УДК 004.49: 004.056.57

ГОЛОВНЯ АМІНА ІГОРІВНА

Курсантка 3 курсу факультету №4

Харківського національного університету внутрішніх справ.

ГНУСОВ ЮРІЙ ВАЛЕРІЙОВИЧ

кандидат технічних наук, доцент,

завідувач кафедри кібербезпеки та DATA-технологій факультету №6

Харківського національного університету внутрішніх справ

ЗАХИСТ ВІД ВІРУСІВ-ШИФРУВАЛЬНИКІВ

Сьогодні найпоширеніша проблема в світі цифрових технологій є віруси-шифрувальники. Вони шифрують всі файли на комп'ютері таким чином, що власник втрачає до них доступ. Вірус-шифрувальник (шифратор, криптор) – особливий різновид шкідливих програм-здирників, чия діяльність полягає в шифруванні файлів користувача і, в подальшому, вимоги викупити засіб розшифровки. Суми викупу починаються десь від $200 і досягають десятків і сотень тисяч.

Частіше за все, такий вірус може потрапити на Ваш ПК через електронну пошту, якщо точніше, через файли та посилання, прикріплені до повідомлення. Перейти по них/завантажити файл змушує текст повідомлення: «Терміново погасіть борг по кредиту», «Ой, це ти на фото?», «Позовна заява подана до суду», «Сплатіть штраф / внесок / податок», «Донарахування комунального платежу», «Лена попросила терміново передати це тобі» та інші провокуючі фрази. Існують і інші шляхи завантаження вірусу: соціальні мережі, розсилка у месенджерах, шкідливі і заражені веб-ресурси, банерна реклама, розсилка через месенджери зі зламаних акаунтів, сайти розповсюджувачі кейгенів і кряків, сайти з порнографічним контентом, магазини додатків і контенту.

Як діяти для того, щоб зберегти важливі файли та не потрапити в пастку?

По-перше, якщо Ви – директор фірми чи підприємства, для якого є не бажаним описана вище ситуація, поясніть своїм підлеглим про можливість настання такої ситуації, про можливість загрози та наслідки, що чекають на

Вашу кампанію у разі успішної атаки. Важливо вказати на те, що не можна переходити по невідомим посиланням та завантажувати не перевірені файли.

Якщо ж Ви - рядовий користувач ПК, Вам теж не слід забувати про вказані вище речі. Не переходьте за посиланнями, якщо не впевнені в їх безпечності. Та не встановлюйте файли чи документи.

По-друге, бажано створити резервну копію всіх файлів, що буде зберігатися на сервері. Та будь-які нові файли також довантажувати на цей сервер.

По-третє, за можливості, працювати лише у віртуальному, ізольованому середовищі.

Розуміння можливостей вірусу – перший крок в його подоланні. Отож, будучи освідомленим у цьому питанні, та слідуючи представленим вказівкам, Ви будете відчувати себе захищеним.

УДК 004.942:004.946

Д'ЯКОВ АНДРІЙ ВОЛОДИМИРОВИЧ

кандидат технічних наук,

доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів

Львівського державного університету внутрішніх справ

ВИКОРИСТАННЯ СИСТЕМ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ, ЯК ПОТУЖНИЙ ЗАСІБ ПІДГОТОВКИ ФАХІВЦІВ МВС

Вдосконалення системи підготовки кадрів МВС, зокрема пошук найбільш дешевих та в той же час ефективних форм і методів підготовки є найголовнішою задачею розвитку Національної поліції та Національної гвардії України. Економічні аспекти з одного боку та розвиток інформаційних технологій з іншого вимагають застосовувати разом з традиційними нові форми і методи організації проведення підготовки. Цими новими формами, в тому числі і як показує досвід провідних країн НАТО, є заходи підготовки з