17 березня вітчизняні веб-ресурси зазнали чергової кібератаки держави-агресора, зокрема системи компанії, що спеціалізується на веб-рекламі, зазнали несанкціонованого втручання, що призвело до заміщення на ресурсах партнерів соціальної та комерційної реклами кольорами прапору, що колись майорів на знищеній та покинутій техніці окупантів.

Завдяки конструктивній позиції представників постраждалої компанії в стислі терміни встановлений механізм кібератаки та вжиті необхідні заходи реагування. Кібератака в загальних рисах складалась з декількох етапів:

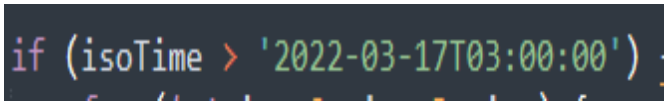
1. вивчення системи достави контекстної реклами та виявлення вразливості її програмного коду;

2. написання зловмисниками java-script для його розміщення в рекламних блоках,

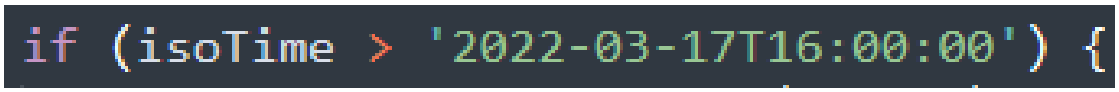
3. додавання java-script до рекламних блоків сайтів-партнерів шляхом експлуатації виявленої вразливості.

За результатом проведеного аналізу java-script встановлено:

- Скрипт включав у себе масив доменів, на які кожні 2 секунди, тричі, виконувались запити різними способами (через src атрибут тегів <iframe> та <img>), що створювало навантаження на відповідні сайти імітуючи атаку типу ddos. Виконання даного функціоналу було заплановане в коді на початок роботи з 03:00:01 17.03.2022. Домени відповідають сайтам компаній у сфері розробки програмного забезпечення (більшість), надання послуг з хостингу, фінансових послуг та Інернет-магазину.



- Наступна частина скрипта відповідає за генерацію зображення (defacement) при відвідуванні вебсайту — партнера, на сторінці якого розміщено скрипт інформера. Даний функціонал також є запланованим та активувався о 16:00:01 17.03.2022. Даний скрипт генерує на сторінці зображення прописане за допомогою html та css, зображення є адаптивним та підлаштовується під будь яке розширення дисплею.



За попередніми висновками кібератака була попередньо ретельно спланована, весь код зловмисників є самописним та не використовував готові рішення, кількість запитів, ціллю яких було навантаження вищеописаних ресурсів, була чітко розрахована для того щоб навантажувати ресурси та одночасно не бути поміченими користувачами ресурсу, з якого робляться запити, або фаєрволами. Окремі елементи кібератаки вже зараз вказують на причетність до її проведення спецслужбами рф, які відшуковують можливості масового поширення деструктивного контенту. Проте співробітники спецслужб рф досі не розуміють справжнього відношення українців до росії і те, що максимальний ефект який вони досягли — певна кілька наших співвітчизників одночасно послали їх за “руським кораблем”.

За вказаним фактом проводиться розслідування, Ситуаційний центр забезпечення кібербезпеки СБУ оперативно надав постраждалій компанії допомогу в проведенні реагування на кібератаку та вжитті додаткових заходів кіберзахисту.

Єднання та взаємна допомога принесе нам перемогу як на полі бою, так і на інформаційному та кіберфронті.

Разом ми переможемо! Слава Україні!