روز صفرم

ماهنامه علمی

سال سوم / شماره بیست‌ودوم / بهمن‌ماه ۰۰

انجمن رمز ایران
Iranian Society of Cryptology

این ماهنامه با حمایت مادی و معنوی اداره کل امور فرهنگی دانشگاه اصفهان چاپ و منتشر شده است.

نشریه علمی روز صفرم
شماره ۲۲ - بهمن ۱۴۰۰

صاحب امتیاز:
شاخه دانشجویی انجمن رمز ایران در دانشگاه اصفهان

سردبیر:
محمد آقائی

مدیر مسئول:
الهه رهبران

طراح جلد و صفحه‌آرا:
نوریه سادات مدنیان
محمد آقائی

هیئت تحریریه:
بهار خلیلیان
امیر فیض
حسین علی ترکان
علی دادخواه

اخبار:
سروش ذوالفقاری

ویراستار:
الهه رهبران

t.me/SBISC

SBISC.UI.AC.IR

t.me/CTFPREP

twitter.com/SBISC1

instagram.com/SBISC_UI

درباره انجمن:

شاخه دانشجویی انجمن رمز ایران در دانشگاه اصفهان از سال ۱۳۸۶ فعالیت خود را پیرامون مباحث مرتبط با امنیت اطلاعات آغاز کرد. این انجمن که هم‌اکنون یازده دوره از آغاز فعالیت آن می‌گذرد، تصمیم به انتشار نشریه‌ای با عنوان "**روز صفرم**" گرفته است تا از این طریق بتواند دانش امنیتی در فضای سایبر را به مخاطبان خود منتقل کند.این نشریه به صورت ماهانه و از اردیبهشت ۹۸ منتشر شده است.


روز پدر مبارک
علی
علیه السلام

معماری امنیت اطلاعات

Information Security Architecture

بهار خلیلیان
bahaar.khalilian@gmail.com

معماری امنیت اطلاعات چیست؟

معماری امنیت به مجموعه‌ای از نمایش‌های فیزیکی و منطقی معماری سیستم گفته می‌شود که به ما اطلاعاتی راجع‌به نحوه تقسیم‌بندی سیستم به حوزه‌های امنیتی می‌رساند و از عناصر مرتبط با امنیت برای اعمال سیاست‌های امنیتی در داخل و بین حوزه‌های امنیتی براساس نحوه محافظت از داده‌ها و اطلاعات استفاده می‌کند.

معماری امنیت، نحوه قرارگیری عناصر مرتبط با امنیت، ارتباطات متقابل و روابط اعتمادی و رفتار و تعاملات بین آن‌ها را معکوس می‌کند. درواقع معماری امنیتی یک طرح امنیتی یکپارچه است که به ضرورت‌ها و خطرات احتمالی موجود در یک سناریو یا محیط خاص می‌پردازد. همچنین زمان و مکان اعمال کنترل‌های امنیتی را مشخص می‌کند و نشان‌دهنده رابطه بین اجزا مختلف در معماری فناوری اطلاعات و نحوه وابستگی آن‌ها به یکدیگر است. مزیت اصلی معماری امنیتی استاندارد بودن آن است که به دلیل استفاده مجدد از کنترل‌ها آن را مقرون به‌صرفه می‌کند. (به دیگر مزایا استفاده از معماری امنیت به طور مفصل اشاره خواهد شد).

معماری امنیت، مشابه با معماری سیستم ممکن است در سطوح مختلف انتزاعی و با دامنه‌های مختلف بیان شود. معماری سیستم را می‌توان طرحی در نظر گرفت که شامل یک ساختار است و به ارتباطات بین اجزای آن ساختار می‌پردازد.

معماری امنیتی با معماری فناوری اطلاعات مرتبط است. با این حال، ممکن است اشکال مختلفی داشته باشد. به‌طور کلی شامل یک کاتالوگ از کنترل های معمولی علاوه بر نمودارهای روابط، اصول و غیره است. این کنترل‌ها بر اساس چند فاکتور اصلی مشخص می شوند: مدیریت ریسک، معیار و تمرین خوب، مالی، قانونی و نظارتی.

مزایا معماری امنیت اطلاعات چیست؟

۱.ساختار امنیتی قوی منجر به نقض امنیتی کمتر می‌شود :

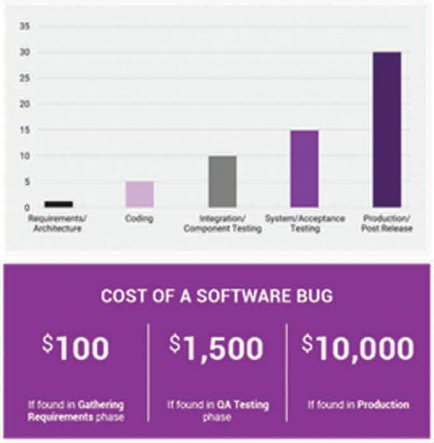
کسب‌وکارهای مدرن برای حفاظت از مهمترین دارایی‌های اطلاعاتی خود، باید یک چارچوب معماری امنیتی قوی داشته باشند. با تقویت معماری امنیتی خود برای بستن نقاط ضعف رایج، می‌توان خطر موفقیت مهاجم در نفوذ به سیستم را به شدت کاهش داد.

یکی از مهمترین مزایا معماری امنیتی، توانایی آن در ترجمه الزامات منحصربه‌فرد هر سازمان به استراتژی‌های اجرایی برای ایجاد یک محیط بدون ریسک بالا، هم‌سو با نیازهای کسب‌وکار و آخرین استانداردهای امنیتی است.

به عنوان یک مزیت اضافی، با اعمال این اقدامات، سازمان‌ها می‌توانند قابل اعتماد بودن خود را به شرکای بالقوه نشان دهند و به آن‌ها کمک کند تا کسب‌وکار خود را از رقبا جلوتر ببرند. این در نهایت معماری را ارائه می‌دهد

که برای سازمان منفعت طولانی مدت دارد.

۲.اقدامات امنیتی پیشگیرانه باعث صرفه‌جویی در هزینه می‌شوند:
شناسایی و رفع آسیب‌پذیری‌های امنیتی هزینه بالایی دارد، تولید را متوقف می‌کند، نیاز به بررسی کامل دارد و می‌تواند منجر به فراخوان های آسیب‌رسان محصول یا کنفرانس‌های مطبوعاتی شرم‌آور شود. به این ترتیب، هرچه دیرتر در چرخه توسعه محصول خطا تشخیص داده شود، هزینه آن بیشتر خواهد بود. تشخیص یک خطا در مرحله کدنویسی توسعه می‌تواند هزینه رفع آن را تا ۵۰۰٪ افزایش دهد. تشخیص همان خطا در مراحل بعدی، در مراحل تولید یا پس از انتشار، می‌تواند تا ۳۰۰۰٪ هزینه بیشتری داشته باشد.
یکپارچه‌سازی امنیت در هر سطح از توسعه محصول می‌تواند احتمال رد شدن یک خطا را کاهش دهد. محصولات با زمینه امنیتی از مرحله ایده‌پردازی توسعه می‌یابند و ابزارها و فرآیندهای جدید توسعه یافته (نصب شده به عنوان بخشی از فرآیند معماری امنیتی) به کاهش خطر خطا در مراحل بعدی کمک می‌کنند.



۳.ممکن است به کاهش اقدامات انضباطی در صورت تخلف کمک کند:
درحالی‌که قوانین در سراسر جهان از نظر عواقب نقض امنیت سایبری متفاوت است، یکی از عناصر رایج این است که هرچه یک کسب‌وکار بیشتر تلاش کند ریسک خود را کاهش دهد و از آسیب پذیری‌ها جلوگیری کند، در صورت حمله ممکن است نتیجه مطلوب‌تری داشته باشد. به‌طور کلی، تنظیم‌کننده‌ها نشان داده‌اند که به زمانی احترام می‌گذارند که سازمان‌ها تمام تلاش خود را انجام می‌دهند و مشاغلی را که فقط وانمود می‌کنند که تلاش می‌کنند یا اصلا تلاش نمی‌کنند را مجازات می‌کنند.

نکته مهم دیگر این است که مقررات در حال سخت‌تر شدن هستند. قبل از سال ۲۰۱۶، هیچ کس درباره GDPR نشنیده بود و مطمئنا مجبور نبود استانداردهای آن را رعایت کند. اما اکنون بسیاری از چشم‌اندازهای دیجیتال در اروپا و جهان را هدایت می‌کند. چشم‌انداز قانون‌گذاری سخت کار می‌کند تا به فناوری برسد، و برای کسب‌وکارها این بدان معنی است که احتمالا قوانین سخت‌گیرانه‌تری در آینده وجود خواهد داشت.
ایجاد یک معماری امنیتی قوی، ادغام امنیت در چرخه توسعه، استفاده از ابزارها و فرآیندها برای شناسایی خطاها، همه نشان می‌دهند که سازمان تمام تلاش خود را می‌کند تا از خود در برابر تهدیدات سایبری دفاع کند و از تمام مقررات مربوطه در حد توانش پیروی کند.

چارچوب‌های معماری امنیت چه هستند؟

درست همان‌طور که معماران املاک دستورالعمل‌هایی برای کار کردن دارند، معماران امنیتی نیز چنین هستند. این‌ها معمولا به عنوان "چارچوب" (framework) نامیده می‌شوند.
چارچوب معماری امنیتی چیست؟ می‌تواند معانی متفاوتی داشته باشد، اما به‌طور کلی مجموعه‌ای ثابت از اصول و دستورالعمل‌ها برای اجرای معماری امنیتی در سطوح مختلف کسب وکار درنظر گرفته می‌شود. استانداردهای بین المللی زیادی وجود دارد که هر کدام مشکل متفاوتی را حل می‌کند.
برخی از شرکت‌ها نیز چارچوب‌های خود را طراحی خواهند کرد. با ترکیب استانداردها، می توانیم خدمات همه‌کاره‌تری ارائه کنیم که از بهترین راهنمایی‌ها از هر کدام استفاده می‌کنند. این ما را قادر می‌سازد تا نیازمندی‌ها و راه حل های امنیتی متناسب را طراحی، پیاده‌سازی و اندازه‌گیری کنیم.

نمونه‌هایی از چارچوب‌های معماری امنیتی رایج:

- **TOGAF**:

برگرفته از اصطلاح The Open Group Architecture Framework. این چارچوب به تعیین مشکلاتی که یک کسب‌وکار می‌خواهد با معماری امنیتی حل کند کمک می‌کند. این بر مراحل اولیه معماری امنیتی، محدوده و هدف سازمان تمرکز می‌کند و مشکلاتی را که یک کسب‌وکار قصد دارد با این فرایند حل کند را مشخص می‌کند. با این حال، راهنمایی خاصی در مورد چگونگی رسیدگی به مسائل امنیتی ارائه نمی‌دهد.

- **SABSA**:

برگرفته از اصطلاح Sherwood Applied Business Security Architecture. این چارچوب یک چارچوب کاملا مبتنی بر سیاست است که به تعریف سوالات کلیدی که باید توسط معماری امنیتی پاسخ داده شوند کمک می‌کند: چه کسی، چه چیزی، چه زمانی و چرا. هدف آن اطمینان از طراحی، ارائه و پشتیبانی خدمات امنیتی به عنوان بخشی جدایی‌ناپذیر از مدیریت فناوری اطلاعات شرکت است. در حالی که اغلب به عنوان یک "روش معماری امنیتی" توصیف می‌شود، در مورد اجرا فنی به جزئیات نمی‌پردازد.

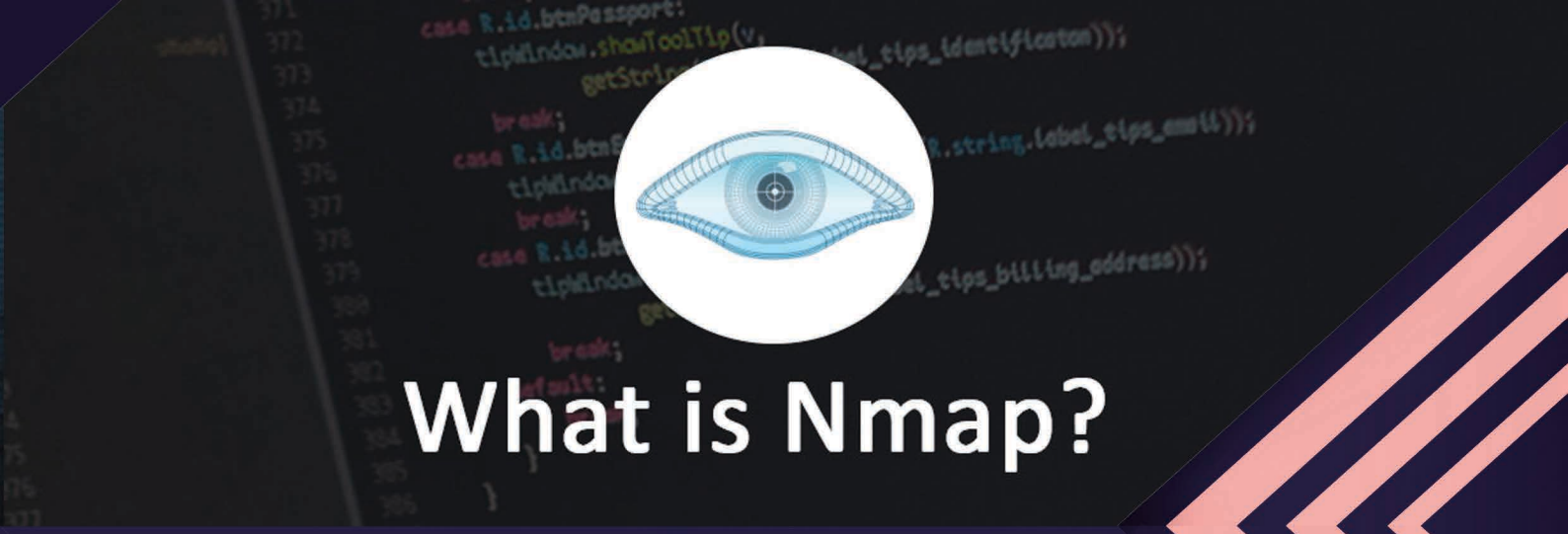
- **OSA**:

برگرفته از اصطلاح Open Security Architecture. این چارچوب یک چارچوب مربوط به عملکرد و کنترل‌های امنیتی فنی است. این یک مرور کلی از مسائل کلیدی امنیتی، اصول، اجزا و مفاهیم اساسی تصمیمات معماری است که هنگام طراحی معماری‌های امنیتی موثر درگیر هستند. گفته می‌شود، معمولا فقط زمانی می‌توان از آن استفاده کرد که معماری امنیتی قبلا طراحی شده باشد.

پیاده‌سازی یک معماری امنیتی چقدر زمان خواهد برد؟

متاسفانه پاسخ قطعی برای این سوال وجود ندارد. یک نقشه راه ساده ممکن است هفته‌ها طول بکشد، درحالی‌که یک ارزیابی دقیق و جامع از کسب‌وکار ممکن است ماه‌ها طول بکشد. فراتر از آن، فرایند تحول واقعی به مقیاس کسب‌وکار و دامنه پروژه بستگی دارد.
به طور خلاصه: فرآیند معماری امنیتی بسیار به اهداف شما، اندازه کسب‌وکار شما، بودجه شما، وضعیت فعلی شما و عوامل مشابه بستگی دارد.

منابع:
- security architecture, csrc.nist.gov
- Security Architecture, techopedia.com
- Security architecture for cloud applications, ibm.com
- CDSA, techopedia.com



What is Nmap?

آشنایی با انمپ-قسمت دوم

Getting To Know Nmap-part 2

امیر فیض

amir.feiz.1381@gmail.com

در شماره بیست و یکم نشریه با ابزار nmap آشنا شدیم، در این مقاله به معرفی ادامه کاربردهای آن می‌پردازیم.

اسکن IPv6 توسط nmap:

ابتدا به معرفی IPv6 می‌پردازیم، IPv6 در واقع یک سبک آدرس‌دهی می‌باشد به‌نحوی‌که از ۱۲۸ بیت تشکیل شده و به‌صورت ترکیب خاصی از حروف و اعداد وظیفه آدرس‌دهی را بر عهده می‌گیرد. برای انجام اسکن IPv6 توسط انمپ با دستوری مانند دستور زیر با استفاده از پارامتر 6- اسکن را آغاز می‌کنیم:

```
└─$ sudo nmap -6 ::1                                                    255 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-03 15:45 EST
Nmap scan report for localhost (::1)
Host is up (0.0000050s latency).
All 1000 scanned ports on localhost (::1) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

اسکن لوکیشن هدف:

یکی دیگر از کارهای جالبی که با انمپ می‌توان انجام داد اسکن لوکیشن و به‌دست آوردن مختصات تقریبی محل سرورها می‌باشد. سوالی که پیش می‌آید این است که یافتن محل استقرار سرورها چه سودی برای ما دارد؟ اسکن محل سرور به شما اطلاعات فراوانی نخواهد داد و صرفا برای این است که شما بدانید با چه کشوری طرف هستید و سرعت انتقال داده‌ها به سرور مورد نظر را تا حدودی حدس بزنید. البته این نکته هم باید گفته شود که هرچه فاصله شما تا محل قرارگیری سرورها بیشتر باشد، زمان انتقال اطلاعات بین شما و سرور بیشتر می‌شود. همیشه هم بحث هک اطلاعات نیست، برخی اوقات صحبت از نابودی اطلاعات است که دانستن محل قرارگیری سرورها ممکن است باعث خراب‌کاری و حملات غیر سایبری و فیزیکی مانند بمب‌گذاری‌ها و حملات موشکی از راه دور شود.

همان‌طور که در تصویر پایین نشان داده شده است با استفاده از دستور Sudo nmap -script ip-geolocation-* آدرس سایت انمپ شروع به اسکن کرده و لوکیشن را همانند عکس پایین در قسمتی که علامت‌گذاری شده است به ما نشان می‌دهد.

```
└─$ sudo nmap --script ip-geolocation-* scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-04 04:36 EST
NSE: [ip-geolocation-maxmind] You must specify a Maxmind database file with the maxmind_db argument.
NSE: [ip-geolocation-maxmind] Download the database from http://dev.maxmind.com/geoip/legacy/geolite/
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.069s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 964 filtered ports, 33 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
9929/tcp open  nping-echo

Host script results:
| ip-geolocation-geoplugin: coordinates: 37.5625, -122.0004
|_location: California, United States

Post-scan script results:
Unprotected error in Lua:
(null)
```

اسکن سیستم‌عامل هدف:

اسکن سیستم‌عامل یا os از مهمترین اسکن‌ها است زیرا پس از انجام این اسکن، سیستم‌عامل هدف شناسایی می‌شود و همه چیز برای نوشتن یک ویروس و فرستادن برای هدف مهیا می‌شود. یکی دیگر از مزیت‌های شناسایی سیستم‌عامل این است که می‌توان حفره‌های امنیتی آن را بهتر شناسایی کرد و حمله بهتر و اثربخش‌تری داشت. همان‌طور که در تصویر زیر مشخص است، با استفاده از دستور

sudo nmap -O آدرس سایت

می‌توان مشخص کرد چه سیستم‌عاملی بر روی سرور سایت در حال ران شدن است.

```
└─$ sudo nmap -O scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-04 14:45 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.018s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 987 filtered ports
PORT      STATE  SERVICE
21/tcp    closed ftp
22/tcp    open   ssh
53/tcp    closed domain
80/tcp    open   http
135/tcp   closed msrpc
143/tcp   closed imap
256/tcp   closed fw1-secureremote
443/tcp   closed https
587/tcp   closed submission
1723/tcp  closed pptp
8888/tcp  closed sun-answerbook
9929/tcp  open   nping-echo
31337/tcp open   Elite
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.47 seconds
```

جعل مک‌آدرس

در درجه اول به این می‌پردازیم که مک‌آدرس چست؟ مک‌آدرس یک آدرس ۴۸ بیتی است که توسط شرکت سازنده کارت شبکه شما تعیین می‌شود. این تعریف تا حدودی شبیه تعریف IP بود که در بالا به آن اشاره شد، اما تفاوت این دو در این است که مک‌آدرس یک شناسه سخت‌افزاری منحصر به فرد به کاربر می‌دهد اما IP یک شناسه خاص نرم‌افزاری. این دو تفاوت‌های دیگری نیز دارند، اما یکی از مهم‌ترین آن‌ها در بالا ذکر شد. جعل مک‌آدرس باعث سخت‌تر شدن ردیابی اسکن‌ها می‌شود.

همان‌طور که در تصویر زیر پیداست با استفاده از دستور

sudo nmap –spoof-mac 0 آدرس سایت

می‌توان مک آدرس را عوض کرد.

توجه کنید که دستور بالا یک مک‌آدرس تصادفی را برای شما در نظر می‌گیرد و امکان وارد کردن دستی مک‌آدرس هم وجود دارد که ما در این مقاله به آن نمی‌پردازیم.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --spoof-mac 0 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-05 17:55 UTC
Spoofing MAC address C0:72:39[redacted] (No registered vendor)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 54.00% done; ETC: 17:56 (0:00:09 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.022s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 28.09 seconds
```

استفاده از دام یا decoy:

اصولا شخصی که عمل اسکن را انجام می‌دهد علاقه‌ای به شناسایی هویتش ندارد و سعی می‌کند تا جایی که ممکن است خود را از نظرها پنهان کند. یکی از قابلیت‌های nmap این است که اسکن‌کننده می‌تواند تا حدودی خود را مخفی کند. این عمل چگونه صورت می‌گیرد؟ خود را در میان جمعیتی انبوه تصور کنید، همان‌طور که در حال لذت بردن از فضای اطراف خود هستید متوجه می‌شوید تلفن شما در جیبتان نیست. در انبوهی از جمعیت شما نمی‌دانید چه کسی تلفن شما را دزدیده است. در nmap همین ماجرا حالت نرم‌افزاری به خود گرفته و به این صورت عمل می‌کند که گویا از چندین دستگاه مختلف، اسکن انجام شده است. بنابراین وقت بیشتری باید صرف شود تا شخص اسکن‌کننده پیدا شود و یا حتی در برخی موارد پیدا نمی‌شود!

همان‌طور که در تصویر زیر مشخص است، با دستور

sudo nmap -D RND: تعداد تله‌ها آدرس سایت

می‌توان تعداد تله‌ها و اسکن را روی هدف انجام داد.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -D RND:20 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-05 08:22 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.044s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 94.90 seconds
```


منابع:

- Ipv6 چیست؟, respina.net
- تفاوت ipv6 با ipv4, mizbanfa.net
- پیدا کردن محل قرارگیری سرور های یک سایت, sarzamindownload.com
- کتاب آموزش اسکن شبکه با انمپ, netamooz.net

دارک وب

Dark web

حسین علی ترکان

h.alitorkan1380@gmail.com

احتمالا تا به‌حال اسم دارک وب به گوشتان خورده است. قسمت ناشناس و مخوفی از اینترنت که فضای بسیار مناسبی برای کلاهبرداران، قاچاقچی‌ها، مجرمان، هکرها و ... است. اما دارک وب در اصل چیست؟ چگونه می‌توان وارد آن شد و در آن فعالیت کرد؟ برای چه پدید آمده و چه استفاده‌هایی دارد و چرا مورد توجه مجرمان است؟

دارک وب چیست و چگونه می‌توان به آن متصل شد؟

دنیای اینترنت امروزه بسیار پرکاربرد و بزرگ شده است و بی‌انتها به‌نظر می‌رسد. در حال حاضر بیش از ۱.۷ میلیارد وب‌سایت در اینترنت وجود دارد و روزانه بیش از ۵۰۰ هزار وب‌سایت به آن‌ها اضافه می‌شود. با این حال این تنها نوک کوه یخ است و بخش عظیمی از اینترنت برای کاربران عادی از دسترس خارج است. به طور کلی فضای اینترنت را از نظر دسترسی کاربران می‌توان به سه دسته سرفیس وب (Surface Web)، دیپ وب (Deep Web) و دارک وب (Dark Web) تقسیم کرد.

• سرفیس وب :

این بخش شامل وب‌سایت‌هایی است که برای عموم مردم قابل دسترس هستند و توسط موتورهای جست‌وجو ایندکس (index) می‌شوند و قابل جستجو هستند. اندازه این بخش کمتر از ۵ درصد از کل اینترنت تخمین زده می‌شود.

• دیپ وب:

دیپ وب شامل صفحاتی از وب است که توسط موتورهای جست‌وجو ایندکس نمی‌شوند و از چشم کاربران عادی پنهان است. مانند صفحات لاگ‌این، دیتابیس‌ها، شبکه‌های داخلی ادارات و ... .

این بخش از اینترنت بسیار بزرگ است و نمی‌توان اندازه آن را تشخیص داد ولی تخمین زده می‌شود که حدود ۹۶ درصد اینترنت را شامل می‌شود.

• دارک وب:

دارک وب بخشی از دیپ وب محسوب می‌شود که روی دارک نت قرار دارد. برای دسترسی به این بخش به ابزار نرم‌افزای خاصی نیاز است، مانند مروگرهای تور (Tor). وب‌سایت‌هایی که در دارک وب میزبانی می‌شوند، دارای دامنه onion هستند.

دارک وب شبکه‌ای رمزنگاری شده و ناشناس است که با ارسال ترافیک کاربر از طریق هزاران گره شبکه در سراسر جهان، ردپای اینترنتی او را می‌پوشاند. در دارک وب، آدرس IP کاربر مخفی شده تا ردیابی ارتباطات اینترنتی او بسیار دشوار شود.

دارک وب محافظت از IP کاربر را با پنهان کردن آن در چندین لایه رمزنگاری شده و عبور دادن ترافیک او از میان شبکه‌ای از کامپیوترهای تصادفی انجام می‌دهد که هر یک از آن‌ها پیش از فرستادن داده به دستگاه

بعدی، یک لایه رمزنگاری را حذف می‌کند؛ بدین ترتیب، اطلاعات به‌صورت کاملا رندوم و ناشناس منتقل می‌شود، به‌طوری‌که نمی‌توان مبدا، مقصد یا محتویات آن را شناسایی کرد.
رایج‌ترین راه دسترسی به دارک وب استفاده از شبکه تور Tor است. تور مخفف The Onion Router (روتر پیازی) است و نرم‌افزاری آزاد و رایگان است. تور یک ابزار مخفی‌سازی است که بر خلاف بقیه مرورگرها از روتینگ چند لایه‌ای و به اصطلاح پیازی استفاده می‌کند که در آن ترافیک را از طریق چندین سرور در جهان رمزگذاری و هدایت می‌کند تا آدرس IP شما را مخفی کند.
تعداد کاربران روزانه دارک وب مشخص نیست، اما این تعداد نمی‌تواند زیاد باشد. پروژه تور که مسئول پنهان کردن هویت کاربران در دارک وب است، مدعی است تعداد کاربران روزانه این شبکه، ۲ میلیون نفر است و تنها ۱.۵ درصد از کل ترافیک حاضر در این شبکه، از وب‌سایت‌های دارک بازدید می‌کنند و دارک وب تنها ۰.۰۳ درصد کل فضای اینترنت تخمین زده می‌شود.

چرا دارک وب پدید آمد؟

ویژگی اصلی محیط دارک وب توانایی ناشناس بودن و داشتن اختیار بیشتر برای فعالیت به دور از نظارت ارگان‌ها و دولت‌های مختلف است. دارک وب فقط مخصوص افراد تبهکار و برای کارهای مجرمانه نیست و در مورد آن زیاد اغراق می‌شود. درست است که این محیط به دلیل ناشناس بودن پتانسیل بالایی برای کارهای مجرمانه دارد ولی تاثیر آن در مقایسه با تمام جرایم سایبری اینترنت آن‌قدرها هم زیاد نیست. از طرفی دارک وب آن‌چنان هم از دسترس قانون خارج نیست. در سال ۲۰۱۱ بیش از ۳۰۰ کاربر دارک وب به‌خاطر فعالیت‌های غیر قانونی دستگیر شدند. اگر بخش مجرمانه دارک وب را کنار بگذاریم پتانسیل زیادی دارد و می‌تواند جایی باشد که ایده‌ها بدون ترس از کنترل شدن بتوانند به اشتراک گذاشته شوند. مثلا در دارک وب می‌توانید عضو کلوپ‌های مختلف شوید و یا در BlackBook عضو شوید که نسخه دارک فیسبوک است و هیچ اطلاعاتی از کاربر نمی‌گیرد. در ضمن، بسیاری از سازمان‌های معتبر نیز نسخه‌ای از وب‌سایت خود را در دارک وب میزبانی می‌کنند تا کاربرانی که به حریم شخصی خود اهمیت می‌دهند، با نوعی شنل نامرئی و نقاب به گشت‌وگذار در آن‌ها بپردازند.

چگونه دارک وب پدید آمد؟

تولد اینترنت اولین قدم در جهت پیدایش دارک وب بود. ولی برای پیدایش و تکمیل به دو مولفه اصلی دیگر نیاز داشت. سیستمی برای مخفی کردن هویت کاربران و ارزهای دیجتالی غیرمتمرکز و خارج از دسترس دولت‌ها.
پروژه تور از وزارت دفاع آمریکا شروع شد اما مدتی بعد به پروژه‌ای متن‌باز و رایگان تبدیل شد و در سال ۲۰۰۲ نسخه آلفا و ناپایدار شبکه تور با ۱۲ گره از کاربران داوطلب راه‌اندازی شد و بعدا توسعه پیدا کرد.
در سال ۲۰۰۹ نرم افزار استخراج بیت‌کوین برای عموم عرضه شد و در نتیجه آن، اولین بازار سیاه به نام سیلک رود (Silk Road) در سال ۲۰۱۱ در بستر اینترنت پدید آمد. سیلک رود به دلیل ترکیب خلاقانه بیت‌کوین و سامانه تور که هم هویت کاربران و هم تراکنش‌های آن‌ها را ناشناس می‌کرد به موفقیت رسید. جای تعجب نیست که این فروشگاه به سرعت به جایی برای خرید و فروش مواد مخدر و اکانت‌های هک شده و دیگر وسایل غیرمجاز و حتی محلی برای اجیر کردن آدم کش‌ها تبدیل شد. اما این بازار زیاد دوام نیاورد و FBI در سال ۲۰۱۳ موفق شد سایت را مصادره کرده و صاحب ۲۹ ساله آن، راس اولبریکت را به حبس ابد محکوم کند. بعد از سیلک رود بازارهای سیاه دیگری نیز پدید آمدند که آن‌ها هم به سرنوشت مشابه دچار شدند ولی تا وقتی تقاضا وجود دارد و تکنولوژی مورد نیاز فراهم باشد، این جریان ادامه خواهد داشت و دارک وب به حیات خود ادامه می‌دهد.

منابع:
- دارک وب چیست, zoomit.ir
- What is the Deep and Dark Web?, kaspersky.com

حملات سایبری امروزه گستره زیادی پیدا کرده‌اند. از وسایل و اشیا کوچک خانه گرفته تا قوی‌ترین سرورهای دنیا. در این مقاله قصد داریم حملات سایبری و جنبه‌های آن در رابطه با ماهواره‌ها را بررسی کنیم.
حملات سایبری به ماهواره به دو دسته کلی تقسیم می‌شوند. حملات و تکنیک‌های مربوط به تجهیزات الکترونیک یا Electronic Warfare و دسته دیگر حملاتی که مربوط به شبکه و نرم‌افزارهای کنترل ماهواره‌ها می‌شوند. دسته مربوط به حملات الکترونیک مانند Jamming یا بستن سیگنال‌های ارسالی و دریافتی از ماهواره که در کل مربوط به فرکانس‌های ارتباطی بین ماهواره و ایستگاه‌های زمینی می‌شود، مورد بحث قرار نمی‌گیرند و تمرکز بر روی شبکه و نرم‌افزار می‌باشد.

در مدار امنیت

On Cybersecurity Orbit

علی دادخواه
ali.t_lt@yahoo.com

درباره علت و انگیزه حملات به ماهواره می‌توان به نقش کلیدی آن‌ها در تمامی زمینه‌ها اشاره کرد. ارسال و دریافت سیگنال‌های تلویزیونی، ارتباطات رادیویی نظامی و انتقال داده‌های هواشناسی از جمله زمینه‌هایی هستند که ماهواره در آن‌ها نقشی مهم را ایفا می‌کند و در صورتی که ماهواره‌ای مورد حمله قرار گیرد، امور قشر بزرگی از مردم مختل می‌شود. برای مثال تداخل در ماهواره‌های GPS باعث می‌شود که اپلیکیشن‌های ناوبری و خدمات تاکسی‌رانی دچار مشکل شوند و یا حتی شرکت‌های صنعتی که از ساعت دقیق ماهواره GPS به عنوان مبنا استفاده می‌کنند نیز به مشکل بر می‌خورند.

نقاط ضعف

دسته‌بندی نقاط ضعف ماهواره‌ها به شکل زیر است: ۱- ضعف در تجهیزات شبکه اعم از ایستگاه‌های زمین، شرکت‌های مرتبط و کاربران ۲- وجود ضعف در خود ماهواره‌ها ۳- ضعف در زنجیره تامین
مورد سوم از این دسته‌بندی از دو مورد دیگر آسیب‌زننده‌تر است چرا که ضعف در تجهیزات شبکه و یا خود ماهواره‌ها مواردی هستند که به چشم می‌آیند و حتی تا قبل از پرتاب ماهواره بر روی آن‌ها بسیار کار می‌شود تا این نقاط ضعف پوشش داده شوند. اما به دلایل اقتصادی و زمان‌بندی پروژه‌ها ممکن است بخشی از ساخت برون‌سپاری شود و یا به علت انحصاری بودن صنایع فضایی، تنها شرکت‌های محدودی قادر به تولید قطعات ماهواره‌ها باشند. از این رو ممکن است بک‌دور (BackDoor)هایی در نرم‌افزار و یا عیوبی در سخت‌افزارها وجود داشته باشند که بعد از پرتاب معلوم شوند و یا حتی بدتر از آن هیچ‌گاه به وجود آن‌ها پی برده نشود و به دلیل این‌که تامین امنیت سایبری از سوی دیگر شرکت‌های تولیدکننده از حیطه کاری شرکت مالک ماهواره خارج است، خود به خود به ریسک‌های امنیتی پروژه افزوده می‌شود.

انگیزه‌های حمله

انگیزه‌های حمله به ماهواره‌ها بیشتر به طرفین مالک ماهواره و حمله‌کننده بستگی دارد. به علت هزینه‌بر بودن ساخت و پرتاب آن‌ها با بازیگران ثابت و مشخصی روبه‌رو هستیم. دولت‌ها و شرکت‌های خاص. چند مورد از علل حملات عبارتند از: از کار انداختن سرویس‌دهی ماهواره، به دست گرفتن کنترل ماهواره، اخاذی و باج‌گیری و همچنین جاسوسی. از کار انداختن سرویس‌دهی ماهواره بیشتر اهداف مالی و اقتصادی را دنبال می‌کند. طرف حمله‌کننده با ایجاد اختلال در سرویس‌دهی ماهواره‌ها برای مثال می‌تواند شبکه‌های تلویزیونی را دچار ضرر مالی کند و برنامه‌های ثابت آن‌ها را به‌هم بریزد. باج‌گیری نیز هدف مالی دارد، منتها برعکس مورد قبل به ضرر مالکین کار نمی‌کند و فقط تامین سود خود را مدنظر دارد. موارد دیگر بیشتر در بین دولت‌ها و دشمنانشان رواج دارد و به اهداف و پیام‌های سیاسی مرتبط می‌شود.

روش‌های مختلف نفوذ

اولین بخش مورد بررسی در این مقاله، ایستگاه‌های زمینی متصل به ماهواره هستند. این تجهیزات با اتصال به بخش دیگری به نام مرکز فرمان، اطلاعات را از ماهواره دریافت می‌کنند و دستورات را به آن ارسال می‌کنند. جایی که معمولا حملات از آن‌جا آغاز می‌شوند پرسنل و افراد مسئول در این مکان‌ها هستند. با تکنیک‌های مهندسی اجتماعی و پیدا کردن آدرس ایمیل و صفحات مجازی پرسنل، آن‌ها را وادار به باز کردن لینک‌های مخرب یا اجرای هر روش دیگری می‌کنند تا بتوانند فایل‌های خود را بر روی شبکه ایستگاه‌های زمینی پیاده کنند و نفوذ را از آن‌جا دنبال کنند. همچنین بخش‌های دیگر که مسئول پردازش داده‌های دریافتی از ماهواره می‌باشند نیز می‌توانند به عنوان حفره‌ای برای نفوذ استفاده شوند. مانند سال ۲۰۱۴ که هکرها از طریق شبکه NOAA[1] اطلاعات ماهواره‌های هواشناسی ملی آمریکا را به سرقت بردند و در روند دریافت داده اختلال ایجاد کردند که در نتیجه آن، دو روز تمامی سرویس‌های اعلام وضعیت هوای ملی تعطیل شد تا اینکه ماهواره‌ها به روند عادی خود بازگردانده شدند.

راه نفوذ بعدی از طریق رادیو فرکانس‌های در ارتباط با ماهواره است که به آن روش مستقیم گفته می‌شود. فرکانس‌های ارسالی و دریافتی از ماهواره‌ها این نقطه ضعف را ایجاد می‌کنند که از هر مکانی که ماهواره پوشش داشته باشد، حمله نیز صورت بگیرد. ماهواره‌های تجاری و یا مرتبط با مسائل جغرافیایی معمولا پوشش گسترده‌ای دارند و ارتباطات خود را نیز رمزگذاری نمی‌کنند و این موضوع باعث بالا رفتن ریسک حملات می‌شود. همچنین ماهواره‌ها علاوه بر فرکانس‌های دریافت داده‌های معمول، یک لینک به‌خصوص برای دریافت فرمان‌های جابه‌جایی و کنترل نرم‌افزاری دارند که در موارد نادر لینک کنترلی نیز تحت حمله قرار می‌گیرد.

متد بعدی برای نفوذ استفاده از اطلاعات محرمانه زنجیره تامین است که قبلا هم ذکر شد. ممکن است با بررسی آن اطلاعات راه نفوذ به مراتب راحت‌تری در سخت‌افزار یا نرم‌افزارهای شرکت‌های دیگر یافت شود و مهاجمان را در پیدا کردن حفره‌ها یاری کند. با توجه به این‌که حتی بزرگترین سازمان‌های فضایی دنیا مانند NASA نیز قطعات مورد نیاز خود را از دیگر شرکت‌ها تهیه می‌کنند، جلوگیری از وجود حفره امنیتی در محصولات تقریبا اجتناب‌ناپذیر است و مدیران باید برای به حداقل رساندن ریسک، در تامین و لجستیک شرکت ریزبینانه عمل کنند و ساده از مسائل امنیت سایبری نگذرند.

ماهواره‌هایی که مورد حمله قرار گرفته‌اند

گفته شد که مالکیت بیشتر ماهواره‌ها در جهان در دست دولت‌ها و شرکت‌های بزرگ بین‌المللی است. برای همین اخبار و اطلاعات کمی از حملات انجام شده به ماهواره‌ها به بیرون درز می‌کند و این بازیگران فضایی بزرگ ترجیح می‌دهند اخبار شکست خود در زمینه‌های فضایی را به بیرون مخابره نکنند. اما با این حال چندین مورد وجود دارد که حمله انجام شده توسط مقامات مربوطه تایید شده‌اند.

مورد اول مربوط به ماهواره ROAST است. ماهواره X-Ray آلمانی-آمریکایی که توسط هکرهای روس در سال ۱۹۹۸ مورد حمله از طریق ایستگاه‌های زمینی قرار گرفت. در طی این حمله کامپیوترهای NASA در مرکز Goddard در مریلند هک شد و هکرهای روسی کنترل ماهواره را به‌دست گرفتند و آن را به سمت خورشید برگرداندند. این چرخش باعث شد که باتری‌ها و دیگر تجهیزات ماهواره از شدت تابش گرما بسوزند و ماهواره به کلی بدون استفاده شود. همچنین گفته شده که اطلاعات دریافت شده از ماهواره به مسکو منتقل شده است.

ماهواره بعدی Landsat 7 بود که در سال ۲۰۰۷ مورد حمله قرار گرفت. این ماهواره به طور مشترک توسط NASA و سازمان زمین‌شناسی آمریکا کنترل می‌شد و نوع حمله از نوع مستقیم به خود ماهواره از طریق لینک‌های کنترلی بود. این حمله ۱۲ دقیقه طول کشید و یک حمله دیگر نیز مشابه همین حمله در سال ۲۰۰۸ اتفاق افتاد که در هیچ یک از این دو هکرها نتوانستند کنترل ماهواره را در دست بگیرند. (این دو حمله به هکرهای چین نسبت داده شد.)

در سال ۲۰۰۸ ماهواره Terra EOS AM-1 نیز دوبار مورد حمله قرار گرفت. یک‌بار در ژوئن و یک‌بار دیگر در اکتبر. در حمله ژوئن دو دقیقه و در حمله اکتبر نه دقیقه کنترل ماهواره‌ها به دست هکرها افتاد و آن‌ها کنترل کامل بر روی ماهواره داشتند اما هیچ‌گونه دستوری اجرا نکردند. این حمله نیز به هکرهای چینی منتسب شده است و گفته می‌شود که از نوع حمله مستقیم به خود ماهواره بوده است.

دفاع

جلوگیری و دفاع از وقوع چنین حملاتی نیازمند سیستم‌هایی از پیش تعیین شده در سخت‌افزار ماهواره می‌باشد. اولین و بهترین راه رمزگذاری داده‌ها و انجام احراز هویت‌های صحیح و اصولی در ابتدای برقراری ارتباط است. می‌توان گفت تمام ماهواره‌های نظامی و دولتی از رمزگذاری استفاده می‌کنند اما اطلاعات کاملی از استفاده از این تکنیک در ماهواره‌های خصوصی در دسترس نیست. برخی ماهواره‌ها از پروتکل سازمان ملی استاندارد و تکنولوژی آمریکا استفاده می‌کنند و الگوریتم AES را برای رمزگذاری انتخاب کرده‌اند و برخی دیگر نیز پروتکل‌های مخصوص به خود را دارند. برای مثال یک ماهواره چینی از الگوریتمی به نام QKD[2] برای رمزگذاری استفاده می‌کند و معتقد است که این رمزگذاری کوانتومی حداقل در تئوری غیرقابل هک شدن است.

سرویس‌هایی مانند IDS[3] و IPS[4] گزینه بعدی برای ارتقا سطح دفاعی ماهواره‌ها هستند. این سرویس ها باید بر روی خود ماهواره پیاده‌سازی شوند. سرویس IDS کار مانیتورینگ و بررسی تمام ارتباط برقرار شده را بدون وقفه انجام می‌دهد و اگر به ارتباطی مشکوک و یا دستورهایی بالاتر از محدوده‌های تعیین شده برخورد کند اعلام خطر می‌کند و سرویس IPS اینجا وارد می‌شود و با توجه به شدت هشدار اعلام شده هر یک از اقدامات لازم مثل بلاک کردن دستورات اجرایی، بازخوانی نرم‌افزار اصلی ماهواره و خاموش کردن بخش‌های مشکوک را انجام می‌دهد.

اقدام بعدی قبل از پرتاب ماهواره انجام می‌گیرد. هنگامی که ماهواره آماده پرتاب می‌شود باید تحت حملات سایبری متعدد قرار بگیرد و تست‌های مربوطه را به خوبی بگذراند. در سال ۲۰۲۰ شرکتی به نام ManTech که یک شرکت آمریکایی در حوزه تامین امنیت برای دولت‌ها و شرکت‌های خصوصی است، سرویسی به خدمات خود اضافه کرده است به نام Space Range. این شرکت تست‌های مختلفی در رابطه با امنیت سایبری را بر روی ماهواره‌ها انجام می‌دهد و نتیجه را همراه با پیشنهادات لازم به مالک ماهواره اعلام می‌کند.

اما آخرین توصیه که در تمامی سیستم‌ها باید رعایت شود، چه در فضا و چه بر روی زمین، logging دقیق و با نظم است. لاگ کردن ثبت و ذخیره اطلاعات مربوط به اتفاقات رخ داده در سیستم در طول یک بازه زمانی است که بعدا برای آنالیز و بررسی به‌کار می‌رود. هر دو بخش کنترل زمینی و خود ماهواره باید logging داشته باشند و هر از چند گاهی باید این دو لاگ برای پیدا کردن تفاوت‌ها بین دستورات ارسال شده از ایستگاه و دستورات دریافت شده در ماهواره با یکدیگر مقایسه شوند.

در آخر اما باید دانست که ریسک‌های امنیتی ماهواره‌ها هر روز رو به رشد هستند و متاسفانه در طرف مقابل نه تنها سازمان و برنامه جامعی برای استاندارد سازی زمینه‌های امنیتی وجود ندارند بلکه از نشر دادن و به اشتراک گذاشتن تجربه‌های ناموفق قبلی نیز خودداری می‌شود. این موضوع مانع از این می‌شود که تجهیزاتی عمدتا به ارزش میلیون دلاری راهی فضا شوند، بدون آن‌که امنیت شان به‌طور کامل تامین شده باشد.

[1] National Oceanic and Atmospheric Administration

[2] Quantum key distribution

[3] Intrusion Detection System

[4] Intrusion Prevention System

منبع:

• Luke Shadbolt, Technical Study Satellite Cyberattacks and Security, HDI Global Specialty SE

خبرهای مهم

گزیده اخبار بهمن‌ماه

گردآورنده: سروش ذوالفقاری
zolfaghari.soroush@gmail.com

مهاجمان از یک ترفند 20 ساله برای فیشینگ کاربران مایکروسافت 365 استفاده می کنند

هکرهای مخرب تکنیک قدیمی بازگردانی راست به چپ (RLO: Right to left override) را برای پنهان کردن فایل‌های مخرب و جمع‌آوری اعتبار حذف کرده‌اند. شرکت امنیتی ایمیل Vade افزایشی را در حملات RLO مشاهده کرده است.

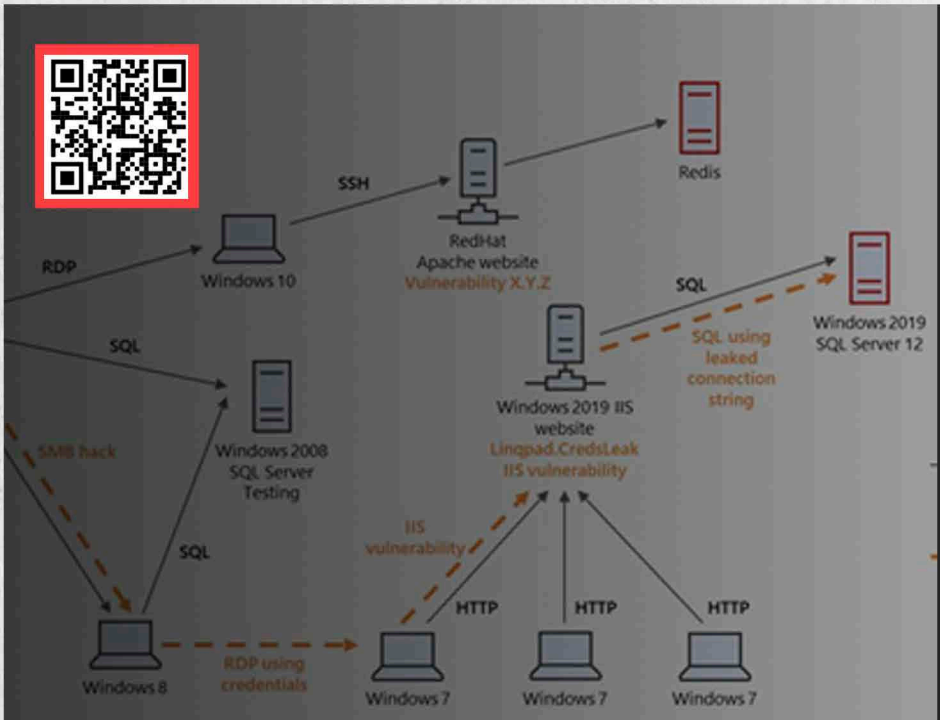
RLO یک کاراکتر Unicode غیرچاپی [U+202e] است که عمدتا برای پشتیبانی از زبان‌های عبری و عربی استفاده می‌شود. این کاراکتر به جای ترتیب خواندن انگلیسی از چپ به راست، تمام متن‌های بعدی را به سمت راست به چپ تغییر می‌دهد. به عنوان مثال، فایلی به نام "HelloCyberNews" با کاراکتر Unicode اضافه شده به عنوان "Hello{U+202e]CyberNews" با نام "HellosweNrebyC" نمایش داده می‌شود.

ناظر فرانسوی می‌گوید گوگل آنالیتیکس خطراتی را برای حفظ حریم خصوصی داده‌ها به همراه دارد

ناظر (Watchdog) فرانسوی، CNIL اعلام کرد گوگل آنالیتیکس، پرکاربردترین سرویس تجزیه و تحلیل وب جهان که توسط گوگل آلفابت توسعه یافته است، خطر دسترسی سرویس‌های اطلاعاتی ایالات متحده به داده‌های کاربران وب‌سایت‌های فرانسوی را فراهم می‌کند.

تحقیقات اخیر بر اساس تجزیه و تحلیل بلاکچین منتشر شده توسط Chainalysis نشان می‌دهد که سال گذشته ۷۴ درصد از درآمد باج‌افزار به عوامل تهدید وابسته به روسیه اختصاص یافته است. به عبارت دیگر، حدود ۴۰۰ میلیون دلار ارز دیجیتال در نهایت جیب مجرمان سایبری مرتبط با روسیه را پر کرد.

۴۰۰ میلیون دلار درآمد باج‌افزار در سال ۲۰۲۱ نصیب گروه‌های مرتبط با روسیه شد



محیط هوشمند و شبیه‌سازی‌شده مقابله با حملات

مایکروسافت، نرم‌افزاری را متن‌باز کرده است که با به‌کارگیری الگوریتم‌های یادگیری تقویتی، محیطی آسیب‌پذیر در شبکه می‌سازد و براساس یافته‌های مهاجم، آموزش می‌بیند که حملات بعدی مهاجم برای پیش‌روی (lateral movement) و ارتقا سطح دسترسی را بشناسد و از آن‌ها جلوگیری کند. اگرچه این پلتفرم هنوز در فاز تحقیق و توسعه قرار دارد اما به‌عنوان گسترش ایده و به‌کارگیری آزمایشی آن می‌تواند به ما کمک کند.

@offsecmag

شناخت در پشتی (back door) در پردازنده‌های اینتل

طبق بررسی‌های اخیر یکی از محققان شرکت گوگل، در پردازنده‌های شرکت اینتل یک استک نرم‌افزاری به‌همراه یک سیستم‌عامل ساده MINIX مخفی وجود دارد که شامل یک وب‌سرور نیز می‌باشد. دسترسی به آن بسیار سخت، کند و به همان اندازه خطرناک است.

معماری امنیت اطلاعات

آشنایی با انمپ-قسمت دوم

دارک وب

در مدار امنیت

Cyber news

روز صفرم ترجمه ی عبارت Zero Day می‌باشد که در تعبیر لغوی یعنی روزی که هنوز به آن نرسیده‌ایم و از وجود چنین چیزی هم خبر نداریم، وقتی صحبت از حمله Zero Day می‌شود یعنی در خصوص حمله ای صحبت می کنیم که هیچکس تا کنون آن را شناسایی نکرده است و هیچ دانشی هم در خصوص آن وجود ندارد که چگونه آن را تشخیص و بعضا از بروز آن جلوگیری کنیم.

در این نشریه سعی بر آن است تا زوایای پنهان و ناشناخته در دنیای امنیت اطلاعات مورد بررسی قرار گرفته و به جدیدترین اخبار و تکنولوژی‌های این حوزه پرداخته شود. مخاطبین این نشریه تمامی دانشجویان و افرادی خواهند بود که به حوزه امنیت اطلاعات علاقمند هستند.

برای ارسال مقالات جهت چاپ در نشریه به @elahe_rahbaran در تلگرام پیام دهید.