АБЕТКА
інформаційної безпеки

"Кіберзахист від А до Z"

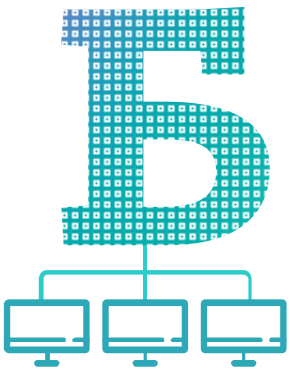
А

Антивірус

Програма, яка виявляє, знешкоджує та попереджає потрапляння на комп'ютер вірусів та інших видів шкідливого ПЗ, а також відновлює заражені ними файли.

Перші дві антивірусні програми CHK4BOMB і BOMBSQAD написав американський програміст Енді Хопкінс у 1984 році.

Б



Ботнет (robot+network)

Мережа пов'язаних між собою вірусом комп'ютерів, якою зловмисники керують з єдиного центру, який може знаходитися в будь-якій точці світу. Заражені комп'ютери використовуються для спам-розсилок, Ddos-атак на Інтернет-ресурси, крадіжки персональних даних користувачів тощо.

Один з найбільших ботнетів в історії – Srizbi botnet. Він надіслав більше половини спаму із загальної кількості небажаної пошти, відправленої великими ботнетами в 2008 році. Після його знешкодження обсяг світового спаму зменшився на 75%.

В

Вірус

Вид шкідливих комп'ютерних програм, здатних до самокопіювання та розмножування. Користувачі помилково називають вірусами інші види шкідливого програмного забезпечення – такі як трояни, хробаки, руткіти, рекламні модулі та ін.

Щодня в базі української антивірусної лабораторії Zillya! з'являється близько 60 тисяч нових видів шкідливого ПЗ.

Г

ПАРОЛЬ

Генератор паролів

Онлайн-сервіс, який дозволяє користувачам створити безпечний пароль будь-якої довжини та складності за заданими налаштуваннями (цифри, великий і малий реєстри літер, спецсимволи).

Найпопулярнішим паролем у світі є пароль 123456. На другому місці – трохи довший – 123456789. Замикає трійку варіант password. За статистикою, 10 % користувачів обирають однакові паролі.

Ґ

Ґеймерський режим роботи

Одна з можливостей антивіруса, призначена для використання під час повноекранної гри. Вона дозволяє скоротити час сканування заражених файлів та скасувати виведення на екран повідомлень про виявлення загроз.

Zillya! Антивірус

Д

«Дарвін»

Комп'ютерна гра, розроблена трьома інженерами фірми Bell Telephone Laboratories, у якій програми-«організми» завантажувалися на комп'ютери друзів, копіювали себе і знищували опонентів. Переможцем ставав той, чия програма зробить більше власних копій і «інфікує» більше комп'ютерів.

Ці програми-«організми» можна вважати першими комп'ютерними вірусами.

Е

Евристичний аналізатор

Модуль антивірусу, який здійснює аналіз поведінки комп'ютерних програм та пошук в них частин коду, схожого на код відомих вірусів.

В основі евристичного аналізу лежить припущення, що нові віруси будуть подібними до вже існуючих. Завдяки евристичному аналізатору антивіруси виявляють до 40% нових шкідливих програм.

Є

Єдиний український антивірус

Zillya! Антивірус, на 100% розроблений українськими програмістами, перша версія якого з'явилася в 2009 році, на сьогоднішній день - єдиний вітчизняний антивірус для домашніх та бізнес-користувачів.

Zillya! Антивірус Безкоштовний, єдиний антивірус в світі з "однією кнопкою", було випущено в травні 2014 року.

Ж

Живий диск, або Live CD

Завантажувальний диск, за допомогою якого можна відновити роботоздатність операційної системи, яка дала збій, чи запустити антивірус, щоб «лікувати» файли в неактивній системі.

З

«Зомбі»-вірус

Вид комп'ютерного віруса, який дозволяє зловмиснику керувати комп'ютером без відома користувача, зазвичай запускається троянською програмою.

Один з найскладніших «троянів» за історію, який зміг перетворити на «зомбі» чотири мільйони комп'ютерів – TDL-4. Його автори придумали власну систему кодування, щоб захистити зв'язок між вірусом та зараженими комп'ютерами, що зробило знищення шкідливого ПЗ практично неможливим.

И

МИтнИк, Кевін

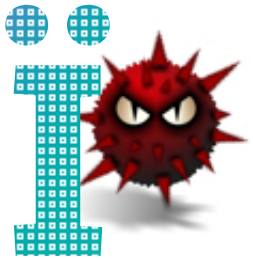
Легендарний американський хакер 90-х, колись найбільш розшукуваний кіберзлочинець Америки та світу, сьогодні – консультант з інформаційної безпеки уряду США. Відомий численними зломами телефонних та комп'ютерних мереж різного рівня складності захисту.

Перший злом Митника – локальна шкільна мережа. Увійшовши в систему, він міг виправити собі оцінки, але не став цього робити, оскільки цікавився лише самим процесом злому.

І

Інформаційна безпека

Сукупність процесів, спрямованих на забезпечення стану збереження конфіденційності, цілісності та доступності інформації.



«Їжак»

Жартівливе позначення вірусної загрози в Zillya! Антивірус.

Й

Йохансен, Йон, або DVD John

Норвезький хакер, відомий створенням програми DeCSS, яка зчитує захист з DVD та CD-дисків. Одна з найпопулярніших програм Йохансена QTFairUse могла знімати захист із DRM-даних (керування цифровими правами) з музичних файлів, які продавалися в Apple iTunes.

К

Кейлогер, або клавіатурний шпигун

Різновид програмного забезпечення, що фіксує час, тривалість, місце натискання клавіш на клавіатурі і кліки мишею, які робить користувач. Застосування кейлогерів зловмисниками призводить до крадіжки даних аутентифікації користувача.

Ці програми також активно використовуються правоохоронними органами. Так, наприклад, у 2000 році за допомогою клавіатурного шпигуна FlashCrest iSpy ФБР розсекретило паролі Ніккі Скарфо-молодшого – члена відомого філадельфійського мафіозного клану.

Л

«Лист щастя», або ILOVEYOU

Один з найбільш оригінальних вірусів. Користувачу на електронну пошту надходило повідомлення «I LOVE YOU» із вкладеним файлом. Після його відкриття комп'ютер отримувача починав надсилати величезну кількість спаму та видаляв важливі файли на ПК.

На той час (2000 рік) «Лист щастя» інфікував 10 % всіх комп'ютерів світу.

М

Морріс Роберт

Автор першого у світі мережевого хробака, який паралізував роботу шести тисяч комп'ютерів мережі ARPANET – прототипу сучасного Інтернет. Морріс став першим у світі обвинувачуваним у кібершахрайстві та засновником нового типу шкідливих програм.

Під враженням від атаки хробака Морріса американська асоціація комп'ютерного обладнання започаткувала День захисту інформації (30 листопада), який відзначається і сьогодні.

«Нігерійський лист»

Відома спам-схема, яка набула популярності ще до появи Інтернет, а потім почала широко в ньому застосовуватися. Шахраї з Нігерії масово розсилали листи, у яких від імені, начебто місцевого багатія пропонували людині взяти участь у фінансовій операції в обмін на солідний відсоток. Для цього жертва спочатку мала перевести на рахунок аферистові певну грошову суму, але потім, звичайно, нічого не отримувала.

Сьогодні понад 8% випадків інтернет-шахрайства – махінації з «нігерійськими листами».

Онлайн-сервіси перевірки на віруси

Спеціальні служби-сканери, які дають змогу користувачеві здійснити аналіз підозрілих файлів на наявність у них вірусного коду через мережу Інтернет.

До трійки найбільш популярних онлайн-сервісів перевірки на віруси входить Virus Total, MetaScan, VirSCAN. Двоє з них – Virus Total та MetaScan – використовують ядро українського Zillya! Антивірус.

Проактивний захист

Сукупність технологій, які використовуються в антивірусному програмному забезпеченні і спрямовані на аналіз поведінки програми, а не її програмного коду, виявлення підозрілих дій та припущення, що така програма може бути шкідливою.

Спам

Масова розсилка небажаних електронних листів зазвичай рекламного характеру. Традиційно до головних країн-спамерів входять США, Індія, Росія, Південна Корея, Китай та В'єтнам.

Троянська програма

Один з найнебезпечніших та найпоширеніших видів шкідливого ПЗ, яке маскується в корисних програмах. Часто використовується для крадіжки персональних даних користувача. Наприклад, представник сімейств троянів – Trojan.Banker.Win32 – «спеціалізується» на крадіжці персональних даних користувачів банківських систем та систем електронних платежів. Сьогодні в базах української антивірусної лабораторії Zillya! нараховується 1,5 млн різновидів банківських троянців.

Український національний антивірус, УНА

Перший антивірус вітчизняної розробки, що масово використовувався українцями для захисту своїх ПК. Проект проіснував до 2007 та був закритий через збитковість.

Zillya! Антивірус

Фішинг

Розповсюджений вид інтернет-шахрайства, метою якого є отримання конфіденційних даних користувача та здійснення фінансових махінацій. Часто зловмисники розсилають жертвам електронні листи від імені відомих компаній чи брендів з проханням перейти за їх посиланням – тобто на підробний сайт, де користувач залишає персональну інформацію.

Найбільше підробних сайтів «замасковані» під банки та інтернет-магазини. Також сьогодні набуває популярності QR-фішинг: користувачі смартфонів, зчитуючи підроблений QR-код, потрапляють на сайт шахраїв.

Хмарні технології в антивірусах

Сукупність методик виявлення шкідливого програмного забезпечення, які характеризуються тим, що підозрілий файл аналізується на серверах вендорів, дозволяючи користувачеві не зберігати громіздку антивірусну базу в себе на комп'ютері.

Деякі з вендорів, наприклад іспанський розробник антивірусу Panda, позиціонують свої продукти виключно як хмарні антивіруси.

Центр по боротьбі з кіберзлочинністю (ЄС)

Інституція Європейського Союзу, створена в січні 2013 року, головною метою якої є захист громадян від злочинів у сфері інформаційної безпеки. Центр займається протидією нелегальній діяльності злочинних угруповань в Інтернет, аналізом загроз та тенденцій, пов'язаних з кібербезпекою.

Штаб-квартира Центру знаходиться в нідерландському місті Гаага.

Чорний хакер

IT-спеціаліст, діяльність якого спрямована на виявлення недоліків у системах інформаційного захисту та їх нелегальне використання для власних інтересів.

Один з найвідоміших чорних хакерів світу – Кевін Поулсен – тепер працює журналістом у культовому виданні Wired. Завдяки своєму хакерському минулому Поулсену вдалося розсекретити 744 сексуальних маніяків, які безперешкодно користувалися популярною американською мережею MySpace.

Шпигунська програма

Клас шкідливого ПЗ, який може збирати інформацію про користувача без його відома: сканувати жорсткий диск, відстежувати відвідуваність сайтів у браузері, викрадати паролі та контактні дані тощо.

Щит

Логотип українського Zillya! Антивірус.

Zillya! Антивірус

Ь

ЬлораП

Умовний секретний набір знаків чи слово, яке дає право доступу до інформації і призначене для її захисту від несанкціонованого використання.

Ю

Юнікс/UNIX

Сімейство операційних систем, на яких “живе” сучасний Інтернет. Як мінімум 90% серверів в глобальній мережі працюють на даній операційній системі або її родичі Linux. Багато користувачів вважають, що для цієї ОС не існує вірусів. Насправді, це не так – віруси для UNIX існують у достатньо великій кількості.

Я

Ядро антивіруса

Внутрішня сервісна частина антивіруса, яка реалізовує його основну функцію – знаходити та знешкоджувати шкідливе програмне забезпечення. У світі існує практика ліцензування антивірусних ядер із подальшим використанням їх у різних антивірусних продуктах. Як приклад, антивірусне ядро українського Zillya! використовують більше 20 продуктів в 15 країнах світу.

Z

Zillya!
Антивірус

Абетку розроблено спеціалістами Української антивірусної лабораторії Zillya! під редакцією Олега Сича, технічного директора лабораторії.