CERT-UA

Archived: 2026-04-05 12:46:02 UTC

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA у тісній взаємодії з фахівцями Національного банку України (CSIRT-NBU) та Департаменту кіберполіції Національної поліції України вжито окремих заходів з дослідження інцидентів інформаційної безпеки, що мали місце 15.02.2022.

Зауважимо, що згадані кібератаки, на відміну від типової точкової діяльності окремих груп зловмисників, пов’язаної із розповсюдженням шкідливих програм, спір-фішингу, викраденням даних тощо, в більшості своїй були спрямовані на інфраструктурні елементи кіберпростору та окремі галузі, в тому числі, маючи підтекст інформаційно-психологічних операцій, спрямованих на дестабілізацію ситуації в країні.

Серед основних способів реалізації зловмисного задуму можна виділити такі.

1. Розсилання фейкових SMS-повідомлень громадянам про, начебто, порушення штатного режиму функціонування банкоматів окремих державних фінансових установ.

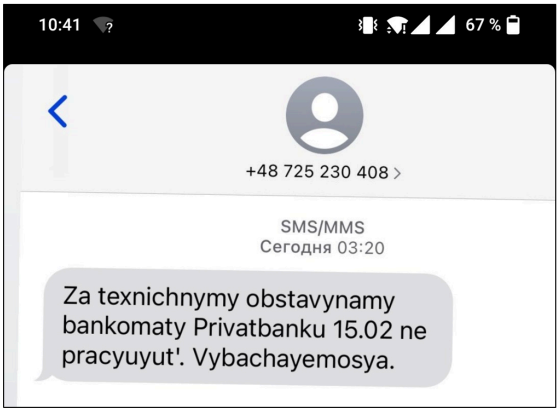

Рис.1 Приклад фейкового SMS-повідомлення

2. Розсилання електронних поштових повідомлень серед низки фінансових установ про мінування приміщень та будівель останніх. Було встановлено, що зазначена діяльність може здійснюватися мешканцем Донецької області.


Отделения банка заминированы

To info

Настоящим информирую вас о том, что в отделениях вашего банка в городах Киев, Харьков, Днепр, Чернигов, Ровно и Одесса заложены взрывные устройства, которые могут быть активированы в любой момент. Надеюсь, вы успеете вовремя эвакуировать сотрудников и клиентов и никто не пострадает.

Рис.2 Приклад електронного листа з повідомленням про мінування

3. Проведення розподілених атак на відмову в обслуговуванні (DDoS) у відношенні веб-ресурсів українських банків та державних установ. В рамках дослідження, в тому числі, з урахуванням інформації від партнерів, визначено, що до здійснення атак, серед іншого, залучено бот-мережі Mirai (https://twitter.com/360Netlab/status/1493797519725367302) та Meris (шкідливий інформаційний потік спрямовується через тисячі зламаних маршрутизаторів Mikrotik та ряду інших IoT пристроїв з фільтрацією джерел за допомогою ACL, що дозволяє приховати згадані пристрої від пошукових систем на кшталт Shodan). Зазначене, з високим рівнем впевненості, дозволяє припустити, що для проведення атак використано наявні потужності зловмисників, що надаються як послуга (DDoS as a Service).

У зв’язку з тим, що кількість подібних пристроїв налічує більше 30000, список IP-адрес розповсюджено серед суб’єктів координації за допомогою платформи MISP.

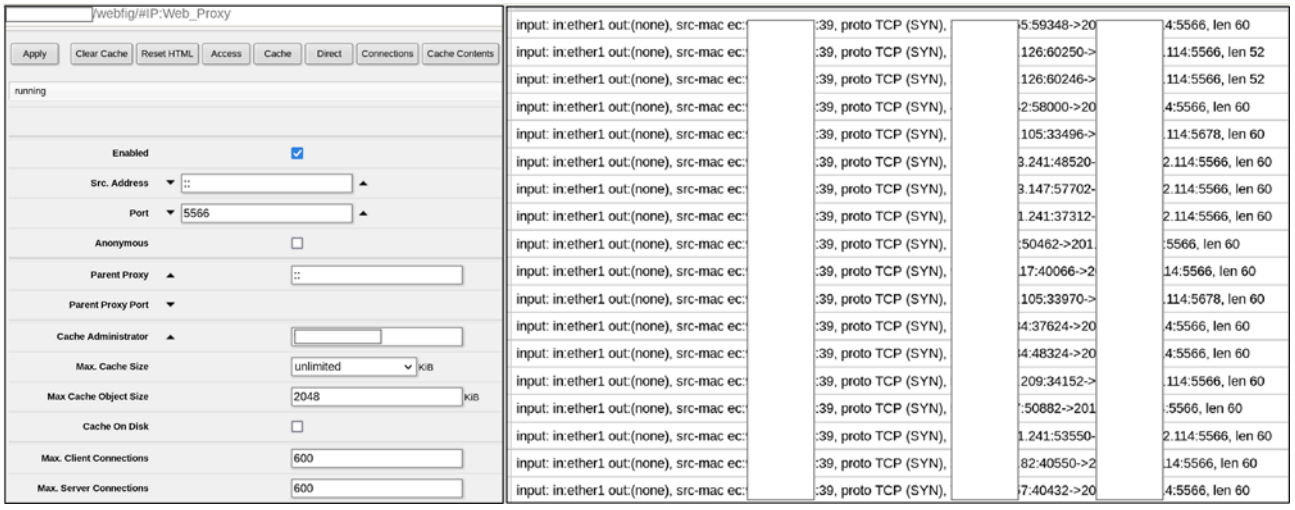

Рис.3 Приклад налаштування проксі-серверу Mikrotik та транзитного передавання інформаційних потоків

4. Унеможливлення доступу до веб-ресурів в зоні gov.ua шляхом здійснення DDoS-атаки на обслуговуючі DNS-сервери (https://hostmaster.ua/news/?pr20220216). Виведення з ладу декількох серверів доменних імен призвело до тимчасового порушення доступу до значної кількості веб-ресурсів державних органів у зв’язку з неможливістю визначення А-запису (IP-адреси) для відповідних доменних імен.

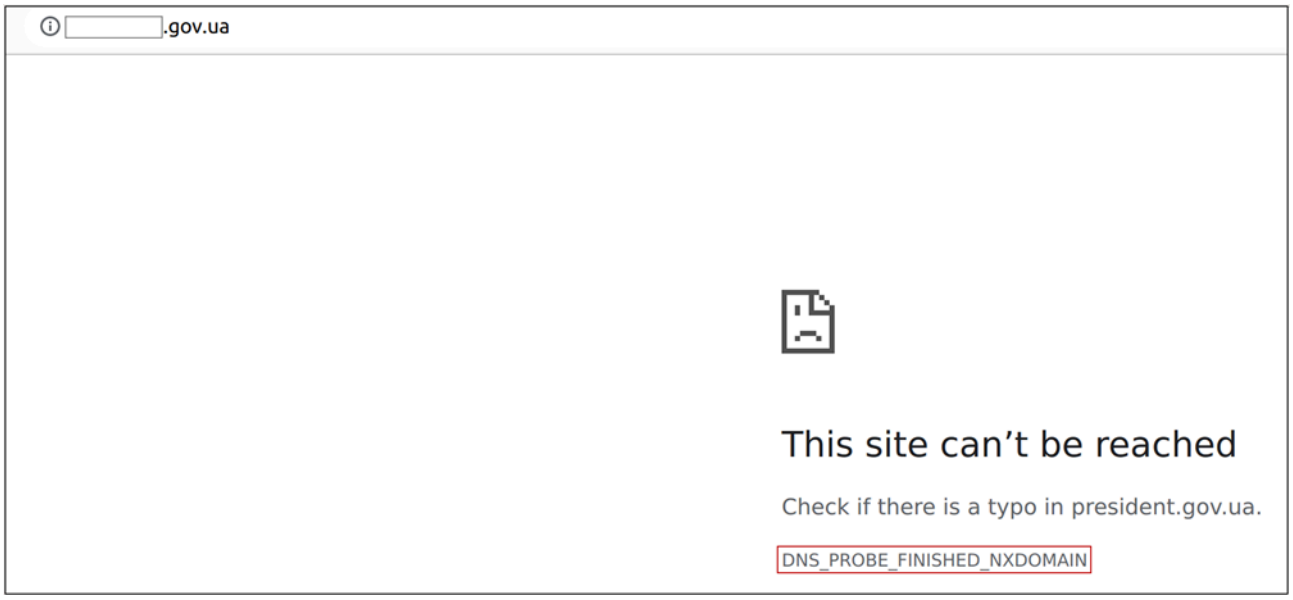

Рис.4 Приклад неможливості отримання A-запису для веб-ресурсу в зоні gov.ua

5. Підозріла маніпуляція з налаштуваннями автономних систем на рівні протоколу BGP. Так, за даними Cisco Crosswork (http://bgpstream.com/event/287011) протягом більше ніж двох годин, починаючи з 15:30 15.02.2022, префікс 217.117.7.0/24, який фактично належить Inq-Digital-Nigeria-AS (AS16284), було анонсовано від імені автономної системи Приватбанку (AS15742) через автономну систему нігерійського оператора телекомунікацій AS37148.

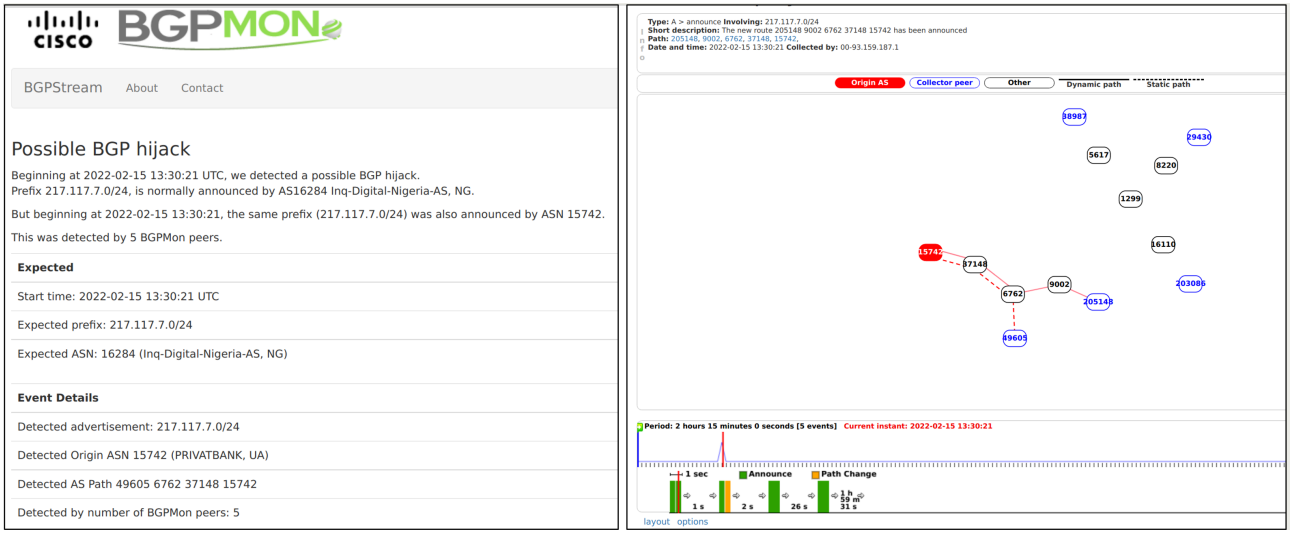

Рис.5 Приклад анонсування префіксу 217.117.7.0/24, начебто, від AS15742

Зважаючи на значний зріст кількості кіберінцидентів, а також, ураховуючи той факт, що під час реагування на події інформаційної безпеки значну частину часу займає процес налагодження комунікації з суб’єктом координації та збір і передавання цифрових доказів, наполегливо рекомендуємо державним органам, об’єктам критичної інфраструктури налагодити оперативний зв’язок та процес інформаційного обміну з CERT-UA.

Source: https://cert.gov.ua/article/37139