Ransomware-атаки:

як їх виявити та як запобігти

SOCRadar пропонує всеохопний набір інструментів, які дають змогу відстежувати витоки даних, вразливості, індикатори компрометації і негайно вживати заходів.

В часи пандемії, коли світ почав стрімко цифровізуватися, кіберздирництво (Ransomware) стало найпоширенішою проблемою для підприємств, перетворившись на фундаментальну частину злочинного бізнесу. Років з десять тому цей вид кіберзлочинності був прерогативою лише обмеженої кількості хакерів, але сьогодні він складає цілу індустрію, і обсяги таких атак зросли в рази. Ці угруповання не лише створюють програми-вимагачі, але й мають власні служби підтримки, куди жертви можуть звернутися, щоб дізнатися, як сплатити викуп.

Крім того, з появою моделі Ransomware-as-a-Service (RaaS) творці шкідливих програм почали надавати свої дітища так званим партнерам. Ті, попри малу технічну компетентність, можуть розповсюджувати вірусне програмне забезпечення, а сплачений викуп розділяється між операторами здирницького бізнесу (розробниками програм) та партнерами. Така співпраця дозволяє масштабувати атаки та робить їх більш доступними для широкого кола зловмисників, що збільшує загальну загрозу для глобальної кібербезпеки.

Як поширюється Ransomware?

Ransomware заражає системи шляхом використання трьох найпоширеніших векторів атак: неправильно налаштованого програмного забезпечення для спільного використання робочого столу або вбудованих служб віддаленого робочого столу (RDP), фішингових електронних листів та вразливих веб-застосунків. Для кожного вектора зловмисники використовують різні інструменти.

Вкрадені облікові дані RDP

Сервіси RDP вже давно є відомим вектором атак – особливо там, де фішингові електронні листи можуть приносити менший зиск. Однак пандемія та популярність роботи з дому зробили атаки через RDP ще більш поширеними. Хакери задіюють програмне забезпечення для спільного використання робочого столу у 40% Ransomware-атак. І в межах цього вектора вони найбільш активно використовують скомпрометовані облікові дані. Вкрадені облікові дані RDP можна придбати на чорному ринку в «дарквебі» за кілька баксів. Це перша і легка опція для отримання початкового доступу до мережі, яка не потребує взаємодії з користувачем або інших значних зусиль з боку злочинців. Після того, як хакери отримують доступ до цих облікових даних, вони можуть обійти заходи захисту на кінцевих точках та порушити роботу системи.

Фішингові електронні листи

Фішинг – ще один з найпоширеніших векторів атак типу Ransomware (близько 35% випадків). Цей метод включає в себе використання посилань та/або вкладень для непомітного виконання зловмисних дій. Вдаючись до прийомів соціальної інженерії, злочинці спонукають жертву відкрити заражене вкладення або перейти за шкідливим посиланням. Такі дії призводять до непомітного завантаження та активації здирницького ПЗ на пристрої жертви. Згодом програма-вимагач може легко поширитися мережею, шифрувати важливі файли та експортувати дані, створюючи сприятливі умови для вимагання викупу.

Вразливості

Третім ключовим вектором атак, який сприяє поширенню програм-вимагачів, є експлуатація вразливостей у веб-застосунках, що становить 20% інцидентів з Ransomware. Ці вразливості, якщо їх не усунути своєчасно та оперативно, відкривають широкі можливості для непомітного проникнення в системи.

Як виявити та знешкодити Ransomware за допомогою SOCRadar?

Запобігання атакам програм-вимагачів та їх виявлення у разі компрометації є ключовими завданнями в сфері кібербезпеки. SOCRadar пропонує комплексний підхід до вирішення цих завдань за допомогою низки важливих функцій, спрямованих на зміцнення безпеки та підвищення готовності до інцидентів.

Виявлення витоку облікових даних та конфіденційної інформації

Набір інструментів **SOCRadar Digital Risk Protection** розшукує в Інтернеті будь-які скомпрометовані облікові дані та витоки конфіденційної інформації. Ця система активно сканує «дарквеб», чат-канали, чорні ринки, а також відкриті сховища коду (**рис. 1**) на предмет виявлення активів компанії або ключових слів, пов'язаних з нею. В разі виявлення такої інформації

SOCRadar негайно сповіщає відповідні команди, що дозволяє своєчасно вжити необхідних заходів. Команда SOCRadar Dark Web пропонує спеціалізовану підтримку, допомагаючи зі збиранням та аналізом цих даних. Використовуючи ці інструменти та ресурси, організації мають можливість виявляти загрози та реагувати на них ще до того, як вони Реалізуються, значно знижуючи ризик кібератак та забезпечуючи вищий рівень кібербезпеки.

Виявлення активів

Інструментарій **SOCRadar Attack Surface Management** дозволяє ідентифікувати ваші Інтернет-активи та стежити за ними. Використовуючи SOCRadar, ви отримуєте:

- **повне розуміння доступних в Інтернеті цифрових активів вашої компанії**, які є доступними не тільки для потенційних відвідувачів, але й для можливих зловмисників;
- **можливість відслідковувати критичні відкриті порти** у вашій організації за допомогою регулярних активних сканувань;
- **здатність моніторити та оперативно усувати критичні вразливості** в інфраструктурі за допомогою планових активних сканувань на наявність вразливостей (**рис. 2**).

Завдяки цим функціям SOCRadar дає змогу ефективно запобігати Ransomware-атакам, надаючи своєчасні та точні сповіщення про виявлення потенційних портів та вразливостей. Наприклад, у разі виникнення критичної вразливості, такої як RCE (Remote Code Execution), SOCRadar швидко ідентифікує всі ваші активи з потенційно уразливим програмним забезпеченням і миттєво сповістить про це. Без належної системи управління вразливостями ви ризикуєте залишити вашу систему відкритою для атак через невідомі вразливості.

Threat Intelligence

Набір ***SOCRadar Threat Intelligence*** надає різні можливості та функції для допомоги виявленню та запобіганню Ransomware-атакам. Сторінка **Пошуку загроз** дозволяє вам шукати індикатори компрометації (IoCs) та отримувати дані про атрибуцію з 2,5 мільярдів записів. Окрім ручного пошуку під час реагування на інциденти, ви також можете легко інтегрувати дані у ваше рішення з SOAR за допомогою Restful API.

Сторінка пошуку загроз дозволяє вам створювати індивідуальні колекції IoC, особливо для Ransomware (**рис. 3**). Таким чином, ви можете інтегрувати ці нові колекції індикаторів компрометації у ваші продукти з оркестрації, системи управління інформацією та подіями (SIEM), мережеві екрани (FW), засоби виявлення загроз та реагування (EDR) або будь-які засоби безпеки, які підтримують моніторинг, виявлення та нейтралізацію трафіку з цих зловмисних джерел. SOCRadar має широкі можливості для

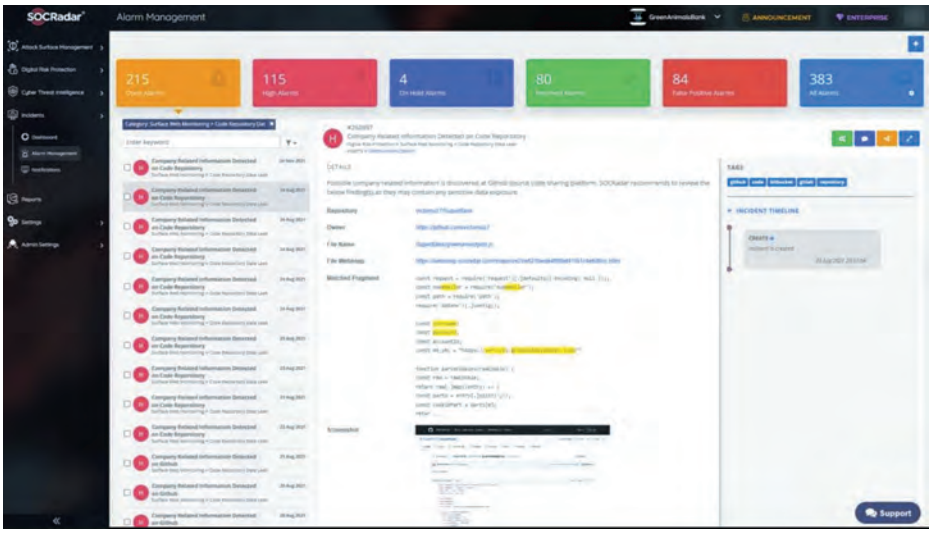

Рис. 1 Виявлення витоку даних у публічному сховищі коду

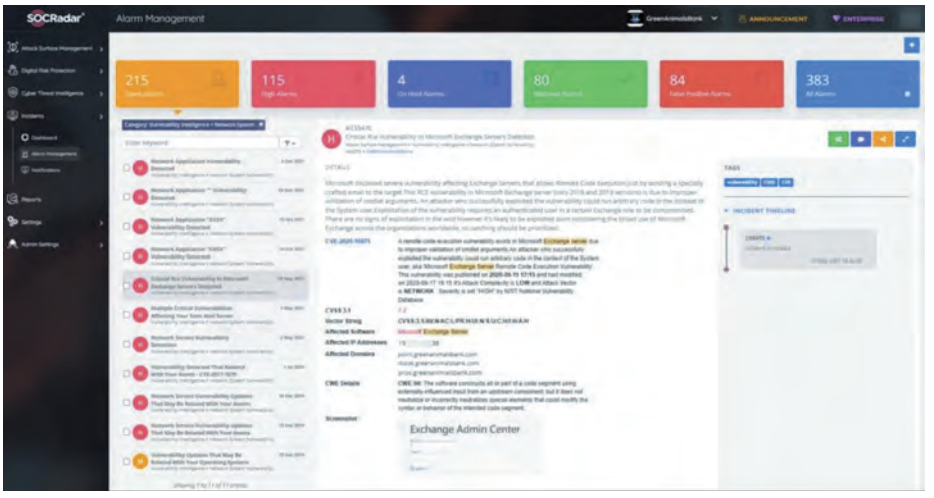

Рис. 2 Виявлення критичної вразливості

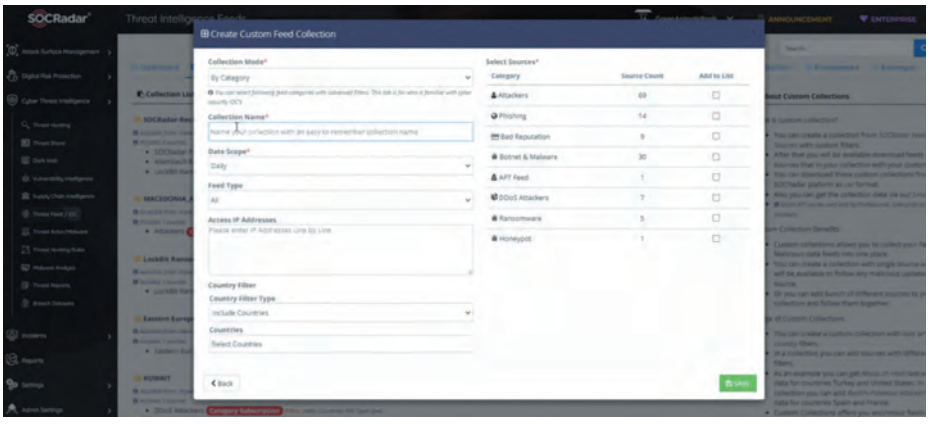

Рис. 3 Створення спеціальної колекції IoC

детектування фішингу і додає виявлені фішингові URL-адреси до своїх внутрішніх колекцій IoC.

SOCRadar стала першою компанією, що об'єднала технології **EASM** (управління зовнішньою поверхнею атаки), **DRPS** (захист від цифрових ризиків) та **CTI** (розвідка кіберзагроз) у спільну концепцію – **Extended Threat Intelligence** (**XTI**). Цей новий напрямок передбачає інтегрований підхід до ідентифікації загроз, їх аналізу та реагування на них, надаючи організаціям комплексне бачення їхніх цифрових ризиків.