WINDOWS INTERNALS & SYSINTERNALS

WİNDOWS NEDİR ?

Windows, Microsoft tarafından geliştirilen, grafiksel kullanıcı arayüzüne (GUI) sahip, çok görevli (multitasking) bir işletim sistemi ailesidir.

- **1. Windows NT Mimarisi (Temel Yapı)**
- Modern Windows sürümleri (XP'den Windows 11'e ve Server sürümlerine kadar), **Windows NT (New Technology)** çekirdeği üzerine kuruludur. Bu mimari, sistem kararlılığını sağlamak için iki temel çalışma moduna ayrılmıştır:
- **User Mode (Kullanıcı Modu - Ring 3):** Sizin yazdığınız uygulamalar, Word, Chrome veya arka plandaki servisler burada çalışır. Bu moddaki bir yazılımın donanıma (RAM, CPU, Disk) doğrudan erişimi yoktur. Bir işlem yapmak istediğinde (örneğin diske dosya yazmak), işletim sisteminden "rica eder" (System Call / API çağrısı yapar).
- **Kernel Mode (Çekirdek Modu - Ring 0):** Burası "Tanrı Modu"dur. İşletim sistemi çekirdeği, donanım sürücüleri (ekran kartı sürücüsü vb.) burada çalışır. Tüm belleğe ve donanıma sınırsız erişim vardır.
- *Kritik Nokta:* Eğer User Mode'da bir program çökerse, sadece o program kapanır. Ancak Kernel Mode'da bir sürücü hata verirse, tüm sistem çöker ve meşhur **Mavi Ekran (BSOD)** ile karşılaşırsınız

2. HAL (Hardware Abstraction Layer - Donanım Soyutlama Katmanı)

- Windows, binlerce farklı donanım kombinasyonunda çalışabilir. Bunu sağlayan yapı **HAL**'dir.
- **Görevi:** İşletim sistemi çekirdeği ile fiziksel donanım (anakart, işlemci) arasında tercümanlık yapmaktır.
- **3. İşlem ve Bellek Yönetimi (Process & Memory)**
- Windows, her programa sanki bilgisayardaki tek program oymuş gibi davranır.
- **Sanal Bellek (Virtual Memory):** Fiziksel RAM 16 GB olsa bile, Windows her 32-bit işleme (process) 4 GB'lık, 64-bit işleme ise çok daha büyük, kendine özel sanal bir bellek alanı verir. İşlemci ve Windows, bu sanal adresleri fiziksel RAM adreslerine eşler. RAM yetmezse diskin bir kısmını (Pagefile.sys) RAM gibi kullanır.

- **Zamanlayıcı (Scheduler):** Windows, saniyede binlerce kez hangi işlemin (thread'in) işlemciyi kullanacağına karar verir. Öncelik (Priority) seviyesine göre (örneğin fare imleci hareketi yüksek önceliklidir) CPU zamanını dağıtır.
- **4. Dosya Sistemi: NTFS**
- Windows, varsayılan olarak **NTFS (New Technology File System)** kullanır. FAT32 gibi eski sistemlerden farkı şunlardır:
- **İzinler (ACL - Access Control Lists):** "Ali bu dosyayı okusun ama Ayşe sadece yazsın" gibi detaylı güvenlik ayarları tutar.
- **Journaling (Günlükleme):** Elektrik kesilirse veri kaybını önlemek için yapılan işlemleri önce bir "günlüğe" yazar, sonra diske işler.
- **ADS (Alternate Data Streams):** Bir dosyanın arkasına gizli veriler ekleyebilir. (Örneğin, internetten indirdiğiniz bir dosyaya Windows'un "Bu dosya internetten geldi, dikkatli ol" etiketi yapıştırması ADS ile yapılır).

Dosya sistemi ve ADS(Alternate Data Streams) Demosu

Amacımız bir dosyanın arkasına nasıl gizli veri eklendiğini canlı olarak kanıtlamak.

•Bir komut istemcisi açıp şu komutları yazın: **echo "Slayt İcin Gorunen Metin" > deneme.txt**

•Dosyanın arkasına , ADS özelliğini kullanarak gizli bir veri akışı ekleyin: **echo "Bu veri gizlidir ve boyut hesaplamasinda gorunmez" > deneme.txt:gizli.txt.**

• **dir** komutunu çalıştırın. Dosya boyutunun **deneme.txt:gizli.txt**

Eklendikten sonra bile değişmediğini görürsünüz.

•dir/r komutunu çalıştırın. Bu komutun gizli akışları ortaya çıkardığını ve ekranda belirlendiğini görürsünüz.

•Gizli veriyi okumak için notepad deneme.txt:gizli.txt komutunu girin.

- **5. Windows API (Win32 API)**
- Yazılımcılar için Windows, **Win32 API** demektir. Bir Python scriptiyle veya C# ile "Dosya Aç" dediğinizde, arka planda derleyici bunu Windows'un anlayacağı CreateFile fonksiyonuna dönüştürür. Ekrandaki pencerelerin çizilmesi, klavye girdisinin alınması, ağ bağlantısının kurulması; hepsi bu devasa kütüphane seti (DLL dosyaları: kernel32.dll, user32.dll, gdi32.dll) üzerinden yürütülür.
- **6. Hizmetler (Services)**

- Linux'taki "Daemon"ların karşılığıdır. Kullanıcı oturum açmasa bile arka planda çalışan işlemlerdir.
- svchost.exe: Görev yöneticisinde onlarca svchost.exe görürsünüz. Bunlar, tek başlarına .exe olamayan küçük hizmetlerin (örneğin Windows Update, Ses Hizmeti) içine doluşup çalıştığı "taşıyıcı" süreçlerdir.

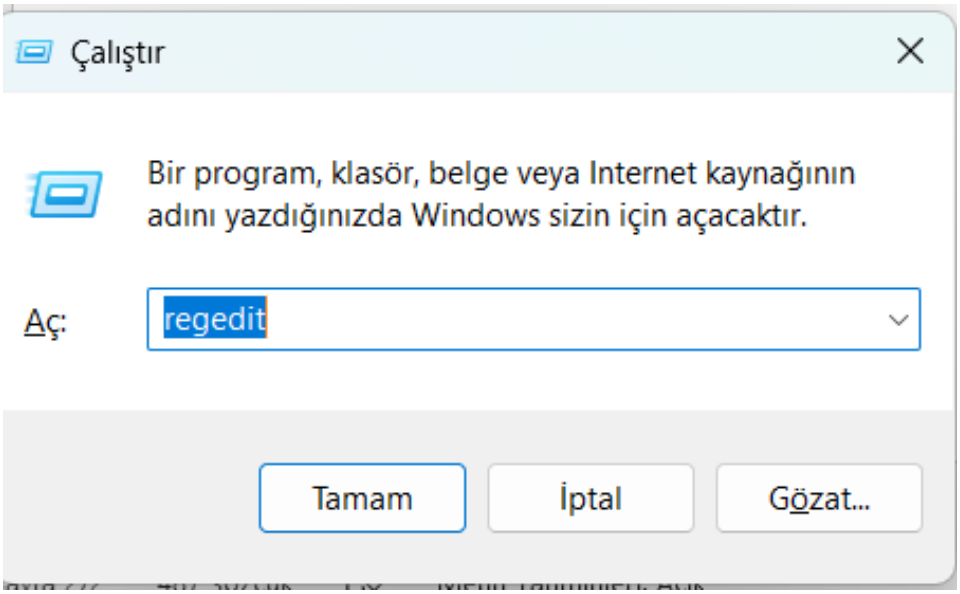
Registry (Kayıt Defteri):

Windows Kayıt Defteri (Registry), işletim sisteminin DNA'sıdır. Kullanıcı arayüzünde yaptığınız basit bir "tıkla" işleminin arkasında, genellikle Registry üzerinde bir değerin 0'dan 1'e değişmesi veya yeni bir anahtarın (Key) oluşturulması yatar.

Kayıt Defteri Mimarisi: Ayarlar Nerede Tutulur?

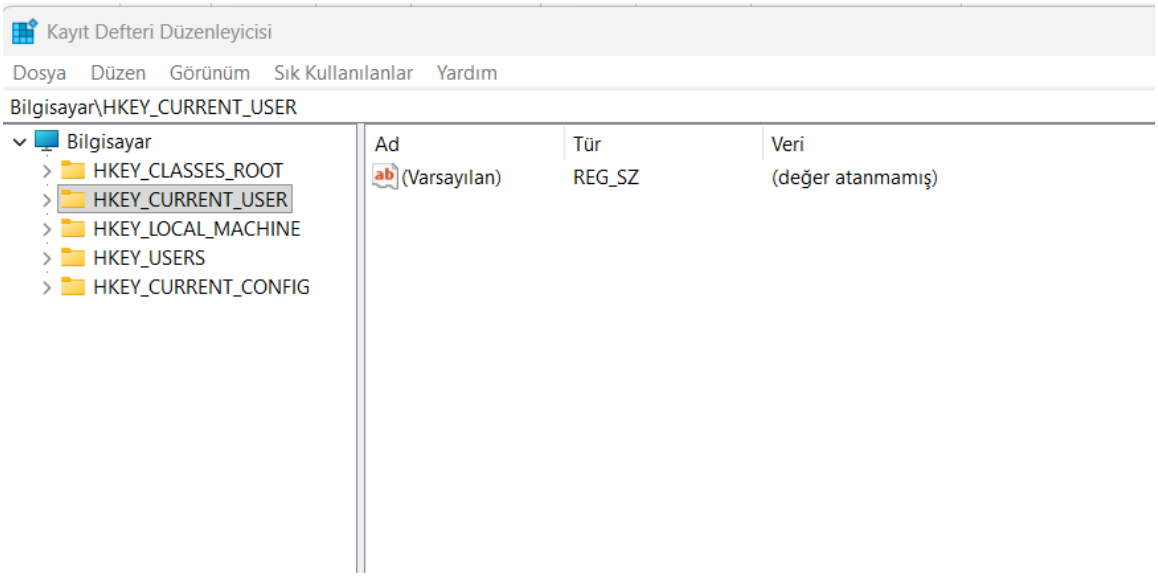
Linux tabanlı sistemlerde ayarlar genellikle düz metin dosyalarında (.conf vb.) tutulurken, Windows'ta bu işlem hiyerarşik bir veritabanı olan Registry'de yapılır. Bu veritabanı, çekirdek (kernel), aygıt sürücüleri, hizmetler ve kullanıcı arayüzü tarafından sürekli okunur ve yazılır.

regedit.exe'yi açtığınızda gördüğünüz yapı sanaldır.



Aşağıdaki ekran görüntüsü kayıt defteri görüntüsü:

- . En tepede "Root Keys" (Kök Anahtarlar) bulunur. En kritik olan ikisi şunlardır:



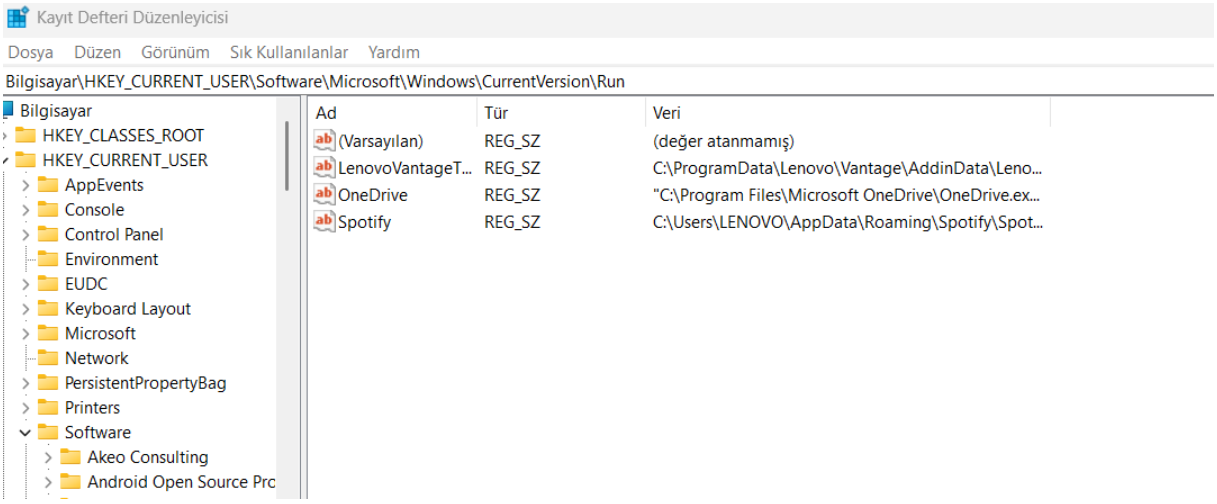
- **HKLM (HKEY_LOCAL_MACHINE):** Bilgisayardaki donanım ve yazılım konfigürasyonunu içerir. Buradaki ayarlar, o an hangi kullanıcının oturum açtığından bağımsızdır (Global ayarlar).
- **HKCU (HKEY_CURRENT_USER):** O an oturum açmış kullanıcıya özel ayarları (duvar kağıdı, tema, fare hızı vb.) barındırır. Aslında bu anahtar, HKEY_USERS altındaki kullanıcıya özel SID (Security Identifier) klasörüne bir kısayoldur (sembolik link).

Fiziksel Yapı (Disktekiler)

- Registry, disk üzerinde tek bir dosya değildir. **"Hives" (Kovanlar)** adı verilen binary dosyalarda tutulur. İşletim sistemi önyükleme (boot) sırasında bu dosyaları belleğe yükler.
- **HKLM\SYSTEM, SAM, SECURITY, SOFTWARE:** Bu kovanlar fiziksel olarak C:\Windows\System32\config\ klasöründe bulunur. (Örn: SYSTEM dosyası).
- **HKCU:** Kullanıcıya özel ayarlar ise kullanıcının profil klasöründe (C:\Users\<KullaniciAdi>\NTUSER.DAT) gizli bir dosya olarak tutulur.
- **Internals Notu:** İşletim sistemi açılırken Kernel, önce SYSTEM kovanını belleğe yükler. Bu, sürücülerin ve hizmetlerin nasıl başlatılacağını belirler. Bu yüzden zararlılar burayı manipüle etmeyi sever.

Standart Run Anahtarları

1. Windows, oturum açma (Logon) işlemi sırasında Explorer.exe başlamadan önce belirli Registry yollarını tarar ve burada listelenen programları sırayla çalıştırır.



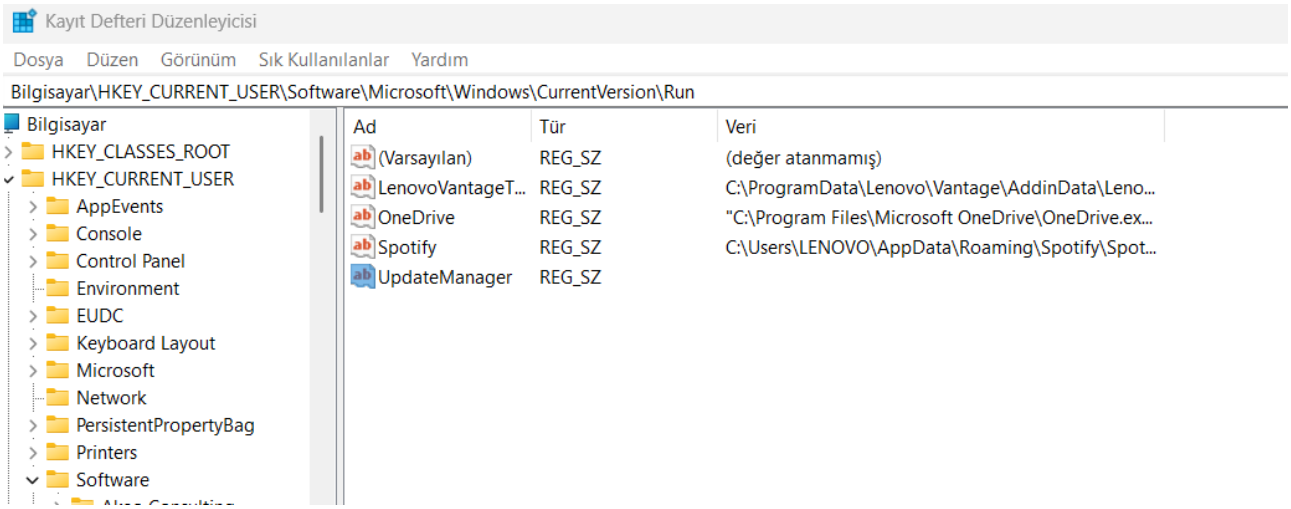
- Kullanıcı Bazlı (HKCU): Sadece o kullanıcı oturum açtığında çalışır.
- Yetki yükseltmesi gerektirmediği için zararlılar burayı çok sever.
- **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run**
- Sistem Bazlı (HKLM): Bilgisayardaki herhangi bir kullanıcı oturum açtığında çalışır.
- Buraya yazmak için Yönetici (Admin) yetkisi gerekir.
- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**

Sysinternals ile Analiz (Görünmeyeni Görmek)

- Standart Görev Yöneticisi veya Başlangıç sekmesi, Registry'deki tüm başlangıç noktalarını göstermez. İşte burada Mark Russinovich'in **Sysinternals** araçları devreye girer.
- **Autoruns:** Bu araç, sadece standart Run anahtarlarını değil, tarayıcı eklentilerini, zamanlanmış görevleri, hizmetleri ve DLL hijacking noktalarını da tarar. Windows'un başlangıcında devreye giren her şeyi gösteren en kapsamlı haritadır.
    - *Kullanım:* Autoruns'ı yönetici olarak çalıştırıp "Logon" sekmesine bakarsanız, yukarıda bahsettiğimiz Registry anahtarlarını ve hedefledikleri dosyaları renkli kodlarla (imzalı/imzasız) görebilirsiniz.
- **Process Monitor (Procmon):** Bir programın Registry'ye ne zaman ve ne yazdığını anlık olarak izler.
    - *Senaryo:* Bir zararlının başlangıca nasıl yerleştiğini anlamak için Procmon açılır, RegSetValue işlemi filtrelenir ve zararlının HKCU\...\Run altına hangi değeri yazdığı saniye saniye yakalanır.

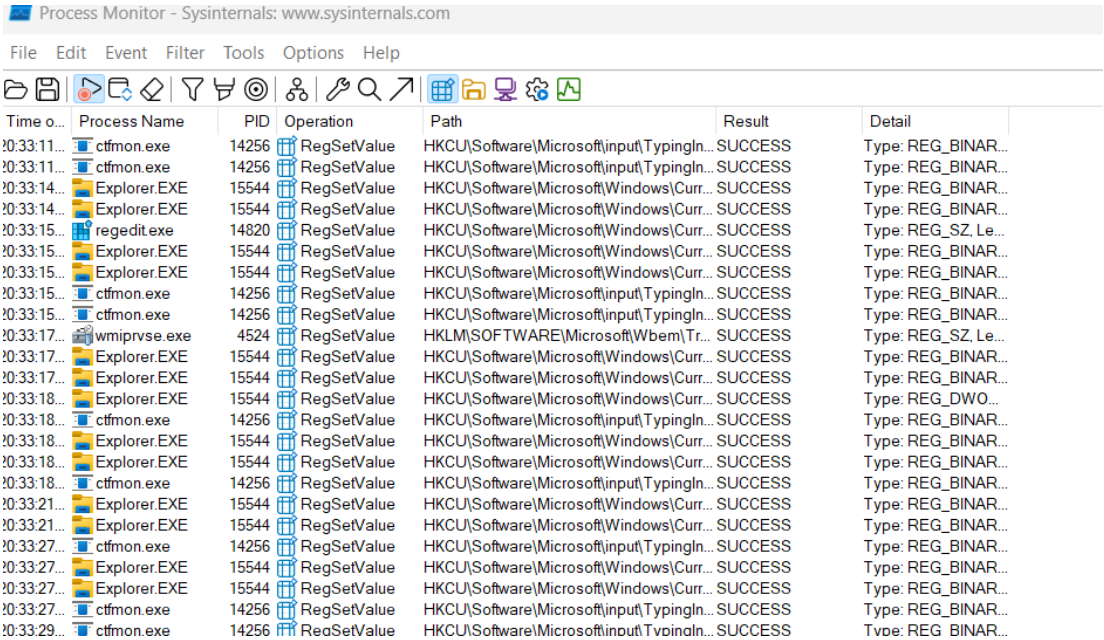
Zararlıların Kullandığı Taktikler

- Basit Ekleme: Zararlı, kendini C:\Users\Public\malware.exe gibi bir yere kopyalar ve yukarıdaki Run anahtarına "UpdateManager" gibi masum bir isimle yeni bir dize değeri (String Value) ekler. Değer verisi olarak dosya yolunu gösterir.
- RunOnce: Run anahtarının hemen yanında RunOnce anahtarı bulunur. Buradaki programlar bir kez çalıştırıldıktan sonra Windows tarafından listeden silinir. Bazı zararlılar, kendilerini her çalıştıklarında tekrar RunOnce'a ekleyerek tespit edilmeyi zorlaştırır (çünkü analiz sırasında liste bazen boş görünebilir).
- Fileless (Dosyasız) Zararlılar: Diskte bir .exe dosyası bırakmak yerine, zararlı kodlarını (örneğin bir PowerShell scripti) doğrudan Registry değerinin içine gömerler. Run anahtarı bir dosyayı çağırmak yerine powershell.exe -WindowStyle Hidden -EncodedCommand ... gibi bir komut çalıştırır. Böylece antivirüslerin dosya taramasından kaçarlar.



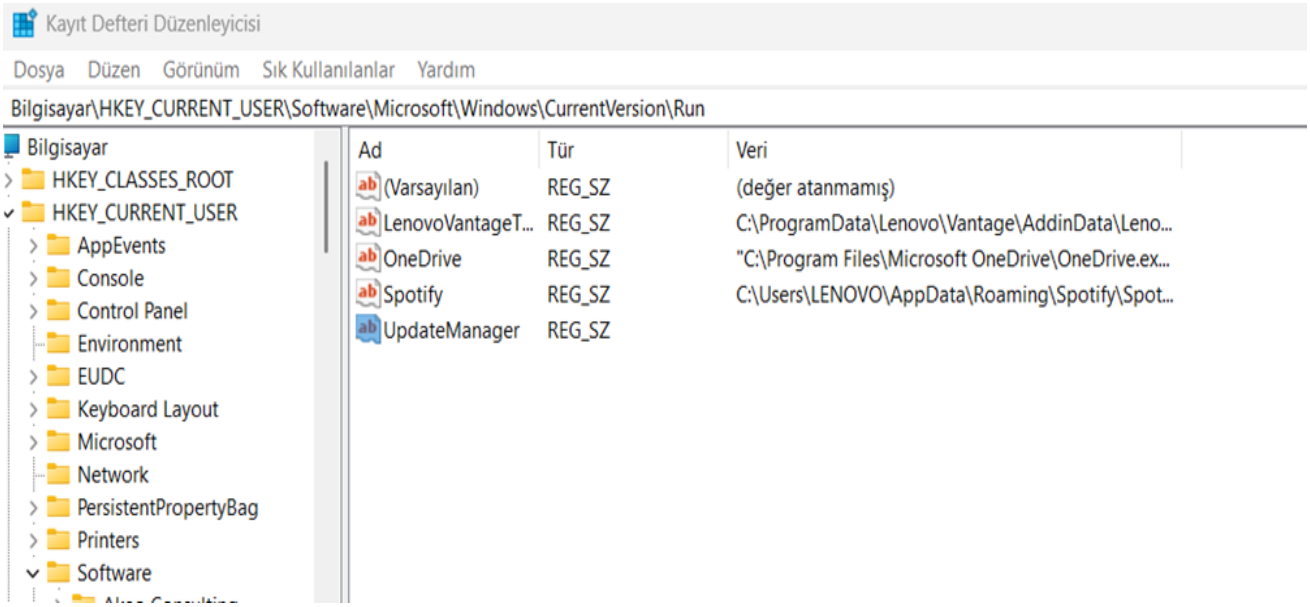
Ekran görüntüsünde sağ tıklayıp yeni->Dize Değer diyerek “Yeni Dize #1” diye oluşur adını ekran görüntüsündeki gibi “UpdateManager” olarak değiştirdik.

Procmon’u açın. Filtre kısmından sadece **Operation is RegSetValue** filtresini ekleyerek ekranı temizleyin.



```
Time o...  Process Name   PID    Operation    Path                                        Result    Detail
0:33:11... ctfmon.exe     14256  RegSetValue  HKCU\Software\Microsoft\input\TypingIn...   SUCCESS   Type: REG_BINAR...
0:33:11... ctfmon.exe     14256  RegSetValue  HKCU\Software\Microsoft\input\TypingIn...   SUCCESS   Type: REG_BINAR...
0:33:14... Explorer.EXE   15544  RegSetValue  HKCU\Software\Microsoft\Windows\Curr...     SUCCESS   Type: REG_BINAR...
0:33:14... Explorer.EXE   15544  RegSetValue  HKCU\Software\Microsoft\Windows\Curr...     SUCCESS   Type: REG_BINAR...
0:33:15... regedit.exe    14820  RegSetValue  HKCU\Software\Microsoft\Windows\Curr...     SUCCESS   Type: REG_SZ, Le...
0:33:15... Explorer.EXE   15544  RegSetValue  HKCU\Software\Microsoft\Windows\Curr...     SUCCESS   Type: REG_BINAR...
0:33:15... Explorer.EXE   15544  RegSetValue  HKCU\Software\Microsoft\Windows\Curr...     SUCCESS   Type: REG_BINAR...
0:33:15... ctfmon.exe     14256  RegSetValue  HKCU\Software\Microsoft\input\TypingIn...   SUCCESS   Type: REG_BINAR...
0:33:15... ctfmon.exe     14256  RegSetValue  HKCU\Software\Microsoft\input\TypingIn...   SUCCESS   Type: REG_BINAR...
0:33:17... wmiprvse.exe    4524  RegSetValue  HKLM\SOFTWARE\Microsoft\Wbem\Tr...          SUCCESS   Type: REG_SZ, Le...
0:33:17... Explorer.EXE   15544  RegSetValue  HKCU\Software\Microsoft\Windows\Curr...     SUCCESS   Type: REG_BINAR...
0:33:17... Explorer.EXE   15544  RegSetValue  HKCU\Software\Microsoft\Windows\Curr...     SUCCESS   Type: REG_BINAR...
0:33:18... Explorer.EXE   15544  RegSetValue  HKCU\Software\Microsoft\Windows\Curr...     SUCCESS   Type: REG_DWO...
0:33:18... ctfmon.exe     14256  RegSetValue  HKCU\Software\Microsoft\input\TypingIn...   SUCCESS   Type: REG_BINAR...
0:33:18... Explorer.EXE   15544  RegSetValue  HKCU\Software\Microsoft\Windows\Curr...     SUCCESS   Type: REG_BINAR...
0:33:18... Explorer.EXE   15544  RegSetValue  HKCU\Software\Microsoft\Windows\Curr...     SUCCESS   Type: REG_BINAR...
0:33:18... ctfmon.exe     14256  RegSetValue  HKCU\Software\Microsoft\input\TypingIn...   SUCCESS   Type: REG_BINAR...
0:33:21... Explorer.EXE   15544  RegSetValue  HKCU\Software\Microsoft\Windows\Curr...     SUCCESS   Type: REG_BINAR...
0:33:21... Explorer.EXE   15544  RegSetValue  HKCU\Software\Microsoft\Windows\Curr...     SUCCESS   Type: REG_BINAR...
0:33:27... ctfmon.exe     14256  RegSetValue  HKCU\Software\Microsoft\input\TypingIn...   SUCCESS   Type: REG_BINAR...
0:33:27... Explorer.EXE   15544  RegSetValue  HKCU\Software\Microsoft\Windows\Curr...     SUCCESS   Type: REG_BINAR...
0:33:27... Explorer.EXE   15544  RegSetValue  HKCU\Software\Microsoft\Windows\Curr...     SUCCESS   Type: REG_BINAR...
0:33:27... ctfmon.exe     14256  RegSetValue  HKCU\Software\Microsoft\input\TypingIn...   SUCCESS   Type: REG_BINAR...
0:33:29... ctfmon.exe     14256  RegSetValue  HKCU\Software\Microsoft\input\TypingIn...   SUCCESS   Type: REG_BINAR...
```

- Arka planda Procmon kayıt yaparken,regedit.exe’ yi açın ve **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run** yoluna gidin.

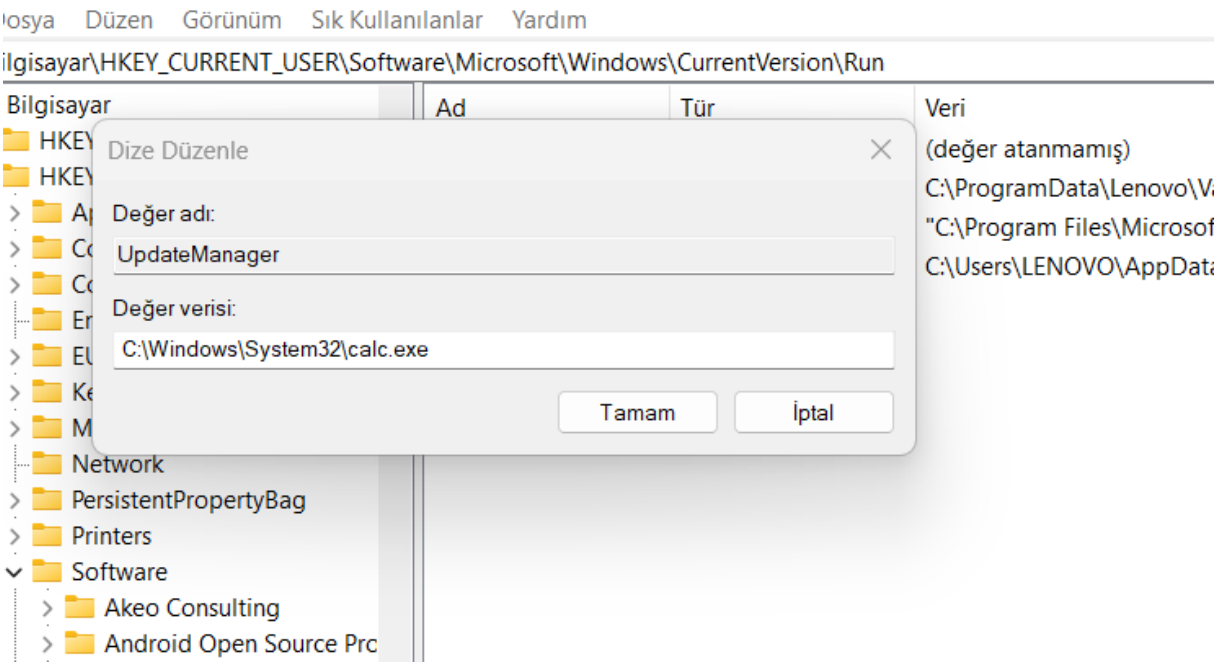


Bilgisayar\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

- Bilgisayar
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
    - AppEvents
    - Console
    - Control Panel
    - Environment
    - EUDC
    - Keyboard Layout
    - Microsoft
    - Network
    - PersistentPropertyBag
    - Printers
    - Software

Ad	Tür	Veri
(Varsayılan)	REG_SZ	(değer atanmamış)
LenovoVantageT...	REG_SZ	C:\ProgramData\Lenovo\Vantage\AddinData\Leno...
OneDrive	REG_SZ	"C:\Program Files\Microsoft OneDrive\OneDrive.ex...
Spotify	REG_SZ	C:\Users\LENOVO\AppData\Roaming\Spotify\Spot...
UpdateManager	REG_SZ	

Boşluğa sağ tıklayıp yeni->Dize Değer diyerek “Yeni Dize #1” diye oluşur adını ekran görüntüsündeki gibi “UpdateManager” olarak değiştirdik. Sonrasında değer verisi olarak masum bir program yolu, örneğin C:\Windows\System32\calc.exe gösterdik.



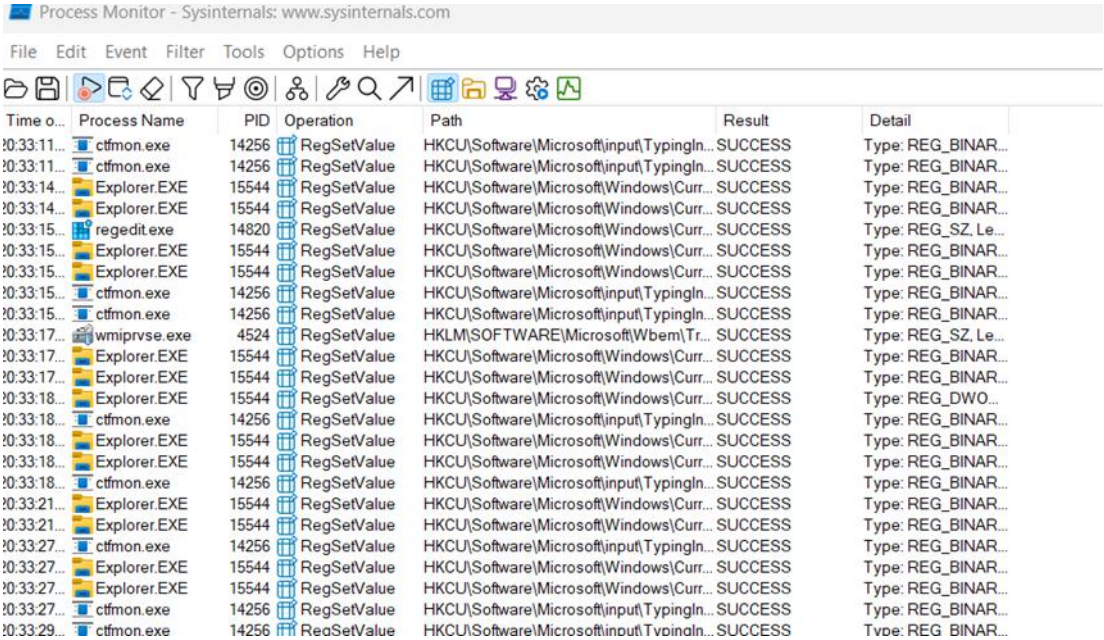
ilgisayar\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Değer adı: UpdateManager

Değer verisi: C:\Windows\System32\calc.exe

(değer atanmamış)
C:\ProgramData\Lenovo\V
"C:\Program Files\Microsof
C:\Users\LENOVO\AppDat

Anında Procmon ekranına geri döndük. Regedit'in yaptığı bu yazma işleminin listeye nasıl düştüğünü gördük.



Time o...	Process Name	PID	Operation	Path	Result	Detail
0:33:11...	ctfmon.exe	14256	RegSetValue	HKCU\Software\Microsoft\input\TypingIn...	SUCCESS	Type: REG_BINAR...
0:33:11...	ctfmon.exe	14256	RegSetValue	HKCU\Software\Microsoft\input\TypingIn...	SUCCESS	Type: REG_BINAR...
0:33:14...	Explorer.EXE	15544	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_BINAR...
0:33:14...	Explorer.EXE	15544	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_BINAR...
0:33:15...	regedit.exe	14820	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_SZ, Le...
0:33:15...	Explorer.EXE	15544	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_BINAR...
0:33:15...	Explorer.EXE	15544	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_BINAR...
0:33:15...	ctfmon.exe	14256	RegSetValue	HKCU\Software\Microsoft\input\TypingIn...	SUCCESS	Type: REG_BINAR...
0:33:15...	ctfmon.exe	14256	RegSetValue	HKCU\Software\Microsoft\input\TypingIn...	SUCCESS	Type: REG_BINAR...
0:33:17...	wmiprvse.exe	4524	RegSetValue	HKLM\SOFTWARE\Microsoft\Wbem\Tr...	SUCCESS	Type: REG_SZ, Le...
0:33:17...	Explorer.EXE	15544	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_BINAR...
0:33:17...	Explorer.EXE	15544	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_BINAR...
0:33:18...	Explorer.EXE	15544	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_DWO...
0:33:18...	ctfmon.exe	14256	RegSetValue	HKCU\Software\Microsoft\input\TypingIn...	SUCCESS	Type: REG_BINAR...
0:33:18...	Explorer.EXE	15544	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_BINAR...
0:33:18...	Explorer.EXE	15544	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_BINAR...
0:33:18...	ctfmon.exe	14256	RegSetValue	HKCU\Software\Microsoft\input\TypingIn...	SUCCESS	Type: REG_BINAR...
0:33:21...	Explorer.EXE	15544	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_BINAR...
0:33:21...	Explorer.EXE	15544	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_BINAR...
0:33:27...	ctfmon.exe	14256	RegSetValue	HKCU\Software\Microsoft\input\TypingIn...	SUCCESS	Type: REG_BINAR...
0:33:27...	Explorer.EXE	15544	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_BINAR...
0:33:27...	Explorer.EXE	15544	RegSetValue	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Type: REG_BINAR...
0:33:27...	ctfmon.exe	14256	RegSetValue	HKCU\Software\Microsoft\input\TypingIn...	SUCCESS	Type: REG_BINAR...
0:33:29...	ctfmon.exe	14256	RegSetValue	HKCU\Software\Microsoft\input\TypingIn...	SUCCESS	Type: REG_BINAR...

Neden Görev Yöneticisi Yetmez?

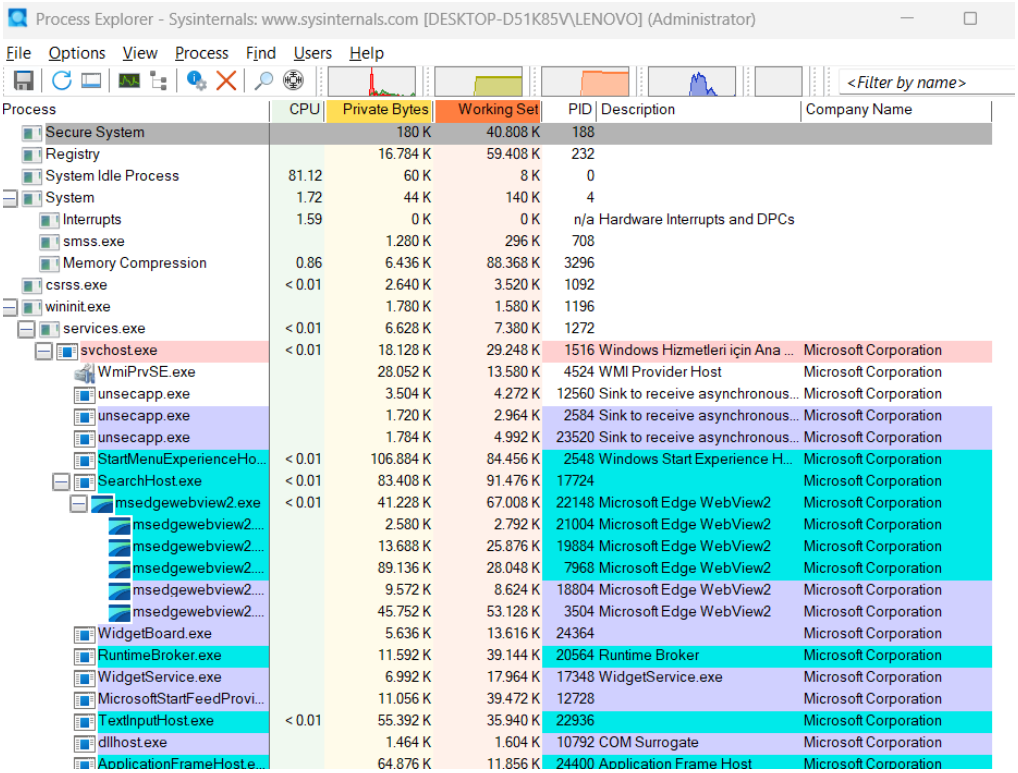
Standart Görev Yöneticisi, süreçleri genellikle "Alfabetik" veya "Kaynak Kullanımına" göre sıralayan düz bir liste (flat list) sunar. Bu liste, bağlamı gizler.

Eksik Parça: Bir sürecin *nereden geldiği* bilgisi.

Analoji: Bir suç mahalinde sadece elinde silah olan kişiyi görmek (Task Manager) ile o kişiye silahı vereni ve emri vereni görmek (Process Explorer) arasındaki farktır.

Parent-Child (Ebeveyn-Çocuk) İlişkisi

- Windows'ta (istisnalar hariç) her süreç, başka bir süreç tarafından yaratılır.
- **Parent (Ebeveyn):** CreateProcess API çağrısını yaparak yeni bir iş başlatan süreçtir.
- **Child (Çocuk):** Yeni oluşturulan süreçtir.
- Bu ilişki bir **"Process Tree" (Süreç Ağacı)** oluşturur.
- **PID (Process ID):** Sürecin kimlik numarası.
- **PPID (Parent Process ID):** Süreci doğuran atanın kimlik numarası.
- **Normal Bir Hiyerarşi Örneği:** smss.exe -> wininit.exe -> services.exe -> svchost.exe (Bu zincir Windows'un sağlıklı önyükleme sırasını gösterir.)



Process Explorer / Process Hacker ile Görünürlük

- Ağaç Görünümü (Tree View): Süreçlerin altına girintili (indent) şekilde listelenmesi. Bir süreci kimin başlattığını anında görürsünüz.

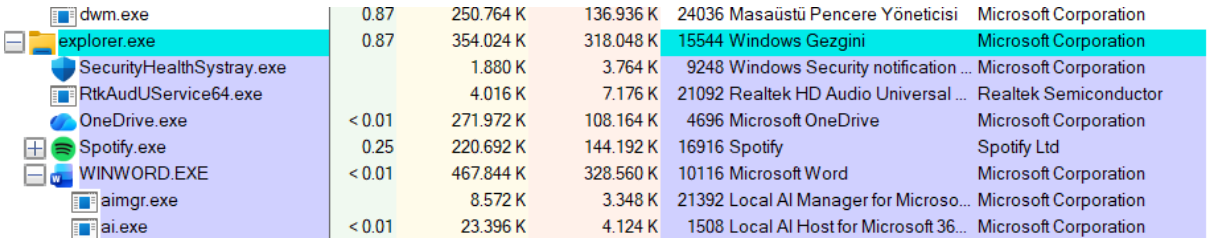
- Renk Kodları:
    - Yeşil: Yeni başlayan süreç.
    - Kırmızı: Kapanan/Ölen süreç.
    - Mor/Pembe: "Packed" veya sıkıştırılmış (şüpheli olabilir) görüntüler.
- İmza Doğrulama (Verify Signatures): Microsoft imzası gibi görünen ama aslında sahte olan zararlıları ifşa eder.

Oltalama (Phishing) Simülasyonu

Amacımız anormal süreç hiyerarşisini ve komut satırı gizleme taktiklerini tespit etmek.

Kritik Senaryo – Word Belgesinden PowerShell Açılması

- **1. Normal Davranış Nedir?**
- Kullanıcı masaüstündeki bir Word belgesine tıkladığında:
- **Parent:** explorer.exe (Masaüstü ortamı)
- **Child:** winword.exe (Word uygulaması)
- *Durum:* Word açılır, kullanıcı yazısını yazar. winword.exe'nin altında başka bir çocuk süreç (child process) görmemeniz gerekir (belki yazıcı sürücüsü veya yardım aracı hariç).



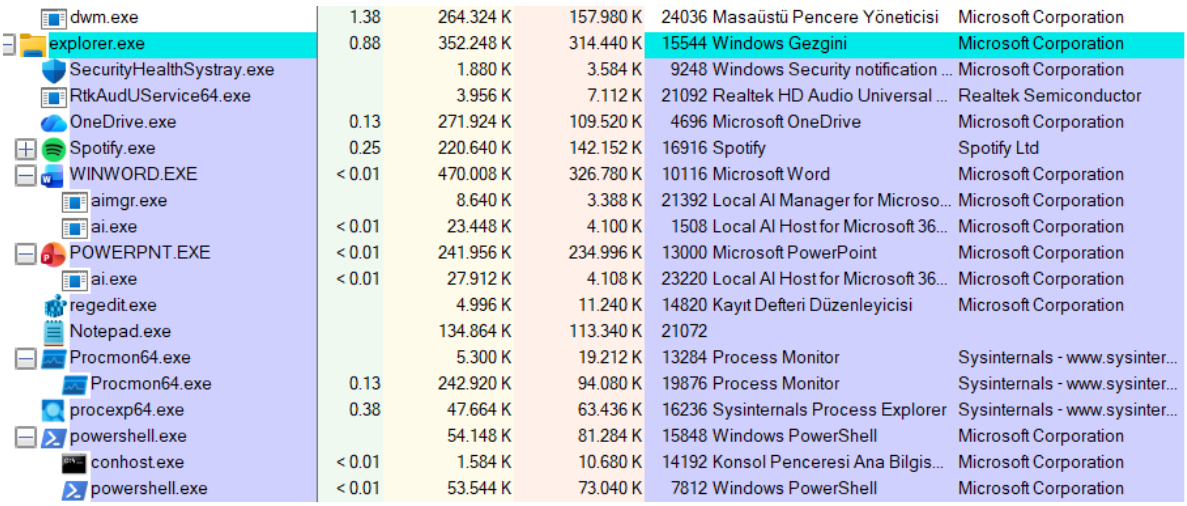
dwm.exe	0.87	250.764 K	136.936 K	24036 Masaüstü Pencere Yöneticisi	Microsoft Corporation
explorer.exe	0.87	354.024 K	318.048 K	15544 Windows Gezgini	Microsoft Corporation
SecurityHealthSystray.exe		1.880 K	3.764 K	9248 Windows Security notification ...	Microsoft Corporation
RtkAudUService64.exe		4.016 K	7.176 K	21092 Realtek HD Audio Universal ...	Realtek Semiconductor
OneDrive.exe	< 0.01	271.972 K	108.164 K	4696 Microsoft OneDrive	Microsoft Corporation
Spotify.exe	0.25	220.692 K	144.192 K	16916 Spotify	Spotify Ltd
WINWORD.EXE	< 0.01	467.844 K	328.560 K	10116 Microsoft Word	Microsoft Corporation
aimgr.exe		8.572 K	3.348 K	21392 Local AI Manager for Microso...	Microsoft Corporation
ai.exe	< 0.01	23.396 K	4.124 K	1508 Local AI Host for Microsoft 36...	Microsoft Corporation

- **2. Anormal (Zararlı) Davranış Nedir?**
- Kullanıcı, e-posta ile gelen "Fatura.docx" dosyasına tıklar.
- **Adım 1:** explorer.exe -> winword.exe başlatır. (Buraya kadar normal)
- **Adım 2:** winword.exe aniden bir **Child Process** doğurur: cmd.exe veya powershell.exe.

  Zararlı bir makroyu simüle etmek için komut satırından powershell.exe -WindowStyle Hidden komutunu çalıştırdık.

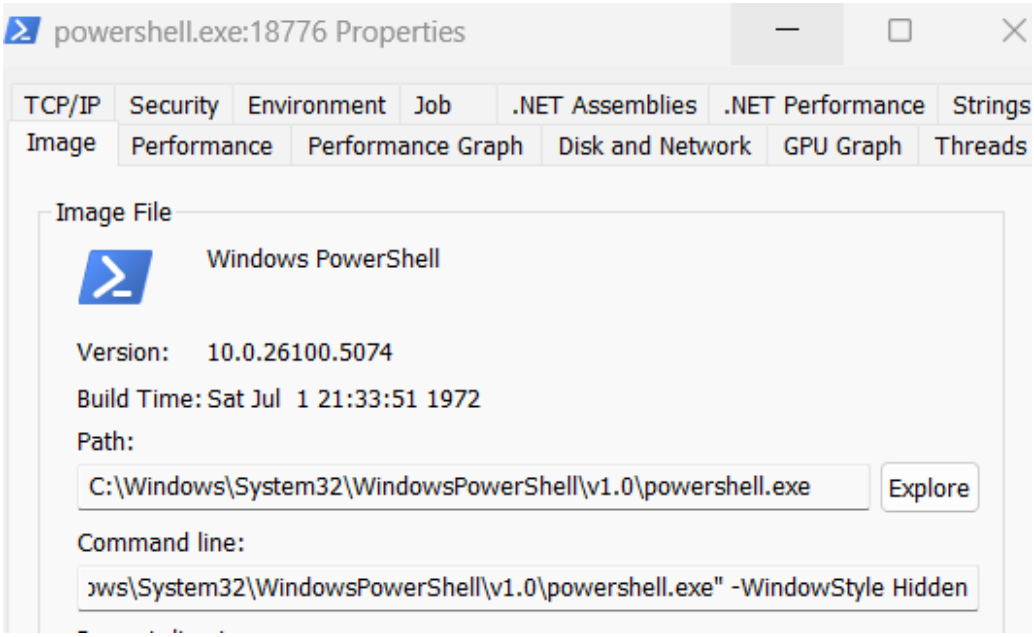
```
PS C:\Users\LENOVO> powershell.exe -WindowStyle Hidden
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
```

Process Explorer'a döndüğümüzde aşağıdaki görüntü ortaya çıktı.



dwm.exe	1.38	264.324 K	157.980 K	24036 Masaüstü Pencere Yöneticisi	Microsoft Corporation
explorer.exe	0.88	352.248 K	314.440 K	15544 Windows Gezgini	Microsoft Corporation
SecurityHealthSystray.exe		1.880 K	3.584 K	9248 Windows Security notification ...	Microsoft Corporation
RtkAudUService64.exe		3.956 K	7.112 K	21092 Realtek HD Audio Universal ...	Realtek Semiconductor
OneDrive.exe	0.13	271.924 K	109.520 K	4696 Microsoft OneDrive	Microsoft Corporation
Spotify.exe	0.25	220.640 K	142.152 K	16916 Spotify	Spotify Ltd
WINWORD.EXE	< 0.01	470.008 K	326.780 K	10116 Microsoft Word	Microsoft Corporation
aimgr.exe		8.640 K	3.388 K	21392 Local AI Manager for Microso...	Microsoft Corporation
ai.exe	< 0.01	23.448 K	4.100 K	1508 Local AI Host for Microsoft 36...	Microsoft Corporation
POWERPNT.EXE	< 0.01	241.956 K	234.996 K	13000 Microsoft PowerPoint	Microsoft Corporation
ai.exe	< 0.01	27.912 K	4.108 K	23220 Local AI Host for Microsoft 36...	Microsoft Corporation
regedit.exe		4.996 K	11.240 K	14820 Kayıt Defteri Düzenleyicisi	Microsoft Corporation
Notepad.exe		134.864 K	113.340 K	21072	
Procmon64.exe		5.300 K	19.212 K	13284 Process Monitor	Sysinternals - www.sysinter...
Procmon64.exe	0.13	242.920 K	94.080 K	19876 Process Monitor	Sysinternals - www.sysinter...
procexp64.exe	0.38	47.664 K	63.436 K	16236 Sysinternals Process Explorer	Sysinternals - www.sysinter...
powershell.exe		54.148 K	81.284 K	15848 Windows PowerShell	Microsoft Corporation
conhost.exe	< 0.01	1.584 K	10.680 K	14192 Konsol Penceresi Ana Bilgis...	Microsoft Corporation
powershell.exe	< 0.01	53.544 K	73.040 K	7812 Windows PowerShell	Microsoft Corporation

Process Explorer'a dönüp yeni doğan powershell sürecine çift tıkladık ve aşağıdaki görüntü ortaya çıktı.



- **3. Bu Neden Tehlikeli?**
- Bir kelime işlemci (Word), neden bir komut satırı aracına (PowerShell) ihtiyaç duysun?
- **Mekanizma:** Belge içinde gizlenmiş **Kötü Amaçlı Makro (VBA Script)** çalışmıştır.
- **Amaç:** Makro, bilgisayarda komut çalıştırmak için PowerShell'i tetikler ("Spawn" eder).
- **Komut Satırı Analizi:** Process Hacker'da powershell.exe üzerine çift tıkladığınızda "Command Line" satırında şunları görebilirsiniz:

- -WindowStyle Hidden (Kullanıcı siyah pencereyi görmesin diye)
- -EncodedCommand (Komutları Base64 ile şifreleyerek güvenlik yazılımlarından saklamak için)
- DownloadString (İnternetten zararlı dosya indirmek için)

• NTFS İzinleri:

- * Dosyaya "Sadece Admin erişsin" demek ile "System erişsin" demek arasındaki fark.
- Bu ayrım, Windows güvenliğinin ve "Erişim Kontrolü" (Access Control) mekanizmasının kalbidir. Bir dosya üzerinde sağ tıklayıp "Güvenlik" sekmesine geldiğinizde gördüğünüz bu iki kimlik, yetki hiyerarşisinde bambaşka dünyaları temsil eder.

1. **Administrators (Yöneticiler Grubu): "Binanın Müdürü"**

   "Administrators", içinde kullanıcıların (sizin, benim, IT ekibinin) bulunduğu bir gruptur.

Kimdir?

İnsanlardır (veya hizmet hesaplarıdır).

Yetki Seviyesi: Çok yüksektir ama mutlak değildir.

Çalışma Mantığı (UAC - Kullanıcı Hesabı Denetimi):

Siz "Administrator" olsanız bile, Windows sizi varsayılan olarak "Standart Kullanıcı" yetkileriyle çalıştırır (Split Token). Ne zaman ki sağ tıklayıp "Yönetici olarak çalıştır" derseniz, o zaman "Admin" şapkanızı takarsınız.

Sınırlamalar:

İşletim sistemi, kendi bütünlüğünü korumak için Administrator grubuna bile bazı dosyaları (örneğin Registry'deki SAM dosyası veya bazı System32 dosyaları) "Yasak"lar.

a. *Örnek:* Bir Admin olarak C:\Windows\System32\config\SAM dosyasını silmeye çalışırsanız "Erişim Engellendi" hatası alırsınız. Çünkü o dosya anlık olarak işletim sistemi tarafından kilitlenmiştir ve sahibi SYSTEM'dir.

2. SYSTEM (LocalSystem): "Binanın Kendisi / Sahibi"

"SYSTEM", bir kullanıcı grubu değildir. İşletim sisteminin **kendisidir**.

Kimdir?

Windows Kernel'ı, sürücüler ve arka planda çalışan kritik Windows servisleri (Services).

Yetki Seviyesi: Tanrı Modu (God Mode). Makine üzerindeki en yüksek yetkidir.

Çalışma Mantığı: Bir parola sormaz, oturum açmaz. Bilgisayar açıldığı andan itibaren vardır. Kullanıcı profil klasörü (C:\Users\...) yerine kendi profili olan C:\Windows\System32\config\systemprofile dizinini kullanır.

Ayrıcalıklar: Administrators grubunun sahip olmadığı özel "Privileges" (Ayrıcalıklar) setine sahiptir (Örn: SeTcbPrivilege - İşletim sisteminin bir parçası gibi davranma yetkisi).

Kritik Senaryo: Neden "Sadece Admin" Yetmez?

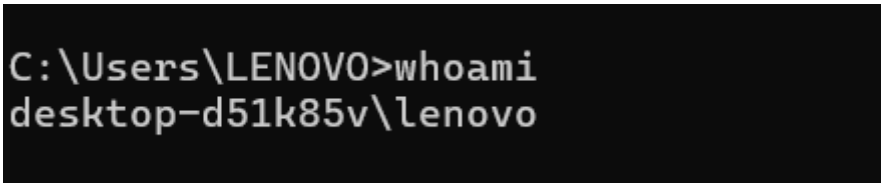
- Bir dosya veya klasöre izin verirken **SYSTEM** hesabını kaldırırsanız ne olur?
- **Senaryo:** Bir klasöre "Sadece Administrators grubu tam yetkili olsun, diğer herkesi (SYSTEM dahil) sileyim" dediniz.
- **Sonuç (Felaket):** O klasörün içindeki dosyalarla işi olan Windows servisleri (örneğin Windows Search, Backup servisi veya Antivirüs yazılımı) o klasöre erişemez.
    - *Örnek:* Eğer C:\Program Files içindeki bir uygulamanın izinlerinden SYSTEM'i kaldırırsanız, o uygulama güncellenemez, arka plan servisi başlatılamaz ve muhtemelen çöker. Çünkü güncellemeyi yapan "Windows Installer" servisi **SYSTEM** yetkisiyle çalışır, sizin Admin yetkinizle değil.

Hacker Perspektifi: "Privilege Escalation" (Yetki Yükseltme)

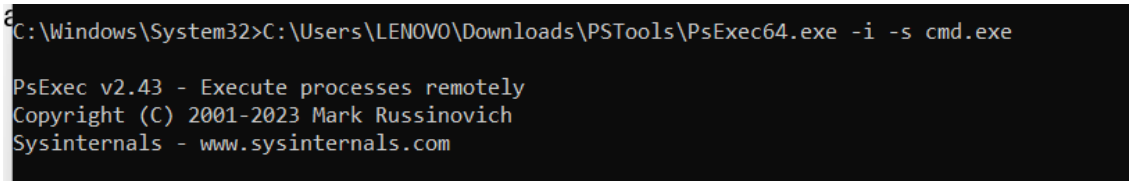
1. Bir siber saldırgan sisteme sızdığında genellikle ilk hedefi bir "Admin" hesabı ele geçirmektir. Ancak nihai hedef (End Game) SYSTEM yetkisine ulaşmaktır.
2. Admin olduğunuzda bile her şeyi yapamazsınız (örneğin çalışan bir Antivirüs sürecini sonlandıramazsınız).
3. Ama SYSTEM yetkisine geçen bir saldırgan, Antivirüs'ü bellekten silebilir, olay günlüklerini (Event Logs) iz bırakmadan temizleyebilir ve sistemi tamamen "root"layabilir.

Admin vs.SYSTEM Demosu

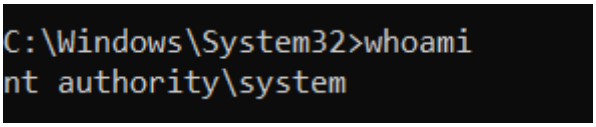
- Amacımız makine üzerindeki en yüksek yetkiyi kanıtlamak.
- Yönetici olarak bir Komut İstemcisi açın ve whoami komutunu çalıştırın.



•Sysinternals araçlarının bulunduğu klasöre giderek şu komutu çalıştırın: psexec -i -s cmd.exe



•Bu komut, ekrana yeni siyah bir komut istemcisi getirecektir.



İşte siber saldırganlarınların asıl ulaşmak istediği nihai hedef(End Game) budur. Dikkat ederseniz bana hiçbir şifre sormadı, yeni bir oturum açmadım. ‘Psexec’ aracına -s(System) parametresini vererek işletim sisteminin tam kalbine sızdık. Artık bir kullanıcı değiliz, ‘Binanın kendisiyiz’ . Bu siyah ekrandan şu an çalışan bir antivirüsü bile silebilir,olay günlüklerinizi iz bırakmadan yok edebiliriz.