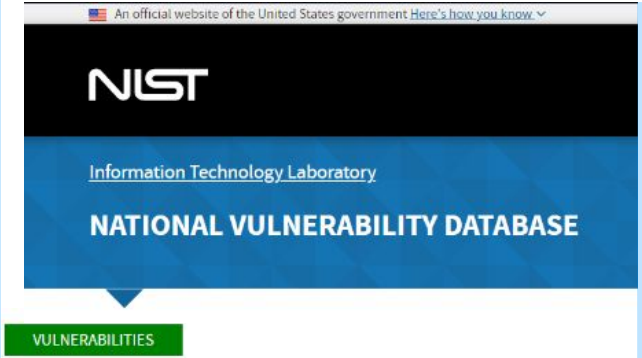
Giorno 4:

GINA (Graphic authentication & authentication) è un componente lecito di Windows che permette l'autenticazione degli utenti tramite interfaccia grafica - ovvero permette agli utenti di inserire **username** e **password** nel classico riquadro Windows, come quello in figura a destra che usate anche voi per accedere alla macchina virtuale.

EPICODE

Anatoliy Prysyazhnyuk
Antonio De Cesare
Alessandro Bossi
Rossella Amore
Claudio La Torre
Riccardo Lupieri
Riccardo Di Pasquale
Pietro Laera
Davide Bassolino



GINA è una libreria **dll** (**Dynamic Link Library**) fornisce il supporto per l'interfaccia grafica dell'accesso e implementa le politiche di autenticazione per l'accesso al sistema. **Viene richiamata da Winlogon** che gestisce le attività legate all'accesso interattivo,mentre **GINA** si occupa delle interazioni dell'utente durante il processo di autenticazione.

CVE-2018-5353 Detail

Description

The custom GINA/CP module in Zoho ManageEngine ADSelfService Plus before 5.5 build 5517 allows remote attackers to execute code and escalate privileges via spoofing. It does not authenticate the intended server before opening a browser window. An unauthenticated attacker capable of conducting a spoofing attack can redirect the browser to gain execution in the context of the WinLogon.exe process. If Network Level Authentication is not enforced, the vulnerability can be exploited via RDP. Additionally, if the web server has a misconfigured certificate then no spoofing attack is required

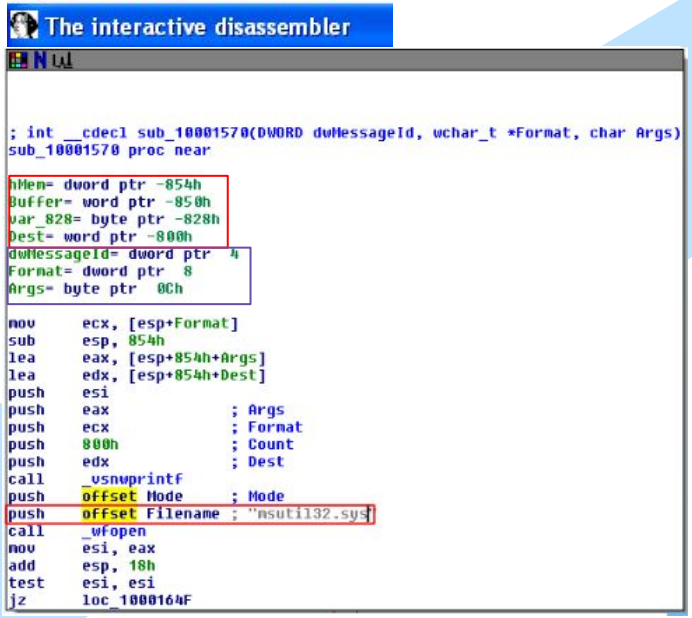
Cosa può succedere se il file .dll lecito viene sostituito con un file .dll malevolo, che intercetta i dati inseriti?

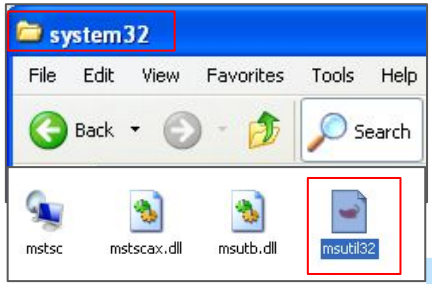
La **sostituzione di un file DLL lecito con uno malevolo** può causare gravi problemi, come il **furto di dati sensibili, keylogging, corruzione dei dati, esecuzione di codice dannoso e diffusione di malware**. Il **sistema** potrebbe subire danni, essere instabile e gli strumenti di sicurezza potrebbero avere difficoltà a rilevare la minaccia. È essenziale utilizzare software di sicurezza aggiornato e fare attenzione alle fonti dei file DLL per prevenire tali attacchi.

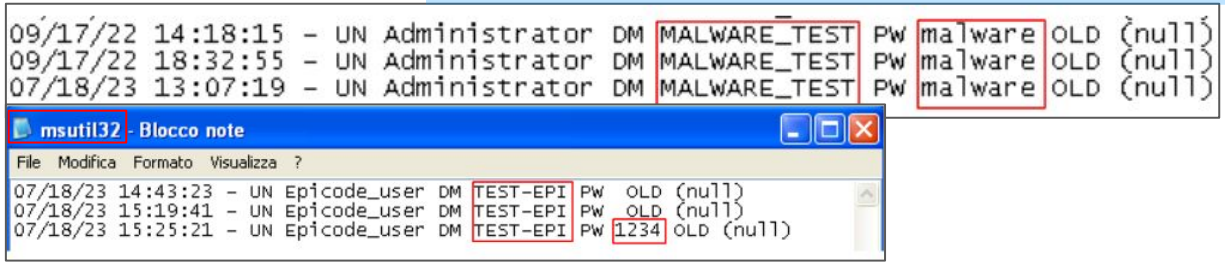
Cosa può succedere se il file .dll lecito viene sostituito con un file .dll malevolo, che intercetta i dati inseriti?

Una volta riavviato il sistema e apparsa la **schermata di login**, quando andiamo a inserire la **password**, essa verrà automaticamente salvata su un file log in system32 chiamato "**msutil32**".

Per verificare che questo sia effettivamente un log, abbiamo cambiato la password dell'utente amministratore **dal pannello di controllo** per poi rileggere il file log. Anche la nuova password è stata salvata con successo.







Sulla base della risposta sopra, delineate il profilo del Malware e delle sue funzionalità.
Unite tutti i punti per creare un grafico che ne rappresenti lo scopo ad alto livello.