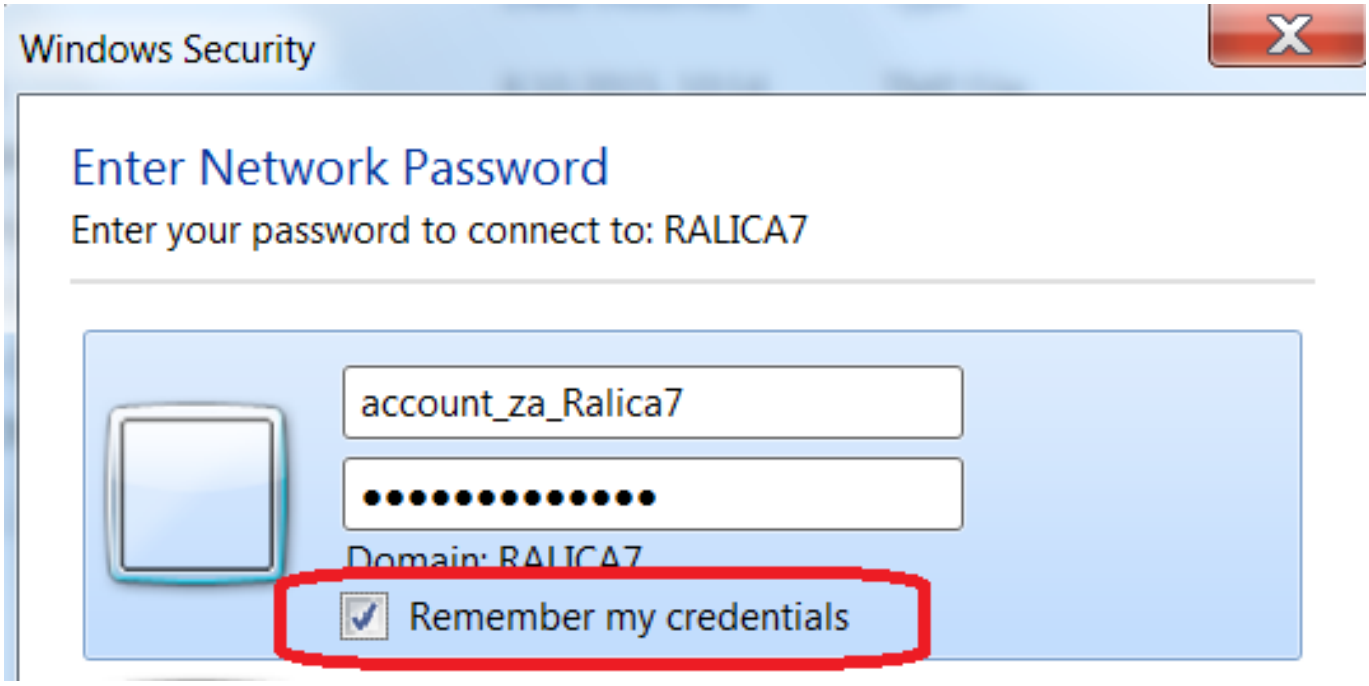
Sjaj i bijeda Windows Credentials Managera

Windows Credentials Manager (dalje: WCM) imaju sve desktop i serverske Windows edicije, od XP/2003 naovamo, uključujući još neslužbeni Win Server 2016. Dostupan je kroz Control Panel, njegov komandnolinijski ekvivalent je ***cmdkey***. WCM je u stvari front end programske logike (lokalnog servisa) koja korisniku windoza omogućuje upravljanje korisničkim računima potrebnim za autentikaciju na mrežne resurse - dijeljene mape i pisači, web proxy, web ili mail servisi, aplikacije za udaljeni pristup računalu... i slično.

Vjerodajnicu koju rabimo za autentikaciju na neki udaljeni resurs WCM upamti tako da ju spremi u takozvani Windows Vault, nakon što korisnik to naredi/odobri u aplikaciji poput Windows Explorer, Internet Explorer, Outlook, Remote Desktop, Skype.... a ponešto spremi i mimo korisnika. Da skratimo priču, niže je ilustrirana tipična situacija: WCM će spremiti vjerodajnicu za pristup dijeljenoj mapi na domaćinu Ralica7, jer smo mu tako naredili opcijom *Remember my credentials.*



Bez ikakve dvojbe, korisna je to stvarca jer u konačnici omogućuje Single Sign-On u nedomenskom prostoru tj. kad trebamo rabiti udaljeni resurs na kojega naš aktivni account nema prava. Budući spadam u IT profiće, dakle, kadar koji intenzivno „šara“ po LAN i WAN resursima, godinama koristim WCM servis. Čovjek prihvati stvari kakve jesu, posebno ako mu, barem nazivno, idu u prilog, i više o tome ne razmišlja... Loša navada, kako ćemo vidjeti!
Prije par dana poželih urediti vjerodajnice nagomilane u WCM-u, ta skupilo ih se kojih četrdesetak (jednom spremljeni akreditiv WCM pamti bez vremenskog ograničenja), ali shvatih da ih ne mogu brisati grupno nego jednu po jednu. Pa skoknuh na Internet po neku skriptu, računam, nisam ja jedini gotovan na ovom svijetu, netko je već nešto smislio.... Skriptu sam našao, no naletjeh i na nešto puno važnije – ranjivost WCM-a kao servisa. Ta ranjivost pogađa svakog korisnika windoza, a najviše onog s admin pravima!

Idemo redom. Za brisanje svih vjerodajnica iz Vaulta iskoristite nižu skriptu, hvala nepoznatom

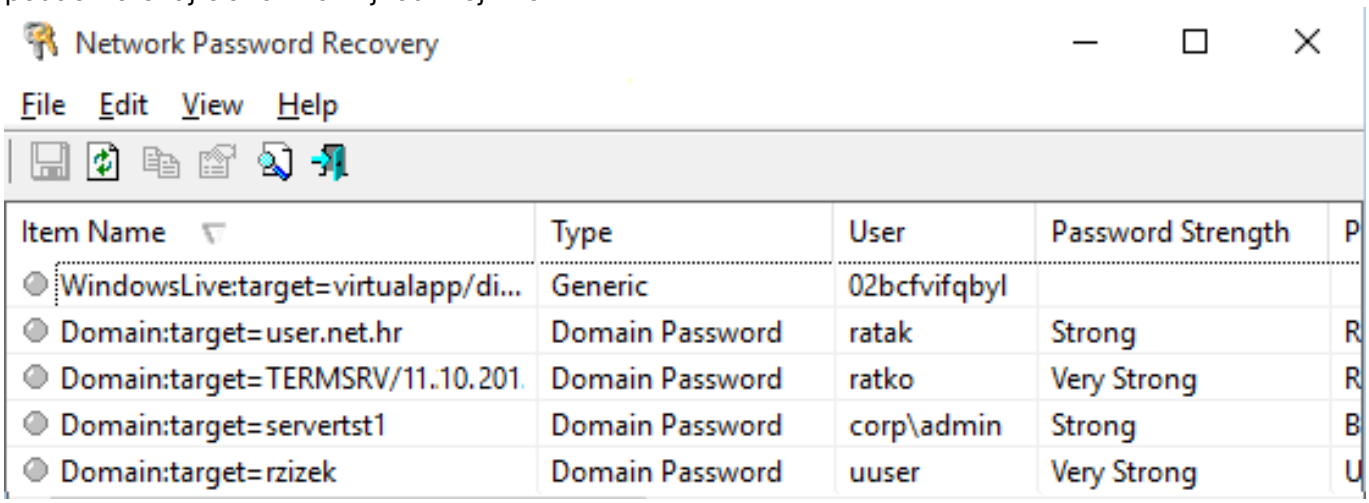
Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

autoru.

```
cmdkey.exe /list > "%TEMP%\List.txt"
findstr.exe Target "%TEMP%\List.txt" > "%TEMP%\tokensonly.txt"
FOR /F "tokens=1,2 delims= " %%G IN (%TEMP%\tokensonly.txt) DO cmdkey.exe /delete:%%H
del "%TEMP%\List.txt" /s /f /q
del "%TEMP%\tokensonly.txt" /s /f /q
```

Za selektivno brisanje prilagodite gornju skriptu ili iskoristite Nirsoftov Network Password Recovery jer je ovaj, od Microsofta anatemiziran programčić (vidi niže zašto), opremljen i funkcijom brisanja više vjerodajnica odjednom.

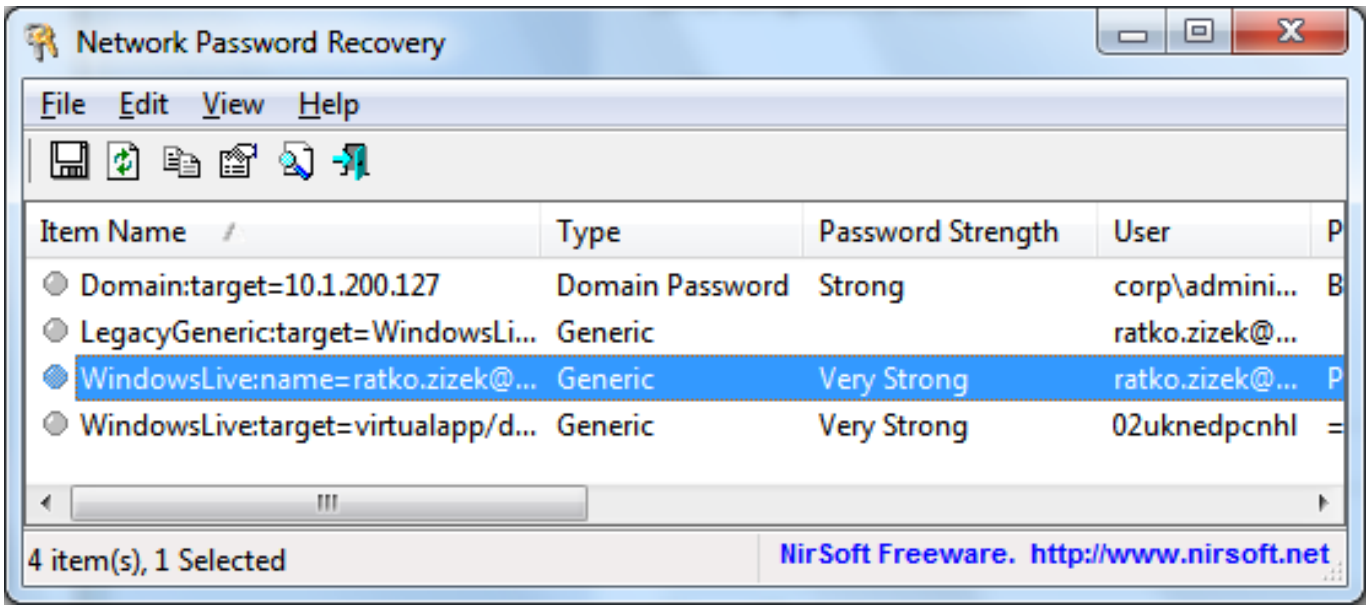
Ahilova peta WCM servisa je iznenađujuće slaba zaštita lozinki ukeširanih vjerodajnica pa ih alati poput Network Password Recovery (dalje: NPR) ekspresno deenkriptiraju. Za razbijanje mojih lozinki, a većina ih je ekstradugačkih i kompleksnih, NPR utroši 4 – 5 sekundi! Niža slika prikazuje gornji dio popisa razotkrivenih vjerodajnica; razumljivo, prekrio sam polje Password (na slici P), no vidimo da su neke lozinke jačine Very Strong, također, da su uspješno iščitane razne vrste vjerodajnica, a ti su podaci za ovaj članak važniji od mojih lozinki.



NPR spada u lako dobavljive alate, besplatan je, portabilan je (jedan .exe veličine 50-ak kilobajta) i, srećom za sve potencijalne žrtve, ima neka ograničenja. Najvažnije ograničenje je to da radi samo u sigurnosnom kontekstu administratora konkretnog računala. Ali oprez - to ne znači da drugi alati, posebno oni kojima se služe cyber kriminalci, imaju takva ograničenja! Jer nije problem u NPR-u nego u WCM servisu.

Uočite kako neka zlonamjerna osoba, opremljena samo NPR-om, može ozbiljno nauditi nama sistemcima (i sličnima s admin ovlastima). Alat je, kako rekosmo, monolitan i portabilan, k tomu, može se pokretati i skriptom uz parametar za spremanje svih nalaza u log datoteku. Znači, dovoljno je da admin računala ostavi svoj stroj nezaključan svega 5 - 10 minuta pa da mu neki-lik-u-prolazu sa NPR-om na USB sticku ukrade sve ukeširane accounte. Nadalje, ako taj lik raspolaže naprednijim alatom i vještinama hakiranja... uz ovako slabo štićene akreditive „samo nebo je granica“!
Istina je, Microsoft pomalo unaprijeđuje WCM i kao aplikaciju i kao servis, ali sve je to nedostatno jer NPR radi podjednako uspješno na tek iskovanoj Desetki kao i na sada već ocvaloj Sedmici. Kažem „podjednako“ zato jer na Desetki alat ipak nije uspio iščitati moj Live ID za Microsoft cloud usluge, a na Sedmici jest. Što ne znači, podsjećam, da će i neki drugi alat te namjene zatajiti na Desetki.

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr



Tehnološki aspekt cijele priče – koji su (a)simetrični enkripcijski algoritmi u igri, rabi li se uistinu enkripcija ili samo hashiranje, što je od svega toga (i)reverzibilno (i bla-bla) – potpuno je nebitan u odnosu na realno stanje, a ono nije dobro. Žargonom security officera sumirano: Potencijalni vektor napada identificiran je na svakoj novijoj Windows serverskoj i desktop instalaciji; trenutna razina kritičnosti je High za Windows instalacije dohvatljive s Interneta, za vlasnike prijenosnika i IT administratore. Srećom, ti „sigurnjaci“ stalno nešto dramatiziraju... :o)

Svakako, na Microsoftu je da ovo konačno riješi, ta previše je windoza rasijano po svijetu, a i kupci MS-ovih OS-ova ne zaslužuju takav ignorantski odnos. Ili neka se u WCM UI postavi neka obavijest na temu slabe zaštite lozinki. Na nama je, pak, da se u međuvremenu osiguramo kako najbolje znamo. Zato par savjeta tipa „obrana i zaštita u kontekstu WCM-a“:

a) U mjere zaštite Windows računala uvrstite i ovu glede WCM servisa.

b) Provjerite i pročistite ukeširane vjerodajnice na svim važnijim desktop i serverskim Windows instalacijama. Na kritično važnim instalacijama deaktivirajte servis Credential Manager (Admin Tools > Services).

c) Testovima sam potvrdio slutnju da WCM ne pamti vjerodajnice za pristup dijeljenim mapama ako se rabi legacy naredba net use. Zgodno je znati jer na LAN-u jako često moramo mapirati disk na dijeljeni direktorij (share).

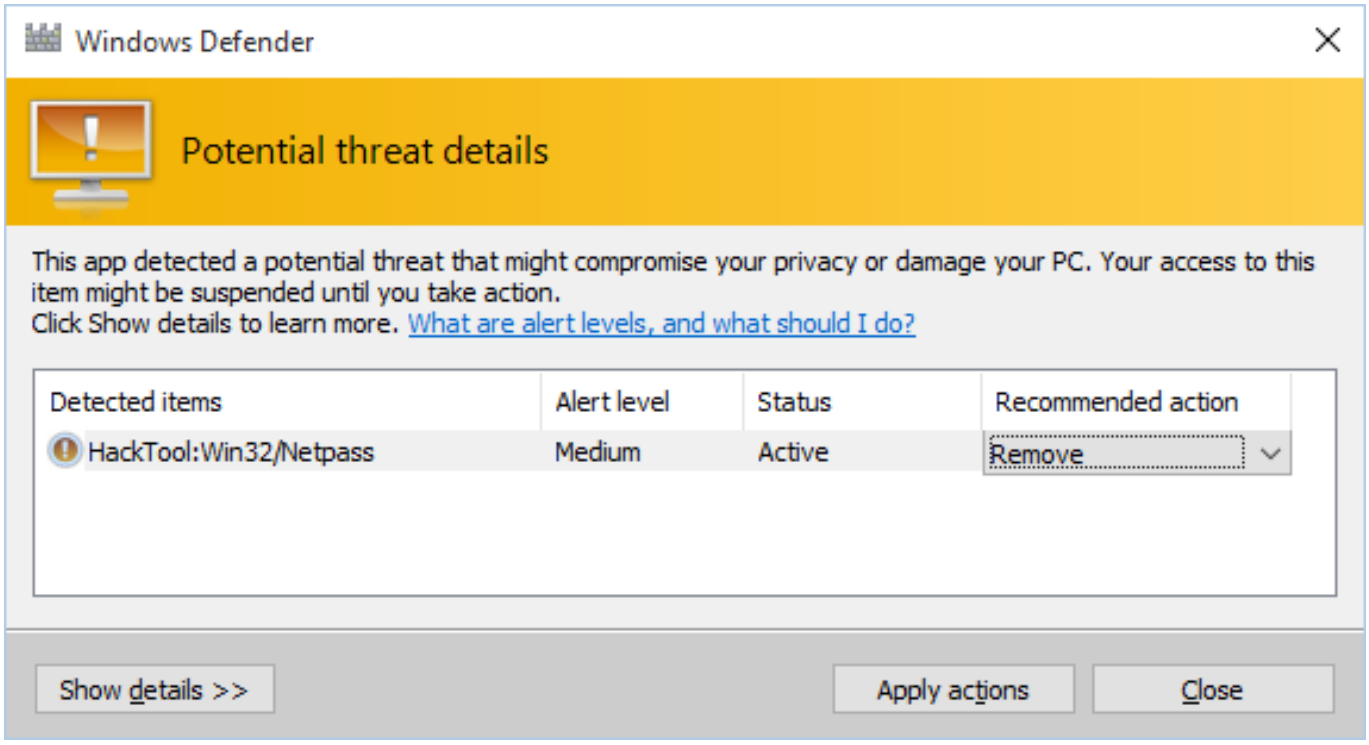
d) Ako baš morate rabiti WCM, povremeno prekontrolirajte stanje. Ja sam si, recimo, na svom prijenosniku složio task koji jednom mjesečno poziva cmdkey /list.

e) IT persone sa većim ovlastima na računala pod Windows OS-ovima trebaju paziti kad riješavaju neki problem na tuđoj Windows instalaciji kako im WCM ne bi ukeširao njihov admin account. U mom WCM-u našao sam, i NPR-om učas iščitao account administratora foresta!

f) Ako to ikome može pomoći, znajte da se vjerodajnice spremaju u %systemdrive%\Users\UserName\AppData\Roaming\Microsoft\Credentials.

Jooj, pokušao sam, al’ ne mogu ovo prešutjeti! Pogledajte kako Korporacija rješava problem dugogodišnje ranjivosti WCM-a: instruirali su svoj Defender da prijavi NPR kao maliciozni program. Poruka je jasna - problem je ono što ukazuje na problem! Defender ne sprečava NPR u djelovanju, samo ponekad javi da je na disku. Istovremeno, TrendMicro, antivirusno rješenje enterprise razine, uopće ne reagira na NPR, bio ovaj pasivan (na disku) ili aktivan u RAM-u.

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr



čet, 2015-10-22 13:26 - Ratko Žižek**Vote:** 4

Vaša ocjena: Nema Average: 4 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1574

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr