УДК 004.49

ЗВ'ЯЗОК КІБЕРАТАК ІЗ НАЗЕМНИМИ БОЙОВИМИ ДІЯМИ

Товкун Юлія Ігорівна
студентка VI курсу факультету Інфокомунікацій
Харківський національний університет радіоелектроніки, Україна
Добринін Ігор Станіславович
кандидат технічних наук, доцент, доцент кафедри інфокомунікаційної інженерії імені В.В. Поповського
Харківський національний університет радіоелектроніки, Україна

Анотація. На тлі військового вторгнення в Україну кібератаки та операції були націлені на критично важливу інфраструктуру та цивільні об'єкти.

Нанесення ударів по об'єктах критичної інфраструктури викликає особливу стурбованість, оскільки ця інфраструктура необхідна для виживання цивільного населення. Кібератаки на інфраструктуру, таку як енергетика, водопостачання, охорона здоров'я, фінансові установи, транспорт і послуги зв'язку, можуть мати руйнівні наслідки для цивільного населення.

Крім ризиків для критичної інфраструктури та цивільних об'єктів, кібератаки сіють недовіру й обмежують доступ до достовірної інформації або поширюють неправдиву інформацію.

Ключові слова: кібератака, Wiper, бойові дії, атака, хакер, безпека.

Незадовго до вторгнення в Україну в лютому компанія Microsoft повідомила про 237 кібератак, у яких брали участь шість державних груп, пов'язаних із Росією. З них близько 40 було класифіковано як "руйнівні" атаки, спрямовані на зниження можливостей цілі [1].

У звіті показано кілька великих російських кібератак, які передували фізичним нападам на об'єкти в Україні.

У середині січня потужної хакерської атаки зазнали держсайти, а також портал "Дія", що зберігає персональні дані мільйонів українців: адреси, телефони, е-мейли тощо. У залишеному повідомленні хакери писали: "Уся інформація про вас стала публічною, бійтеся і чекайте гіршого". Влада запевняла, що особисті дані викрадені не були. Але пізніше з'явилися відомості про те, що 2 млн записів із "Дія" продають в інтернеті за $15 000.

Найпотужніша DDoS-атака в довоєнній історії України почалася 15 лютого, коли вивели з ладу десятки сайтів банків і держструктур. Вона не припинялася до самого передодня війни.

1 березня за кібератакою на українську телекомпанію з руйнівним витоком даних послідував ракетний удар по одній з її телевеж.

2 березня дані було вкрадено в організації з ядерної безпеки під час захоплення наземними військами військ атомних електростанцій у країні.

11 березня держоргани міста Дніпро зазнали цілеспрямованої атаки, трохи згодом, цього самого дня було завдано перших ударів по урядових будівлях Дніпра.

На початку наступу на місто Маріуполь було здійснено масштабну розсилку електронною поштою з дезінформацією, надходили листи від людини, яка видавала себе за жителя міста і стверджувала, що уряд збирається кинути його населення [1].

Також видно, що кібератаки на Україну з боку Росії перед вторгненням розпочалася ще на початку 2021 року, коли пов'язані з Росією хакери досліджували організації всередині України, щоб визначити мету подальших атак.

Кібератаки з використанням шкідливого програмного забезпечення типу Wiper почалися на початку 2022 року, коли дипломатичні зусилля зазнали невдачі і можливість війни стала більш імовірною. Найбільша хвиля російських кібератак такого роду припала на період безпосередньо перед і після початку вторгнення: з 23 лютого по 2 березня.

Кібератака, спрямована на Viasat, яка тимчасово вимкнула модеми KA-SAT 24 лютого 2022 року, того самого дня, коли російські збройні сили вторглися в Україну, була наслідком шкідливого ПЗ Wiper.

Висновки було отримано наступного дня після того, як американська телекомунікаційна компанія повідомила, що вона стала ціллю багатогранної та навмисної кібератаки на свою мережу KA-SAT, пов'язавши її з "вторгненням у наземну мережу зловмисника, який використовував неправильну конфігурацію у пристрої VPN", для отримання віддаленого доступу до довіреного сегмента управління мережі KA-SAT [2].

Отримавши доступ, зловмисник віддав "деструктивні команди" десяткам тисяч модемів, що належать службі супутникового широкосмугового зв'язку, які "переписали ключові дані у флеш-пам'яті модемів, зробивши модеми нездатними отримати доступ до мережі, але не назавжди".

Другою версією є IsaacWiper. IsaacWiper знаходиться або в Windows DLL, або в EXE без підпису Authenticode [3].

Для зразків DLL ім'я в каталозі експорту PE - Cleaner.dll , і він має єдиний експорт _Start@4.

За допомогою VirusTotal вийшло дізнатися, що IsaacWiper у %programdata% і C:\Windows\System32 міг перебувати під такими іменами:

- **clean.exe;**
- **cl.exe;**
- **cl64.dll;**
- **cld.dll;**
- **cll.dll.**

IsaacWiper починає з перерахування фізичних дисків і викликає DeviceIoControl, щоб отримати їхні номери пристроїв. Потім він стирає перші 0x10000 байт кожного диска, використовуючи генератор псевдовипадкових чисел Mersenne Twister. Генератор заповнюється з використанням значення GetTickCount [2].

Потім він перераховує логічні диски і рекурсивно стирає кожен файл кожного диска випадковими байтами, також згенерованими PRNG Mersenne Twister. Він рекурсивно стирає файли в одному потоці, а це означає, що стирання великого диска займе багато часу.

25 лютого 2022 року зловмисники скинули нову версію IsaacWiper з журналами налагодження . Це може вказувати на те, що зловмисники не змогли стерти деякі з цільових машин і додали повідомлення журналу, щоб зрозуміти, що відбувається.

Третя версія Wiper – CaddyWiper була виявлен а в Україні 14 березня 2022 р. під час розгортання в мережі банку. Він був розгорнутий через об'єкт групової політики, що вказує на те, що зловмисники заздалегідь мали контроль над мережею цілі. Wiper стирає призначені для користувача дані та інформацію про розділи з підключених дисків, роблячи систему непрацездатною і такою, що не підлягає відновленню [4].

На відміну від програм-вимагачів, мета розгортання вайпера не фінансова, його єдина мета – знищити все, що можна. В умовах триваючої війни між Росією та Україною кіберзлочинці використовуватимуть такі можливості, щоб отримати вигоду з конфлікту.

Список джерел:

1. Special Report: Ukraine - An overview of Russia's cyberattack activity in Ukraine [Електронний ресурс] – Режим доступу до ресурсу: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.
2. A Modem Wiper Rains Down on Europe [Електронний ресурс] – Режим доступу до ресурсу: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.
3. IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine [Електронний ресурс] – Режим доступу до ресурсу: https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/.
4. CaddyWiper: More destructive wiper malware strikes Ukraine [Електронний ресурс] – Режим доступу до ресурсу: https://www.zdnet.com/article/caddywiper-more-destructive-wiper-malware-strikes-ukrainian-targets/.