MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Najbežnejšie metódy útočníkov

V dnešnej digitálnej dobe sú osobné údaje ohrozené viac ako kedykoľvek predtým. Kreativita útočníkov na získanie Vašich osobných údajov nemá hranice. Útočníci môžu použiť rôzne metódy na zbieranie osobných údajov svojich obetí, vrátane sociálneho inžinierstva, phishingových útokov alebo prehľadávanie voľných zdrojov, ako napríklad fotografií na sociálnych sieťach...

Najbežnejšie metódy útočníkov:

Sociálne inžinierstvo: Zahŕňa manipuláciu obetí za účelom prezradenia ich citlivých informácií. Útočníci vykonávajú online prieskum aktivít svojich obetí a používajú informácie, ktoré nájdu, na získanie ich dôvery a na ich presvedčenie.

Reverzné sociálne inžinierstvo: Útočník vytvorí situáciu, pri ktorej obeť sama príde za útočníkom. Ide o sofistikovanú metódu psychickej manipulácie, pri ktorej útočník za použitia štandardných metód sociálneho inžinierstva uvedie obeť do omylu a presvedčí ju, že on je osoba z dôveryhodnej organizácie a iba on vie obeti pomôcť s jej problémom, ktorý rovnako vytvoril on. Viac informácií nájdete tu.

Taktika: Baiting, Pretexting, DNS spoofing, Scareware, Position of authority, Sense of urgency

Prevedenie: Mail, Smishing, Vishing, podvodná webstránka/aplikácia

Extrakcia metadát z fotografií:

Útočník dokáže získať rozličné dáta z fotografií, napr. EXIF, dátum a čas, GPS, popis fotky alebo autorské práva. Z fotografií vie útočník získať citlivé informácie o osobe, hlavne ak informujú o dennej rutine človeka, špeciálnych príležitostiach, alebo plánoch a úspechoch.

Web scraping:

Je proces získavania dát z webových stránok pomocou automatizovaných nástrojov alebo softvéru. Web scraping zo sociálnych sietí umožňuje útočníkom získať rôzne druhy údajov o používateľoch. Napríklad kontaktné informácie, súkromné správy, príspevky a komentáre, sledovanie používateľov alebo profilové informácie.

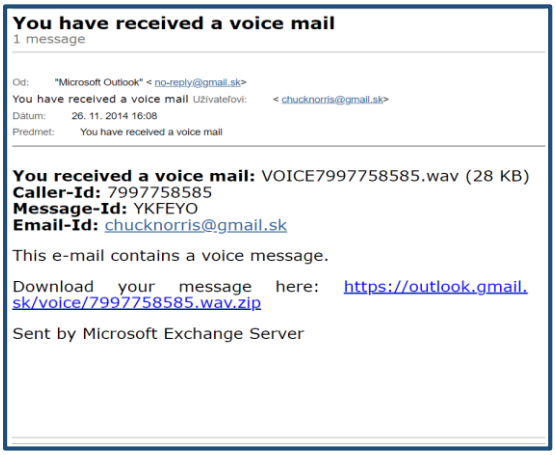
Obsah na sociálnych sieťach:

Útočník môže získať informácie o identite a polohe používateľa na základe jeho profilu na sociálnych sieťach. Používatelia často zdieľajú citlivé informácie, ako sú napríklad dátum narodenia, miesto narodenia, rodinný stav, zamestnanie a vzdelanie. Tieto informácie môžu byť použité na vytvorenie falošného profilu alebo na sledovanie používateľa.

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Najbežnejšie metódy útočníkov

Na obrázku nižšie môžeme vidieť príklad phishingového útoku, ktorý navádza obeť na stiahnutie hlasovej správy z aplikácie Outlook. V prvom rade si všimnime emailovú adresu, z ktorej nám prišiel email. Táto doména nepatrí spoločnosti Microsoft, čo si vieme overiť na ich oficiálnej stránke alebo pomocou webovej platformy who.is alebo centralops. Po presunutí kurzora na tento odkaz sa nám v ľavom spodnom rohu ukázala webová stránka, kam by sme boli presunutí po kliknutí na odkaz. Nikdy na takýto odkaz ***NEKLIKAJTE!*** Za druhé si treba skontrolovať, či vôbec aplikácia Outlook dovoľuje odosielanie hlasových správ, pričom po krátkom prieskume zistíme, že táto možnosť neexistuje. Dbajte na obsah emailu a informácie, ktoré sú v ňom zahnuté. V prípade úspešného presvedčenia obete by sa útočníkovi mohlo podariť získať od nej prihlasovacie údaje, finančné či osobné informácie alebo citlivé informácie, ktoré dokáže zneužiť.



You have received a voice mail
1 message

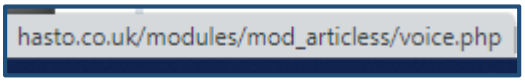
Od: "Microsoft Outlook" < no-reply@gmail.sk>
You have received a voice mail Užívateľovi: < chucknorris@gmail.sk>
Dátum: 26. 11. 2014 16:08
Predmet: You have received a voice mail

You received a voice mail: VOICE7997758585.wav (28 KB)
Caller-Id: 7997758585
Message-Id: YKFEYO
Email-Id: chucknorris@gmail.sk

This e-mail contains a voice message.

Download your message here: https://outlook.gmail.sk/voice/7997758585.wav.zip

Sent by Microsoft Exchange Server



Buďte opatrní voči žiadostiam o priateľstvo a správam od neznámych jednotlivcov. Používateľ sociálnych sietí by mal obmedziť množstvo zdieľaných osobných informácií. Okrem toho odporúčame skontrolovať nastavenie súkromia a upraviť ich tak, aby sa obmedzila viditeľnosť osobných údajov pre verejnosť. Je dôležité byť si týchto rizík vedomý a prijať kroky na svoju ochranu. Týmito opatreniami môžete chrániť samých seba a svojich najbližších pred útočníkmi, ktorí sa snažia zneužiť Vaše osobné údaje na útok proti Vám. **INTERNET NEZABÚDA !!!**

Pripravili sme si pre Vás krátky phishingový test, kde si môžete na praktických príkladoch overiť svoje znalosti.
Phishingový test: https://www.csirt.gov.sk/archiv/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html?csrt=6113910499060114075