# DNS over HTTPS چیست و در ویندوز چگونه فعال میشود؟

DNS over HTTPS (DoH) پروتکلی است که ترافیک DNS را با ارسال Queries DNS از طریق یک Session رمزگذاری شده HTTPS رمزگذاری می کند. DoH می تواند به بهبود امنیت و حریم خصوصی آنلاین کمک کند و از Queries DNS در برابر حملات محافظت کند.

DoH که در سال 2018 معرفی شد، مشابه DNS کار می کند، اما از Session HTTPS برای ایمن نگه داشتن درخواست ها و به حداقل رساندن رصد اطلاعات رد و بدل شده در طول پرس و جوها استفاده می کند.

مرورگرهای وب پیشرو، از جمله موزیلا فایرفاکس، مایکروسافت اج و گوگل کروم، از DoH برای افزایش حریم خصوصی و امنیت داده ها برای کاربران استفاده می کنند.

نحوه فعال سازی در ویندوز :

وارد تنظیمات کارت شبکه و DNS شده و از طریق منو مربوطه نسبت به فعالسازی آن می توان به صورت قالب های پیش فرض و یا قالب های شخصی اقدام نمود.

|  |  |
| --- | --- |
| نحوه فعالسازی | سرور های قابل استفاده و رایج  Server Owner    Server IP addresses |
|  | Cloudflare           1.1.1.1                                1.0.0.1                                2606:4700:4700::1111                                2606:4700:4700::1001  Google                 8.8.8.8                                8.8.4.4                                2001:4860:4860::8888                                2001:4860:4860::8844  Quad9                  9.9.9.9                               149.112.112.112                               2620:fe::fe                               2620:fe::fe:9 |

# DNS Tunneling چیست و چگونه تشخیص داده میشود؟

تونل DNS نوعی حمله است که از بد افزار استفاده می کند که در آن هکرها کد یا برنامه های مخرب را در پیامی قرار می دهند که در ظاهر به نظر می رسد یک درخواست DNS است. از آنجایی که DNS جزء ضروری اکثر فعالیت های شبکه و اینترنت است، این نوع ترافیک اغلب بدون بررسی دقیق قادر به عبور از فایروال ها و سایر سیستم ها است.

شمای کلی نحوه انجام یک حمله DNS به شرح زیر است:

**ثبت دامنه میزبان:** یک هکر یک دامنه را ثبت می کند و حتی ممکن است یک سایت با ظاهر قانونی ایجاد کند. در این سایت، هکر همچنین برنامه های بدافزار تونل زنی DNS را نصب کرده و در صورت دسترسی کاربران به بد افزار آماده توزیع در شبکه خواهد بود.

**آلوده کردن رایانه هدف با بدافزار:** مرحله بعدی که اغلب دشوارترین است، آلوده کردن رایانه ای در شبکه هدف به بدافزار است. این را می توان به روش های مختلف انجام داد، از جمله استفاده از سایر وب سایت های آلوده، ایمیل های آلوده، یا حتی سخت افزارهای آسیب دیده وارد شده به زیرساخت های یک شرکت.

**اتصال رایانه آلوده را به وب سایت هکر:** هنگامی که بد افزار آماده شد، رایانه آلوده سعی می کند به وب سایت هکر متصل شود. بخشی از این اتصال، ارسال یک درخواست DNS برای پیدا کردن آن وب سایت است. درخواست‌های DNS همیشه مجاز به عبور از فایروال‌ها هستند و به هکر یک اتصال ساده در ساختار سیستم‌های محافظت‌شده می‌دهند.

**عبور دادن کد مخرب از طریق DNS Resolver:** هنگامی که یک اتصال برقرار و تأیید شد، سرور میزبان هکر می‌تواند کد یا برنامه‌های اضافی را به شبکه هدف ارسال کند. این کد می‌تواند برای جمع‌آوری داده‌ها، قرار دادن برنامه‌ها در سیستم‌ها یا انجام هر کار دیگری که می‌تواند امکان بهره‌برداری طولانی‌مدت از سیستم‌های در معرض خطر را فراهم کند، استفاده شود.

**شناسایی حملات DNS Tunneling**

شناسایی یک حمله تونل زنی DNS می تواند دشوار باشد

* اولین قدم در شناسایی حمله تونل زنی DNS آنتی ویروس/ضد بدافزار پیشرفته است.
* اسکن‌های عمیق تمام ترافیک، از جمله درخواست‌های DNS
* بررسی ترافیک ورودی و خروجی از شبکه
* بررسی اندازه Request و Response

اندازه درخواست و پاسخ می تواند به افشای تلاشهای مشکوک تونل DNS کمک کند. از آنجایی که بایت های اضافی در هدر بسته به عنوان بخشی از تونل سازی DNS درج می شوند، نظارت بر نسبت بایت های استفاده شده در زمینه منبع به بایت های استفاده شده در قسمت مقصد می تواند به شناسایی یک فعالیت مشکوک کمک کند. ابزارهای تشخیصی ابتدا بسته‌ها را ضبط می‌کنند، تعداد بایت‌ها را ذخیره می‌کنند و نسبت را اندازه‌گیری می‌کنند و به دنبال یک تغییر در این نسبت هستند.

# حمله FTP Bounce Back را تشریح کنید

فرض کنید X یک کاربر در attacker.com است و X می خواهد یک فایل را از target.com منتقل کند. اما X مجوز انتقال فایل ها از target.com را ندارد. ماشین دیگری به نام Middle-man.com وجود دارد که اجازه انتقال فایل ها از target.com را دارد.

بنابراین، X یک برنامه ریزی می کند. او یک اتصال FTP را به middle-man.com باز می کند. و سپس، به middle-man.com دستور می دهد تا فایل را با استفاده از پروتکل FTP از target.com به attacker.com منتقل کند. به این سبک از حمله FTP Bounce Back میگویند. این حمله زمانی ممکنه است که FTP سرور middle-man.com از حالت Passive پشتیبانی می کند.

X یک اتصال FTP را از attacker.com به FTP Server middle-man.com باز می کند

X فرمان پورت را صادر می کند و از سرور می خواهد که یک اتصال داده به پورت M باز کند. اما او سرور FTP را فریب می دهد. به جای مشخص کردن آدرس IP sulmer.com، آدرس IP target.com را می دهد.

X اکنون فایلی از دستورات فهرست شده را به سرور FTP ارسال می کند و از آن درخواست می کند تا آن را اجرا کند.

این فایل دارای مجموعه دستورات زیر است:

1. ایجاد یک اتصال FTP به target.com

2. middle-man.com از حالت Passive استفاده می کند. بنابراین، باید یک شماره پورت ارسال کند که target.com باید یک اتصال داده را به آن باز کند. Middle-man.com آن را با دستور پورت مشخص می کند، اما به جای دادن آدرس IP Middle-man.com، آن فایل آدرس IP attacker.com را در درون خود دارد.

3. فایل مد نظر بر روی اتصالی که بدین ترتیب ایجاد شده است، انتقال داده میشود.

# امن سازی ایمیل را تحقیق کنید

امنیت سرور ایمیل، مانند هر نوع دیگری از امنیت سایبری، تلاشی مداوم است که مستلزم سازگاری با تهدیدات جدید و به روز رسانی منظم برای پیش دستی از خطرات احتمالی است. روش های متداول

نحوه امن سازی ایمیل:

عدم استفاده از پیکربندی رله باز

پیاده سازی چارچوب خط مشی فرستنده (SPF)

پیاده سازی DomainKeys Identified Email (DKIM)

پیاده سازی گزارش و انطباق احراز هویت پیام مبتنی بر دامنه (DMARC)

انسداد فرستنده های مخرب را با Reversed DNS

استفاده از Blocklist مبتنی بر Domain برای مسدود کردن ایمیل ها و دامنه های مخرب

برای مسدود کردن URI های مخرب، از یک Blocklist real-time URI هرزنامه استفاده کنید

مسدودی فیشرها و هرزنامه‌ها را با یک Local Blocklist IP

پیاده سازی امنیت لایه Transport

# انواع حملات ایمیل

فیشینگ: فیشینگ نوعی کلاهبرداری است. مجرمان سایبری از ایمیل، پیام‌رسانی فوری یا سایر رسانه‌های اجتماعی برای جمع‌آوری اطلاعاتی مانند اعتبار ورود به سیستم با ظاهر شدن به عنوان یک شخص معتبر استفاده می‌کنند. فیشینگ زمانی اتفاق می‌افتد که یک طرف مخرب ایمیلی جعلی ارسال می‌کند که در ظاهر از یک منبع مجاز و قابل اعتماد است. هدف پیام فریب گیرنده برای نصب بدافزار بر روی دستگاهش یا به اشتراک گذاری اطلاعات شخصی یا مالی است.

Spear phishing یک حمله فیشینگ بسیار هدفمند است. در حالی که فیشینگ و فیشینگ هدفمند هر دو از ایمیل ها برای دسترسی به قربانیان استفاده می کنند، فیشینگ هدفمند ایمیل های سفارشی شده را برای یک شخص خاص ارسال می کند. مجرم قبل از ارسال ایمیل در مورد علایق هدف تحقیق می کند.

Vishing: Vishing فیشینگ با استفاده از فناوری ارتباط صوتی است. مجرمان می توانند با استفاده از فناوری صوتی از طریق IP، تماس های منابع مجاز را جعل کنند. قربانیان همچنین ممکن است پیام ضبط شده ای دریافت کنند که مجاز به نظر می رسد. مجرمان می خواهند شماره کارت اعتباری یا سایر اطلاعات را برای سرقت هویت قربانی به دست آورند. Vishing از این واقعیت استفاده می کند که مردم به شبکه تلفن اعتماد دارند.

Smishing: Smishing فیشینگ با استفاده از پیام های متنی در تلفن های همراه است. مجرمان در تلاش برای جلب اعتماد قربانی جعل منبع مشروع هستند. به عنوان مثال، یک حمله smishing ممکن است یک لینک وب سایت را برای قربانی ارسال کند. هنگامی که قربانی از وب سایت بازدید می کند، بدافزار بر روی تلفن همراه نصب می شود.

نهنگ: یک حمله فیشینگ است که اهداف با مشخصات بالا در یک سازمان مانند مدیران ارشد را هدف قرار می دهد. اهداف اضافی شامل سیاستمداران یا افراد مشهور است.

Pharming: Pharming جعل هویت یک وب سایت مجاز به منظور فریب کاربران برای وارد کردن اعتبار آنها است. Pharming کاربران را به سمت وب سایت جعلی هدایت می کند که به نظر رسمی می رسد. سپس قربانیان با این تصور که به یک سایت قانونی متصل شده اند، اطلاعات شخصی خود را وارد می کنند.

Spyware: نرم افزار جاسوسی نرم افزاری است که مجرم را قادر می سازد تا اطلاعاتی در مورد فعالیت های رایانه ای کاربر به دست آورد. نرم‌افزارهای جاسوسی اغلب شامل ردیاب‌های فعالیت، جمع‌آوری ضربه کلید و ضبط داده می‌شوند. در تلاش برای غلبه بر اقدامات امنیتی، نرم افزارهای جاسوسی اغلب تنظیمات امنیتی را تغییر می دهند. نرم افزارهای جاسوسی اغلب خود را با نرم افزارهای قانونی یا اسب های تروجان همراه می کنند. بسیاری از وب سایت های اشتراک افزار پر از نرم افزارهای جاسوسی هستند.

Scareware: Scareware کاربر را متقاعد می کند که بر اساس ترس اقدام خاصی انجام دهد. Scareware پنجره های پاپ آپی را ایجاد می کند که شبیه پنجره های گفتگوی سیستم عامل است. این پنجره ها پیام های جعلی را ارسال می کنند مبنی بر اینکه سیستم در معرض خطر است یا برای بازگشت به عملکرد عادی نیاز به اجرای یک برنامه خاص دارد. در واقع هیچ مشکلی وجود ندارد و در صورت موافقت کاربر و اجازه اجرای برنامه مذکور، بد افزار سیستم او را آلوده می کند.

ابزارهای تبلیغاتی مزاحم: ابزارهای تبلیغاتی مزاحم معمولاً پاپ آپ های آزاردهنده ای را برای ایجاد درآمد برای نویسندگان خود نمایش می دهند. این بدافزار ممکن است با ردیابی وب‌سایت‌های بازدید شده، علایق کاربر را تحلیل کند. سپس می تواند تبلیغات پاپ آپ مربوط به آن سایت ها را ارسال کند. برخی از نسخه های نرم افزار به طور خودکار Adware را نصب می کنند.

هرزنامه: هرزنامه (همچنین به عنوان نامه های ناخواسته شناخته می شود) ایمیل ناخواسته است. در بیشتر موارد، هرزنامه یک روش تبلیغاتی است. با این حال، هرزنامه می تواند لینک های مضر، بدافزار یا محتوای فریبنده را ارسال کند. هدف نهایی به دست آوردن اطلاعات حساس مانند شماره تامین اجتماعی یا اطلاعات حساب بانکی است. بیشتر هرزنامه ها از چندین رایانه در شبکه های آلوده به ویروس یا کرم می آیند. این کامپیوترهای در معرض خطر تا حد امکان ایمیل انبوه ارسال می کنند.

# NAS های در دسترس اینترنت

[**89.41.42.179**](https://www.shodan.io/host/89.41.42.179)

* [Asiatech Data Transmission Co.](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+org%3A%22Asiatech+Data+Transmission+Co.%22)
* [Iran, Islamic Republic of](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+country%3A%22IR%22), [Tehran](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+city%3A%22Tehran%22)

[self-signed](https://www.shodan.io/search?query=NAS+country%3A%22IR%22+tag%3Aself-signed)

**SSL Certificate**

* Issued By:
  + - |- Common Name: **QNAP NAS**
    - |- Organization: **QNAP Systems, Inc.**
* Issued To:
  + - |- Common Name:**QNAP NAS**
    - |- Organization:**QNAP Systems, Inc.**

Supported SSL Versions:  
**TLSv1.2, TLSv1.3**

HTTP/1.1 200 OK

Date: Sat, 17 Feb 2024 18:18:40 GMT

Server:

X-Frame-Options: SAMEORIGIN

Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval' ; object-src 'self' ; worker-src 'self' blob:

Content-type: text/html; charset=UTF-8

Last-modified: Sat, 29 Jan 2022 03:03:37 GM...

# LOM برای Storage Unity

|  |  |  |
| --- | --- | --- |
| **Part Number** | **Description** | **تعداد** |
| **210-ASLF** | **UNITY 2U 25X2.5 DRIVE DAE FLD RCK** | **8** |
| **D3-2S12FX-1600** | **UNITY 1.6TB FAST VP SSD 25X2.5 DRIVE** | **200** |
| **D3MSHDMSSHD5** | **Unity 2x5M MINI SAS HD Cables** | **10** |
| **D3MSHDMSSHD2** | **UNITY 2X2M MINI SAS HD CABLES** | **10** |
| **VNXB6GSDAE25F** | **EMC VNX/VNXe Disk Array Enclosure** | **4** |
| **V4-2S15-600** | **EMC Insignia 2.5 inch VNX2 600 GB 15K SAS DPE DAE** | **140** |
| **VNXBOEPerfTB** | **VNXB OE PER TB PERFORMANCE** | **84** |

# Wipe چیست و ابزارهای رایج را نام ببرید.

به دلایل مختلف، ممکن است رایانه یا هارد دیسک قدیمی واگذار شود. اما ترسی نشت اطلاعات همواره وجد دارد. ممکن است ابتدا Format یا حذف داده ها صورت گیرد اما با این حال، این راه ها به اندازه کافی ایمن و کارآمد نیستند تا این نیاز را برآورده کنند. اما این اقدام کافی نبوده و اطلاعات موجود در هارد دیسک را می توان به راحتی با برخی از نرم افزارهای حرفه ای بازیابی اطلاعات در هر زمان بازیابی کرد!

پس باید به طرزی اطلاعات را حذف نمود که قابل بازیابی نباشد.

برای این هدف باید از ابزارهای Wipe استفاده نمود تا حذف اطلاعات به صورت کامل انجام شود.

از ابزار های Wipe به این ابزار ها اشاره نمود:

* AOMEI Partition Assistant Standard
* DBAN
* KillDisk
* CCleaner
* WipeDisk

# معرفی انواع RAID

شش نوع RAID با شماره‌‌های 0 تا 5 معرفی شده است. این اعداد روش‌‌های مختلفی در چگونگی ایجاد آرایه‌‌های افزونگی و در کل نوع Raid کردن را نشان ‌می‌دهد. تعداد دیگری از انواع Raid ها باعث شد که انواع Raid کردن به 3 دسته اصلی تقسیم شوند:

* استاندارد
* ترکیبی
* غیر استاندارد

Raid های استاندارد به شرح زیر است:

**Raid 0**

پیکربندی این نوع RAID به این صورت است که اطلاعات را تقسیم ‌می‌کند اما هیچ اطلاعات افزوده شده‌ای ندارد. دلیل اصلی Striping در سیستم این است که برای خواندن یک فایل اطلاعات ‌می‌تواند همزمان از چند هارد خوانده شده استفاده کند.

برای تنظیم این نوع RAID به حداقل یک هارد دیسک نیاز است. بیشترین سرعت و بهترین کارایی را در میان مابقی RAID ها را دارد اما در زمانی که یکی از دیسک‌‌ها خراب شود هیچ نوع تحمل امنیت و خطا را ندارد و اطلاعات از بین خواهد رفت.

**Raid 1**

این نوع Raid نیاز به حداقل دو دیسک دارد و اطلاعات از یک دیسک عینا بر روی دیسک دیگر کپی ‌می‌شود. هیچ نواربندی انجام نیز نمی‌شود.

سرعت خواندن اطلاعات بالا می‌رود چرا که به طور همزمان ‌می‌توان از هر دو دیسک اطلاعات را خواند. سرعت نوشتن در این نوع Raid کردن تغییری نمی‌کند و مانند آن است که روی یک دیسک عملیات نوشتن انجام ‌می‌شود.

RAID 1 معمولا برای دو دیسک اجرا ‌می‌شود، اما ‌ با استفاده از RAID 1 ADM (advanced data mirroring) تعداد بسیاری از دو هارد را نیز با هم Mirror کرد که در این صورت امنیت به نسبت بالاتر رفته اما عملا از تمام هاردها فقط به اندازه فضای یک دیسک امکان ذخیره سازی وجود دارد.

**Raid 2**

Raid2 از نوار بندی در دیسک‌‌ها استفاده ‌می‌کند. بعضی از دیسک‌‌ها اطلاعات ECC که برای چک کردن و تصحیح خطاهای احتمالی است را ذخیره ‌می‌کنند. نسبت به RAID 3 مزیت بیشتری ندارد و در زمان حاظر نیز استفاده چندانی از آن نمی‌شود.

**Raid 3**

این روش از نواربندی اطلاعات استفاده ‌می‌کند و یک هارد دیسک را برای ذخیره اطلاعت parity اختصاص ‌داده است. به طور کلی دارای یک سیستم ECC است که خطاها را تشخیص و تصحیح ‌می‌کند.بازیابی داده‌‌ها با استفاده از عملیات منطقی XOR از اطلاعات موجود در هاردهی دیگر انجام ‌می‌شود. از آنجایی که در عملیات خواندن و نوشتن I/O به همه هاردها آدرس ‌داده می‌شود، هیچ تداخلی در هنگام خواندن و نوشتن به وجود نمی‌‌‌‌آید. در این رو RAID 3 بهترین انتخاب برای سیستم ‌­های تک کاربره با برنامه‌‌هایی است که به نواربندی بلند نیاز دارند دارند.

**Raid 4**

این نوع تکنیک از نواربندی اطلاعات استفاده ‌می‌کند اما این نوارها بسیار بزرگ هستند. بدین معنی که ‌می‌توان نوارها یا رکورد‌ها را تنها از یک هارد خواند.

همین باعث ‌می‌شود که بتوانید عملیات I/O را با همپوشانی انجام دهید. از آنجایی که عملیات نوشتن باید هر بار درایو parity را به روز رسانی کند، هیچ تداخلی در عملیات خواندن و نوشتن اتفاق نمی‌افتد.RAID 4 هیچ مزیتی نسبت به RAID 5 ندارد.

**Raid 5**

این تکنیک نوارها را در سطح block-level با استفاده از نوار parity تقسیم ‌می‌کند. این اطلاعات parity در همه‌ای درایوها وجود دارد و این امکان را به وجود ‌می‌آورد که اگر یک درایو به مشکل برخورد آرایه به کار خود ادامه ‌می‌دهد. معماری آرایه‌‌ها به صورتی است که عملیات خواندن و نوشتن در طول دیسک‌‌های متفاوت انجام ‌می‌شود.

این کارایی بسیار بالاتری را نسبت به یک دیسک منجر ‌می‌شود، اما نه به اندازه آرایه RAID 0. RAID 5 که حداقل به سه دیسک نیاز دارد ولی معمولا پیشنهاد ‌می‌شود که استفاده از حداقل 5 دیسک عالی‌ترین کارایی را دارد. و در زمان استفاده از تعداد n دیسک، فضای قابل کارایی، فضایn-1 دیسک ‌است.

این تکنیک به دلیل ساخت اطلاعات parity عموما انتخاب بسیار ضعیفی برای سیستم‌‌هایی با عملیات نوشتن سنگین است. وقتی یکی از هارد درایوها خراب شود مدت زمان بسیاری طول ‌می‌کشد تا آرایه RAID 5 ساخته شود. کارایی معمولا در زمان ساخت دوباره کاهش ‌خواهد یافت و آرایه در زمان خرابی یک دیسک تا وقتی که ساخت دوباره RAID کامل شود آسیب پذیر می‌باشد.

تنها نقطه ضعف این سیستم این است که با Failed شدن بیشتر از یک دیسک همه‌ای داده‌‌ها از بین ‌می‌رود یا به عبارتی تحمل خطای این تکنیک برابر با یک دیسک ‌است.

**Raid 6**

این تکنیک مشابه RAID 5 است اما یک parity دوم در طول آرایه‌‌های درایوها ساخته ‌می‌شود. این parity اضافه این امکان را می‌دهد که در زمان خرابی دو دیسک آرایه به کار خود ادامه دهد. هر چند این تکنیک محافظت بسیار بالای دارد اما هزینه بسیار بیشتری را تحمیل ‌می‌کند. RAID 6 هزینه بیشتری را برای هر GB حافظه ‌می‌برد و به طور کلی سرعت نوشتن در آن از RAID 5 پایین‌تر است.

در زمان استفاده از تعداد n دیسک، فضای قابل استفاده، فضای n-2 دیسک است. یعنی به طور کلی تحمل خطای این سیستم (سوختن هارد درایو) برابر با دو دیسک است و با Failed شدن بیش از دو دیسک همه‌ای داده‌‌ها از بین خواهد رفت.

