Write-Up: Retro Calculator (Forensics)

Ομάδα: mousiko_gymsasio_agriniou_lt_1 (Μουσικό Γυμνάσιο Αγρινίου - Λ.Τ.)
Μαθητές/Μαθήτριες Πέτρος Παπαθανασίου

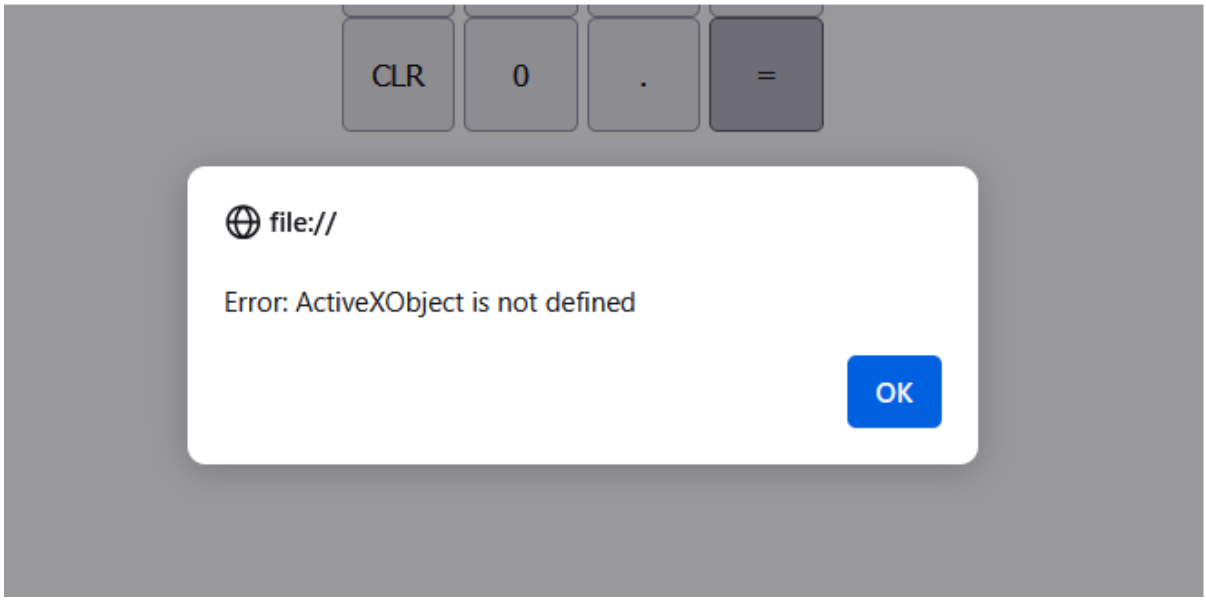
Επισκόπηση Δοκιμασίας

Η δοκιμασία μας δίνει ένα αρχείο τύπου html. Από την εκφώνηση φαίνεται ότι είναι μία αριθμομηχανή.

Επίλυση

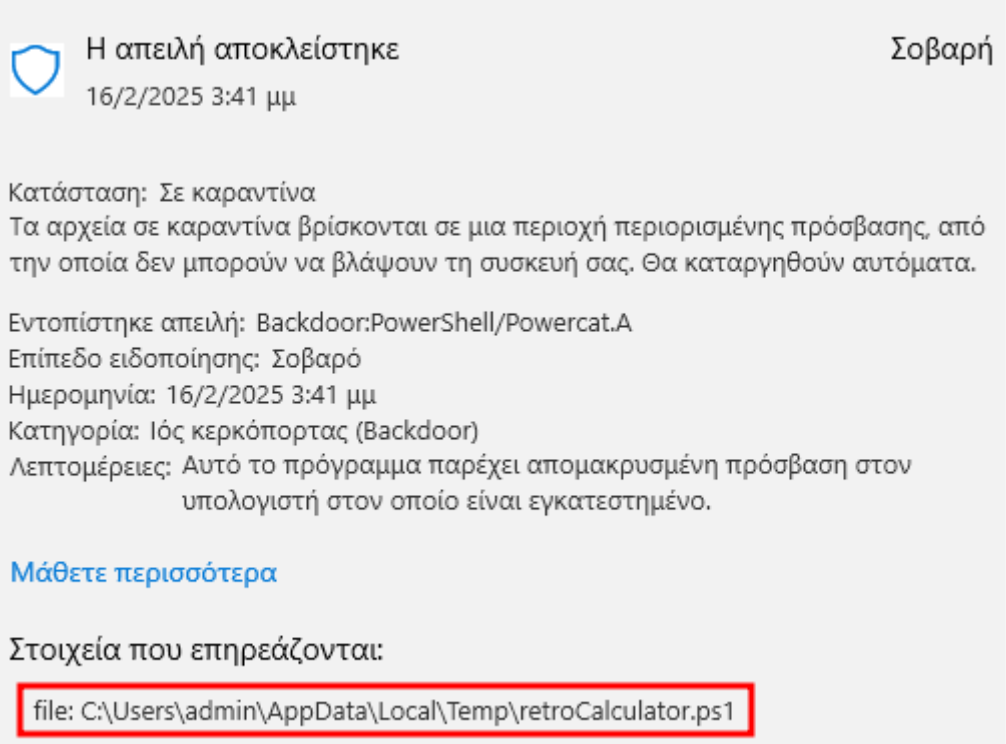
Αρχική ανάλυση

Όταν πήγα να το ανοίξω από λειτουργικό linux δεν δούλευε κανένα κουμπί. Για αυτόν τον λόγο άλλαξα λειτουργικό σε windows. Όμως εκεί το έπιασε το anti-virus. Έτσι, σκέφτηκα ότι πίσω από το κουμπιουτεράκι τρέχει κάποιος κρυφός κώδικας. Όταν έκλεισα το anti-virus, άνοιξε κανονικά η εφαρμογή. Αλλά την στιγμή που πάτησα το κουμπί “ίσον”(=), εμφανίστηκε ένα powershell prompt, όπως αναφέρεται στην εκφώνηση.



Έψαξα στο ίντερνετ για πληροφορίες για το σχετικό μήνυμα και είδα ότι το ActiveXOnject υπάρχει μόνο στον Internet Explorer.

Μετά προσπάθησα να το ανοίξω με το internet explorer και μου έβγαλε ειδοποιήση το windows defender για μία απειλή που αποκλείστηκε. Πήγα στο defender και είδα ότι σχετίζεται με ένα αρχείο powershell στον φάκελο Temp.



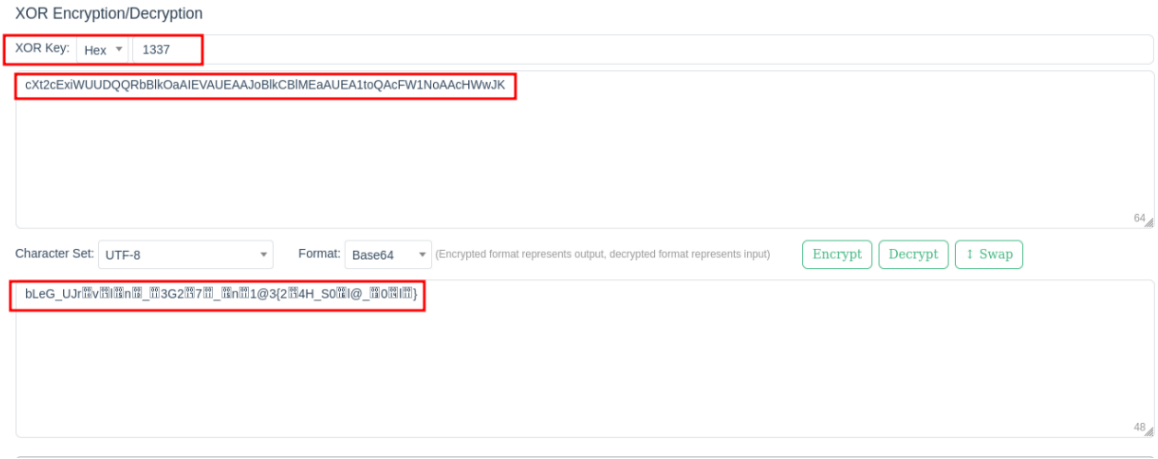
Εκμετάλλευση ευπάθειας

Πήρα το αρχείο powershell και προσπάθησα να το τρέξω. Όμως δεν εμφάνιζε κανένα αποτέλεσμα. Για αυτό το άνοιξα με το VSCode για να δω τον κώδικα. Διαπίστωσα ότι σχετίζεται με ένα εργασλείο που ονομάζεται powercat και έχει σκοπό την επικοινωνία δύο υπολογιστών, σαν το netcat. Παρακάτω στον κώδικα είδα μία if, η οποία ελέγχει την ύπαρξη μιας μεταβλητής secret και οδηγείται σε μία αποκωδικοποιήση. Επειδή δεν ήξερα με ποιον τρόπο δουλεύει η secret, άλλαξα την if σε True. Παρ' όλ' αυτά ακόμα δεν μου έδειχνε κάποιο αποτέλεσμα όταν έτρεχα το πρόγραμμα.

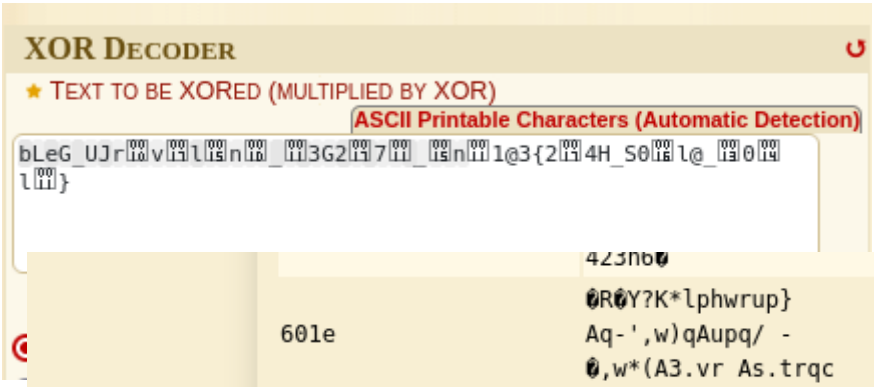
```powershell
}
if ($secret)
{
  Write-Host "Secret option detected. Starting decryption..."

  $base64EncryptedCheck = "cXt2cExiWUUDQQRbBlkOaAIEVAUEAAJoBlkCBlMEaAUEA1toQAcFW1NoAAcHWwJK"

  $xorKey = 0x1337

  $encryptedBytes = [System.Convert]::FromBase64String($base64EncryptedCheck)

  $decryptedBytes = @()
  foreach ($byte in $encryptedBytes) {
      $decryptedByte = ($byte -bxor $xorKey) % 256
      $decryptedBytes += [byte]$decryptedByte
  }

  $decryptedCheck = [System.Text.Encoding]::UTF8.GetString($decryptedBytes)
```

```powershell
if (True)
{
  Write-Host "Secret option detected. Starting decryption..."
```

Με δεδομένο αυτό, αποφάσισα να κάνω μόνος μου την αποκωδικοποιήση. Αρχικά χρησιμοποίησα ένα εργαλείο Xor Decryptor και πήρα ένα αποτέλεσμα που μοίαζει με την μορφή της σημαίας.



Έπειτα μετά από διάφορες δοκιμές σκέφτηκα ότι μπορεί να έιναι cipher. Για αυτό το έτρεξα με ένα εργαλείο xor cipher και μου έδωσε την σωστή σημαία.



Σημαία

Η σημαία που βρέθηκε:

	423n6b
601e	R Y?K*lphwrup} Aq-',w)qAupq/ - ,w*(A3.vr As.trqc
7e1e	R Y! K4lnhirkpcAo-9,i)oAkp o/>- ,i*6A-.hr>Am.jroc
781a	V]'O2hhlovmteEi)? (o- iEmti+8)(o.0E+*nv8Ek *lvig
2400	FLAG{Unr4v3l1n9_53c23 75_1n51d3_234l_w02ld_ 700l5}
2b1c	IPN[tIan;j<p>r6C:/ l.<+:C>r:-k/ P.<(cCx,=pkC8,?p:a
2100	CLDG~Ukr1v6l4n<_03f26 70_4n01a3Z264i_r07la_ 205l0}
721a	V]- O8hblevgtoEc)5(e- cEgtc+2) (e.:E! *dv2Ea*fvcg
2600	DLCGyUlr6v1l3n;_73a21 77_3n71f3]214n_u00lf_ 502l7}
251c	GP@[zIon5j2p0r8C4/ b.2+4C0r4-e/ ^.2(mCv,3peC6,1p4a
	[W\

```
FLAG{Unr4v3l1n9_53c2375_1n51d3_234l_w02ld_7001s}
```