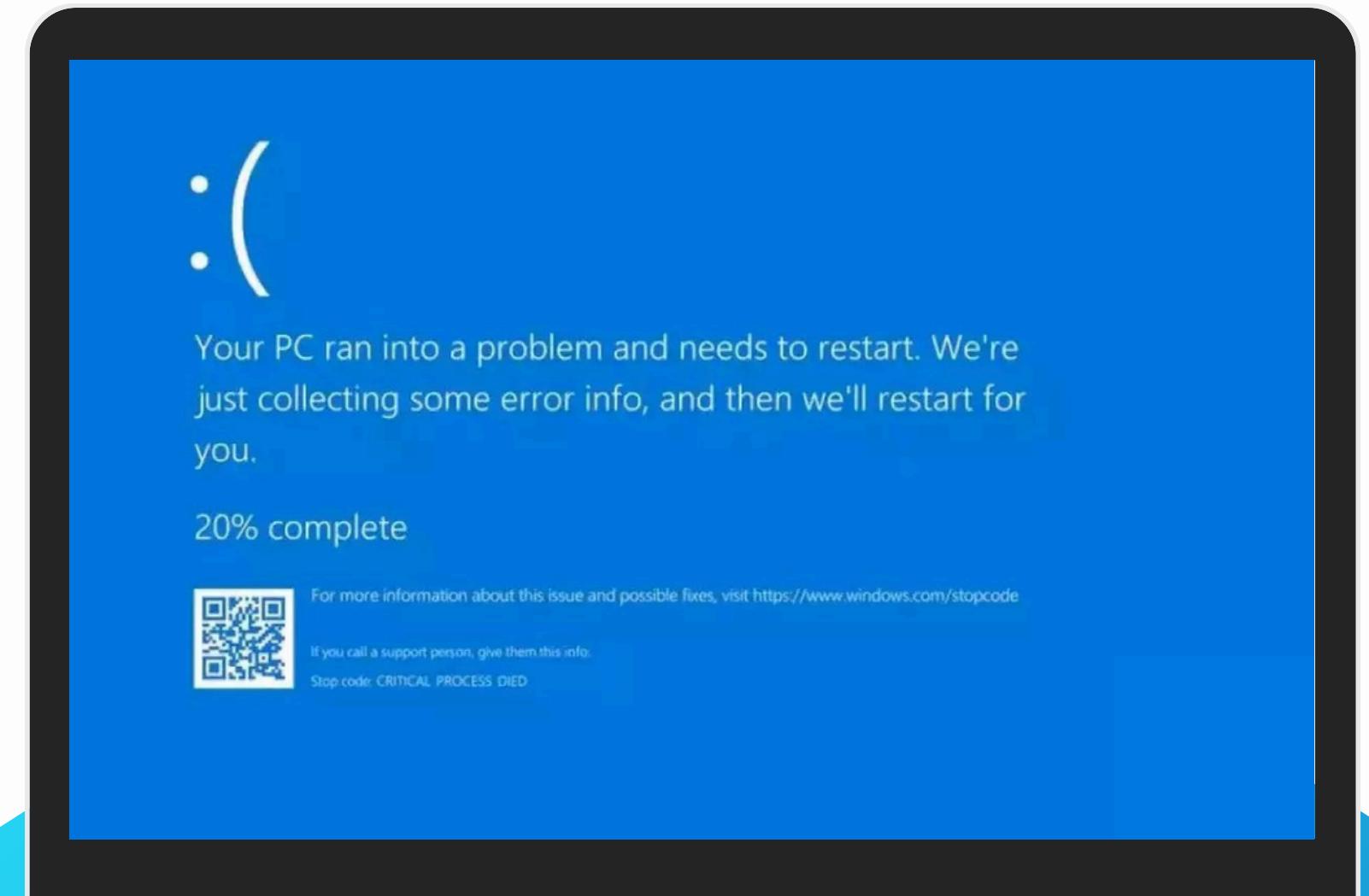


Microsoft CrowdStrike Krizi



- 
- Ne Oldu? 01
 - CrowdStrike 02
 - Neden Böyle Bir Sorun Oldu? 03
 - Etkilenen Şirketler 04
 - Etkilenmeyen Şirketler 05
 - Nasıl Çözüldü? 07
 - Daha Önce Oldu Mu? 08
 - Sorunun Sonuçları 09
 - Alınabilecek Önlemler 11

CrowdStrike

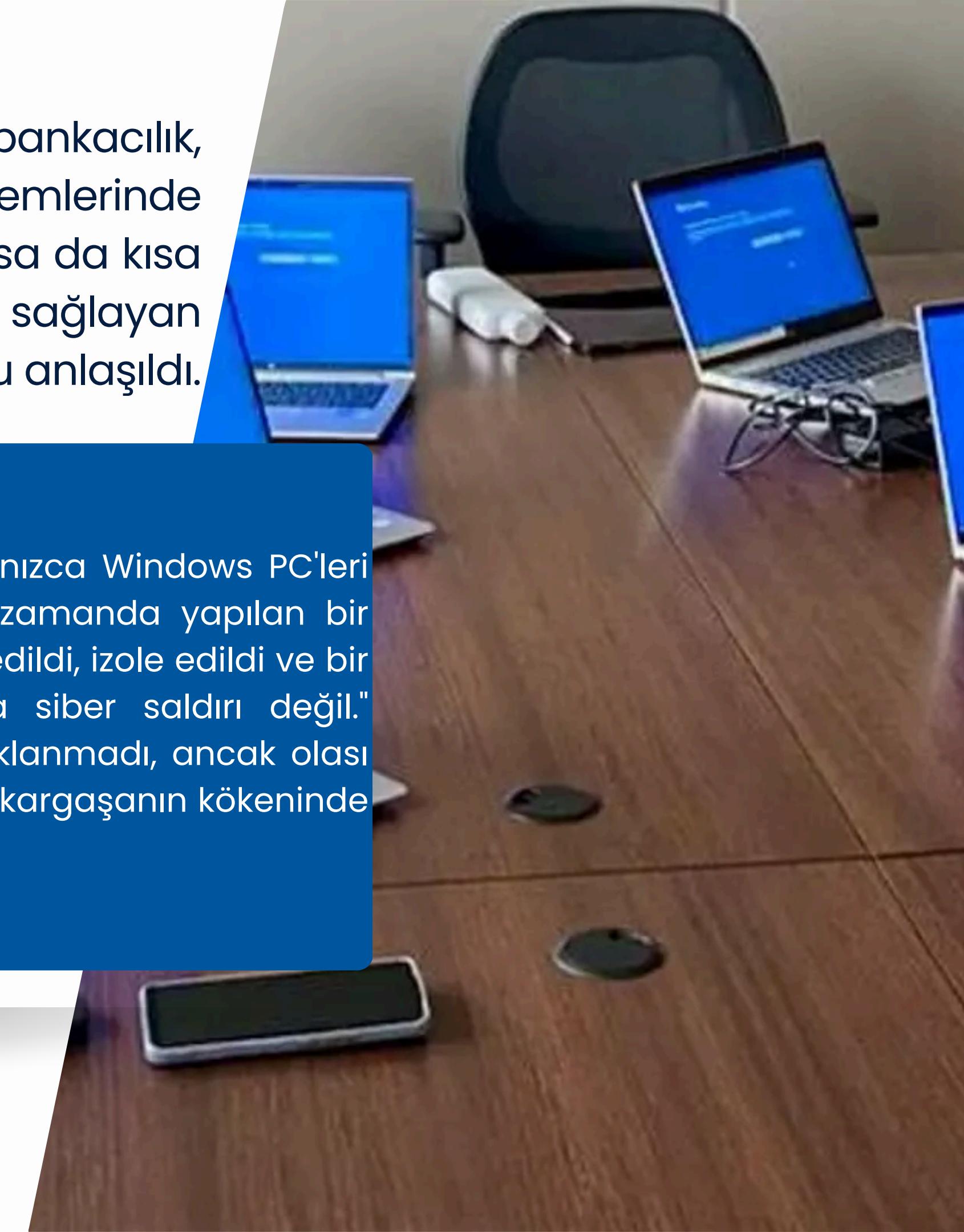
CrowdStrike tanınmış bir siber güvenlik firmasıdır ve Falcon Sensor yazılımı, sistemleri siber saldırınlara karşı korumak için tasarlanmıştır. Perşembe günü CrowdStrike, Windows sistemlerinin BSOD(blue screen of death) hatalarıyla çökmesine neden olan Falcon Sensor ile ilgili bir hata konusunda kullanıcıları uyardı.



NE OLDU?

Dünyanın birçok yerinde pek çok ülkede havacılık, bankacılık, sağlık, medya ve diğer birçok sektördeki bilgisayar sistemlerinde kesintiler meydana geldi. Sorun ilk etapta siber saldırı sanılsa da kısa zamanda, krize Microsoft'a siber güvenlik yazılımı sağlayan CrowdStrike şirketinin sistemlerindeki sorunun neden olduğu anlaşıldı.

CrowdStrike patronu George Kurtz'a göre sorunlar yalnızca Windows PC'leri etkiliyor, başka işletim sistemlerini etkilemiyor ve yakın zamanda yapılan bir güncellemedeki bir kusurdan kaynaklanıyor. "Sorun tespit edildi, izole edildi ve bir düzeltme uygulandı" dedi. "Bu bir güvenlik olayı veya siber saldırı değil." Güncellemede tam olarak neyin yanlış olduğu henüz açıklanmadı, ancak olası bir düzeltme tek bir dosyanın silinmesini içerdiginden, tüm kargaşanın kökeninde yalnızca tek bir sahte dosyanın bulunması mümkündür.



Ne Oldu?

0x0000009C "mavi ekran" (BSOD) hataları kusurlu donanımdan, eksik veya bozuk Android 6.0.1 sürücülerinden veya bozuk kernel modu sürücülerinden kaynaklanır.

Bilgisayarlardaki bellek dev bir sayı dizisi olarak düzenlenmiştir. Bu sayılar burada onaltılık olarak temsil edilmiş. Bilgisayar 0x9c (diğer adıyla 156) bellek adresini okumaya çalıştı. Bu neden kötü? Bu, herhangi bir program için geçersiz bir bellek bölgesidir. Bu bölgeden okumaya çalışan herhangi bir program, **WINDOWS TARAFINDAN HEMEN ÖLDÜRÜLECEKTİR**. Burada bu yığın dökümünde gördüğünüz şey budur. Peki neden 0x9c bellek adresi okunmaya çalışıyor? Çünkü... programcı hatası. C++'in, kullandığı dilin, "burada hiçbir şey yok" anlamına gelen özel bir değer olarak 0x0 adresini kullanmayı sevdiği ortaya çıktı, ona erişmeye çalışmayı, yoksa ölürsün.

$\text{NULL} + 0x9C = 0x9C = 156$. Bu geçersiz bir hafıza bölgesi. Ve bunun kötü yanı, bunun sistem sürücüsü adı verilen ve bilgisayara AYRICALIKLI erişime sahip özel bir program olmasıdır. Bu nedenle işletim sistemi, çok fazla tedbir nedeniyle derhal çökmeye zorlanır.

```
EXCEPTION_RECORD: ffffffb0d18d3ec28 -- (.exr 0xfffffb0d18d3ec28)
ExceptionAddress: fffff8021df335a1 (csagent+0x000000000000e35a1)
  ExceptionCode: c0000005 (Access violation)
    ExceptionFlags: 00000000
NumberParameters: 2
  Parameter[0]: 0000000000000000
  Parameter[1]: 000000000000009c
Attempt to read from address 000000000000009c

CONTEXT: ffffffb0d18d3e460 -- (.cxr 0xfffffb0d18d3e460)
rax=fffffb0d18d3f2b0 rbx=0000000000000000 rcx=0000000000000000
rdx=fffffb0d18d3f280 rsi=ffff9a81b596f9a4 rdi=ffff9a81b596605c
rip=ffff8021df335a1 rsp=fffffb0d18d3ee60 rbp=fffffb0d18d3ef60
r8=000000000000009c r9=0000000000000000 r10=0000000000000000
r11=0000000000000014 r12=fffffb0d18d3ef28 r13=fffffb0d18d3f0d0
r14=000000000000001a r15=0000000000000004
iopl=0 nv up ei pl nz na po nc
cs=0010 ss=0018 ds=002b es=002b fs=0053 gs=002b
csagent+0xe35a1: fffff8021df335a1 45ff08 NOV r9d.dword ptr [r8] ds:002b:00000000`0000009c=??
Resetting default scope

BLACKBOXBSD: 1 (!blackboxbsd)

BLACKBOXNTFS: 1 (!blackboxntfs)

BLACKBOXPNP: 1 (!blackboxpnsp)

BLACKBOXVINLOGON: 1

PROCESS_NAME: System

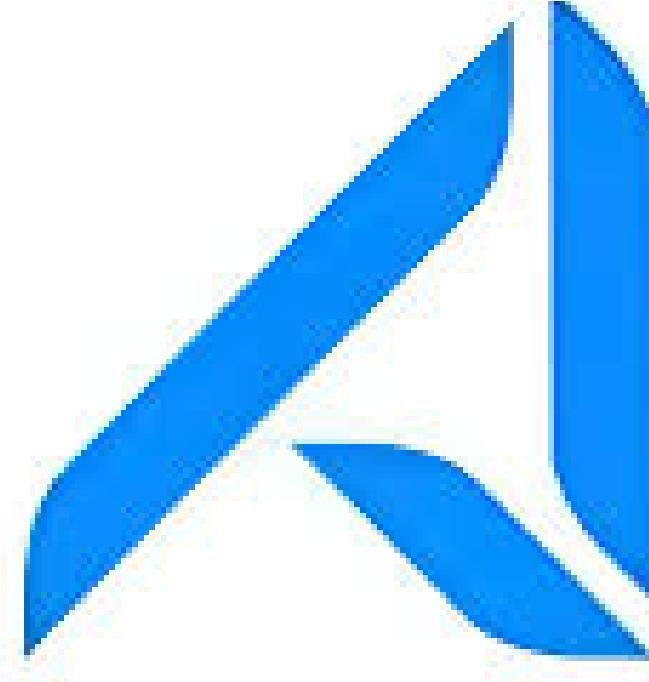
READ_ADDRESS: 000000000000009c

ERROR_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%p referenced memory at 0x%p. The memory could not be read.

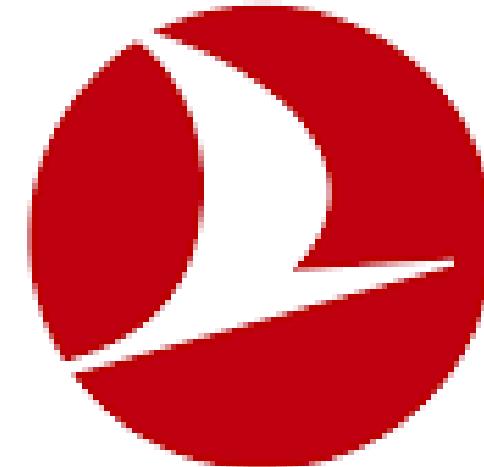
EXCEPTION_CODE_STR: c0000005

EXCEPTION_PARAMETER1: 0000000000000000
```

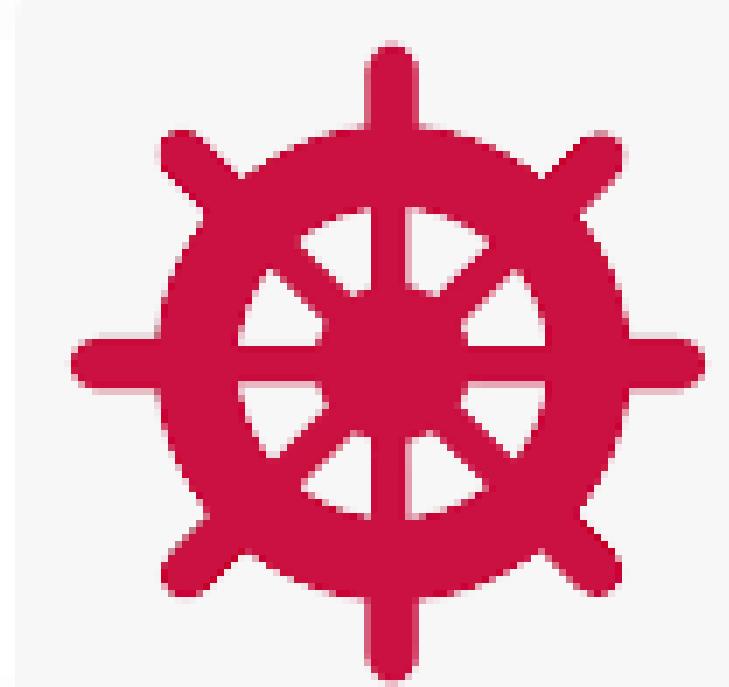
ETKİLENEN ŞİRKETLERDEN BAZILARI



A JET



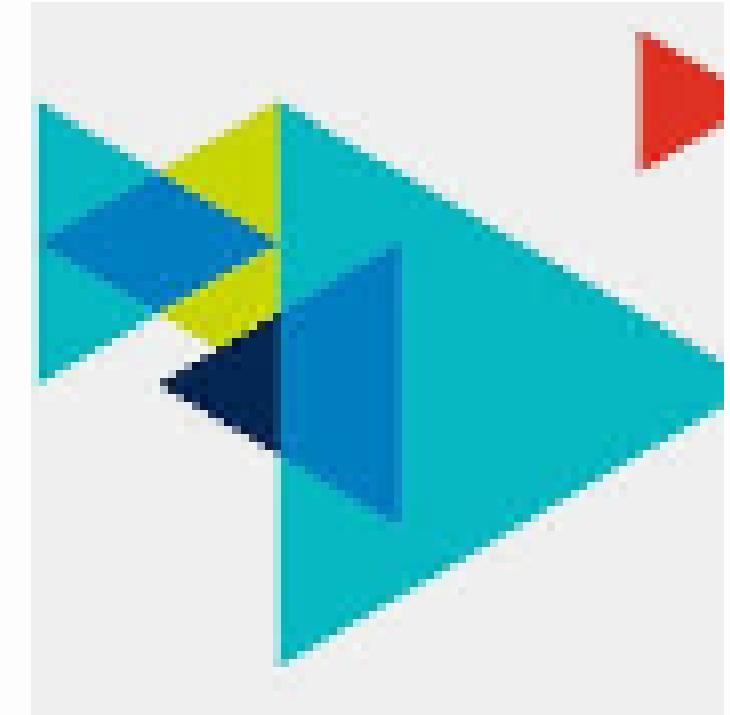
TURKISH AIRLINES



DENİZBANK



TÜV TÜRK



TÜRK TELEKOM

Etkilenmeyen Ülkeler Neden Etkilenmedi?

Dünyada bu olaydan hiç etkilenmeyen birkaç ülke vardı. Bunlar arasında Rusya, Çin ve İran dikkat çekiyor. Bu ülkelerin kaos yaşamamasının nedeni, kendi işletim sistemlerini kurmaları.

Çin, ülkenin ABD teknolojisine karşı olan bağımlılığını azaltmak için yerli teknolojilere odaklanmıştı. Hükümet, yabancı kaynaklı işletim sistemlerine karşı açık kaynaklı işletim sistemi OpenKylin'i piyasaya sürmüştü.

Bu sistem, açık kaynaklı Linux işletim sistemine dayanıyor. Hatta Çin, devlet dairelerine alınacak yeni bilgisayarlarda AMD ve Intel işlemcilerin tercih edilmesini yasaklamış, Windows yerine yerli işletim sistemi kullanılmasını önermişti.



Sorun Nasıl Çözüldü?

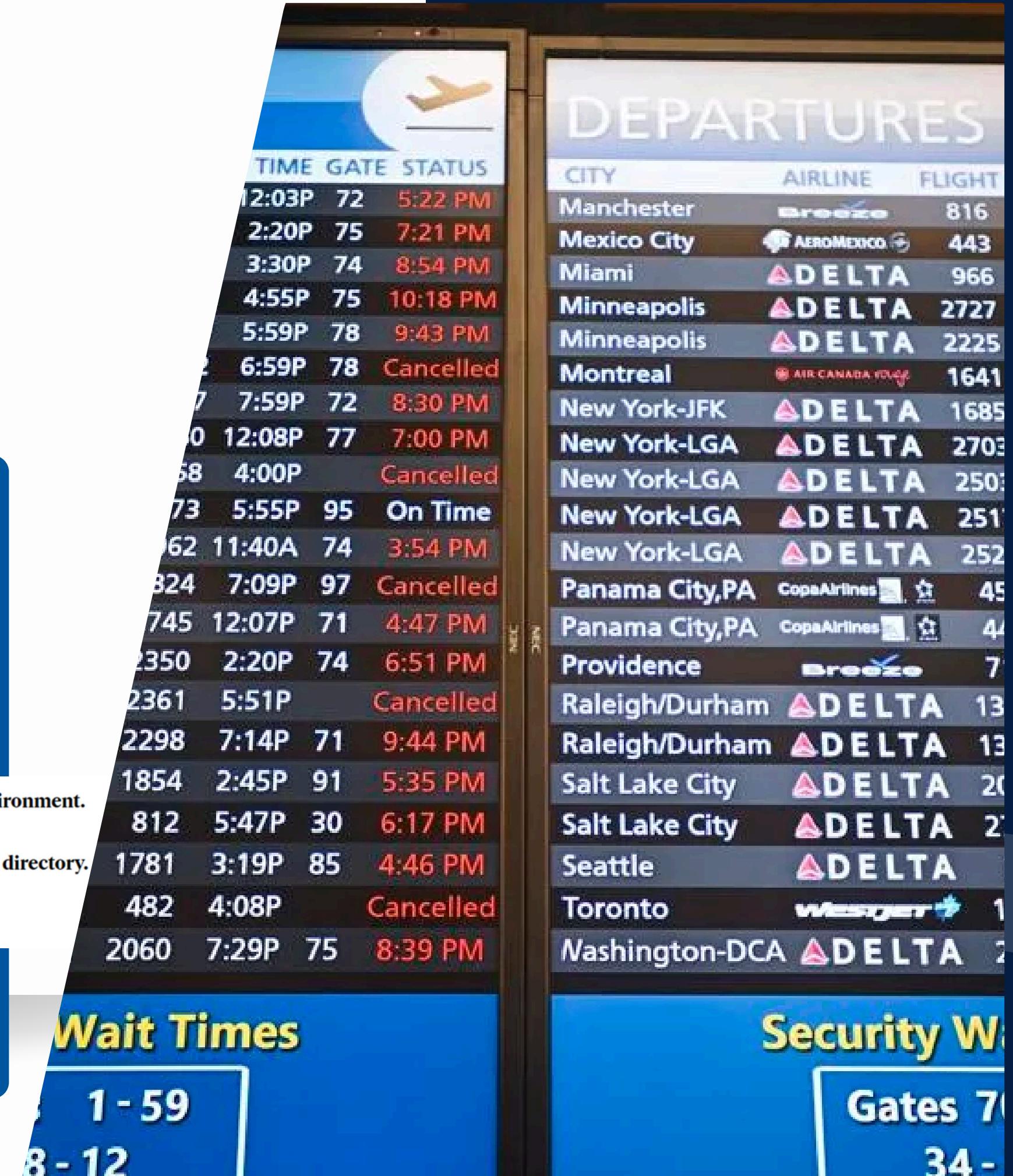
Çözüm 1

Microsoft, Azure bulutunu kullanan bazı müşterilerin, sistemleri 15 defaya kadar yeniden başlatarak bilgisayarlarını düzeltibildiklerini söyledi. Amazon ayrıca bilgisayarların yeniden başlatılmasının da AWS bulut yazılımını kullanan müşteriler için sorunu çözebileceğini öne sürdü.

Çözüm 2

Ulusal Siber Olaylara Müdahale Merkezi (USOM) sosyal medya hesabından CrowdStrike sorununa ilişkin bir de çözüm yolu paylaştı.

1. Boot Windows into safe mode or the Windows Recovery Environment.
2. Navigate to the C:\Windows\System32\drivers\CrowdStrike directory.
3. Locate the file matching “C-00000291*.sys” and delete it.



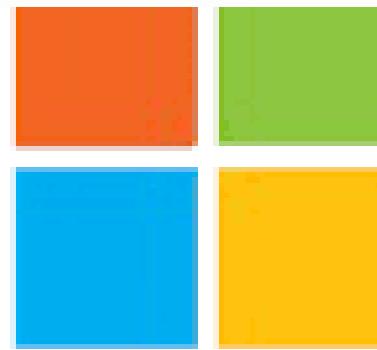
Daha Önce Böyle Bir Kriz Oldu Mu?

21 Nisan 2010'da antivirüs şirketi McAfee, kurumsal müşterilerinin kullandığı yazılımına yönelik bir güncelleme yayınladı. Güncelleme, önemli bir Windows dosyasını sildi ve dünya çapında milyonlarca bilgisayarın çökmesine ve tekrar tekrar yeniden başlatılmasına neden oldu. CrowdStrike hatasına benzer şekilde McAfee sorununun da manuel olarak düzeltilmesi gerekiyordu.

Kurtz o sırada McAfee'nin baş teknoloji sorumlusuydu. Aylar sonra Intel, McAfee'yi satın aldı. Ve birkaç ay sonra da Kurtz şirketten ayrıldı. 2012 yılında ise CrowdStrike'ı kurdu ve o zamanandan beri şirketin CEO'su olarak görev yapıyor .



Sorundan Doğan Sonuçlar



Microsoft

Microsoft, en büyük kesintilerinden biri olarak tanımlanan olayda, dünya genelinde 8,5 milyon bilgisayarın etkilendiğini tahmin ediyor.

parametrix

Sigorta şirketi Parametrix, Microsoft dışındaki ABD'li 500 büyük şirketin geçen hafta gerçekleşen CrowdStrike kaynaklı teknik aksaklıktan dolayı 5,4 milyar dolar mali kayıp yaşayacağını açıkladı.

Şirket, bu zararın 540 milyon dolar ile 1,1 milyar dolar arasındaki bölümünün sigortalanmış kayıplardan olduğunu belirtti.



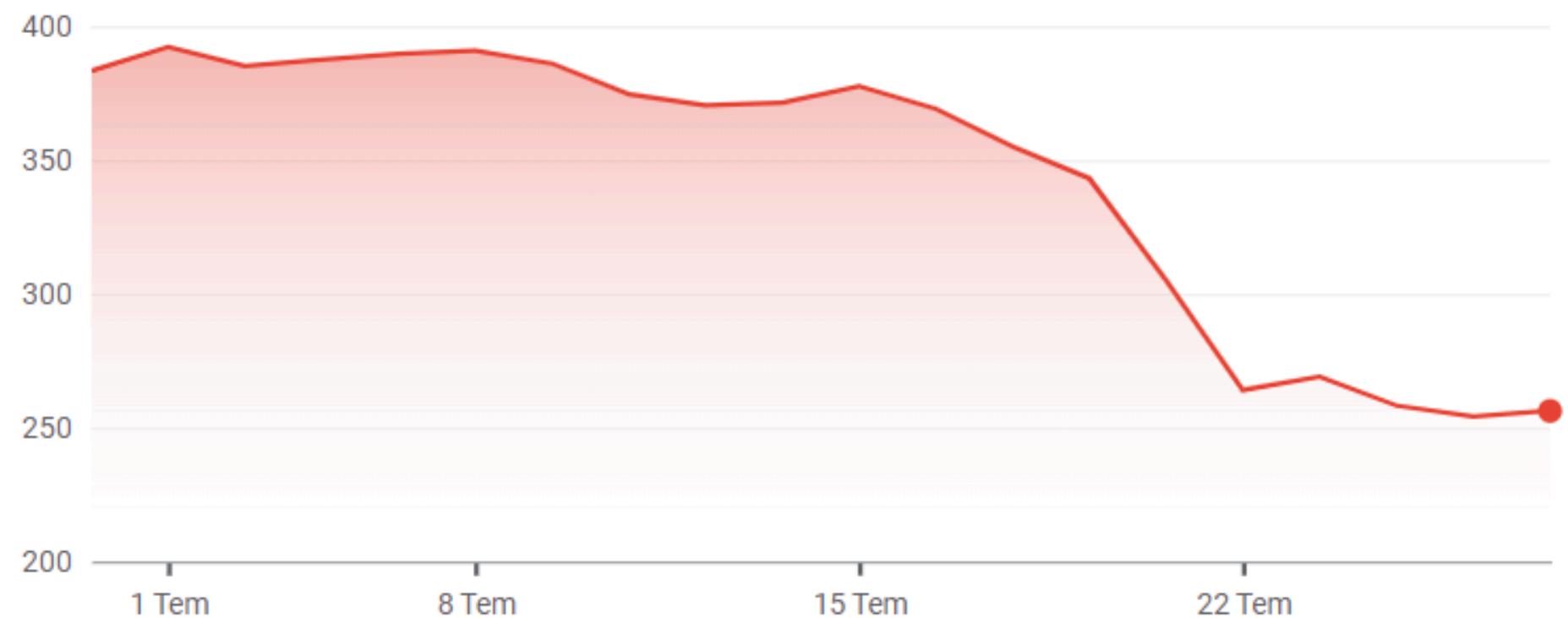
Küresel çapta 5 binden fazla uçuşun iptal edilirken, bazı ülkelerde finans sistemi devre dışı kalmıştı.

CrowdStrike Hisse Durumu

ABD'de piyasaların açılmasının ardından Teksas merkezli CrowdStrike'in hisseleri, Türkiye saatıyla 16.31'de yüzde 14'ün üzerinde değer kaybetti.

Şirketin hisselerinde açılışta kaydedilen düşüşün, hız kesse de devam ettiği görüldü. CrowdStrike'in hisseleri Türkiye saatıyla 17.00 itibarıyla yüzde 9'un üzerinde düşüşle 309,89 dolardan işlem gördü.

Microsoft'un hisseleri de açılışın hemen sonrasında yüzde 1'in üzerinde değer kaybetti. Şirketin hisselerindeki düşüş, Türkiye saatıyla 17.00 itibarıyla yüzde 1'in altına indi.



Teknik Detaylar

Windows sistemlerinde, Kanal Dosyaları şu dizinde bulunur:

C:\Windows\System32\drivers\CrowdStrike\ ve "C-" ile başlayan bir dosya adına sahiptir. Her kanal dosyasına benzersiz bir tanımlayıcı olarak bir numara atanır. Bu olayda etkilenen Kanal Dosyası 291'dir ve "C-00000291-" ile başlayan ve .sys uzantısıyla biten bir dosya adına sahip olacaktır. Kanal Dosyaları SYS uzantısıyla bitmesine rağmen çekirdek sürücülerini değildir. Kanal Dosyası 291, Falcon'un Windows sistemlerinde adlandırılmış kanal1 yürütmesini nasıl değerlendirdiğini kontrol eder. Adlandırılmış kanallar, Windows'da normal, işlem içi veya sistemler arası iletişim için kullanılır. 04:09 UTC'de gerçekleşen güncelleme, siber saldırıarda yaygın C2 çerçeveleri tarafından kullanılan yeni gözlemlenen, kötü amaçlı adlandırılmış kanalları hedeflemek için tasarlanmıştır. Yapılandırma güncellemesi, işletim sistemi çökmesine neden olan bir mantık hatasını tetikledi.

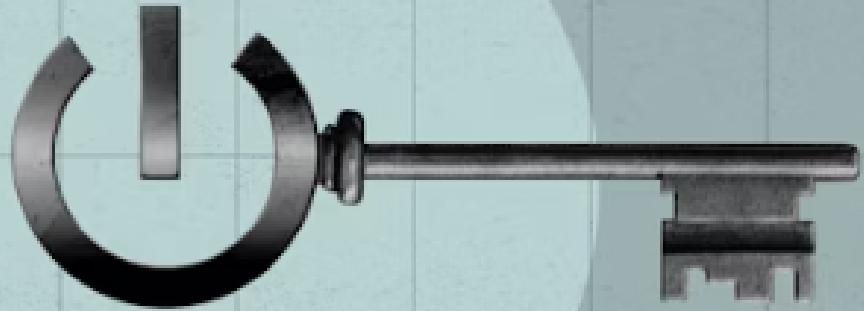
Daha Büyük Etkili Sonuçlar Ne Olabilirdi?

THE GREAT RESET

The Great Reset," Dünya Ekonomik Forumu (WEF) tarafından hazırlanan 2020'de başlatılan bir girişimdir. Bu girişimin amacı, COVID-19 pandemisinin yarattığı küresel krizin ardından dünyayı daha sürdürülebilir, dirençli ve adil bir şekilde yeniden inşa etmektir. The Great Reset, Prens Charles tarafından tanıtılmış ve sadece insanlar isterse gerçekleşeceğini belirtmiş. Daha sonrasında bir komplot teorisi atılmış ve bunun "**Yeni Dünya Düzenini**" getirmek için kullanılacağı iddia edilmiş.

A PODCAST
FROM THE
WORLD
ECONOMIC
FORUM

WORLD
ECONOMIC
FORUM



THE
GREAT
RESET



Alınabilecek Önlemler

Uygulama yerine kurumların güncellemeleri daha sıkı test etmeleri, genel olarak bu ve benzeri sorunların önüne geçilmesi konusunda yeterli bir önem. Bilişim teknolojileri süreçlerinde yedekleme, güncelleme, değişiklik yönetimi konularının önemini bu sorumlarda daha ciddi olarak ortaya çıkıyor

TEŞEKKÜRLER!

ZEYNEP SELCEN DOĞAN