**Read Me**

<https://github.com/RobinPerris/DarkUI>

<https://www.makeuseof.com/winforms-themes-add-application>

<https://learn.microsoft.com/en-us/windows/apps/desktop/modernize/apply-windows-themes>

https://github.com/leocb/MaterialSkin

**Color Palettes:**

https://flatuicolors.com/

<https://flatuicolors.com/palette/gb>

<https://coolors.co/palettes/trending/dark>

<https://colorhunt.co/palettes/dark>

**Persian Anti Malware**

**https://PersianAntiMalware.ir**

**Free, Open Source, .NET 8, With over 50 Million Malware Definition!**

**Malware:**

Virus

Trojan (Backdoor)

Self

Audio

Web Cam

Key Logger

Others

DDOS Attack

Ransomware

Worm

…

**متأسفانه اکثر کاربران و سازمان‌های ایرانی، نسبت به امنیت داده‌های شخصی و شرکتی خود، به شدت ماجراجو و غافل هستند!**

**نمونه:** عکسی که می‌گیریم و منتشر می‌کنیم!

[https://VirusTotal.com](https://VirusTotal.com/) (Google)

Free API: x in Hour, y in Day, z in Month

متاسفانه! تعبیر! یا توصیف! **هکرهای خارجی** از سایت‌های ایرانی!

**عدم هماهنگی دانش بین متخصصین امنیت و متخصصین برنامه‌نویسی!**

بدافزارها به طور خلاصه به دو دسته تقسیم می‌شوند:

* به تنهایی
* یا به فایلی متصل می‌شوند! (سایز فایل تغییر نمی‌کند!)

**Portable Executable:**

https://en.wikipedia.org/wiki/Portable\_Executable

**List of file signatures:**

https://en.wikipedia.org/wiki/List\_of\_file\_signatures

**Forensic / Malware Analysis**

**Static**

**Offline**

Real Time

**Dynamic**

Offline

**Real Time**

- REMnux: A Linux Toolkit for Malware Analysis

https://remnux.org/

- HxD:

https://mh-nexus.de/en/hxd

- Explorer Suite (CFF Explore):

https://ntcore.com/?page\_id=345

https://ntcore.com/?page\_id=388

- PEStudio:

https://www.winitor.com/download

- Process Hacker:

https://processhacker.sourceforge.io

- Process Explorer

https://learn.microsoft.com/en-us/sysinternals/downloads/procmon

- DNSpy:

https://github.com/dnSpy/dnSpy/releases

References:

https://github.com/neilharvey/FileSignatures

https://www.nuget.org/packages/FileSignatures

https://en.wikipedia.org/wiki/List\_of\_file\_signatures

Online Virus Scanners:

https://www.virustotal.com

https://virusscan.jotti.org

https://metadefender.opswat.com

- YARA:

https://virustotal.github.io/yara

https://github.com/virustotal/yara

https://github.com/InQuest/awesome-yara

https://github.com/Yara-Rules/rules

https://github.com/reversinglabs/reversinglabs-yara-rules

https://launchpad.net/~remnux/+archive/ubuntu/stable/+packages

- UPX:

https://upx.github.io

https://github.com/upx/upx

- Ghidra

https://ghidra-sre.org/

**این که با چه زبان برنامه‌نویسی کار می‌کنیم،**

**اصلاً اهمیتی ندارد! بلکه صرفاً ایده‌های تکنولوژی اهمیت دارد!**

var directoryInfo =

new System.IO.DirectoryInfo(path: path);

var directoryInfos =

directoryInfo.GetDirectories();

معایب:

* در ریشه درایو، خطا می‌دهد!
* فقط پوشه‌های، پوشه (درایو) جاری را نمایش می‌دهد!

var directoryInfo =

new System.IO.DirectoryInfo(path: path);

var directoryInfos =

directoryInfo.GetDirectories(searchPattern: "\*.\*",

searchOption: System.IO.SearchOption.AllDirectories);

مزایا:

* علاوه بر پوشه‌های Path، تمام پوشه‌های تودرتو را نیز بدست می‌آورد!

معایب:

* در ریشه درایو، خطا می‌دهد!
* زمان بسیار زیادی طول می‌کشد تا فهرست همه پوشه‌ها را بدست آورد! مثلاً برای درایو :C، با یک دستگاه نسبتاً قوی، در حدود ۲ دقیقه طول می‌کشد!

var enumerationOptions =

new System.IO.EnumerationOptions

{

BufferSize = 4096,

IgnoreInaccessible = true,

**RecurseSubdirectories = true,**

ReturnSpecialDirectories = false, // Not (.) and (..)

MaxRecursionDepth = int.MaxValue,

MatchType = System.IO.MatchType.Win32,

AttributesToSkip = System.IO.FileAttributes.None,

MatchCasing = System.IO.MatchCasing.PlatformDefault,

};

var directories =

System.IO.Directory.EnumerateDirectories(path: path,

searchPattern: "\*.\*", enumerationOptions: enumerationOptions)

.ToList()

;

مزایا:

* علاوه بر پوشه‌های Path، تمام پوشه‌های تودرتو را نیز بدست می‌آورد!
* در ریشه درایو، خطا نمی‌دهد!

معایب:

* زمان بسیار زیادی طول می‌کشد تا فهرست همه پوشه‌ها را بدست آورد! مثلاً برای درایو :C، با یک دستگاه نسبتاً قوی، در حدود ۲ دقیقه طول می‌کشد!

پس باید خودمان به صورت Recursive، فهرست تمام پوشه‌ها را بدست آورده! و آن‌ها را در یک List قرار دهیم! و باید این کار را با استفاده از یک Thread دیگری انجام دهیم:

* تا هم پروژه ما قفل نشود!
* تا با یک Thread دیگری، هم‌زمان، شروع به Scan کردن فایل‌های آن پوشه‌ها نماییم! و معطل نمانیم، تا ابتدا کار بدست آوردن کلیه پوشه‌ها خاتمه یافته و سپس اقدام به اسکن کردن فایل‌ها کنیم!

جلسه پنجم

(1)

افتتاح سایت

[https://PersianAntiMalware.ir](https://PersianAntiMalware.ir/)

(2)

ScanFilesForm →

StartButton\_Click() →

GetDirectoriesThread.Priority = …

(3)

Dtat →

ThreadSafeHelper.cs →

SetControlPropertyDelegate()

(4)

ScanFilesForm →

GetAllDirectories() →

scanTimeTakenTextBox.Text =

ScanTimeTaken.ToString();

DisplayScanTimeTaken();

Dtat.ThreadSafeHelper.SetControlProperty

(control: scanTimeTakenTextBox,

propertyName: nameof(scanTimeTakenTextBox.Text),

propertyValue: ScanTimeTaken.ToString());

(5)

معماری:

private System.Threading.Thread? ScanFilesThread { get; set; }

private System.Threading.Thread? GetDirectoriesThread { get; set; }

(6)

https://virusshare.com

https://virusshare.com/hashes

(7)

Application →

Infrastructure →

ApplicationSettings.cs

**D:\\PAMUpdates (1.3 GB)**

(8)

Application →

Infrastructure →

DownloadHelper.cs