СКОМОРОХОВ Владислав Андрійович
Київський інститут Національної гвардії України

СУЧАСНІ ЗАГРОЗИ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ (MALWARE)

Світ настільки швидко розвивається та прогресує в інформаційному просторі, що сучасні мобільні технології, незважаючи на зручність, стикаються з численними загрозами в інформаційній безпеці.

На основі останніх звітів та повідомлень від CERT-UA (Команда реагування на комп'ютерні надзвичайні події України) [1] та Держспецзв'язку (SSSCIP) [2], а також аналізу кібербезпекових компаній, можна виділити такі типи шкідливого програмного забезпечення, що активно використовуються зловмисниками проти українських користувачів, організацій та державних установ станом на початок 2025 року:

1. **Інфокралери (Infostealers):** Це один із найпоширеніших типів. Вони націлені на викрадення облікових даних (логінів, паролів від браузерів, поштових клієнтів, месенджерів, VPN, банківських додатків), файлів cookie, даних автозаповнення, криптогаманців та іншої чутливої інформації.

Приклади (з недавніх звітів): **AgentTesla, Formbook, Vidar, StealC, SmokeLoader.** Часто розповсюджуються через фішингові електронні листи зі шкідливими вкладеннями (архіви, документи) або посиланнями.

Інформація, отримана інфокралером, може бути використана для різноманітних зловмисних цілей, таких як викрадення особистих даних, шахрайство з кредитними картками або навіть шантаж. Викрадачі інформації є одним із найнебезпечніших типів шкідливого програмного забезпечення, оскільки вони можуть викрасти величезні обсяги конфіденційної інформації, не усвідомлюючи, що їхня конфіденційність була скомпрометована [3].

2. **Програми-вимагачі (Ransomware):** Хоча масові атаки програм-вимагачів на приватних користувачів можуть бути менш помітними, вони залишаються серйозною загрозою для бізнесу та організацій. Зловмисники шифрують дані та вимагають викуп за їх відновлення. Деякі угруповання також крадуть дані перед шифруванням і погрожують їх опублікувати [4].

3. **Вайпери (Wipers):** Це деструктивне ПЗ, головна мета якого – не викуп, а знищення даних та виведення з ладу комп'ютерних систем. Їх використання значно зросло з початком повномасштабного вторгнення РФ і часто пов'язане з діяльністю угруповань, що спонсоруються державою-агресором.

Приклади (активні під час війни): **CaddyWiper, HermeticWiper, IsaacWiper, Prestige Ransomware (діє як вайпер), NikoWiper.** Часто націлені на державний сектор, енергетику, телекомунікації [5].

4. **Завантажувачі (Loaders/Droppers):** Програми, основна функція яких – непомітно завантажити та встановити на систему жертви інше, більш небезпечне шкідливе ПЗ (стилери, трояни, вимагачі). *Останнім часом дуже розповсюджені:* **SmokeLoader, Guloader.**

5. **Трояни віддаленого доступу (RAT - Remote Access Trojans):** Надають зловмиснику повний контроль над зараженим комп'ютером, дозволяючи виконувати команди, красти файли, записувати натискання клавіш, активувати веб-камеру та мікрофон, характерні приклади таких вірусів **Remcos RAT, DarkCrystal RAT (DCRat).**

6. **Банківські трояни (Banking Trojans):** Спеціалізуються на крадіжці даних для доступу до онлайн-банкінгу та фінансових рахунків. Можуть перехоплювати паролі, коди підтвердження, підміняти реквізити під час платежів.

Одні із частіших методів розповсюдження загрозливого програмного забезпечення:

Фішинг: Найпоширеніший метод. Маскування під офіційні повідомлення (від банків, держустанов, сервісів), рахунки-фактури, судові повідомлення, пропозиції роботи, оновлення програмного забезпечення. Часто

використовуються теми, пов'язані з війною, соціальними виплатами, гуманітарною допомогою.

Шкідливі вкладення: Архіви (ZIP, RAR), документи Word/Excel з макросами, PDF-файли. В таких вкладеннях можуть міститись заздалегідь прописані скрипти котрі можуть надати доступ до певного виду інформації зловмисникам.

Компрометація легітимних веб-сайтів: Взлом сайтів для розміщення шкідливого коду або перенаправлення користувачів на фішингові сторінки. Часто зустрічаються одно сторінкові сайти що дуже схожі на оригінальні сайти, в таких сайтах заздалегідь налаштовані посилання, що можуть здійснити прикований доступ до вашого пристрою.

Торенти та неліцензійне програмне забезпечення (ПЗ): Завантаження програм з неофіційних джерел часто містить «у комплекті» шкідливе ПЗ. Таке неліцензоване ПЗ може дуже часто призводить до витоку або доступу до інформації.

Сучасний ландшафт загроз у сфері інформаційної безпеки характеризується стрімким зростанням кількості та складності шкідливого програмного забезпечення. Від інфокраулерів, які непомітно викрадають конфіденційну інформацію, до руйнівних вайперів, які спрямовані на повне знищення даних, кожен тип загрози становить серйозну небезпеку як для окремих користувачів, так і для цілих організацій. Особливої актуальності ці загрози набувають в умовах воєнного стану, коли зловмисники активно використовують фішинг, компрометацію сайтів та неліцензійне програмне забезпечення для реалізації атак.

Ці тенденції вимагають від користувачів постійної пильності, регулярного оновлення систем захисту, підвищення обізнаності про кіберзагрози та обережного ставлення до невідомих файлів і посилань. Лише поєднання технічних рішень та цифрової грамотності здатне забезпечити ефективний захист в умовах сучасного кіберпростору.

В умовах триваючої російської агресії, кіберпростір став одним із ключових полів бою. Держава-агресор та її підконтрольні угруповання активно використовують кібератаки для досягнення своїх військово-політичних цілей, тому протидія цим загрозам є критично важливим завданням для забезпечення національної безпеки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. CERT-UA. Урядова команда реагування на комп’ютерні надзвичайні події України (Computer Emergency Response Team of Ukraine). URL: https://cert.gov.ua.

2. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua.

3. Антивірусне програне забезпечення ESET. URL: https://help.eset.com/glossary/uk-UA/infostealer.html.

4. Wise IT - лідер комплексних IT рішень для бізнесу в Україні. URL: https://wiseit.com.ua/0xxx-ransomware-vyyavlennya-zahyst-ta-vidnovlennya/.

5. WeLiveSecurity - Провідний вебресурс на котрому спеціалісти ESET публікують дослідження, новини та поради, пов’язані з кібербезпекою. URL: https://www.welivesecurity.com/2023/02/24/year-wiper-attacks-ukraine/