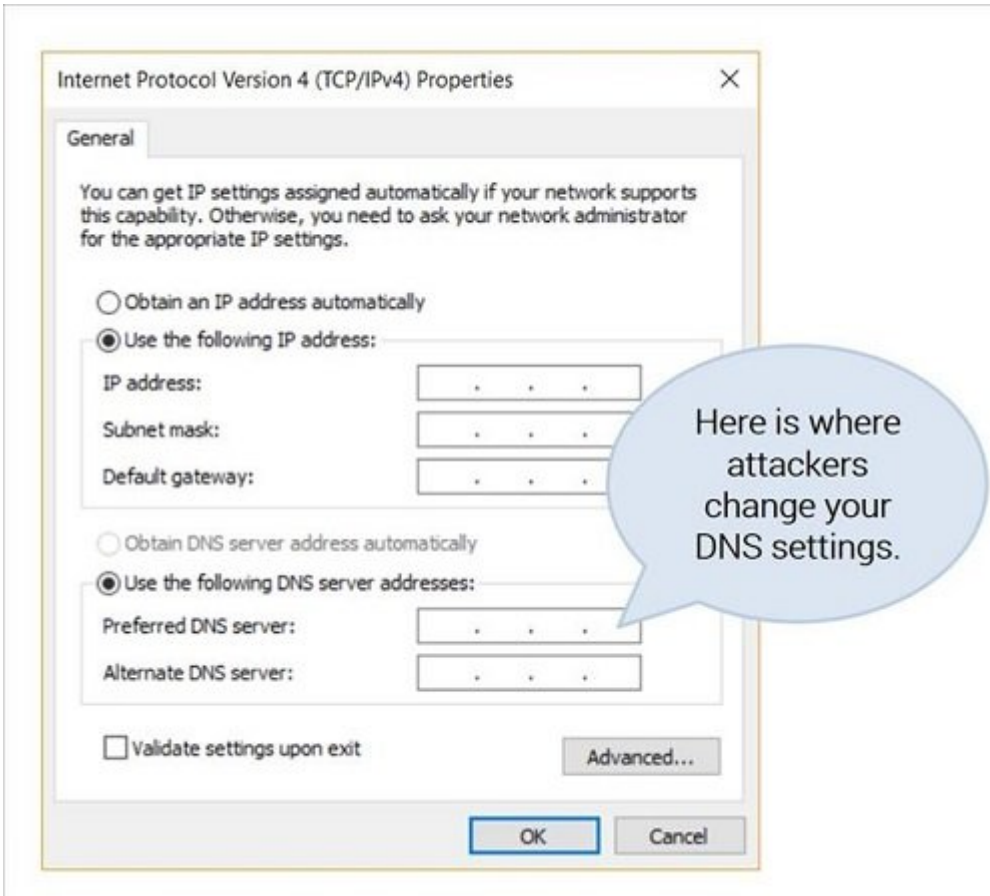
آدرس آی‌پی نادرست را برای آن‌ها ارسال می‌کند. در این حالت هکر می‌تواند ترافیک اینترنت قربانی را به سرورها و سایت‌های مخربی که تحت کنترل دارد هدایت کند. شکل 3 مکانیزم حمله مسموم‌سازی کش سامانه نام دامنه/ جعل سامانه نام دامنه را نشان می‌دهد.



پس از پیاده‌سازی موفقیت‌آمیز این حمله، هکر می‌تواند بدافزارهای مختلف را از وب‌سایتی که طراحی کرده به سمت سامانه قربانی ارسال کند. این امکان وجود دارد که سرور سامانه نام دامنه را به شکلی آلوده و دست‌کاری کرد که محتوای ورودی از سرورهای غیرمجاز را قبول کند تا بدافزارهای مخرب و نرم‌افزارهای آلوده به سمت کامپیوتر قربانیان ارسال شود و قربانی بدون هیچ‌گونه نشانه‌ای دال بر آلودگی از نرم‌افزارها استفاده کند. همان‌گونه که می‌دانیم سرور سامانه نام دامنه منحصر به یک کامپیوتر خاص نیست و صدها یا هزاران دستگاه کلاینت به آن مراجعه می‌کنند. اگر سرور سامانه نام دامنه متعلق به یک شرکت ارائه‌دهنده خدمات اینترنتی آلوده شود، دست‌کم هزاران مشترک تحت تاثیر یک حمله غیرمستقیم قرار می‌گیرند، به‌طوری که ترافیک تمامی مشترکان شرکت ارائه‌دهنده خدمات به سمت سایت‌های آلوده به کدهای مخرب و بدافزارها هدایت شده و در نهایت کدهای مخرب و کیت‌های بهره‌برداری به راحتی می‌توانند از آسیب‌پذیری مستتر در کامپیوترهای قربانیان سوء استفاده کنند. در این مرحله هکرها می‌توانند از بردارهای مختلف حمله همچون باج‌افزارها، تروجان‌های صنعتی یا بدافزارهای تولیدکننده بات‌نت استفاده کنند. شناسایی آلودگی مسموم‌سازی یا جعل سامانه نام دامنه برای کاربران عادی ساده نیست، به ویژه اگر هکرها از بدافزارهای نسل دوم استفاده کنند که ضریب بالایی در پنهان‌کاری دارند و در بیشتر موارد غیرقابل شناسایی هستند.

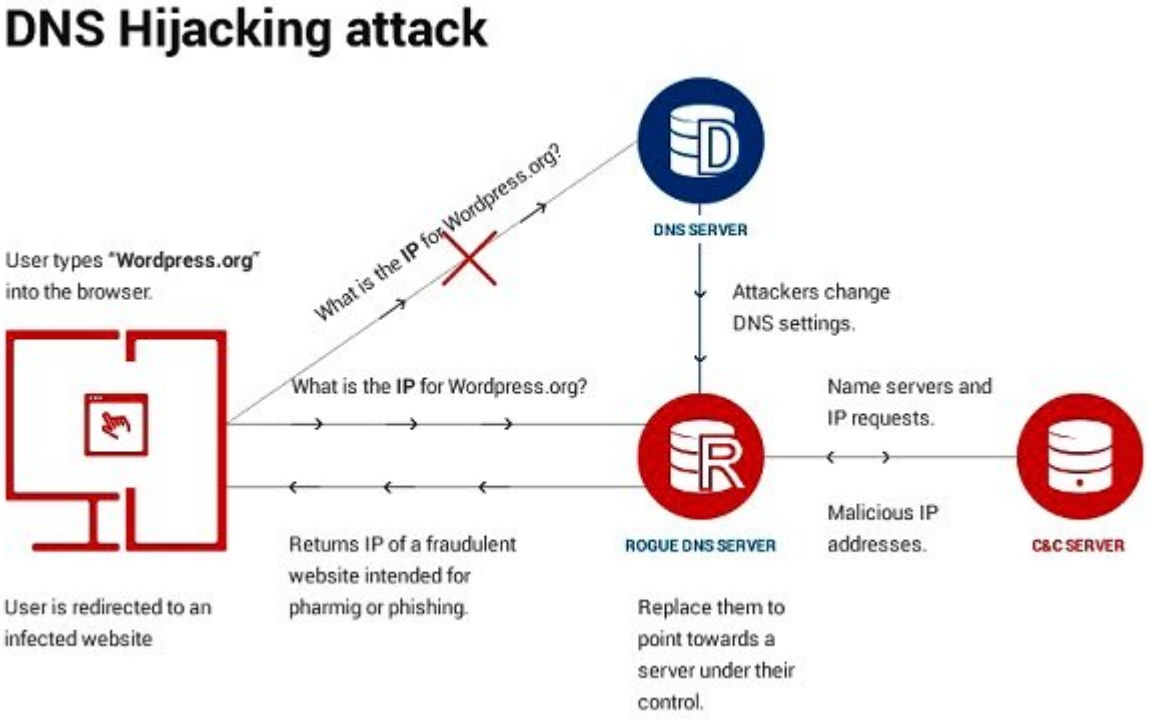
روبایش سامانه نام دامنه

این حمله به دست‌کاری و تغییر تنظیمات سامانه نام دامنه اشاره دارد. در این حمله تمام درخواست‌های ترافیک اینترنت قربانی برای یک سرور سامانه نام دامنه آلوده هدایت می‌شود. در این حالت تمامی نتایجی که قربانی دریافت می‌کند و روی مرورگر خود مشاهده می‌کند، دست‌کاری شده و آلوده هستند. هکرها با تغییر تنظیمات آدرس سرور سامانه نام دامنه در بخش ویژگی‌های پروتکل TCP/IP4 کامپیوتر قربانی را آلوده می‌کنند. مکانی که هکرها اقدام به آلوده‌سازی تنظیمات سامانه نام دامنه می‌کنند در شکل 4 نشان داده شده است.



درک حمله ربایش سامانه نام دامنه در مقایسه با مسموم‌سازی سامانه نام دامنه ساده‌تر است، اما به سختی شناسایی می‌شود. هکرها از بدافزارهای ویژه برای تغییر تنظیمات سامانه نام دامنه از وضعیت خودکار به دستی استفاده می‌کنند. برخی موارد ربایش سامانه نام دامنه یک پیش‌نیاز دارد که ابتدا کامپیوتر آلوده قربانی در یک شبکه بات (botnet) ثبت می‌شود تا هکرها کنترل کاملی روی سامانه کاربر به دست آورند. حمله فوق به شکل دیگری نیز اجرا می‌شود که عملکرد سامانه نام دامنه سرور تغییر پیدا می‌کند تا متفاوت از روش‌های مرسوم اینترنتی کار کند.

در هر دو حالت، نتایج یکسانی به دست می‌آید و قربانی به سمت سایت‌های مخرب هدایت می‌شود که برای کلاه‌برداری فیشینگ یا فارمینگ (pharming) آماده شده‌اند. سایت‌هایی که طراحی ظاهری یکسان با نمونه اصلی دارند تا کاربر را فریب دهند اطلاعات شخصی خود را درون سایت‌ها وارد کند یا کاربر را به سایت‌هایی هدایت می‌کنند که طراحی کاربری جذابی دارند و قربانی را متقاعد می‌کنند اطلاعات شخصی خود را درون سایت وارد کند. شکل 5 نحوه پیاده‌سازی حمله ربایش سامانه نام دامنه را نشان می‌دهد.



در بیشتر مواقع، هدف از پیاده‌سازی این حمله استخراج اطلاعات با ارزش همچون گذرواژه‌ها ، نام کاربری، اطلاعات کارت‌های اعتباری و هرگونه اطلاعاتی

است که
به هکر اجازه می‌دهد به حساب‌های بانکی قربانی نفوذ کند. این مدل حمله محدود به هکرها نیست و برخی از ارائه‌دهندگان سرویس‌های اینترنتی برای کسب درآمد بیشتر از چنین روشی استفاده می‌کنند، در حالی که هدف واقعی آن‌ها پیاده‌سازی یک حمله مخرب نیست. حملات مسموم‌سازی/جعل و ربایش سامانه نام دامنه عملکردی شبیه به حمله مرد میانی دارند. در حمله مرد میانی هکرها میان کامپیوتر قربانی و یک سرویس مبتنی بر وب که قربانی قصد استفاده از آن‌را دارد قرار می‌گیرند. هکرها می‌توانند با تزریق اطلاعات سامانه نام دامنه نادرست، نسخه‌های جعلی از سایت‌های مختلف را روی مرورگر قربانی نشان دهند. به‌طور مثال، اگر سامانه نام دامنه‌ای که از آن استفاده می‌کنید آلوده باشد، هکرها یک کپی جعلی از سایت بانک را نشان می‌دهند تا اطلاعات حساب را جمع‌آوری کنند و در فرصت مناسب به سرقت پول‌هایی بپردازند که درون حساب بانکی کاربر قرار دارد. ضدویروس‌ها در زمینه شناسایی این مدل حملات خیلی مفید نیستند، زیرا ضدویروس‌ها تنها رفتار فایل‌ها و عملکرد سامانه‌ها را بررسی می‌کنند و کاری با ترافیک اینترنت ندارند. به همین دلیل است که سامانه‌های کامپیوتری به یک لایه محافظتی بیشتر نیاز دارند.

در ارتباط با تنظیم سامانه نام دامنه به چه شرکت‌هایی باید اعتماد کرد؟

اولین مورد شرکت ارائه‌دهنده خدمات اینترنتی است. بهتر است از اپراتوری استفاده کنید که قدمت زیادی دارد و شناخته شده است. پیش از عقد قرارداد حتما خط‌مشی‌های حریم خصوصی شرکت را بررسی کنید. خوشبختانه شرکت‌های ایرانی در این زمینه عملکرد خوبی دارند و جای نگرانی نیست. گزینه دوم سامانه نام دامنه عمومی گوگل است که بیشتر کاربران از آن استفاده می‌کنند. گوگل شرکت معتبر و شناخته شده‌ای است که سرویسی که ارائه می‌دهد سرعت زیادی دارد، اما نگرانی‌های امنیتی در ارتباط با این سرویس وجود دارد. به‌طور مثال، برخی از کاربران معتقد هستند تنظیم سامانه نام دامنه به سرویس گوگل باعث می‌شود اطلاعات خیلی زیادی در ارتباط با عملکردهای شخصی در اختیار گوگل قرار گیرد که چندان جالب نیست. سومین راهکار به‌کارگیری سرویس سامانه نام دامنه‌ای است که برخی از ابزارهای امنیتی ارائه می‌کنند. در صورت به‌کارگیری برخی از این سرویس‌ها، تمام ترافیک شما توسط بانک‌های اطلاعاتی هوشمند این سرویس‌ها فیلتر می‌شود و شما در برابر تهدیدات سایت‌های فیشینگ و فارمینگ، تبلیغات آلوده به بدافزارها، سایت‌هایی که کدهای مخرب در آن‌ها تزریق شده، تغییر مسیر ترافیک اینترنت، دانلود فایل‌های مخرب، کیت‌های بهره‌برداری، نشتی داده‌ها و ترافیک آلوده که راهی برای ارسال بدافزارها به سمت کامپیوتر قربانی است ایمن خواهید بود. پیشنهاد می‌کنیم پیش از نصب هر محصول امنیتی، ابتدا امنیت و عملکرد محصول را بررسی کنید.

چه بدافزارهایی سامانه نام دامنه کاربران را هدف قرار می‌دهند؟

اکنون که با شیوه‌های مرسوم حمله به سامانه نام دامنه آشنا شدید، اجازه دهید با نمونه‌های واقعی بدافزارهایی که به سامانه نام دامنه کاربران حمله می‌کنند و ترافیک اینترنت آن‌ها را کنترل می‌کنند آشنا شویم.

تروجان DNSChanger

در یک بازه زمانی پنج ساله (2007 تا 2012) یک تروجان تغییر دهنده سامانه نام دامنه به‌نام DNSChanger موفق شد چهار میلیون کامپیوتر را آلوده کند. این تروجان که خاستگاه آن کشور استونی بود موفق شد
14 میلیون دلار سود از طریق تبلیغات عاید این شرکت کند. DNSChanger تبلیغات مختلفی روی صفحه‌نمایش قربانی نشان می‌داد. دقت کنید، زمانی که صحبت از کنترل سامانه نام دامنه به میان می‌آید، منظور این است که هکرها می‌توانند هرگونه محتوایی روی مرورگر قربانی نشان دهند. در سال‌های بعد تروجان فوق به‌نام RSPlug دومرتبه در اینترنت شناسایی شد. در اوایل سال 2011 میلادی پلیس فدرال ایالات متحده موفق شد طراحان این تروجان در کشور استونی را بازداشت کند.

DNS Unlocker

یک برنامه ناخواسته (PUA) سرنام potentially unwanted application تابستان 2016 میلادی توسط شرکت امنیتی ESET شناسایی شد. این برنامه روی تمامی نسخه‌های سیستم‌عامل ویندوز قابل اجرا بود تا بتواند کاربران بیشتری را قربانی کند. DNS Unlocker به شکل متفاوتی به سراغ تغییر تنظیمات سامانه نام دامنه می‌رفت و سعی می‌کرد با اعمال تغییراتی در رجیستری ویندوز تغییرات مدنظر را اعمال کند و ردیابی توسط ضدویروس‌ها را سخت کند.

Moose worm

یکی دیگر از تهدیدات جدی پیرامون سامانه نام دامنه کرم Moose worm بود. Moose به سراغ سرویس‌ها و روترهای لینوکسی می‌رفت و سامانه نام دامنه آن‌ها را سرقت می‌کرد. این کرم به جای بهره‌برداری از آسیب‌پذیری‌های نرم‌افزاری برای ورود به سامانه‌ها، سعی می‌کرد با هک نام کاربری و گذرواژه‌های ضعیف استفاده شده در نرم‌افزارها به سامانه‌ها نفوذ کند. Moose سعی می‌کرد از ارتباطات اینترنت کاربران برای پیاده‌سازی حملات مهندسی اجتماعی و کلاه‌برداری استفاده کند و از سامانه‌های آلوده و متصل به اینترنت برای لایک کردن صفحات، مشاهده ویدیوها و دنبال کردن حساب‌ها در شبکه‌های اجتماعی استفاده کند. پژوهشگران ترندمیکرو اعلام کردند این بدافزار از ترکیب دو بردار حمله جست‌وجوی فراگیر و ربایش سامانه نام دامنه اطلاعات شخصی کاربران (گذرواژه‌ها و نام‌های کاربری) را سرقت می‌کرد.
سه مورد یاد شده، تنها بخش کوچکی از بدافزارهایی بودند که هکرها برای حمله به سامانه نام دامنه استفاده می‌کردند. در حالت کلی، مجرمان اینترنتی با آلوده‌سازی سرویس‌های سامانه نام دامنه قابلیت‌های زیر را به دست می‌آورند:

- فعالیت پنهانی و عدم شناسایی به سادگی
- عدم تشخص توسط ضدویروس‌ها که تنها مکانیزم امنیتی مورد استفاده شرکت‌ها و کاربران هستند
- مهیا کردن یک مسیر مناسب برای آلوده کردن سامانه‌ها
- آماده‌سازی کانالی مستقیم برای آلوده‌سازی سامانه‌ها به بدافزار آماده‌سازی راهی برای ترکیب انواع مختلفی از بردارهای حمله تا از سامانه کاربران برای پیاده‌سازی حملات منع سرویس توزیع شده و سایر کمپین‌های بدافزاری استفاده شود.

منبع:
heimdalsecurity
تاریخ انتشار:
04 فروردین 1399

نشانی منبع:
https://www.shabakeh-mag.com/security/16701/%DA%86%D8%B1%D8%A7-%D8%AA%D9%88%D8%AC%D9%87-%D8%A8%D9%87-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87-%D9%86%D8%A7%D9%85-%D8%AF%D8%A7%D9%85%D9%86%D9%87-%D8%A7%D9%87%D9%85%DB%8C%D8%AA-%D8%AF%D8%A7%D8%B1%D8%AF%D8%9F