NO MORE RANSOM!

Potrebujete pomôcť s odomknutím Vášho digitálneho života?

No More Ransom

Potrebujete pomôcť s odomknutím Vášho digitálneho života?

No More Ransom (NMR) je ukážkou dôležitosti verejno-súkromného partnerstva pri rozkladaní kriminálnych aktivít v súvislosti s ransomware. Obete by už viac nemali byť nútené platiť výkupné, alebo stratiť svoje súbory. Vďaka bezplatnému obnoveniu prístupu k ich infikovaným súborom majú používatelia tretiu možnosť, ktorú predtým nemali.

Čo je ransomware?

Ransomware je typ malwaru, ktorý používateľom zabraňuje alebo ich limituje pri pristupovaní k svojim systémom alebo zariadeniam. Žiada ich o zaplatenie výkupného prostredníctvom špecifických online platobných metód do určitého termínu, aby získali svoje dáta späť.

K infekcii môže prísť rôznymi spôsobmi, napr.:

- návštevou kompromitovaných webových stránok;
- stiahnutím falošných aplikačných aktualizácií alebo kompromitovaním softwaru;
- kliknutím na škodlivé linky a prílohy vložené do phishingových e-mailov;
- pripojením infikovaných externých zariadení (napr. USB) do počítačového systému.

Čo je No More Ransom?

No More Ransom je verejno-súkromné partnerstvo medzi orgánmi presadzovania práva a poprednými IT spoločnosťami, ktoré vzniklo v júli 2016.

Prostredníctvom www.nomoreransom.org sa projekt zameriava na tieto ciele:

- pomáhať obetiam s obnovou ich zašifrovaných súborov;
- zvyšovať povedomie o hrozbe ransomware u verejnosti;
- poskytovať priame prepojenia na orgány národných polícií členských štátov EÚ a ďalej nabádať občanov nahlasovať útoky.

Ako to funguje?

1. Obeť nahrá dva zašifrované súbory a vydieračskú správu do No More Ransom Kryptošerifa.
2. Kryptošerif porovná informácie so zoznamom dostupných dešifrovacích nástrojov.
3. V prípade pozitívnej zhody je poskytnutý odkaz na dešifrovací nástroj. Obeť by mala postupovať podľa inštrukcií na odomknutie svojich súborov.
4. Ak aktuálne nástroj nie je k dispozícii, obeti je odporučené, aby vykonala opätovnú kontrolu v budúcnosti, keďže nové nástroje sú pridávané na pravidelnej báze.

Kto sa môže do projektu zapojiť?

Oficiálne entity z akéhokoľvek sektoru, ktoré prispejú jedinečnými schopnosťami alebo zručnosťami (uplatňuje sa schvaľovací postup).

Existujú dve úrovne partnerstva:

- **Pridružený partner:** poskytuje jedinečné dešifrovacie nástroje alebo dešifrovacie kľúče, ktoré zatiaľ nie sú v projektovom portáli dostupné;
- **Podporujúci partner:** propaguje projekt No More Ransom vo svojej geografickej oblasti alebo oblasti pôsobenia, prispieva materiálom na preventívne kampane a prekladá obsah portálu do rôznych jazykov. Vyžaduje sa len vyhlásenie o zhode.

V prípade záujmu kontaktujte
nomoreransom@europol.europa.eu

Rady pre obete

Ako môžete predísť infekcii ransomwarom?

- Pravidelne zálohujte dáta uložené na Vašom počítači. Udržujte najmenej jednu kópiu na médiu, ktoré nebude pripojené k počítaču.
- Neklikajte na odkazy v nevyžiadaných alebo podozrivých e-mailoch.
- Vyhľadávajte a sťahujte len oficiálne verzie softwaru a vždy z dôveryhodných stránok.
- Na ochranu Vašich systémov pred hrozbami (vrátane ransomware) používajte odolné bezpečnostné produkty.
- Uistite sa, že Váš bezpečnostný software a operačný systém sú aktualizované.
- Na internete buďte ostražití a neklikajte na podozrivé odkazy, pop-up okná alebo dialógové boxy.
- Nepoužívajte vysoko privilegované kontá (kontá s administrátorskými oprávneniami) pre každodennú činnosť.

Boli ste infikovaní? Čo robiť ďalej...

- Vždy navštívte www.nomoreransom.org, aby ste zistili, či ste boli infikovaní variantami ransomwarov, pre ktoré sú tu zadarmo dostupné dešifovacie nástroje .
- Neplaťte výkupné. Budete financovať kriminálnikov a povzbudzovať ich v tom, aby pokračovali v ich nelegálnych aktivitách.
- Nahláste to Vašej národnej polícii. Čím viac informácií poskytnete, tým viac môžu byť orgány presadzovania práva efektívnejšie pri rozkladaní kriminálnych aktivít.
- Odpojte Vaše zariadenie od internetu alebo iného sieťového pripojenia (napr. domáca WiFi sieť) ihneď ako je to možné, aby ste zamedzili šíreniu infekcie.
- Preformátujte pevný disk infikovaného zariadenia, nainštalujte operačný systém, aplikácie, aktualizácie a obnovte uzamknuté súbory z Vášho záložného média (ak nejaké máte).

V spolupráci s

EUROPOL | EC3 European Cybercrime Centre

europol.europa.eu
nomoreransom.org