ПРОБЛЕМНІ ПИТАННЯ

ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

к.ю.н. с.н.с. С. А. Кузьмін

ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ПРИЗНАЧЕНЕ ДЛЯ:

- викрадення і передачі інформації та ідентифікаційних даних користувача (логінів та паролей)
- знищення та криптування інформації користувача в тому числі й з метою вимагання коштів
- ураження комп'ютерної техніки користувача для демонстрації рекламних блоків, в тому числі таких, що містять шкідливий код
- доступ до Державних баз даних з метою зміни інформації, внесення нової інформації, отримання інформації з метою шантажу (бази даних нотаріусів, АРМОР, медиків, банків, нова пошта, реєстру судових рішень)

ШЛЯХИ «УРАЖЕННЯ» В ЗАЛЕЖНОСТІ ВІД МЕТИ ЗЛОВМИСНИКА:

- отримання адресних електронних листів, що містять в собі файли з шкідливим кодом
- отримання «фішингових» електронних листів, що містять в собі файли з шкідливим кодом
- оновлення програмного забезпечення (в тому числі призначення для онлайн ігор), що містить в собі шкідливий код
- перехід користувача комп'ютера на сайти, що містять в собі шкідливий програмний код
- завантаження користувачем шкідливого програмного забезпечення
- умисне встановлення шкідливого програмного забезпечення користувачем комп' ютера
- встановлення програмного забезпечення, що одночасно, приховано від користувача, встановлює шкідливе програмне забезпечення
- розповсюдження шкідливого програмного забезпечення (шкідливого коду) через локальну мережу, або при використанні зйомних носіїв інформації

НАСЛІДКИ, ЩО ВИНИКАЮТЬ ПРИ УРАЖЕННІ ШКІДЛИВИМ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ:

- несанкціонований (віддалений) доступ до обладнання користувача
- знищення інформації та зупинення роботи організації (PetyA), блокування комп'ютера, шифрування файлів користувача з метою шантажу та вимагання грошових коштів (Ransomware)
- використання викраденої інформації (персональні дані, керування банківськими рахунками та ін. організація «Cobalt»)
- віддалений доступ з використанням прямого доступу до об’єктів.

СХЕМА ТА АЛГОРИТМ ДОСЛІДЖЕННЯ:

- дослідження файлів реєстру та перегляд встановленого загальноприйнятого програмного забезпечення для віддаленого керування
- дослідження лог-файлів та файлів-конфігураторів для встановлення алгоритму дій зловмисника
- дослідження інформаційного вмісту тимчасових файлів, а особливу увагу приділяти виконуючим файлам та файлам-бібліотекам

СХЕМА ТА АЛГОРИТМ ДОСЛІДЖЕННЯ:

- дослідження програмами-антивірусами програмне забезпечення на наявність шкідливого програмного забезпечення та встановити функціональне призначення останнього. Дослідження встановлених програм зі шкідливим кодом відбувається в ізольованому середовищі (програми Пісочниці)
- аналіз дати та способи встановлення виявленого програмного забезпечення
- в разі виявлення файлів (скриптів) для встановлення шкідливого програмного забезпечення, встановити спосіб їх утворення або походження

СХЕМА ТА АЛГОРИТМ ДОСЛІДЖЕННЯ:

- при наявності дозволу та доступу, дослідження інформації з електронної поштової скриньки користувача, для виявлення файлів, що містять шкідливий код
- аналіз історії відвідування мережі Інтернет
- встановити спосіб адміністрування та передачі звітів виявленого програмного забезпечення/програмного коду

ВИЩЕВКАЗАНІ ДІЇ МОЖУТЬ ДАТИ ІНФОРМАЦІЮ СТОСОВНО ОСОБИ – ЗЛОЧИНЦЯ, МЕТИ ЗЛОВМИСНИКА, ЗМІН ТА ПРОЦЕСІВ, ЩО ВІДБУВАЛИСЯ НА НАДАНОМУ НА ДОСЛІДЖЕННЯ ОБЛАДНАННІ ЗА ПЕВНИЙ ПЕРІОД ЧАСУ.

ТИПОВІ ПИТАННЯМИ ПІД ЧАС ПРОВЕДЕННЯ ЕКСПЕРТИЗИ:

- «Чи міститься на наданому на дослідження об’єкті програми віддаленого доступу (бажано зазначити яке саме програмне забезпечення необхідно досліджувати)? Якщо так, то лог-файли використання даних програм прошу зберегти на окремому носії інформації.»
- «Чи містяться на наданому на дослідження об’єкті програмне забезпечення, елементи програмного коду або сліди використання програмного забезпечення, призначені для віддаленого керування комп’ютером та/або викрадення ідентифікаційних даних користувача комп’ютера (відстеження дій користувача)? Яке призначення даного програмного забезпечення/програмного коду, яким чином і коли відбулася його установка на наданому на дослідження жорсткому диску?»

ТИПОВІ ПИТАННЯМИ ПІД ЧАС ПРОВЕДЕННЯ ЕКСПЕРТИЗИ:

- «У разі виявлення такого програмного забезпечення/програмного коду, вказати спосіб його адміністрування та передачі звітів.»
- «У разі виявлення такого програмного забезпечення/програмного коду, чи визначається він антивірусним програмним забезпеченням?»
- «Які зміни та процеси, відбувалися на наданому на дослідження обладнанні за певний період часу?»

ДЛЯ ТОГО, ЩОБ ВИРІШИТИ ВИЩЕ ЗАЗНАЧЕНІ ПИТАННЯ, НЕОБХІДНО НАДАТИ НАСТУПНІ МАТЕРІАЛИ:

- об’єкт дослідження або побітову копію носія інформації
- матеріали кримінального провадження в частині самого інциденту, а саме дати, пояснення потерпілих, дії потерпілих з комп’ютерним обладнанням
- супутня інформація, що може допомогти для вирішення питань (копія трафіка з wireshark, інформація від провайдера та ін.)

ПРИ УМОВІ УЧАСТІ В ЯКОСТІ СПЕЦІАЛІСТА НЕОБХІДНО ПРОВЕСТИ ПРОВЕСТИ НАСТУПНІ ДІЇ:

- встановити об’єкти огляду (комп’ютери, мережеве обладнання та ін.)
- встановити встановлене програмне забезпечення на предмет його функціонального призначення
- встановити лог-файли виявленого «підозрілого» програмного забезпечення
- встановити дії користувача за період часу коли стався інцидент, в тому числі і дії в мережі інтернет та внутрішній локальній мережі
- встановити наявність зйомних носіїв інформації, що могли бути під’єднані до комп’ютерного обладнання
- провести аналіз тимчасових файлів, трафіку (вхідний, вихідний)

ПРАВИЛЬНО ПРОВЕДЕНИЙ ОГЛЯД НАДДАСТЬ МОЖЛИВІСТЬ ВСТАНОВИТИ:

- спосіб проникнення на об’єкт дослідження
- хронологію подій втручання
- мету зламу та втручання
- наслідки втручання
- дані які можуть вказувати на особу злочинця (IP-адреса, адреса електронної пошти, шлях мережевого розташування)
- відомості, що були отримані зловмисником

ДЯКУЮ ЗА УВАГУ!!!