

«Я не робот»: CERT-UA фіксує масове поширення шкідливого програмного забезпечення

Datum 6.10.2026
Subjekt Урядовий портал
Region Ukrajina
Kategorie IT a komunikace, Technologie, Bezpečnost

Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA, що діє при Держспецзв'язку, виявила нову масштабну кампанію з розповсюдження шкідливого програмного забезпечення. Зловмисники (ідентифікатор кластера UAC-0277) використовують техніку ClickFix, розміщуючи підроблені сторінки перевірки безпеки на легітимних, але скомпрометованих вебсайтах.

Лише у вересні 2026 року фахівці CERT-UA зафіксували понад 100 зламаних вебресурсів, до яких зловмисники додали шкідливий JavaScript-код.

Як працює схема

Під час відвідування скомпрометованого сайту користувачеві демонструється підроблена сторінка перевірки Cloudflare. Під приводом стандартного підтвердження «Я не робот» відвідувачу пропонують скопіювати та виконати певну команду. Якщо людина це робить, на її комп'ютер завантажується та встановлюється шкідливе програмне забезпечення.

Атака є цілеспрямованою: шкідлива сторінка відображається лише користувачам ОС Windows, які перейшли на сайт із пошукових систем (Google, DuckDuckGo, meta.ua, bigmir.net тощо), і показується не частіше ніж двічі на 12 годин.

Фахівці CERT-UA наголошують, що жодна легітимна перевірка (CAPTCHA, Cloudflare тощо) ніколи не вимагає натискати комбінацію клавіш Win+R, відкривати командний рядок чи PowerShell, або вставляти й виконувати будь-які команди. Якщо ви бачите таку вимогу, негайно закрийте сторінку, навіть якщо це відомий вам сайт.

Як хакери керують атакою та викрадають дані

Для керування інфраструктурою атаки хакери використовують технологію блокчейн (зокрема мережі Polygon та Ethereum), що дозволяє їм миттєво та непомітно змінювати свої налаштування. Щоб обійти захист системи, зловмисники маскують вірус LUNEXSTEALER під легітимні файли та експлуатують вразливості системних драйверів Windows.

Після зараження вірус непомітно встановлює у браузер жертви шкідливе розширення під виглядом «Microsoft Office Word Editor». Цей інструмент повністю викрадає логіни, паролі та історію відвідувань, а також дає хакерам змогу віддалено керувати комп'ютером.

Рекомендації для захисту та реагування

Щоб убезпечити IT-інфраструктуру, системним адміністраторам рекомендується заборонити

звичайним користувачам виклик вікна «Виконати» (Win+R) і обмежити встановлення будь-яких MSI-пакетів без прав адміністратора. Крім того, варто увімкнути блокування вразливих драйверів (Microsoft Vulnerable Driver Blocklist) та дозволити використання лише перевірених розширень для браузерів із «білого списку».

Якщо ви натрапили на сайт із підробленою сторінкою перевірки або є власником зламаного ресурсу, негайно зверніться до CERT-UA за адресою: cert@cert.gov.ua. Фахівці нададуть інструкції та допоможуть очистити сайт від шкідливого коду.

Детальніше на сайті CERT-UA. <https://cert.gov.ua/article/6319983>

<https://www.kmu.gov.ua/news/ia-ne-robot-cert-ua-fiksuie-masove-poshyrennia-shkidlyvoho-prohamnoho-zabezpechennia>