лефонувати в службу підтримки банка. Скоріше всього. Вам дадуть відповідь, що ніяких збоїв на сервері не було, і Ваша карта продовжує обслуговуватись банком.

Протидія фішингу потребує постійного моніторингу на предмет нових методів та шляхів обходу системи безпеки в цілому, але дані в основному потрапляють до рук шахраїв через «людський фактор». адже більша частина населення не придає особливого значення звичайним правилам особистої безпеки. Тому шахраї, використовуючи методи соціальної інженерії, мають можливість заволодіти особистими даними людини, які вона мала необережність розкрити.

Одержано 28.04.2016

УДК 004.042

Дмитро Васильович Мільчаков,
курсант 3 курсу факультету № 4 ХНУВС
Науковий керівник: канд. техн. наук Світличний В. А.

ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС АНАЛІТИЧНОГО СУПРОВОДУ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ Й ПІДТРИМКИ УХВАЛЕННЯ РІШЕНЬ – RICAS

Фахівцями Управління інформаційного забезпечення Харківського обласного ГУНП спільно з місцевими ІТ-компаніями розроблений інноваційний комплекс аналітичної обробки інформації різноманітних банків даних з відображенням на детальній інтерактивній карті як самих об'єктів, так і результатів їх аналізу. Комплекс має робочу назву «RICAS» (Real – time Intelligence Crime Analytics System) і на сьогоднішній день знаходиться на етапі тестового впровадження.

Застосування комплексу дає можливість:

- збереження відеоданих на серверах, їх перегляд та аналіз у разі необхідності;
- безпосереднього доступу до кожної відеокамери на детальній інтерактивній карті області;
- відображення на цій карті об'єктів та осіб, які можуть впливати на розвиток ситуації.

В процесі тестування комплексу підтверджується його гнучкість та спроможність інтегрування будь-яких даних, з можливістю часового та просторового аналізу їх зв'язків між собою. Розроблений комплекс не обмежується Харковом та областю, а з легкістю масштабується до рівня країни і навіть більше.

Однією із складових частин комплексу RICAS є зовнішній Інтернет – сервіс взаємодії правоохоронних органів з громадськістю – проект Police.kh.ua, який на даний час користується популярністю в мережі Інтернет.

Проведені тестові випробування впродовж 3-х місяців підтверджують можливості комплексу щодо реагування на кримінальні та інші події. В результаті роботи команди з 3 аналітиків протягом цього часу було надано 152 аналітичних довідки з відомостями про осіб, можливо причетних до вчинення злочинів, більшу половину з яких підтверджено в ході перевірочних та оперативних заходів, зазначених осіб викрито у вчиненні злочинів.

На теперішній час комплекс тестується на обчислювальних потужностях ГУНП в Харківській області. Для його розгортання в робочий режим необхідне створення сучасного дата-центру на базі ГУНП в Харківській області, створення ситуаційно-аналітичного центру та організація підготовки відповідних фахівців для роботи в ньому.

Комплекс RICAS працює в реальному часі і дозволяє розкривати злочини на основі аналізу баз даних, накопичених поліцією/міліцією за останні 20 років. Системі доступні дані про більш ніж 5 мільйонів подій, що сталися на Харкі-

вщині, починаючи з 1995 року. За 4,5 місяця, які в Харкові тестували систему, вона допомогла розкрити близько 300 злочинів.

Для опрацювання зазначених пропозицій доцільним вбачається створення рішенням обласної ради спільної робочої групи, до якої увійшли б представники ГУНП в Харківській області, зокрема Управління інформаційного забезпечення, а також представники зацікавлених департаментів і служб Харківської обласної державної адміністрації та Харківської обласної ради.

Одержано 11.04.2016

*

УДК 004.056:55(043.2)

Алла Петрівна Синиця,
курсант 3 курсу факультету № 4 ХНУВС
Науковий керівник: канд. техн. наук Світличний В. А.

ВИЯВЛЕННЯ ПРИСТРОЇВ ДЛЯ НЕЗАКОННОГО ВТРУЧАННЯ В РОБОТУ БАНКОМАТІВ

За даними експертів та американської компанії Visa Inc., надає послуги проведення платіжних операцій, лідерами серед незаконних операцій з банківськими картами являються скіммінг і online-шахрайство. Скіммінг (від англ. skim – знімати вершки) – створення копії магнітної смуги для виготовлення клону карти користувача за допомогою спеціалізованих пристроїв, які називаються «скімери» і «шиммери» і найчастіше встановлюються на банкомати. За принципом дії ці пристрої не відрізняються один від одного і потребують використання прихованих відеокамер або накладок на клавіатуру банкомату для отримання PIN-коду.

Однак в шиммінгу замість традиційних громіздких скіммерів на щілину приймача пластикових карт банкоматів використовується дуже тонка, гнучка плата, впроваджується через цю щілину в середину банкомата. «Шим» підсаджується за допомогою спеціальної карти – носія: її просовують у щілину банкомату, де тонкий «шим» приєднується до контактів, що прочитує дані з карт, після чого картка-носій видаляється. Далі все працює, як і при традиційному скіммінгу – тобто вставляються в банкомат пластикових карт, де зчитуються всі важливі дані, які потім використовуються зловмисниками для виробництва карток – дублікатів та зняття з їх допомогою грошей. Єдине, але дуже важливе на відміну від скіммінгу полягає у відсутності будь-яких зовнішніх ознак шиммінгу того, що в банкоматі сидить «жучок». Виходячи зі специфікацій, що регулюють розміри щілини кард-рідера, товщина «шима» не повинна перевищувати 0,1 мм, інакше він буде заважати пластиковим картам. Це приблизно вдвічі тонше людської волосини.

Для власників банківських платіжних карток розроблено величезну кількість різноманітних інструкцій і правил безпеки. Основні з них наступні:

1. При проведенні операцій з карткою користуйтеся тільки тими банкоматами, які розташовані в безпечних місцях і обладнані системою відеоспостереження і охороною: у державних установах, банках, великих торгівельних центрах і т. д.

2. Звертайте увагу на картоприймач і клавіатуру банкомату. Якщо вони обладнані якими-небудь додатковими пристроями, то від використання даного банкомата краще утриматися і повідомити про свої підозри за вказаним на моніторі банкомату телефону.

3. У випадку некоректної роботи банкомату – якщо він довгий час перебуває в режимі очікування або мимоволі перезавантажується – відмовтеся від його використання. Велика ймовірність того, що він перепрограмований зловмисниками.