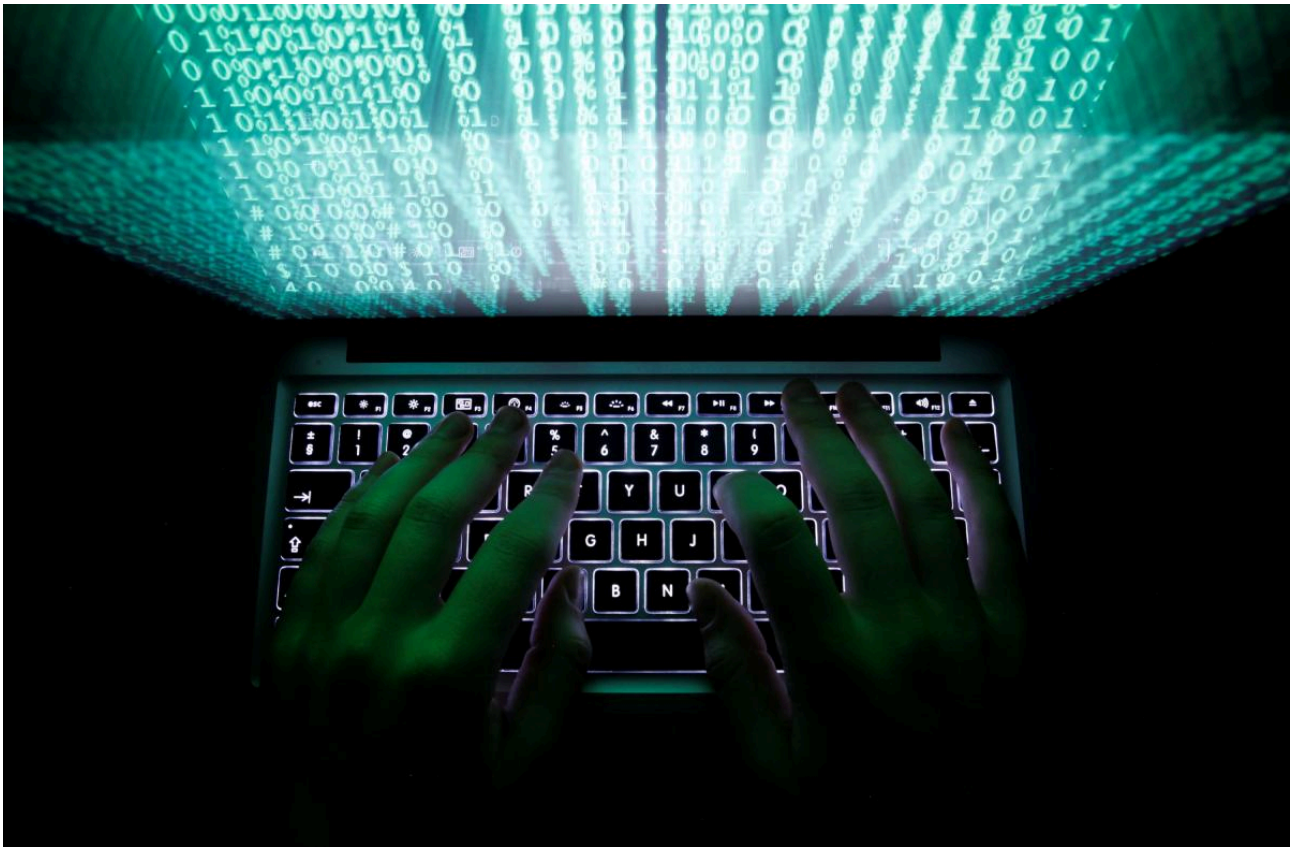
Міжнародна IT-компанія попереджає про низку шпигунських атак на урядові та дипломатичні установи Східної Європи

Published: 2019-10-11 · Archived: 2026-04-05 16:10:30 UTC

За даними компанії ESET, відповідні атаки тривають щонайменше з 2013 року.



Ілюстрація / REUTERS

Один з провідних розробників антивірусного програмного забезпечення – словацька компанія ESET попереджає про низку шпигунських атак на урядові та дипломатичні установи Східної Європи, які здійснюються за допомогою маловідомої платформи для кібершпіонажу.

Відповідну інформацію компанія оприлюднила на своєму сайті.

«Аналіз показує, що ці атаки проводилися з допомогою маловідомої платформи для кібершпіонажу. Платформа має модульну архітектуру, а також дві помітні особливості: AT-протокол, який використовується одним з плагінів для збору цифрових відбитків GSM-пристроїв, а також Tor, який використовується для мережних з'єднань... Діяльність зловмисників, які використовують Attor, переважно спрямована на дипломатичні представництва та урядові установи, а також на користувачів кількох російських сервісів», - йдеться в повідомленні.

Згідно з даними компанії ESET, відповідні атаки тривають щонайменше з 2013 року.

Читайте також Експерти розповіли, як вибір операційної системи впливає на безпеку смартфона

За допомогою шкідливої платформи зловмисники збирають інформацію про підключені модеми, пристрої і накопичувачі, а також інформацію про файли, які на них зберігаються. На думку спеціалістів ESET, кіберзлочинців особливо цікавлять цифрові відбитки GSM-пристроїв, підключених до комп'ютера. Для з'єднання з пристроєм Attor використовує так звані AT-команди.

«Невідомі сьогодні для більшості людей AT-команди для керування модемами були розроблені ще у 80-х роках минулого століття і до цих пір використовуються в більшості сучасних смартфонів», — пояснюють фахівці ESET.

Тому серед можливих причин використання зловмисниками AT-команд може бути те, що шпигунська платформа спрямована на модеми і застарілі моделі телефонів. Крім цього, AT-команди можуть використовуватися для з'єднання з деякими конкретними пристроями. Можливо, зловмисники дізнаються про використання жертвами пристроїв за допомогою інших методів шпигунства.

«Цифрові відбитки можуть стати базою для подальшого викрадення даних, — розповідають спеціалісти ESET. — Якщо зловмисники дізнаються про тип підключеного пристрою, вони можуть створити і розгорнути спеціальний плагін, який за допомогою AT-команд може викрадати дані і вносити зміни в пристрої, зокрема, під вбудоване програмне забезпечення».

Як повідомляв УНІАН, згідно з інформацією компанії ESET, в Україні щодня фіксується близько 300 тис. нових кіберзагроз для інформаційної безпеки. При цьому, знайти хакерів-зловмисників вкрай складно, компаніям залишається лише проводити щохвилинні моніторинги на предмет виявлення кіберзагроз із метою їх подальшого блокування.

Компанія ESET – міжнародний розробник антивірусного програмного забезпечення і рішень в області комп'ютерної безпеки. Компанія була заснована в 1992 році в Словаччині і на сьогодні представлена більш ніж в 180 країнах світу.
