nt konferenca 2021

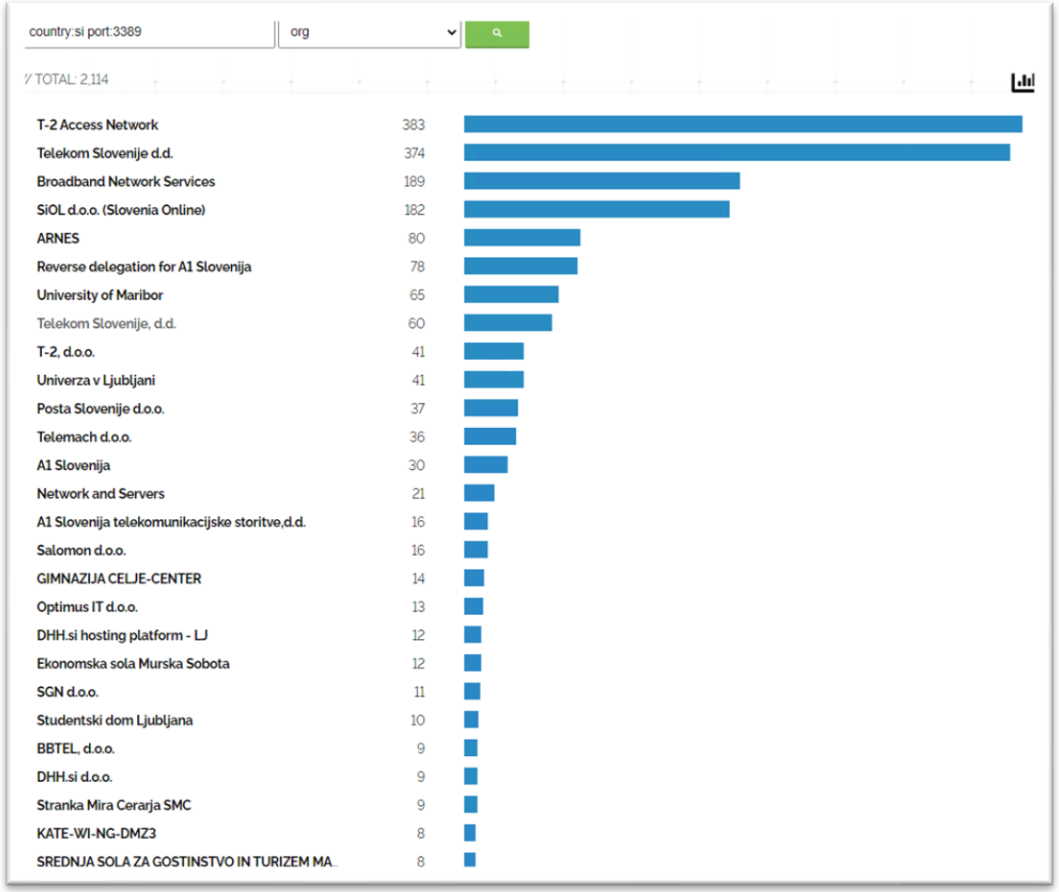
27. – 29. september 2021

Remote Desktop Services in HTML5 dostop

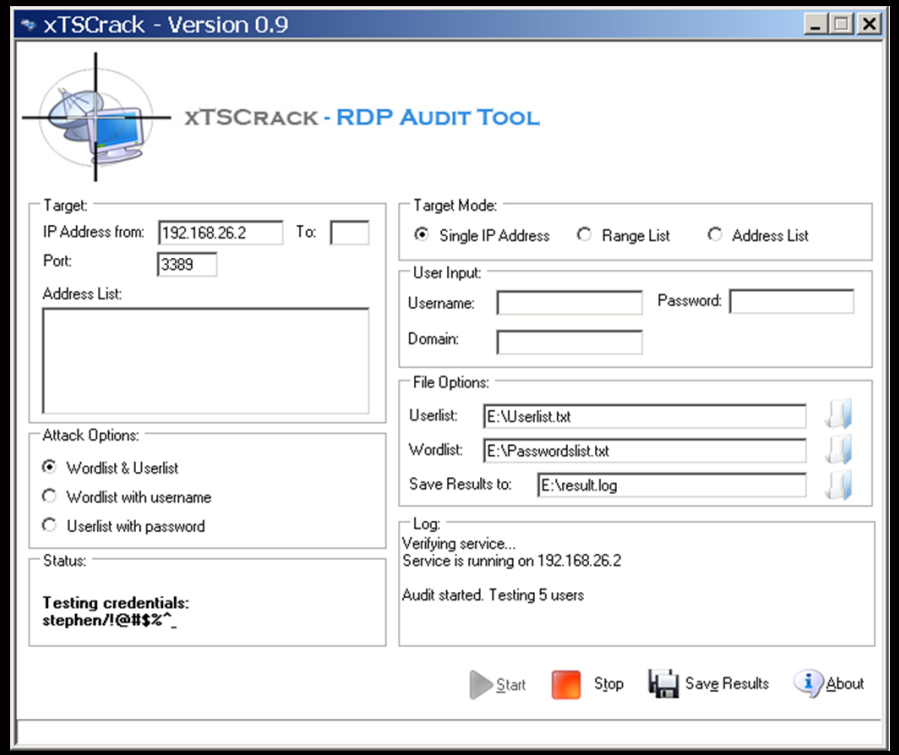
Elvis Guštin
EM-Soft sistemi d.o.o.

Zgodovina

- Nastopil prvič kot Windows RDP V4.0
  - Windows NT 4.0 Terminal Services Eddition
  - Prvič „resno vgrajen“ v Windows Server 2000
  - Od začetka je že precej nevaren in luknjast
  - Trenutno že v verziji 10.0
- Veliko sprememb, tudi v varnosti
  - Network Layer security
  - Printer redirection
  - Video kodeki

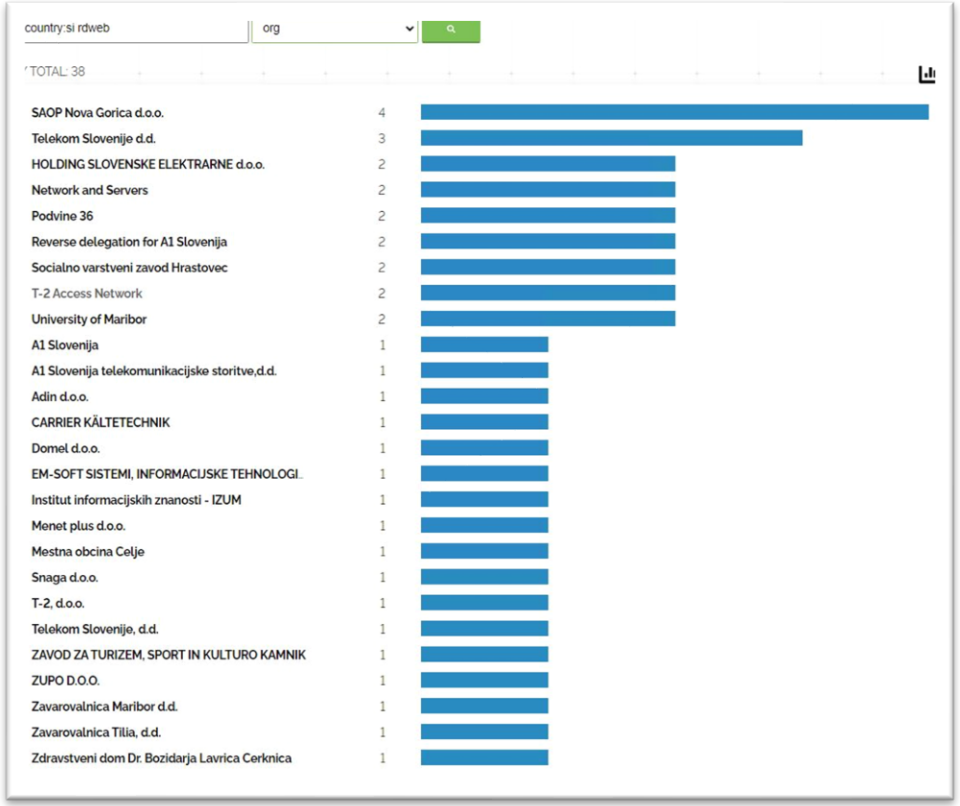


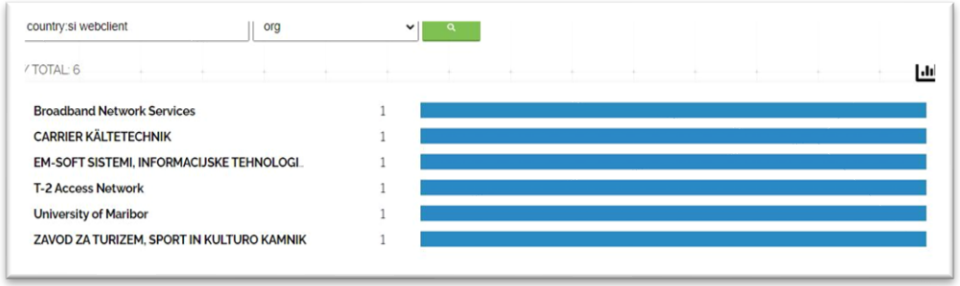
DEMO – Kakšni so admini z odprtim RDP



Zgodovina

- RD Gateway (Server 2008)
  - Tunelira RDP promet v https sejo
  - Ponuja večjo varnost
- RD Web access
  - Dostop in login preko web konzole, varneje
  - Uporablja RD Gateway
  - Dejanski dostopi so tu lahko varljivi (security)
- RD HTML5 web client (2018)
  - Ne uporablja lokalnega RDP klienta
  - Uporablja port 443 (TLS)
  - Ne uporablja RD Gateway storitve





Zahteve in postavitev

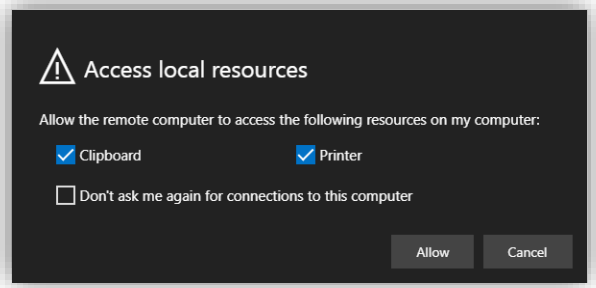
- WEBClient nima veliko dodatnih zahtev in dela
  - Urejena RDP farma na strežniku verzije 2016 ali novejši (RDGW, RDCB in Web Access)
  - Licensing model mora biti per user
  - Javni certifikat za RDS farmo
  - Brskalnik Microsoft Edge, Google Chrome, Safari, Mozilla Firefox ali podobni
- Postavitev
  - Izključno PowerShell, brez možnosti dodatne konfiguracije

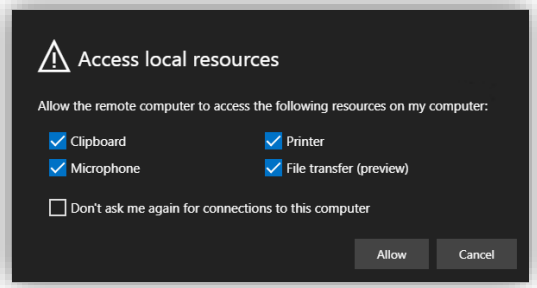
```
Install-PackageProvider -Name NuGet
Install-Module -Name PowerShellGet -Force
Install-Module -Name RDWebClientManagement
Install-RDWebClientPackage
Import-RDWebClientBrokerCert <.cer file path>
Publish-RDWebClientPackage -Type Production -Latest
```

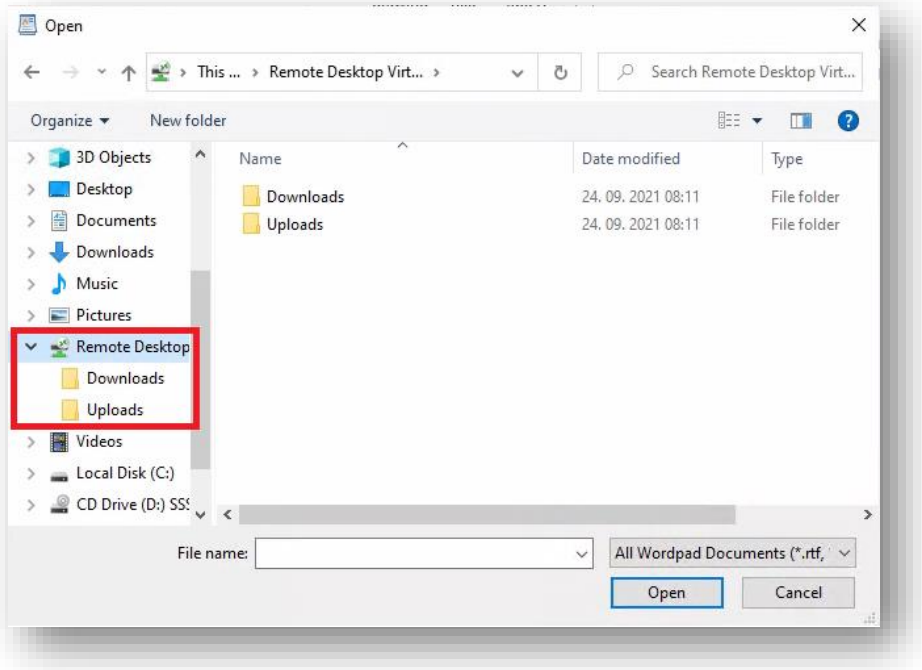
  - Update WEBClienta se izvaja ročno – ne skozi Windows Update servis

Uporabnost

- WEBClient se hitro razvija in dobiva nove funkcionalnosti
  - Potrebno je slediti verzijam
    - https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/web-client-whatsnew
  - Ni izvedljiv za vse zahteve
    - Redirekcija USB naprav (tudi kartic)
    - Redirekcija datotek (dostop do lokalnega računalnika)
    - Določene stvari bodo uporabnikom težke in nelogične
  - Tiskanje
    - Urejeno preko PDF-ja







Uporaba klienta: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-web-client

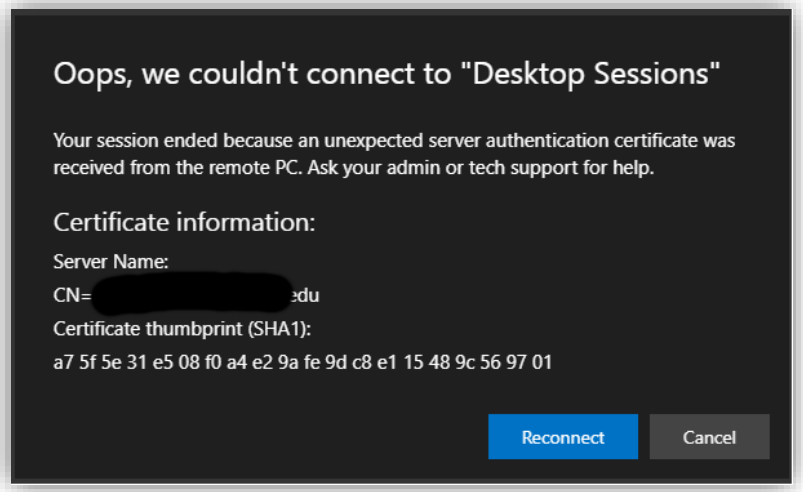
DEMO – Postavitev in uporaba html 5 vmesnika

Varnost

- Glede na to, da ne verjamemo več RDP povezavam…
  - WEBClient ne uporablja RDP protokola v javnem delu povezave (*Wireshark - posnetek*)
    - Enkripcija (https seja – TLS 1.2) se vzpostavi preden karkoli vpisujemo
    - Kar vidimo po internetu je zgolj https promet
    - Iz tega vidika je povezava in delo varno
  - Ne smemo pozabiti login forme
    - Je standardna, brez možnosti dodelave – vsakdo ve kaj se skriva za njo
    - Lahko je občutljiva na bruteforce napade
    - Še vedno je objavljena RDWeb stran
  - Man in the midle napadi
    - Uporaba Proxy strežnikov je lahko kritična (hoteli, bari,…)

Certifikati: Instalacija in obnovitev

- WEBClient je občutljiv na certifikate
  - Certifikat MORA biti javen in veljaven
  - Certifikat mora vsebovati FQDN naslov
  - Pazite pri zamenjavi certifikata (potek)
    - Potrebno je zamenjati certificate v RD Deploymentu (GUI ali PowerShell)
    - Izvozite certifikat v .cer obliko
    - Poženite ponovno PowerShell cmdlet `Import-RDWebClientBrokerCert <.cer file path>`
- Odprava napak
  - Preverite ustreznost certifikata (Thumbprint vsaj RDWA, RDGW in html5)
  - Pobrišite cache v brskalniku
  - Poizkusite še enkrat publish-at klienta (`Publish-RDWebClientPackage`)



V razmislek - razno

- Ostale možnosti povezav (za tiste ki ne zapirate RDP)
  - WEBClient za strežnike in računalnike (Cloudbase)
    - https://cloudbase.it/freerdp-html5-proxy-windows/
    - Brezplačen in deluje (nevarnosti so enake kot pri WEBClientu)
    - Lahko tudi Guacamole (https://guacamole.apache.org/)
- Večfaktorska avtentikacija
  - Še vedno ni 100% rešitev
  - Precej bolje kot geslo
- Preglejte si priporočila
  - https://security.berkeley.edu/education-awareness/securing-remote-desktop-rdp-system-administrators
  - https://rdpwned.adv-gate.com/#

Vprašanja?

Elvis Guštin
elvis@em-soft.si

nt konferenca
2021