EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ZAZNAVANJE GROŽENJ - VAJA

VSEBINA IN CILJI MODULA

Prepoznavanje lažnih sporočil.

Ugotovljanje in povezovanje kazalnikov zlorabe (IoC Indicators of Compromise).

Prvo odzivanje in proženje začetnih ukrepov.

Sodelovanje med deležniki v organizaciji in zunaj nje.

POTEK VAJE

Predstavitev scenarija napada in odzivanja

Udeleženci prejmete simulirano sporočilo s strani Finančne uprave RS, analizirate vsebino in prepoznavate sumljive elemente, izvajate odziv.

Vloge v vaji

Računovodstvo, finance kot prvi stik s napadom.

IT in varnost izvaja analizo dogodkov in tehnične ukrepe.

Vodstvo sprejema odločitve, obvešča, zagotavlja potrebna sredstva.

Način dela

Vsi igrate vse vloge.

Odgovore, mnenje, vprašanja pišete na <tablo>.

Tekom vaje se postopno podajajo nove informacije.

Pomembno!

Ni napačnih odgovorov – cilj je učenje!

Vsi prispevki štejejo – sodelujte, tudi če niste iz IT oziroma še posebej zato!

Razmišljajte, kako bi ravnali v resnični situaciji

SCENARIJ

Prejem lažne e-pošte z zlonamerno datoteko

Udeleženci analizirate simulirano sporočilo s strani Finančne uprave RS, analizirate vsebino in prepoznavate sumljive elemente.

Zaznavanje sumljivih aktivnosti

Prikaz alarmov v SIEM sistemu, antivirusna opozorila, log zapisi, povezovanje sosledja dogodkov.

Izvedba prvega odziva na incident

Odločanje o prvih ukrepih in njihovo izvajanje, komuniciranje in poročanje.

ZLONAMERNA E-POŠTA

Od: Finančna uprava RS <noreply@ddv-furs.si>
Za: [ime.priimek@podjetje.si]
Datum: 20. januar 2026, 10:26
Priponka: Oprostitev_DDV_po_46clenu_ZDDV-1.zip

Spoštovani,

obveščamo vas, da je z dnem 1. 1. 2026 v veljavo stopil nov Pravilnik o načinu in pogojih oprostitve davkov, ki določa subjekte ter vrsto blaga in storitev, za katere se uporablja oprostitev plačila DDV po 46. členu ZDDV-1 (Uradni list RS, št. 123/2025).

Na podlagi razpoložljivih podatkov vaše podjetje posluje s takšnimi subjekti, zato vas zaradi zagotavljanja skladnosti z zakonodajo in uveljavljanja vaših pravic prosimo, da izpolnite priloženi obrazec potrdila o oprostitvi plačila DDV in/ali trošarine v priponki.

Obrazec v priponki je v formatu .ZIP; vsebuje dokument “Potrditev_upravičenosti_46člen.pdf”, ki ga izpolnjenega posredujete nazaj na naslov: oprostitve@ddv-furs.si. Prosimo, da to storite najkasneje do 25. 1. 2026, sicer izdaja računov subjektom s katerim poslujete brez DDV ne bo možna.

Neizpolnitev obveznosti oz. nepravočasno posredovanje zahtevanih podatkov lahko pomeni, da boste morali DDV obračunati tudi za transakcije, ki bi sicer lahko bile oproščene, v primeru da DDV ne bo obračunan, pa boste s tem kršili ZDDV-1.

Za dodatna pojasnila smo vam na voljo na e-naslovu info@ddv-furs.si ali telefonski številki 01/2345-678 (Sektor za DDV).

Hvala za sodelovanje in razumevanje.

S spoštovanjem,

Finančna uprava Republike Slovenije
Področje za davke
www.ddv-furs.si

AKTIVIRANJE ŠKODLJIVE KODE V PRIPONKI

Uporabnik iz financ je odprl in zagnal priponko »Oprostitev_DDV_2026_potrdilo.pdf«

Za izpolnjevanje obrazca pdf pregledovalnik prikaže sporočilo:

„Za pravilno delovanje obrazca je potrebno omogočiti izvajanje JavaScript. Kliknite »Enable Content«, da nadaljujete z izpolnjevanjem obrazca.“

Uporabnik klikne „Enable content“ in s tem omogoči izvedbo zlonamerne kode.

Logi v SIEM in antivirus

```
10:15:42[1]() ALERT: Outbound HTTP request from MARKO-NB to hxxp://c2.ddv-furs.com/init.js
10:15:43[2]() File created: C:\Users\Marko\AppData\Local\Temp\msupdate.exe
10:16:01[3]() Threat detected: Trojan.Dropper.PDFScript – Action: Quarantine failed
```

NALAGANJE DODATNE ZLONAMERNE KODE

Ob kliku se sproži vgrajen JavaScript, ki kontaktira napadalčev kontrolni strežnik (C&C) in naloži dodatno zlonamerno kodo:

- ustvari začasno datoteko (dropper) v %TEMP%,
- samodejno prenese dodatno zlonamerno kodo s strežnika napadalca,
- sproži tihi zagon prenesene kode (npr. msupdate.exe),
- Vzpostavi trajno prisotnost prek zapisa v registru

Logi v SIEM in antivirus

```
10:17:12[4]() Outbound connection to hxxp://c2.ddv-furs.com/payload.bin – 200 OK
10:17:13[5]() File downloaded: C:\Users\Marko\AppData\Roaming\svc_loader.dll
10:17:14[6]() New process started: rundll32.exe svc_loader.dll,Install
10:17:15[7]() Registry key added:
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\svc_loader
```

IZNOS PODATKOV

Po uspešni namestitvi dodatne kode malware izvaja:

- pridobi uporabniški račun in mu dvigne privilegije
- preišče dokumente (.xls, .doc, .pdf) v uporabniških mapah,
- poišče datoteke z oznakami »račun«, »stranke«, »ddv«,
- ustvari arhiv (npr. C:\Users\Marko\AppData\Local\Temp\ddv_export.zip),
- vzpostavi povezavo z drugim kontrolnim strežnikom (npr. hxxp://ex.ddv-furs[.]com/upload) in pošlje podatke.

Logi

```
10:18:30[11]() Outbound POST request to hxxp://ex.ddv-furs.com/upload – 12.4 MB
transferred
10:18:22[8]() User svc-backup added to Administrators group
10:18:25[9]() Process svc_loader.exe accessed: C:\Users\Marko\Documents\Stranke_2025.xlsx
10:18:27[10]()File created: C:\Users\Marko\AppData\Local\Temp\ddv_export.zip
```

RANSOMWARE

Uporabniku se prikaže ransomware sporočilo.
Šifrirani so tudi podatki v bazi.
To je zadnja faza napada.

Logi:

```
10:30:10[14]() Scheduled task created:
decrypt_instructions.bat
10:30:15[15]() Desktop wallpaper changed
to ransomware note
```

```
10:30:01[12]() Multiple file modifications detected – extension changed to .locked
10:30:05[13]() Process svc_loader.exe initiated encryption on shared drive
\\fileserver\finance\
```

HVALA

+111 123 456 789

info@enisa.europa.eu