АНАЛІЗ ДИНАМІКИ КІБЕРІНЦИДЕНТІВ, СПРИЧИНЕНИХ ДІЯЛЬНІСТЮ РОСІЙСЬКИХ КІБЕРЗЛОВМИСНИКІВ ЗА 2022-2024 РОКИ

Момот В.С.

Харківський національний університет радіоелектроніки,
кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Україна.

E-mail: vladyslav.momot1@nure.ua

Abstract

The Russian invasion of Ukraine has significantly escalated cyber activities targeting Ukraine's web resources; especially that of governmental institutions, military organizations and critical infrastructure. Russian cybercriminals and hacktivists, often linked to state-sponsored groups, have become increasingly aggressive and adaptive in leveraging sophisticated tactics, techniques and procedures to disrupt essential services and undermine Ukrainian sovereignty. Analyzing these evolving strategies is crucial for enhancing cybersecurity resilience, forecasting cyberattack trends and protecting national security in an era of cyberwarfare. The purpose of this paper is to explore how the invasion has catalyzed changes in Russian cyber tactics and operations, highlighting the urgency of understanding these shifts to better defend against such threats.

Російсько-українська кібервійна

Повномасштабне вторгнення росії в Україну триває вже третій рік, і разом з активними військовими діями на території України триває війна у кіберпросторі. Тактики, техніки та цілі російських кібертерористів відповідають цілям військової агресії рф, проте кіберзлочинці продовжують адаптуватись та вдосконалювати техніки проведення кібератак. Досвід аналізу кіберінцидентів та оцінювання впроваджених заходів протидії кібератакам в умовах гібридної війни є важливим для підготовки спеціалістів у галузі кібербезпеки та захисту інформації.

Актуальність цього питання полягає у недооціненні суспільством важливості кібербезпеки, а також у необхідності вивчення методів російських кібератак на українські вебресурси для запобігання ймовірним загрозам та прогнозування можливих векторів атак на подальші роки.

Кібертерористичні угруповання

В атаках на українські вебресурси задіяні сили не тільки спецслужб рф (зокрема, фсб, гру, свр), а також зусилля хактивістів та зрадників з тимчасово окупованих територій (Луганськ та Севастополь), що з 2014 року перейшли на бік ворога.

Угруповання UAC-0010 (Gamaredon, Actinium), що пов'язане з фсб [1], проводить масові кібератаки з 2014 року [2] та залишається серед найактивніших угруповань кібертерористів упродовж останніх трьох років. У першому півріччі 2023 року UAC-0010 було активним впродовж 23 тижнів із 26 [3], у середньому проводячи приблизно 4 кібероперації на тиждень.

Спеціалізація Gamaredon – кібершпіонаж (приховане отримання інформації) з використанням шкідливого програмного забезпечення, розісланого у вкладеннях до фішингових листів та повідомлень у месенджерах працівникам організацій, що в основному пов'язані з силами оборони України та органами державної влади.

Gamaredon причетне до проведення 74 кібератак у другому півріччі 2022 року [1], спричинення 102 кіберінцидентів у першому півріччі 2023 року (з них 10 класифіковані як інциденти критичного та високого рівнів) та 94 кіберінцидентів у другому півріччі 2023 року (з них 9 – критичного та високого рівнів) [4].

Критичність кіберінцидентів

Російські кіберзловмисники наносять шкоду українським вебресурсам та інформаційним системам, тим самим спричиняючи інциденти різного рівня критичності.

Упродовж другого півріччя 2022 – першого півріччя 2024 років прослідковується збільшення кількості зареєстрованих кіберінцидентів. Якщо у другому півріччі 2022 року було зареєстровано 855 кіберінцидентів [1], то вже у першому півріччі 2023 року – 1079, у другому півріччі 2023 року – 1463, а у першому півріччі 2024 року – 1739 випадків [2].

Таким чином, кількість зареєстрованих кіберінцидентів у першому півріччі 2024 року була на 100,03% (у 2,03 рази) більше, ніж у другому півріччі 2022 року.

Незважаючи на збільшення кількості зареєстрованих кіберінцидентів, водночас зменшується відсоток кількості кіберінцидентів, визначених критичними та високими. Для порівняння, у першому півріччі 2022 року такими було визначено 644 кіберінциденти (приблизно 48% від загальної кількості), у другому півріччі 2022 року – 353 (41,2% від загальної кількості), у першому півріччі 2023 – 183 (16,9% від загальної кількості), у другому півріччі 2023 [4] – 187 (17,3% від загальної кількості), а у першому півріччі 2024 – 48 [2] (2,7% від загальної кількості).

Слід зауважити, що в аналітичних звітах Державної служби спеціального зв'язку та захисту інформації України загальна кількість кіберінцидентів за категоріями відрізняється, адже аналітика за 2022-2023 роки враховує виключно випадки, зареєстровані підрозділом CERT-UA, а аналітика за перше півріччя 2024 року враховує також і ті випадки, що були зареєстровані SOC Держспецзв'язку.

Цілі та методи кібератак

Головні цілі ворожих кіберугруповань впродовж 2022-2024 років залишаються незмінними: найбільшу кількість зафіксованих кіберінцидентів було зафіксовано під час атак на урядові організації та органи державної влади, енергетичний сектор, сектор безпеки та оборони та Інтернет-провайдери. Лише за останній рік кількість атак на сектор безпеки та оборони зросла зі 111 до 276 (на 148%) [2], що свідчить про спроби дестабілізувати військову потужність України не тільки на полі бою, а ще й на кіберфронті, сфокусувавшись на отримуванні розвідувальної інформації.

Впродовж перших півтора року з початку повномасштабного вторгнення, популярність серед кіберзловмисників мали фішинг, інфікування шкідливим програмним забезпеченням, атаки на відмову в обслуговуванні та компрометація облікових записів користувачів та систем.

З кожним роком кількість інцидентів, пов'язаних з інфікуванням пристроїв шкідливим програмним забезпеченням, продовжує збільшуватись. Упродовж другого півріччя 2022 року було зафіксовано 40 таких кіберінцидентів, першого півріччя 2023 року – 58, другого півріччя 2023 року – 103, першого півріччя 2024 року – 196. Таким чином, у порівнянні з першим періодом, кількість подібних інцидентів збільшилась у 4,9 рази.

Проведення DoS- та DDoS-атак суттєво зменшилось у порівнянні з минулими роками. Кіберзловмисники проводять точкові, проте масові атаки, зокрема, шляхом надсилання шкідливого програмного забезпечення у фішингових листах не тільки на поштові скриньки, а ще і використовуючи SMS-повідомлення (смішинг) та повідомлення у месенджерах, виходячи з того, що користувачі мають миттєвий доступ до смартфонів (на противагу комп'ютерам та ноутбукам).

Прогноз на 2024-2025 роки

З динаміки російських кібероперацій останніх років можна зробити висновок, що кібертерористи працюють у багатьох напрямках, використовуючи різні тактики та інструменти: вони не обмежуються виключно проведенням DDoS-атак або поширенням шкідливого програмного забезпечення.

ІТ-інфраструктура, сфера телекомунікацій та енергетика є найважливішими елементами, що потребують найбільшого захисту від кібератак, особливо під час масованих обстрілів та успіхів Збройних сил України.

Проаналізувавши дані, представлені у звітах Державної служби спеціального зв'язку та захисту інформації України, можна передбачити, що впродовж 2024-2025 років фокус кіберзловмисників зберігатиме точковий характер, а під загрозою кібератак знаходитимуться вищі посадовці міністерств та органів державної влади, підприємства критичної інфраструктури (включно з енергетичним сектором), військовослужбовці, ІТ-компанії та Інтернет-провайдери.

Беручи до уваги акцент на поширенні шкідливого програмного забезпечення у мобільних застосунках, слід очікувати збільшення випадків кібератак на мобільні пристрої користувачів. Тож, для попередження подібних випадків слід подбати не тільки про заборону встановлення застосунків зі сторонніх джерел, а також вебфільтрацію, використання технології управління мобільними пристроями (MDM), регулярні тренінги з протидії фішингу та інформування стосовно актуальних кіберзагроз. Критично важливим є зосередження уваги на працівниках та активна протидія соціальній інженерії, адже саме людина є найслабшою ланкою будь-якої системи.

Посилення кіберстійкості

Жодна система не є абсолютно захищеною, проте існують методи ускладнення роботи кіберзловмисникам та зменшення кількості кіберінцидентів критичного та високого рівнів. До таких методів протидії кіберзагрозам відносяться:

– використання багатофакторної автентифікації та складної парольної політики, що ускладнює доступ кіберзловмисників до облікових засобів та пристроїв користувачів;

– постійне навчання як персоналу відділу інформаційної безпеки організації, так і рядових співробітників стосовно протидії методам соціальної інженерії (зокрема, фішингу);

– налаштування антивірусного програмного забезпечення та своєчасне оновлення баз даних;

– використання міжмережевих екранів та фільтрація запитів на прикладному рівні (DNS) для унеможливлення переходу за зловмисними посиланнями;

– періодичне створення резервних копій баз даних, що надасть змогу швидко відновити роботу при DDoS-атаках або ураженні шкідливим програмним забезпеченням;

– дотримання принципу «Zero trust», що включає в себе метод надання найменших привілеїв;

– захист мобільних пристроїв, включаючи оновлення операційної системи та застосунків;

– заборона встановлення програмного забезпечення з неперевірених джерел;

– обмеження віддаленого адміністративного доступу (зокрема, за протоколом RDP);

– збільшення періоду журналювання робочих станцій та мережевих пристроїв;

– оперативна комунікація з підрозділом CERT-UA щодо виявлених кіберінцидентів.

Висновки

Основні тенденції російських кіберзловмисників за останній рік (друге півріччя 2023 – перше півріччя 2024 року) включають активізацію розповсюдженння шкідливого програмного забезпечення шляхом надсилання фішингових листів з компрометованих облікових записів для дестабілізації сектору безпеки та оборони.

Таким чином, пропонується перелік рекомендацій для підвищення стійкості працівників установ та організацій, що знаходяться під загрозою кібератак з боку російських кіберзловмисників.

Література

1. State Service of Special Communications and Information Protection of Ukraine. Russia's Cyber Tactics. Lessons Learned 2022. 2023. P. 1 – 33. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=53466.

2. State Service of Special Communications and Information Protection of Ukraine. Russian Cyber Operations. APT Activity Report H1 2024. P. 1 – 27. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=65898.

3. Державна служба спеціального зв'язку та захисту інформації України. Російські кібероперації. Аналітика за перше півріччя 2023 року. 2023. С. 1 – 23. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=60201.

4. State Service of Special Communications and Information Protection of Ukraine. Russian Cyber Operations. APT Activity Report #3 H2 2023. 2024. P. 1 – 25. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=64622.