Riasztás a Lazarus „Operation Dream Job” kampányról és a CVE-2026-68820 Windows sérülékenységről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet **riasztást ad ki a Windows kernelt érintő, észak-koreai kötődésű Lazarus csoport által végrehajtott célzott kampánnyal kapcsolatban,** amelyben trójai PDF nézők, fejlett in-memory moduláris kártevők és több zero-day/exploittal támogatott támadási lánc kerül alkalmazásra.

A kampány részeként a támadók a Microsoft Windows AFD.sys illesztőprogram egy **korábban nem publikált** (0-day) use-after-free típusú helyi jogosultságkiterjesztési sérülékenységét (CVE-2026-68820) kihasználva kernel szintű rootkitet (FudModule) telepítenek, és **hosszú távú hozzáférést létesítenek** a kompromittált rendszereken.

A támadók **célzott spear-phishing kampányt folytatnak** „álommunka” ajánlatokra építve (Operation Dream Job), trojanizált PDF nézőt és rosszindulatú PDF dokumentumokat terjesztve, amelyek letöltő (MISTPEN) és backdoor (ForestTiger, Troy) komponenseket töltenek le Microsoft Graph / OneDrive infrastruktúra felhasználásával.

A CVE-2026-68820 egy use-after-free típusú helyi jogosultságkiterjesztési sérülékenység, amelynek sikeres kihasználása esetén **a támadó SYSTEM szintű hozzáférést szerezhet**, kiiktathatja a végpontvédelmi megoldások nagy részét, és tartós, nehezen észlelhető jelenlétet biztosító backdoorokat telepíthet.

A kompromittált Roundcube/WordPress/PrestaShop szerverek RelayShell webshellen keresztül C2 relay szerepet kapnak, így legitim webforgalomba ágyazott, **nehezen szűrhető C2 kommunikáció valósul meg**.

A kampány kiemelten érinti a védelmi szektort, különösen a katonai technológiákkal foglalkozó cégeket (drónok, szenzorok, robotika), de más iparágakban is megjelenhet, ahol a „job offer” narratíva alkalmazható.

+36-1-336-4833 csirt@nki.gov.hu

Érintett rendszerek:

Minden Microsoft Windows rendszer érintett, amelyekben **az AFD.sys** (Ancillary Function Driver for WinSock) **sérülékeny verziója található**, és még nem kapta meg a CVE-2026-68820 javítását (2026. augusztusi Patch Tuesday).

Érintettek az olyan környezetek is, ahol a felhasználók nem ellenőrzött weboldalakról PDF nézegetőket töltenek le. Különösen azok a **PDF nézők veszélyesek, amelyek a MuPDF keretrendszeren alapulnak**.

Azon Roundcube alapú webmail-szerverek is érintettek, amelyek **a** CVE-2025-49113 **sérülékeny verzióját futtatják**, illetve azok a kompromittált WordPress/PrestaShop webes infrastruktúrák, **amelyeken RelayShell webshell található**.

Az eddig ismert indikátorok az alábbiak:

NÉV	ÉRTÉK
DLL Loader\Dropper	2b4987c07a3d9a9a5d1a9bf4efa3d1903e775090b611710edafdc92874265ca8 3a02d0d798e8d35555776886d92b20ff38a101c9ef7e0eebc8ce5d259516525a 92106b0c62a0a42678232f8273f030b2d3c8e92efce81b98b9eec70cfe98afa1 396192d92d17ace1a521f1351eeeba2825e60badd0d799cc5c338e4934b3c82c f7e620134ca935067797ab957317b346ce0df84a4e9b9ca54a6acc9b75afda4d 75b93a7103b0562f6497d30052c0c5cf7aa58c1bf0e9297022b74469a7f096f1 a45144d22cac70a45d71cf4dffa4efbc373658779a56cf1300d6ac863d6cc7e2 1de949c71efcfb0ffc41f33d38833dbc4b082075b1a540fc68c18c535d7ad86c 4c9b804d6155b29f1e27a9ffe531e10bc42a7bdab42f905b50146bf2026768d9 29e24c007549e51319ff3aee011da6f9f93568e8c85a5ad69c9e53bd3f4533a2 4ebdce2f47c23ff8c9e8e80c8b5239c7a5764da31cd3ab8f0505926890adc105 c2aa28bb5e2a749c693712008276f311edd912f689371ef9e8a1ee5fb4167461
MISTPEN	2db25ac41a66aa523c79e23e00443573530dd7bd82b8371bcc87bd7232e141eb 5278ee922838352f1480a73e971161017d643a80b7ec22bf725897dfd088696d b4082d21070d9ddf53fde4ea22524d09e41ec9826ce63cef3c6235e458d21afb fb3fc5626f68677fb1269a2fefbe70e719211b4065e836ab92e06a8210139a2d ea7056f2bf36c66a61ff787ff5be975a85f534c3c5ca178791dac2504db2c619

NÉV	ÉRTÉK
	13d10bc99f7f7abe7ee0902be87920b73b2ea41bd9683dbfcad340dacbcdef79 4fd32432341dfcf54d0517a6bbc38e5d265be70933493e4183c2a340cdde9a2d 4dd792c9f672bbdcc8d363d745994efe90f4ffc5fdc2c059c8e379a48ad6a68a ba96c603e44046de703c67b2c3b7e4ca974afef7b437a0244418bc4edc781bb7
ForestTiger	72dccae85e062f541fecad9ec7a18a3123e7ae5ac5d53c91709b53a46dbbd289 231b1ef8b95bf77887d5377e2a60f649035e78f543af1b82877db36a5759d858 6da9b1e6f3315ceb77dd14a937a26cc3602bf6a7e2c2ecafb3c65ce5319837be a0578a2b7821d7e2c573530648f26d7a0d98b373ab24fb7f0c792736761e542d 82268052f94df6f4870d02e57b18d4c54136cc7a8c8d80ad162631f99462c943
FudModule	3b6378df8442e63a6ed7317075913e4720847a510d95022d4a8347b2637c245d
PDF Payload	a673ae661593c0de9bbb815593b816a6853dad6d55ad5042d2ef1875cd13d6e7 8ce6c29f92dc45b1474417cbdff4ed0c18e58fa63e3a071ee9f85aa9d2aac07c acb97cec84e08b89f41967a24e965d1fd2c51751cef158f7aa35bb4306b87b97 3601060c62edeeaa49def6a13be6e126e1024ce011faad4e2d9f585ccf6bd5a6 fecf12088843801215898442bd1ff3e266f29d14e29a94780e857f69c4915d6b d578c28c9afe7457a0d81f6701332ef8197e8f7468de654935fb29a50ea66459
SecurityPDF.exe	743172aab606974b054a64561534ae66baa3a840657f79d7c6fa18350e8d45d1 db3d69b7eeda2e35e23006bf4b7e206281fce809584207214fc213f9bc30376d
Troy Backdoor	590fb6ae19480d694e08ee85859cad8066f2f87e7e5abba2960c6d115e1615d6 68d4fba7b1300a59cd6212c08910a260cd71b40cd9f51cac933030a68faac0bb a738059ce07c951c31ab2da3d93d8f69bff32f9b7d933dbf5943441b9cc99075
RelayShell	21c3ad4838c4324bc5f081021da5fb2e9073d0c9304087811c21eb47c9e22762 cc4e06aa378a190f71384c03023bb3d18a6d66e297d46701220e132963d2e222
SecurityPDF Website & Troy C2	envell[.]xyz enveil[.]online uxtramine[.]org 135.181.67[.]203 135.181.185[.]158

Javasolt intézkedések:

Telepítsék a Microsoft 2026. augusztusi biztonsági frissítéseit minden támogatott Windows rendszeren, különös tekintettel az AFD.sys-t érintő CVE-2026-68820 javítására.

Vizsgálják felül a HR/Recruitment folyamatokat, és fokozottan ellenőrizzék a „job offer" típusú megkeresésekhez kapcsolódó mellékleteket, különösen a PDF néző telepítőket és ZIP archívumokat.

Végezzék el a Roundcube, WordPress, PrestaShop alapú nyilvános felületek verzió- és sérülékenység ellenőrzését; a CVE-2025-49113 sérülékeny Roundcube verziókat mielőbb frissítsék vagy tegyék védetté.

Alkalmazzanak hálózati és végponti detekciós szabályokataz IoC-k alapján, és vizsgálják az esetleges múltbeli aktivitásokat logokban, proxy, EDR, mail-gateway szinten.

A legfrissebb információkért kérjük ügyfeleinket, hogy folyamatosan kövessék a Nemzeti Kiberbiztonsági Intézet weboldalát.

+36-1-336-4833 csirt@nki.gov.hu