مرکز آپا دانشگاه تربیت مدرس

مقاله آموزشی

تحلیل بدافزار PlugX USB

شناسه گزارش

TMUCERT-1403-05-31

مردادماه ۱۴۰۳

فهرست مطالب

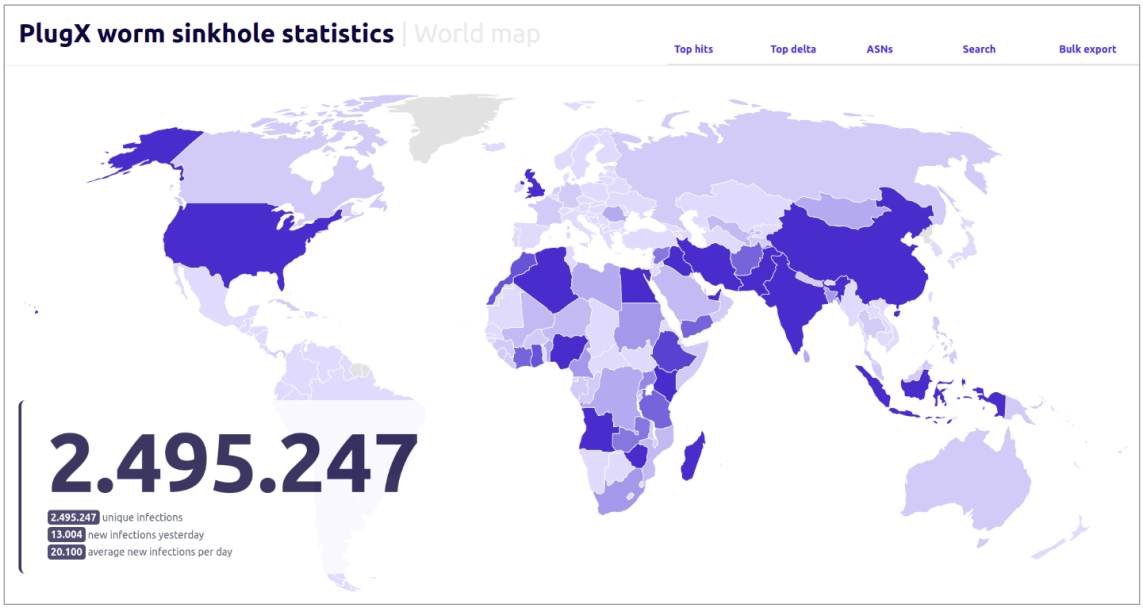
۱- مقدمه

بدافزار PlugX حداقل از سال ۲۰۰۸ میلادی توسط گروه‌های مرتبط با دولت چین در عملیات جاسوسی استفاده شده است. این بدافزار ابتدا با هدف حمله به سازمان‌های دولتی و نظامی در کشورهای آسیایی و سپس کشورهای غربی توسعه داده شده است. برخی پژوهشگران اعتقاد دارند کد منبع این بدافزار در سال ۲۰۱۵ میلادی به بیرون درز کرده و توسط گروه‌های مختلف به‌روزرسانی شده است.

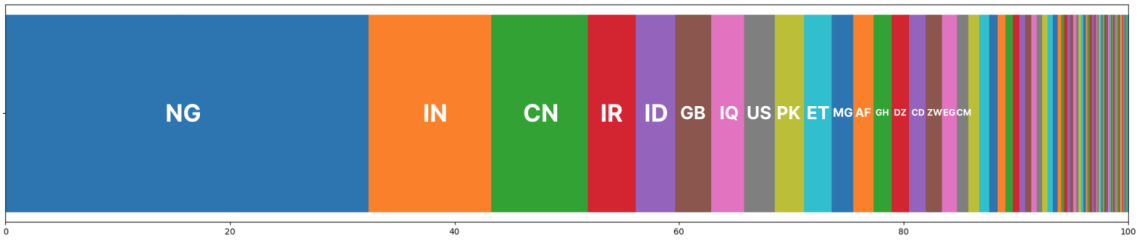
PlugX اغلب با استفاده از روش بارگیری جانبی DLL (DLL Side Loading) در ماشین قربانی اجرا می‌شود [۱]. در این روش، یک برنامه اجرایی قانونی DLL مخربی را بارگیری می‌کند که باعث می‌شود مؤلفه اصلی بدافزار که در یک فایل باینری رمزشده قرار دارد، به حافظه نگاشت شده و سپس اجرا شود.

در سال ۲۰۲۰ میلادی با هدف افزایش قابلیت‌های PlugX مولفه جدیدی به آن اضافه شده است که دستگاه‌های مختلفی که از طریق درگاه‌های USB به یک ماشین آلوده متصل می‌شوند را آلوده می‌کند [۲]. این نسخه جدید که با نام PlugX USB شناخته می‌شود را می‌توان نوعی تروجان دسترسی از راه دور (RAT) و نوعی کرم (Worm) در نظر گرفت که علاوه‌بر فراهم‌کردن امکان دسترسی از راه دور به ماشین قربانی می‌تواند به‌صورت خودکار تکثیر شده و در دستگاه‌های USB جدید منتشر شود.

در ماه مارس سال ۲۰۲۳ میلادی شرکت امنیت سایبری Sophos گزارش داد که همه نمونه‌های PlugX با نشانی 45.142.166.112 (که توسط شرکت GreenCloud میزبانی می‌شود) ارتباط برقرار می‌کنند [۲]. لذا در ماه سپتامبر همان سال، شرکت امنیت سایبری Sekoia پس از درخواست از GreenCloud مالکیت این نشانی IP را به دست آورد و با راه‌اندازی یک کارگزار وب ساده تلاش کرد نقش کارگزار فرماندهی و کنترل PlugX (C&C) را ایفا کند [۳]. بررسی‌های انجام‌شده توسط این شرکت نشان داد که روزانه بین ۹۰ تا ۱۰۰ هزار میزبان آلوده با نشانی IP یکتا از بیش از ۱۷۰ کشور درخواست‌هایی را به این کارگزار وب ارسال می‌کنند [۳]. همان‌طور که در شکل ۱ مشاهده می‌شود، در میان این کشورها، ۱۵ کشور شامل نیجریه، هند، چین، ایران، اندونزی، بریتانیا، عراق و ایالات متحده آمریکا بیش از ۸۰ درصد کل آلودگی‌ها را تشکیل می‌دهند [۴]. در شکل ۲ درصد آلودگی میزبان‌ها به تفکیک هر کشور در سوم ماه آوریل سال ۲۰۲۴ میلادی نمایش داده شده است.



شکل ۱. میزان آلودگی به بدافزار PlugX در کشورهای مختلف



شکل ۲. درصد آلودگی به بدافزار PlugX به تفکیک هر کشور

به‌طور کلی، فعالیت‌های مخرب زیر توسط PlugX گزارش شده است:

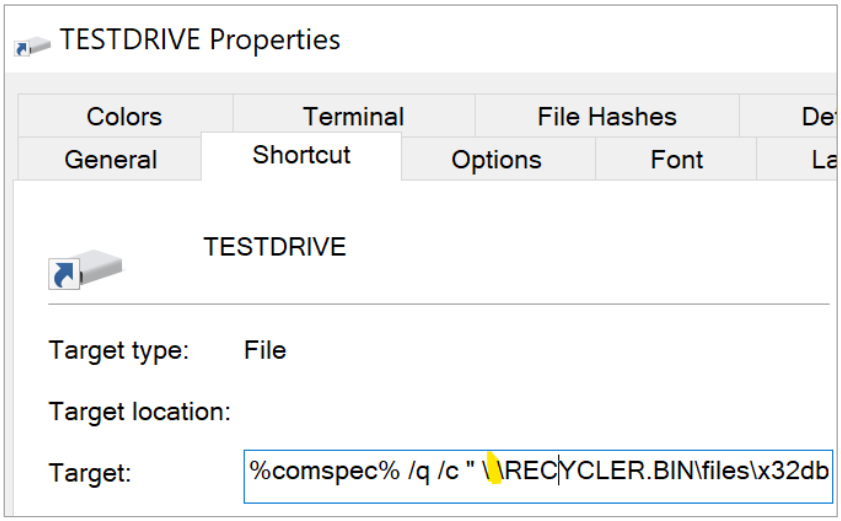
- ثبت کلید
- عکس‌برداری از صفحه نمایش قربانی
- مدیریت پردازه‌ها در ماشین قربانی
- راه‌اندازی مجدد ماشین قربانی
- کنترل از راه دور صفحه کلید
- انتقال اسناد PDF و Word از ماشین قربانی به پوشه‌های پنهان در دستگاه (درایو) USB

۲- تشریح رفتار و نحوه انتشار

هنگام آلوده‌سازی یک دستگاه (درایو) USB به بدافزار PlugX USB تمامی فایل‌ها و پوشه‌هایی که در ریشه این دستگاه قرار دارند به یک پوشه جدید منتقل می‌شوند. برای پنهان‌سازی این پوشه از کاراکتر یونیکد (Unicode) `00A0` استفاده می‌شود. این کاراکتر یونیکد در واقع یک کاراکتر فضای خالی است که Non-breaking space نامیده می‌شود و از نمایش نام پوشه توسط سیستم‌عامل ویندوز جلوگیری می‌کند (به‌جای نمایش یک پوشه بی‌نام آن را پنهان می‌کند). سپس فایل‌های مخرب بدافزار که در روش بارگیری جانبی DLL به آن‌ها نیاز است در پوشه پنهان `RECYCLER.BIN` ذخیره می‌شوند. همچنین، بر روی ریشه دستگاه USB یک فایل میان‌بر (Shortcut) ایجاد می‌شود که به یکی از فایل‌های مخرب اشاره می‌کند [۱].

هنگامی که کاربر قربانی دستگاه USB را باز می‌کند، تنها یک فایل میان‌بر به وی نمایش داده می‌شود. با کلیک بر روی این فایل میان‌بر، زنجیره آلوده‌سازی به بدافزار اجرا می‌شود. در این زنجیره، ابتدا بدافزار پنجره فعلی را بسته و پنجره جدیدی را باز می‌کند که محتویات قانونی در پوشه پنهان (پوشه با نام `00A0`) را نمایش می‌دهد. سپس بدافزار خود را به داخل میزبان قربانی منتقل کرده و یک کلید رجیستری جدید تحت `HKCU[...]\CurrentVersion\Run` برای ماندگاری خود ایجاد می‌کند. در نهایت، خودش را دوباره از میزبان قربانی اجرا کرده و هر ۳۰ ثانیه درگاه‌های USB را بررسی می‌کند و درصورت اتصال یک دستگاه USB جدید آن را به‌طور خودکار آلوده می‌کند [۳].

در برخی از نسخه‌های بدافزار PlugX USB برای پنهان‌سازی مسیر فایل‌های مخرب هم از کاراکتر یونیکد `00A0` استفاده می‌شود. در شکل ۳ مثالی از یک فایل میان‌بر روی دستگاه USB که به یک فایل مخرب اشاره می‌کند نمایش داده شده است [۱]. در این شکل کاراکتر یونیکد `00A0` (فضای خالی) در مسیر فایل مخرب با رنگ زرد برجسته شده است. در شکل ۴ فایل میان‌بر در یک ویرایشگر هگز نمایش داده شده است [۱].



شکل ۳. مثالی از یک فایل میان‌بر روی دستگاه USB که به یک فایل مخرب اشاره می‌کند

```
00000000   43 3A 5C 57 69 6E 64 6F  77 73 5C 53 79 73 74 65   C:\Windows\Syste
00000010   6D 33 32 5C 63 6D 64 2E  65 78 65 00 00 29 00 2F   m32\cmd.exe..)./
00000020   00 71 00 20 00 2F 00 63  00 20 00 22 00 A0 00 5C   .q. ./.c. ."...\
00000030   00 A0 00 5C 00 52 00 45  00 43 00 59 00 43 00 4C   . .\.R.E.C.Y.C.L
00000040   00 45 00 52 00 2E 00 42  00 49 00 4E 00 5C 00 66   .E.R...B.I.N.\.f
00000050   00 69 00 6C 00 65 00 73  00 5C 00 78 00 33 00 32   .i.l.e.s.\.x.3.2
00000060   00 64 00 62 00 67 00 2E  00 65 00 78 00 65 00 22   .d.b.g...e.x.e."
```

شکل ٤. مشاهده فایل میان‌بر در یک ویرایشگر هگز

در ادامه این بخش، مراحل آلوده‌سازی یک دستگاه (درایو) USB توسط بدافزار PlugX USB با جزئیات بیشتر شرح داده می‌شود:

۱) ابتدا پوشه فایل‌های مخرب روی دستگاه USB ایجاد می‌شود:

```
<usb volume>:\u00A0\u00A0\RECYCLER.BIN\files
```

برای مثال،

```
F:\ \ \RECYCLER.BIN\files
```

۲) سپس یک فایل پنهان با نام `desktop.ini` در هر پوشه ایجاد می‌شود. این فایل که آیکون (Icon) پوشه را مشخص می‌کند، شامل داده‌های زیر است:

```
[.ShellClassInfo]
IconResource=%systemroot%\system32\SHELL32.dll,7
```

سیستم عامل ویندوز از فایل Shell32.dll برای بازیابی تصاویر آیکون‌های فایل‌ها، پوشه‌ها و میان‌برها استفاده می‌کند. این فایل حاوی فهرست آیکون‌ها و یک شماره منحصربه‌فرد برای هر آیکون است. در مثال فوق، از آیکون درایو و عدد ۷ استفاده شده است که در شکل ۵ نمایش داده شده است.

شکل ۵. نمایش آیکون درایو

استفاده از این آیکون باعث می‌شود که پوشه‌ها هنگامی که در Windows Explorer ظاهر می‌شوند، به‌صورت درایو نمایش داده شوند.

۳) در زیرپوشه RECYLER.BIN از مسیر فایل‌های مخرب، فایل پنهان desktop.ini ایجاد می‌شود. این فایل شامل داده‌های زیر است:

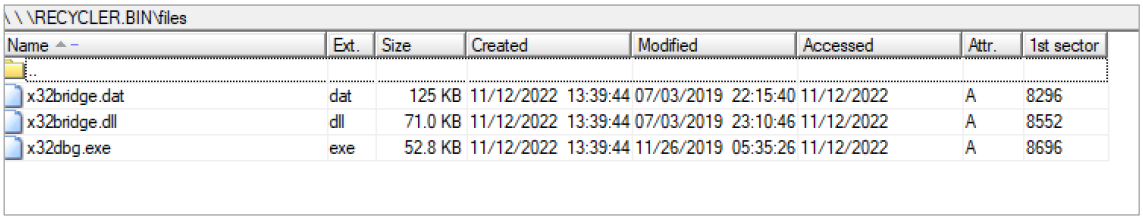
```
[.ShellClassInfo]
CLSID = {645FF040-5081-101B-9F08-00AA002F954E}
```

استفاده از این CLSID باعث می‌شود که Windows Explorer برای نمایش پوشه RECYCLER.BIN از آیکون سطل زباله استفاده کند (شکل ۶).

Name	Date modified	Type	Size
RECYCLER.BIN	12/12/2022 1:47 PM	File folder	
desktop.ini	12/12/2022 1:47 PM	Configuration settings	1 KB

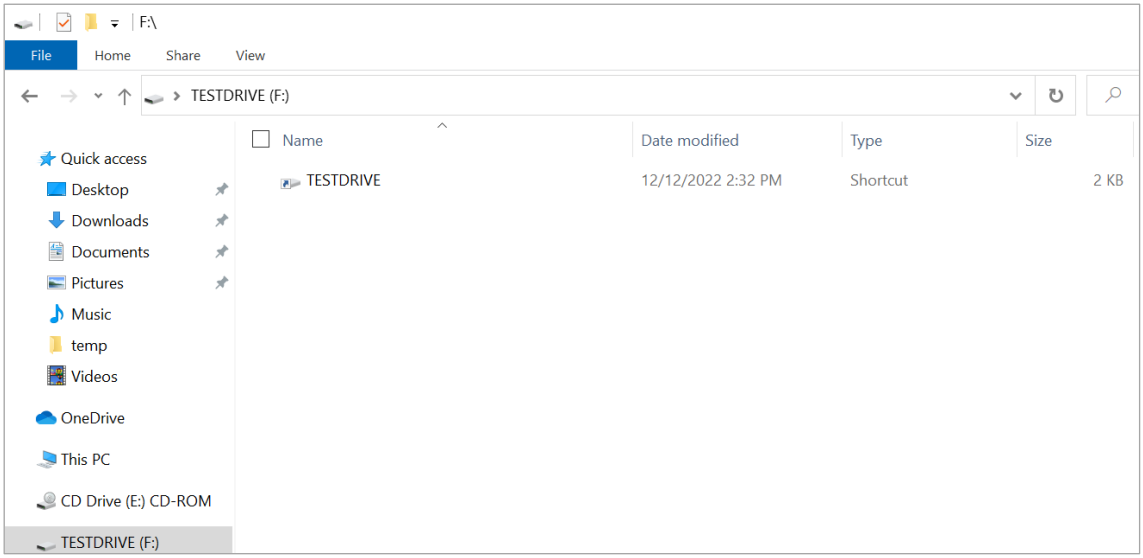
شکل ٦. استفاده از آیکون سطل زباله برای نمایش پوشه RECYCLER.BIN

۴) در زیرپوشه files از مسیر فایل‌های مخرب سه فایل با پسوندهای .dat، .dll و .exe ذخیره می‌شود (شکل ۷).



شکل ۷. ذخیره‌سازی فایل‌ها با پسوندهای `.dat`، `.dll` و `.exe` در زیرپوشه `files` از مسیر فایل‌های مخرب

۵) دستگاه USB آلوده تنها شامل یک فایل با پسوند `.lnk` (فایل میان‌بر) است (شکل ۸). سایر فایل‌ها و پوشه‌ها پنهان شده‌اند. در این شکل نام فایل میان‌بر `TESTDRIVE` است که با نام دستگاه (درایو) USB مطابقت می‌کند.



شکل ۸. نمایش فایل میان‌بر در ریشه دستگاه USB آلوده

فایل میان‌بر مسئول آلوده‌کردن میزبان قربانی با هربار کلیک بر روی آن است. به‌عنوان مثال، فایل میان‌بر در شکل ۸ شامل داده‌های زیر است:

```
%comspec% /q /c " \ \RECYCLER.BIN\files\x32dbg.exe"
```

هنگامی که کاربر روی فایل میان‌بر کلیک می‌کند، برنامه `x32dbg.exe` ماشین قربانی را آلوده کرده و فایل‌ها و پوشه‌های قانونی پنهان‌شده در دستگاه USB آلوده را به کاربر نمایش می‌دهد که باعث می‌شود وی به اشتباه تصور کند همه‌چیز عادی است.

۳- نشانگرهای آلودگی

برای شناسایی میزبان‌های آلوده به بدافزار PlugX USB می‌توان از نشانگرهای آلودگی زیر استفاده کرد:

- کد درهم‌سازی فایل‌های مخرب

```
432a07eb49473fa8c71d50ccaf2bc980b692d458ec4aaedd52d739cb377f3428
e8f55d0f327fd1d5f26428b890ef7fe878e135d494acda24ef01c695a2e9136d
3a53bd36b24bc40bdce289d26f1b6965c0a5e71f26b05d19c7aa73d9e3cfa6ff
2304891f176a92c62f43d9fd30cae943f1521394dce792c6de0e097d10103d45
8b8adc6c14ed3bbeacd9f39c4d1380835eaf090090f6f826341a018d6b2ad450
6bb959c33fdfc0086ac48586a73273a0a1331f1c4f0053ef021eebe7f377a292
b9f3cf9d63d2e3ce1821f2e3eb5acd6e374ea801f9c212eebfa734bd649bec7a
8ec37dac2beaa494dcefec62f0bf4ae30a6ce44b27a588169d8f0476bbc94115
e72e49dc1d95efabc2c12c46df373173f2e20dab715caf58b1be9ca41ec0e172
0e9071714a4af0be1f96cffc3b0e58520b827d9e58297cb0e02d97551eca3799
39280139735145ba6f0918b684ab664a3de7f93b1e3ebcdd071a5300486b8d20
41a0407371124bcad7cab56227078ccd635ba6e6b4374b973754af96b7f58119
02aa5b52137410de7cc26747f26e07b65c936d019ee2e1afae268a00e78a1f7f
2a07877cb53404888e1b6f81bb07a35bc804daa1439317bccde9c498a521644c
5d98d1193fcbb2479668a24697023829fc9dc1f7d31833c3c42b8380ef859ff1
```

- نشانی کارگزارهای فرماندهی و کنترل بدافزار

```
45.251.240.55
45.142.166.112
103.56.53.46
43.254.217.165
```

- پوشه‌های ایجادشده توسط بدافزار

```
C:\ProgramData\UsersDate\Windows_NT\Windows\user\Desktop\
C:\Users\Public\Public Mediae\
<usb volume>:\u00A0\u00A0\RECYCLER.BIN\files
<usb volume>:\u00A0\u00A0\RECYCLER.BIN\files\da520e5
<usb volume>:\u00A0\u00A0\RECYCLER.BIN\1
```

- نام پردازه‌های بدافزار

```
x32dbg.exe
Mediae.exe
Aug.exe
Precious.exe
SafeGuard.exe
Dism.exe
CEFHelper.exe
```

٤- شناسایی و پاک‌سازی

برای شناسایی میزبان‌های آلوده به بدافزار PlugX USB و پاک‌سازی آن‌ها اقدامات زیر توصیه می‌شود:

- مسدودکردن دسترسی به درگاه‌های USB برای کارمندان سازمان
- مسدودکردن نشانی کارگزارهای فرماندهی و کنترل با توجه به نشانگرهای آلودگی
- یافتن و حذف فایل‌های مخرب با توجه به نشانگرهای آلودگی
- یافتن و حذف فایل‌های میان‌بر ایجادشده توسط بدافزار
- یافتن و حذف کلیدهای رجیستری ایجادشده توسط بدافزار
- یافتن پوشه‌های پنهان ایجادشده توسط بدافزار در دستگاه‌های USB
- استفاده از نرم‌افزارهای امنیتی مانند آنتی‌ویروس یا ضدبدافزار
- پایش ترافیک شبکه و شناسایی فعالیت‌های غیرعادی شبکه

٥- منابع و مراجع

[1] Mike Harbison and Jen Miller-Osborn, Chinese PlugX malware hidden in your USB devices?, January 2023. [Online]. Available: https://unit42.paloaltonetworks.com/plugx-variants-in-usbs/

[2] Gabor Szappanos, A border-hopping PlugX USB worm takes its act on the road, March 2023. [Online]. Available: https://news.sophos.com/en-us/2023/03/09/border-hopping-plugx-usb-worm/

[3] Felix Aimé, M. Charles and Sekoia TDR, Unplugging PlugX: Sinkholing the PlugX USB worm botnet, April 2024. [Online]. Available: https://blog.sekoia.io/unplugging-plugx-sinkholing-the-plugx-usb-worm-botnet/

[4] Bill Toulas, Researchers sinkhole PlugX malware server with 2.5 million unique IPs, April 2024. [Online]. Available: https://www.bleepingcomputer.com/news/security/researchers-sinkhole-plugx-malware-server-with-25-million-unique-ips/