НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
липень 2023

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

Підготовлено за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»

Створення цієї публікації стало можливим завдяки підтримці американського народу, наданій через Агентство США з міжнародного розвитку (USAID). Погляди авторів, висловлені у цій публікації, не обов'язково відображають погляди USAID або Уряду США.

ЗМІСТ

ОСНОВНІ ТЕНДЕНЦІЇ

США продовжує модифікацію власної кібербезпекової політики та адаптації її до актуальних викликів. Вперше в історії Стратегій кібербезпеки США було розроблено та прийнято публічний Імплементаційний план. Він складається з 65 ініціатив, керованих відповідальними державними органами, які збільшуватимуть стійкість системи кібербезпеки США та протистояння в першу чергу китайській та російській загрозам. Документ чітко визначає завдання та відповідальних за їх виконання, що відрізняється від традиційного підходу до таких документів, коли Стратегії залишались саме політичними настановами для державних організацій і які імплементували їх відповідно до свого розуміння завдань документа. Одночасно з цим Білий Дім намагається оновити кадровий склад тих, хто відповідає за кібербезпеку в країні. Номіновано нового очільника офісу Національного кібердиректора – посада залишається вільною вже протягом майже пів року після звільнення Криса Інгліса. Також було номіновано і нового керівника NSA Т. Хоу, який вже зробив низку заяв.

Цього місяця в Україні на порядку денному були питання розвитку кібердипломатії, підвищення ефективності реалізації завдань Стратегії кібербезпеки України, а також додаткові заходи кібербезпеки систем управління технологічними процесами на об'єктах критичної інфраструктури, які були розглянуті на засіданні Національного координаційного центру кібербезпеки при РНБО України. В рамках реалізації стратегії кібербезпеки, Адміністрація Держспецзв'язку розробила та затвердила Методичні рекомендації щодо реагування суб'єктів забезпечення кібербезпеки на кіберінциденти. Було засновано Національний кластер з інформаційної стійкості, мета якого – сприяти державному та приватному сектору у зміцненні інформаційної стійкості. Також відбулось підвищення рівня професійних навичок комунікаційників державного сектору у сфері кібербезпеки під час Cyber Communications Workshop.

На фоні змін американської кібербезпекової політики тривають внутрішньоамериканські дискусії щодо актуальних питань кібербезпеки критичної інфраструктури. Комісія Solarium виступила з ініціативою додати до списку секторів ОКІ космічну галузь. Одночасно з цим триває дискусія щодо необхідності додавання операторів хмарних послуг як ще одного сектору (при цьому важливість переходу федеральних установ у «хмару» визначається як критична для кібербезпеки ІТ-систем уряду). Ці дискусії поєднані із загальним занепокоєнням експертів та парламентарів щодо залежності федеральних відомств (зокрема Пентагону) від продуктів Microsoft.

11-12 липня у Вільнюсі відбувся саміт НАТО, на якому, серед іншого, увага була приділена і питанням кібербезпеки. Ухвалені учасниками саміту документи лишаються засекреченими, разом з тим, з публікацій експертів та заяв представників Альянсу можна зробити висновок, що йдеться про підсилення взаємодії з приватним сектором, постійну присутність військових кіберспеціалістів у мережах, а не лише під час міжнародного збройного конфлікту тощо. В інтерв'ю ЗМІ Представник НАТО Крістіан-Марк Ліфлендер закликав Альянс зайняти «проактивну» позицію у кіберпросторі.

Українська сфера кібербезпеки активно інтегрується до міжнародної спільноти. Так, під час візиту до штаб-квартири НАТО, українська делегація розповіла про уроки кібервійни, що триває, а також представила потреби та пропозиції щодо майбутньої співпраці з НАТО у цій сфері. Під час візиту до Брюсселя було обговорено організацію третього раунду кібердіалогу між Україною та ЄС, успіхи України у гармонізації законодавства України із законодавством ЄС у сфері кібербезпеки та напрями подальшої взаємодії. Україна також вкотре виступила на щорічних навчаннях НАТО із взаємосумісності, було започатковано співпрацю з низкою аналітичних європейських структур.

Китай та росія продовжують проводити власні кібероперації. Обидві країни сконцентровані на шпигунських діях (з акцентом на європейські країни). росія додатково проводить кібершпигунські операції в підтримку своєї військової агресії, намагаючись дістатись до листування працівників дипломатичних відомств – на це були спрямовані останні операції RomCom RAT та Cozy Bear. Привернула особливу увагу й атака Китаю на міністра торгівлі США Джину Раймондо, яка є найбільш послідовним затятим противником Китаю в адміністрації Байдена, та офіційних осіб Державного департаменту США напередодні візиту Держсекретаря Блінкена до Китаю.

Спостерігається певний спад атак ransomware (лідером тут залишається сектор охорони здоров'я – 54% атак такого типу в ЄС припадають саме на цей сектор). Такі кібербезпекові організації, як Cisco Talos, навіть вказують на зміну лідера в кількості атак у другому кварталі 2023 року. При цьому ціна зламу все росте, але компанії не бажають вкладати більше у свою безпеку. Ця проблема все більше стосується й індустріального сектору, де загрози стають все помітнішими, а вразливості в промисловому обладнанні знаходять все частіше. Дослідники безпеки та такі організації як CISA намагаються оперативно реагувати на ці загрози, але часто самі виробники не бажають сприяти такій діяльності.

Кіберстійкість, на жаль, залишається для західних компаній концепцією, а не настановою до дії. Це характерно як для приватного сектору, так і урядів (наприклад саме на брак реальних кроків Уряду США в цьому напрямку звертають увагу дослідниці з CSIS). На практиці це призводить до того, що компанії не достатньо готові до ransomware і їх наслідків.

Кількість складних DDoS атак збільшується. Звіт Cloudflare показує, що загальна кількість DDoS-запитів з квітня по червень досягла 5,4 трильйона, що на 15% більше, ніж у першому кварталі цього року. При цьому від них страждають і важливі урядові ресурси – останнім прикладом була DDoS-атака проти системи електронних державних послуг в Кенії. Внаслідок атаки користувачі декілька днів не могли повноцінно користуватись сервісом.

1. ІНІЦІАТИВИ НАЦІОНАЛЬНИХ СУБ'ЄКТІВ: СТРАТЕГІЇ, ЗАКОНОДАВСТВО, КАДРОВІ ЗМІНИ

ANSSI ОПРИЛЮДНИЛО ІНСТРУМЕНТ САМООЦІНКИ ГОТОВНОСТІ ОРГАНІЗАЦІЇ ДО КІБЕРКРИЗОВОЇ СИТУАЦІЇ

4 липня французька ANSSI оприлюднила інструмент самооцінки, який має допомогти організаціям визначити рівень своєї зрілості в питаннях готовності до кіберкризової ситуації. Інструмент побудований як опитувальник з 57 питань. Він розроблений співробітниками ANSSI разом з Клубом директорів з корпоративної безпеки (CDSE). Користування інструментом добровільне, але ANSSI просить учасників, які пройдуть таку самооцінку, надіслати її Агентству для узагальнення матеріалів.

МАЙБУТНІЙ ОЧІЛЬНИК NSA Т. ХОУ ВИСТУПАЄ ЗА РОЗШИРЕНУ ПІДТРИМКУ УКРАЇНИ У ПРОТИДІЇ РОСІЙСЬКІЙ КІБЕРЗЛОВМИСНІЙ ДІЯЛЬНОСТІ

12 липня під час слухань щодо його призначення, генерал-лейтенант ВПС США Т. Хоу підкреслив, що США мають продовжити надавати допомогу у кібербезпековій сфері Україні й надалі: «Ми очікуємо, що росія продовжуватиме використовувати всі наявні у них кіберпотенціали в рамках свого незаконного конфлікту. Там, де ми можемо надати допомогу, ми повинні продовжувати це робити».

КАНДИДАТ НА ПОСАДУ ОЧІЛЬНИКА КІБЕРКОМАНДУВАННЯ АНБ ЗАЯВИВ, ЩО РОЗДІЛ 702 ЗАКОНУ ПРО СПОСТЕРЕЖЕННЯ ЗА ІНОЗЕМНОЮ РОЗВІДКОЮ «НЕЗАМІННИЙ»

12 липня під час номінаційних слухань у Комітеті Сенату з розвідки Кандидат адміністрації Байдена на посаду керівника Кіберкомандування США та АНБ генерал-лейтенант ВПС Тімоті Хо вперше висловився публічно щодо суперечливих програм стеження, шифрування та інших нагальних проблем у сфері кібербезпеки.

Він заявив про свою підтримку суперечливого розділу 702 Закону про спостереження за іноземною розвідкою (FISA), який дозволяє уряду проводити цілеспрямоване спостереження за допомогою постачальників електронних комунікаційних послуг за іноземцями, що перебувають за межами США. Але також попросив продовжити обговорення про те, як конкретні процедури в рамках застосування цього розділу відповідають закону та забезпечують приватність.

Стосовно шифрування Хоу підкреслив його критичну роль у захисті систем національної безпеки та пообіцяв не підривати шифрування для американців.

Хоу також зазначив, що Україна була стійкою проти кібератак з боку росії завдяки партнерству зі США та союзниками по НАТО. Він погодився з принципом «Захищати наперед (Defend Forward)».

ПЛАН РЕАЛІЗАЦІЇ НАЦІОНАЛЬНОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ США

13 липня Білий дім оприлюднив План реалізації Національної стратегії кібербезпеки США. У плані детально описано понад 65 федеральних ініціатив із високим ступенем впливу – від захисту робочих місць у США шляхом боротьби з кіберзлочинністю до формування кваліфікованої робочої сили в кіберпросторі, здатної досягти успіху в економіці. Кожна з них має власні стратегічні цілі, часові рамки та державну установу, відповідальну за керівництво ініціативою разом з іншими зацікавленими сторонами. Адміністрація планує оновлювати завдання щорічно, зважаючи на постійно змінюваний ландшафт загроз.

Короткий виклад основних положень.

КНР ПЛАНУЄ ПОСИЛИТИ ЗАХОДИ КОНТРОЛЮ НАД ВНУТРІШНІМ КІБЕРПРОСТОРОМ

17 липня Генеральний секретар КПК Сі Цзіньпін доручив побудувати «бар'єр кібербезпеки» навколо КНР, а також «підтримувати лідерство партії в інтернет-просторі». Хоча конкретні обриси того, як саме це має бути здійснено не вказуються, однак фахівці очікують, що це може призвести до модернізації «Великого китайського фаєрволу» – сукупності нормативних та технічних рішень, що регулюють Інтернет у КНР (обмежуючи доступ до інтернет-ресурсів, які можуть не відповідати цінностям Комуністичної партії Китаю).

США ЗАПРОВАДЖУЮТЬ ІНІЦІАТИВУ US CYBER TRUST MARK – МАРКУВАННЯ IOT

18 липня Адміністрація президента США оголосила про створення US Cyber Trust Mark – ініціативи з маркування Інтернету речей (IoT). Ініціативу має очолити Федеральна комісія зі зв'язку та Національний інститут стандартів і технологій. Вона має надати споживачам можливість зрозуміти чи відповідають продукти IoT базовому рівню кібербезпеки.

ЄС ЗРОБИВ ЩЕ ОДИН КРОК НА ШЛЯХУ УХВАЛЕННЯ ЗАКОНУ ПРО КІБЕРСТІЙКІСТЬ

19 липня Комітет з промисловості Європарламенту більшістю голосів підтримав проєкт Закону про кіберстійкість. Проєкт закону наразі проходить процедури внутрішнього погодження і має бути найближчим часом винесений на голосування депутатів Європарламенту.

ПУБЛІЧНІ КОМПАНІЇ МАЮТЬ РОЗКРИВАТИ ІНФОРМАЦІЮ ПРО ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ ПРОТЯГОМ ЧОТИРЬОХ ДНІВ – КОМІСІЯ З ЦІННИХ ПАПЕРІВ І БІРЖ США

27 липня стало відомо, що Комісія з цінних паперів і бірж США (SEC) прийняла нові правила щодо управління ризиками кібербезпеки. Ці нові правила вимагають від публічних компаній розкриття інформації про істотні інциденти кібербезпеки протягом чотирьох днів після атаки. Нові правила, прийняті SEC, вимагають від реєстрантів розкривати будь-який інцидент кібербезпеки, який реєстрант вважає суттєвим, а також описувати його істотні аспекти, масштаб та час інциденту, а також його можливий вплив.

КОМІСІЯ SOLARIUM ПРОПОНУЄ УРЯДУ США ВИЗНАЧИТИ КОСМІЧНУ СФЕРУ 17-М СЕКТОРОМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У липні експерт Security Intelligence звернув увагу на квітневу пропозицію міжпартійної Кібербезпекової комісії Solarium щодо необхідності додати космічну сферу як нового 17-го сектору критичної інфраструктури США. Комісія обґрунтовує це тим, що залежність США від космічних технологій та зв'язку з кожним роком зростає, а захист космічних систем знаходиться на незадовільному рівні: багато технологій є застарілими, інформація часто передається через незахищений зв'язок. Наразі це лише пропозиція, яка потребуватиме більш детального опрацювання федеральними органами США.

АДМІНІСТРАЦІЯ БАЙДЕНА НОМІНУВАЛА ГАРРІ КОКЕРА НА ПОСАДУ НАЦІОНАЛЬНОГО КІБЕРДИРЕКТОРА

25 липня американські ЗМІ повідомили, що Гаррі Кокер стане наступним Національним кібердиректором, якщо Сенат затвердить його кандидатуру. Ветеран розвідувальної спільноти обійме посаду керівника в офісі на постійній основі і візьме на себе виконання нової Національної стратегії кібербезпеки адміністрації Байдена. Вакансія в кіберофісі Білого дому залишається незаповненою вже протягом 5 місяців. Багато хто вважав Кембу Уолден, виконувачку обов'язків кібердиректора, ймовірним кандидатом, але вона, як повідомляється, відкликала свою кандидатуру через занепокоєння щодо суми особистого боргу, який вона накопичила.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

ЄС І США ДОМОВИЛИСЬ ПРО ПЕРЕДАЧУ ДАНИХ ЧЕРЕЗ АТЛАНТИКУ

10 липня Європейська комісія прийняла так зване рішення про адекватність, визнаючи США країною, яка належним чином захищає персональні дані європейців. Тому була підписана угода між США та ЄС щодо передачі даних, відома як EU-U.S. Data Privacy Framework. Вона відновлює можливість трансатлантичного обміну даними, яка лежить в основі багатомільярдної цифрової торгівлі після того, як Верховний суд ЄС скасував дві попередні угоди через побоювання шпигунства з боку спецслужб США.

Міністерство юстиції США також оголосило, що завершило виконання своїх зобов'язань згідно з Указом Президента Байдена від жовтня 2022 року, який обмежив доступ розвідувальних агенцій США до цифрової інформації європейців, і створив удосконалений, більш незалежний механізм правового захисту для європейців.

Разом з тим, активіст захисту конфіденційності Макс Шремс, який був автором позовів, що призвели до скасування двох попередніх угод, сказав, що він, ймовірно, оскаржить нову угоду в суді до кінця серпня. Він очікує, що його скарга надійде до Європейського суду на початку 2024 року.

ЗАПИТАННЯ ТА ВІДПОВІДІ: КОНФІДЕНЦІЙНІСТЬ ДАНИХ МІЖ ЄС І США

10 липня Європейська комісія опублікувала роз'яснення рішення про адекватність щодо трансатлантичної передачі даних.

НОВІ КІБЕРЗОБОВ'ЯЗАННЯ СОЮЗНИКІВ ПО НАТО: ЩО ПРО НИХ ВІДОМО

Під час саміту НАТО у Вільнюсі 11-22 липня союзники погодилися прийняти ряд нових зобов'язань щодо кібербезпеки. Суть цих зобов'язань не уточняється, а самі документи засекречені. Разом з тим, відкриті документи дають уявлення про прийняті рішення. Офіційний текст Комюніке Вільнюського саміту повторює позицію Стратегічної концепції альянсу (2022), що «кіберпростір є простором протистояння у будь-який час» і є предметом уваги НАТО не лише в умовах міжнародного збройного конфлікту. У ньому також повторюється доктрина НАТО про те, що «сукупний набір зловмисних дій у кіберпросторі може досягти рівня збройного нападу та може змусити Північноатлантичну раду застосувати статтю 5».

І хоча текст документа під назвою «Концепція посилення довгострокового внеску кібернетичних засобів у загальну позицію стримування та оборони НАТО» лишається засекреченим, з попередньої комунікації відомо, що йдеться про посилення ролі військових кіберзахисників у мирний час разом із механізмами інтеграції можливостей приватного сектору в національні оборонні можливості союзників. На прикладі діяльності таких компаній, як Microsoft та Google в Україні, йдеться про необхідність більш структурованої взаємодії з приватним сектором.

ПРЕДСТАВНИК НАТО КРІСТІАН-МАРК ЛІФЛЕНДЕР ПРО ТЕ, ЯК АЛЬЯНС МОЖЕ ЗАЙНЯТИ «ПРОАКТИВНУ» ПОЗИЦІЮ У КІБЕРСФЕРІ

В інтерв'ю The Record напередодні саміту НАТО голова відділу кібер- та гібридної політики НАТО Крістіан-Марк Ліфлендер сказав, що він стурбований тим чи не схожий Захід на метафоричну жабу в окропі серед зростаючої кількості кібератак. Замість того, щоб вживати заходів, які б зупинили це зростання, він каже, що здається, що «ми начебто стримуємо самі себе».

В інтерв'ю пан Ліфлендер розповідає про плановані рішення НАТО щодо кіберсфери під час Вільнюського саміту, про уроки російської агресії проти України і в кіберсфері та роль приватного сектора. Також він закликає до більш рішучих дій.

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

КИТАЙСЬКА КАМПАНІЯ КІБЕРШПИГУНСТВА ПРОТИ СХІДНОЄВРОПЕЙСЬКИХ УРЯДІВ

У звіті, опублікованому 4 липня, компанія Checkpoint Research повідомила, що протягом кількох останніх місяців відстежує діяльність китайського зловмисного актора, націленого на міністерства закордонних справ і посольства в Європі. У поєднанні з іншими діями Китаю, про які раніше повідомляла Check Point Research, це стало проявом більш масштабної тенденції в китайській екосистемі, яка вказує на перехід до таргетування європейських юридичних осіб з акцентом на тих, що залучені у зовнішній політиці.

Діяльність, описана у звіті, націлена на державні установи у Східній Європі – в Україні, Чеській Республіці, Угорщині, Словаччині та Великій Британії, а також у Франції та Швеції. Ця конкретна кампанія була активна принаймні з грудня 2022 року та, ймовірно, є прямим продовженням кампанії, про яку повідомлялося раніше, приписуваної RedDelta (а також певною мірою Mustang Panda).

У кампанії використовуються нові методи доставлення для розгортання (зокрема – HTML Smuggling) нового варіанту PlugX. Хоча корисне навантаження залишається таким же як і в старих варіантах PlugX, методи його доставлення призводять до низького рівня виявлення, що донедавна допомагало кампанії залишатися поза увагою.

ІРАНСЬКЕ УГРУПУВАННЯ TA453 ПРОДОВЖУЄ СВОЮ КІБЕРШПИГУНСЬКУ КАМПАНІЮ ПРОТИ ЗАХІДНИХ ЕКСПЕРТІВ – PROOFPOINT

6 липня компанія Proofpoint оприлюднила результати свого чергового дослідження діяльності іранської хакерської групи TA453, яка пов'язана із розвідувальними службами Ірану. Вони розширюють ареал своїх операцій проти західних експертів та журналістів, що мають експертизу у питаннях Близького Сходу та іранської ядерної програми. Нові зусилля TA453 зосереджені на поширення вірусів для Mac платформи, прикриваючись фішинговими листами від імені британського аналітичного центру RUSI.

GHOSTWRITER ПРОВОДИТЬ ЗЛОВМИСНУ КАМПАНІЮ ПРОТИ ДЕРЖАВНИХ, ВІЙСЬКОВИХ ТА ЦИВІЛЬНИХ ОРГАНІЗАЦІЙ В УКРАЇНІ ТА ПОЛЬЩІ – ДЕТАЛЬНИЙ АНАЛІЗ ВІД CISCO TALOS

13 липня кібербезпекова компанія Cisco Talos оприлюднила своє детальне дослідження кількох зловмисних кампаній, які проводяться проти державних установ, військових організацій і цивільних користувачів в Україні та Польщі. Компанія триває від квітня 2022 року. Українська група CERT-UA також досліджувала діяльність ворожого угрупування та приписала її групі загроз UNC1151 (як частину операційної діяльності GhostWriter). Дослідження показує багатоетапний ланцюг зараження, ініційований шкідливими документами Microsoft Office, найчастіше з використанням форматів файлів Microsoft Excel і PowerPoint. Основним корисним навантаженням є віруси для віддаленого доступу AgentTesla (RAT), Cobalt Strike і njRAT.

ПРОГРАМА-ВИМАГАЧ BLACKCAT ПРОСУВАЄ COBALT STRIKE ЧЕРЕЗ ПОШУКОВІ ОГОЛОШЕННЯ WINSCP – TREND MICRO

російськомовна банда вимагачів BlackCat (також відома як ALPHV) використовує зловмисну рекламу, щоб обманним шляхом змусити жертв встановити шкідливі версії програми для передачі файлів WinSCP. За результатами дослідження, опублікованого Trend Micro, «зараження починається, коли користувач шукає WinSCP Download у пошуковій системі Bing. Шкідлива реклама програми WinSCP відображається над результатами звичайного пошуку. Оголошення веде на підозрілий вебсайт із посібником з використання WinSCP для автоматизації передачі файлів. З цієї першої сторінки користувач перенаправляється на клоновану вебсторінку завантаження WinSCP (winsccp[.]com). Коли користувач вибирає кнопку «Завантажити», файл ISO завантажується із зараженої вебсторінки WordPress».

ІНСТРУМЕНТ DDOSIA ATTACK РОЗВИВАЄТЬСЯ ТА АТАКУЄ КІЛЬКА СЕКТОРІВ, ЗАПРОВАДЖУЮЧИ ШИФРУВАННЯ

Як 2 липня повідомило видання The Hacker News, зловмисні актори, що стоять за інструментом DDoSia, розробили версію, яка містить новий механізм для отримання списку цілей, щоб засипати їх небажаними HTTP-запитами у спробах їх зламати.

Компанія з кібербезпеки Sekoia описала цей механізм в технічному описі.

DDoSia приписують проросійській хакерській групі під назвою NoName(057)16. Інструмент атаки був запущений у 2022 році та став наступником ботнету Bobik, призначеного для проведення DDoS атак проти цілей, розташованих переважно в Європі, а також в Австралії, Канаді та Японії.

СКЛАДНЕ ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ІРАНСЬКИХ ХАКЕРІВ НАЦІЛЕНО НА КОРИСТУВАЧІВ WINDOWS І MACOS

Proofpoint пов'язала іранського державного актора, відомого як TA453, з низкою нещодавніх фішингових атак, які заражають операційні системи Windows і macOS шкідливим програмним забезпеченням. «TA453 використовував різноманітних хмарних хостинг-провайдерів, щоб створити новий ланцюжок зараження, який розгортає нещодавно ідентифікований бекдор PowerShell GorjolEcho», – йдеться у звіті компанії від 6 липня.

TA453, також відомий під назвами APT35, Charming Kitten, Mint Sand Storm і Yellow Garuda, – це група загроз, пов'язана з Корпусом вартових іранської ісламської революції (IRGC), яка діє принаймні з 2011 року.

ДВІ ШПИГУНСЬКІ ПРОГРАМИ В GOOGLE PLAY, ЯКІ МАЮТЬ 1,5 МІЛЬЙОНІВ КОРИСТУВАЧІВ, НАДСИЛАЮТЬ ДАНІ КИТАЮ

Згідно зі звітом компанії Pradeo, опублікованим 6 липня, дві програми для керування файлами в магазині Google Play є шпигунськими програмами, що ставить під загрозу конфіденційність і безпеку 1,5 мільйона користувачів Android. Ці програми таємно надсилають конфіденційні дані користувачів на шкідливі сервери в Китаї.

Обидві шпигунські програми, а саме File Recovery і Data Recovery (com.spot.music.filedate), встановлена понад один мільйон разів, і File Manager (com.file.box.master.gkd), встановлена понад 500 000 разів, розроблені однією групою. Попри їхні твердження у Google Play Store, де обидві програми запевняють користувачів, що не збирають дані, система аналітики Pradeo виявила, що вони збирають різну особисту інформацію без відома користувачів. Викрадені дані включають списки контактів, медіафайли (зображення, аудіофайли та відео), місцеперебування в реальному часі, код країни мобільного зв'язку, інформацію про оператора мережі, код мережі провайдера SIM-карти, версію операційної системи, марку та модель пристрою.

MICROSOFT ЗАПОБІГЛА КИТАЙСЬКІЙ КІБЕРАТАЦІ, СПРЯМОВАНІЙ НА УРЯДИ ЗАХІДНОЇ ЄВРОПИ

Корпорація Microsoft 11 липня оголосила, що відбила кібератаку, організовану китайським державним актором, спрямовану на два десятки організацій, серед яких також і державні установи країн Західної Європи. Атаки почалися 15 травня 2023 року і мали на меті отримання конфіденційних даних. Microsoft приписала кампанію групі Storm-0558, характеризувавши її як державну активну групу, що базується в Китаї та таргетує урядові установи в Західній Європі.

«Вони в основному займаються шпигунством, крадіжкою даних і отриманням доступу до облікових даних», – заявили в Microsoft. «Відомо також, що для доступу до облікових даних вони використовують спеціальні шкідливі програми, які Microsoft відстежує як Cigril і Bling».

БІЛИЙ ДІМ ЗАЯВИВ, ЩО КИТАЙСЬКІ ХАКЕРИ ЗЛАМАЛИ ЕЛЕКТРОННУ ПОШТУ АМЕРИКАНСЬКИХ УРЯДОВЦІВ

12 липня Білий дім підтвердив, що китайські хакери отримали доступ до електронної пошти міністра торгівлі Джини Раймондо та офіційних осіб Державного департаменту США через вразливість у системах електронної пошти Microsoft.

Раймондо є однією із найбільш голосних противників Пекіна в адміністрації Байдена та відіграє важливу роль у формуванні політики щодо Китаю. Вона допомогла провести Закон про мікросхеми (Chips Act) через Конгрес і через свій департамент відповідає за нагляд за так званим «списком організацій», який класифікує іноземні підприємства, яким заборонено імпортувати американські технології без попереднього дозволу.

Злам стався всього за кілька тижнів до того, як держсекретар Ентоні Блінкен приїхав до Пекіна в червні для переговорів про відносини та торгівлю між Китаєм та США.
Цей інцидент привернув увагу американських сенаторів, які надіслали листа до Державного департаменту, в якому, серед іншого, підіймають питання залежності уряду США від послуг компанії Microsoft.

НОВИЙ ЗВІТ БРИТАНСЬКОЇ РОЗВІДКИ ПОПЕРЕДЖАЄ, ЩО КИТАЙСЬКІ УРЯДОВІ ХАКЕРИ «ЧАСТО» АТАКУЮТЬ ДЕПУТАТІВ

Згідно зі звітом Комітету з розвідки та безпеки (ISC), опублікованому 13 липня, британське агентство радіоелектронної розвідки GCHQ помітило, що китайські державні хакери «часто» атакують британських парламентаріїв. У звіті також встановлено, що відповідь Британії на ці загрози національній безпеці була неадекватною.

Звіт містить попередження, що підхід Китаю до кібероперацій став витонченішим і є частиною стратегії «всієї держави», яка націлена на нинішніх і колишніх держслужбовців. ISC підкреслив свою стурбованість щодо розвитку кіберможливостей Китаю, наголошуючи, що вони потенційно можуть здійснити кібератаку на інфраструктуру Великобританії.

ЧЕРЕЗ НЕПРАВИЛЬНЕ НАПИСАННЯ ДОМЕНУ «.MIL» МІЛЬЙОНИ ЧУТЛИВИХ ДОКУМЕНТІВ СКЕРОВУВАЛИСЬ ДО МАЛІ

18 липня стало відомо, що внаслідок помилки із неправильним написанням суфіксів військових електронних адрес («.ML» замість «.MIL») мільйони електронних листів із конфіденційною інформацією Міністерства оборони США були спрямовані до африканської країни Малі. У результаті було розкрито дипломатичні документи, податкові декларації, паролі та деталі поїздок вищих офіцерів. Міноборони США наполягає, що серед документів не було документів з грифом таємності – лише з чутливими даними.

REUTERS ОПУБЛІКУВАВ ПЕРЕЛІК КИТАЙСЬКИХ УГРУПОВАНЬ, ЯКІ ЗВИНУВАЧУЮТЬСЯ У ХАКЕРСЬКИХ АТАКАХ ПРОТИ США ТА ІНШИХ КРАЇН

21 липня агенція Reuters опублікувала частковий перелік та опис китайських хакерських угруповань, які було виявлено останнім часом. Агенція наголошує, що на думку дослідників, переважна більшість китайських хакерських груп мають державну підтримку, хоча Китай це і заперечує.

НОРВЕГІЯ ПОВІДОМИЛА, ЩО IVANTI ZERO-DAY ВИКОРИСТОВУВАВСЯ ДЛЯ ЗЛОМУ ДЕРЖАВНИХ IT-СИСТЕМ

24 липня Управління національної безпеки Норвегії (NSM) підтвердило, що зловмисники використали вразливість нульового дня в Endpoint Manager Mobile (EPMM) від Ivanti, щоб зламати програмну платформу, яка використовується 12 міністерствами країни. Норвезька організація безпеки та обслуговування (DSS) заявила, що кібератака не торкнулася офісу прем'єр-міністра Норвегії, міністерства оборони, міністерства юстиції та міністерства закордонних справ.

Норвезький орган захисту даних (DPA) також був повідомлений про інцидент, що є індикатором, що хакери вірогідно отримали доступ до конфіденційних даних та/або викрали їх зі зламаних систем.

В ІНДІЇ СТАВСЯ МАСОВИЙ ВИТІК ПЕРСОНАЛЬНИХ ДАНИХ ВАКЦИНОВАНИХ ГРОМАДЯН

24 липня стало відомо про масовий витік персональних даних індійського порталу вакцин CoWIN. Хоча Національне управління охорони здоров'я певний час заперечувало факт витоку, однак у липні серед масиву даних опинились і персональні дані керівника Національного управління. Він включав: імена, національні ідентифікаційні номери Aadhaar, номера мобільних телефонів, ідентифікаційні номери виборців, паспорти та статус вакцинації проти COVID. Експерти закликають індійський уряд поставитись уважніше до питань кібербезпеки систем, які накопичують великі обсяги персональних даних громадян.

РОСІЙСЬКІ ХАКЕРИ ЗДІЙСНИЛИ КІБЕРАТАКУ ПРОТИ ЦЕНТРАЛЬНОГО ПОРТАЛУ ДЕРЖПОСЛУГ КЕНІЇ

29 липня уряд Кенії підтвердив, що зловмисникам вдалось атакувати центральний портал держпослуг Кенії – eCitizen. Через нього громадяни можуть отримати до 5000 державних послуг. Протягом кількох днів користувачі скаржилися на труднощі з доступом до послуг на порталі, зокрема:

- заяви на відновлення паспорта;
- оформлення електронних віз для іноземців;
- видача водійських прав;
- деякі банківські послуги;
- сервіс мобільних грошей M-Pesa для здійснення платежів у магазинах, громадському транспорті, готелях та на інших платформах.

Попередньо збій стався внаслідок DDoS-атаки здійсненою групою Anonymous Sudan. Хоча група відкидає свою російську приналежність, але більшість її дій афільовані з російським злочинним угрупуванням Killnet.

ДО 11 МІЛЬЙОНІВ ЛЮДЕЙ ПОСТРАЖДАЛИ ВІД ЗЛАМУ MOVEIT У КОМПАНІЇ MAXIMUS, ЯКА ЗАЛУЧЕНА У НАДАННІ ДЕРЖАВНИХ ПОСЛУГ США

Станом на 27 липня вважається, що понад 500 організацій та установ постраждали від вразливості програмного забезпечення для передачі файлів MOVEit, про злам якої стало відомо минулого місяця. Однією з нещодавно розкритих жертв є Maximus, підрядник державних послуг США. Maximus розкрив інцидент у формі 8-K від 26 липня до Комісії з цінних паперів і бірж США (SEC), зазначивши, що злам вплинув на особисті дані, що належать від восьми до 11 мільйонів осіб. Бухгалтерська компанія Deloitte також підтвердила, що стала жертвою атаки з використанням MOVEit.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

МОРСЬКА ПІХОТА США ЗБІЛЬШУЄ БОНУСИ ПРИ ПІДПИСАННІ КОНТРАКТУ ДЛЯ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

Третього липня стало відомо, що Морська піхота США значно підвищила бонуси при підписанні контракту для нових фахівців з кібербезпеки. Тепер ця сума становить 15000 доларів (проти 5000 які були оголошені у жовтні 2022 року). На цей бонус можуть розраховувати представники п'яти спеціальностей в яких зараз найбільше відчуває потребу корпус Морської піхоти. Це стало відповіддю на необхідність розширити сферу діяльності Морської піхоти США і на кіберпростір.

ВІД MICROSOFT ВИМАГАЮТЬ РОЗШИРИТИ ДОСТУП КОРИСТУВАЧІВ ДО ДАНИХ, ЯКІ МОЖУТЬ БУТИ ВИКОРИСТАНІ В ІНТЕРЕСАХ ЇХ КІБЕРБЕЗПЕКИ

У липні 2023 року, після успішної кібератаки китайських хакерів проти ряду урядових структур, одразу декілька фахівців з кібербезпеки та американських законодавців розпочали кампанію щодо Microsoft, Вони вимагали, щоб змінили правила щодо доступу до даних, які користувачі продуктів можуть використати в інтересах власної кібербезпеки. Зокрема, мова йде про дані, які наразі доступні лише для преміум користувачів, і які відкривають доступ до інформації, яка може бути використана для розслідування кіберзлочинів. Сенатор США Рон Уайден підкреслив, що Microsoft повинна запропонувати всім своїм клієнтам повні можливості криміналістичної експертизи, бо інакше «стягувати з людей плату за преміум-функції, необхідні для того, щоб їх не зламали, це все одно, що продати автомобіль, а потім стягувати додаткову плату за ремені безпеки та подушки безпеки». Вже 20-го липня Microsoft повідомила, що зробить безкоштовними цілу низку інструментів цифрового аудиту.

ЗБІЛЬШУЄТЬСЯ КІЛЬКІСТЬ АТАК, ДЕ ВИКУП ВИМАГАЄТЬСЯ ЗА НЕРОЗГОЛОШЕННЯ ВИКРАДЕНИХ ДАНИХ – CISCO TALOS

26 липня фахівці Cisco Talos оприлюднили оцінки зловмисної кіберактивності у другому кварталі 2023 року. Нова тенденція – істотне зростання кількості інцидентів, де зловмисники не шифрували дані жертви, а вимагали викуп за нерозголошення викрадених даних. Це не новий тип атаки чи зловмисної діяльності, але він істотно зростає. На думку Cisco Talos це може бути пов'язано із все більшими зусиллями як бізнесів, так і правоохоронних органів у протидії саме вірусам-шифрувальникам.

УРЯД США МАЄ ПРИШВИДШИТИ ПРОЦЕС ПЕРЕХОДУ НА ХМАРНІ РІШЕННЯ ДЛЯ КРАЩОЇ БЕЗПЕКИ – CSIS

28 липня відомий експерт з міжнародної кібербезпеки Дж. Льюіс оприлюднив позиційний матеріал про важливість переходу організацій федерального уряду на хмарні рішення. Він підкреслює, що на підтримку застарілих (і часто погано захищених) IT-систем становить понад 50 млрд на рік, а деякі з цих систем створені більш ніж 50 років тому. Він пропонує низку кроків (в т.ч. - в співпраці з CISA та NIST) до яких має вдатись федеральний уряд аби швидше та ефективніше впроваджувати хмарні технології.

NSA ТА CISA ВИПУСТИЛИ СПІЛЬНУ ОЦІНКУ ЗАГРОЗ ТА ВИКЛИКІВ ПРИ НАРІЗЦІ (SLICING) 5G МЕРЕЖ

17 липня NSA та CISA оприлюднили свої оцінки щодо окремих форм розгортання 5G мереж (Slicing). Оцінка надає учасникам ринку ліпше розуміння, що таке slicing 5G мереж, як вони мають безпечно розгортатись, підтримуватись, а також ознайомити з основними векторами загроз для пом'якшення яких наведено найкращі галузеві практики.

CISA РОЗВИВАЄ МЕРЕЖУ ДАШБОРДІВ CDM В ФЕДЕРАЛЬНИХ ВІДОМСТВАХ США

21 липня CISA опублікувала матеріал, в якому описує проміжні результати впровадження у федеральних відомствах дашбордів CDM (Continuous Diagnostics and Mitigation). Зараз 23 федеральних відомства поєднані в єдину мережу, що дозволяє CISA швидше (майже в режимі реального часу) реагувати на загрози (наприклад, MOVEit Transfer) з якими зіштовхуються ці відомства. CISA вже двічі використовувала цю мережу для швидкого реагування на інциденти та попередження відомств про загрози в їх мережах. Передбачається, що ця взаємодія в найближчі роки стане ще глибшою та динамічною.

СПИСОК БАЖАНЬ ЩОДО КІБЕРБЕЗПЕКИ НАПЕРЕДОДНІ САМІТУ НАТО

У статті, опублікованій напередодні саміту НАТО у Вільнюсі, аналітик Security Week Кевін Таунсенд закликає до більш об'єднаного підходу НАТО щодо питань кібербезпеки. Розуміючи складнощі, що їх становить різниця у технологічному розвитку членів Альянсу та недовіра, що може виникати між ними завдяки складності атрибуції, він вважає, що кіберпростір був би безпечнішим, якби існував такий же сильний альянс з кібербезпеки НАТО, як військовий альянс НАТО.

Він пропонує створити Кіберкомандування НАТО, яке б керувалося досвідом Кіберкомандування США (USCYBERCOM), яке має три основні місії: захист мереж і систем Міністерства оборони, проведення наступальних кібероперацій і побудова кіберпартнерств.

ПОЛОВИНА ЗЛАМАНИХ ОРГАНІЗАЦІЙ НЕ БАЖАЮТЬ ЗБІЛЬШУВАТИ ВИТРАТИ НА БЕЗПЕКУ, ПОПРИ РІЗКЕ ЗРОСТАННЯ ЦІНИ ЗЛАМУ – IBM

24 липня IBM опублікувала звіт про вартість витоку даних за 2023 рік, у якому йдеться про те, що середня вартість витоку даних у 2023 році становила 4,5 мільйона доларів. Дослідники зазначають: «Це на 2,3% більше, ніж у 2022 році, коли витрати становили 4,35 мільйона доларів США. У довгостроковій перспективі середня вартість зросла на 15,3% з 3,86 млн доларів США у звіті за 2020 рік».

Дослідження показало, що хоча 95% досліджуваних організацій зазнали більше ніж одного зламу, вони з більшою ймовірністю перекладуть ціну інциденту на споживачів (57%), ніж збільшать інвестиції в безпеку (51%).

Автори звіту також виявили, що жертви атак програм-вимагачів часто заощаджували значні суми грошей, якщо вони залучали до реагування правоохоронні органи. Вони заощадили в середньому 470 000 доларів США на зламі порівняно з тими, хто вирішив не залучати правозастосування. Попри цю потенційну економію, 37% досліджених жертв програм-вимагачів правоохоронців не залучали.

США ВІДСТАЮТЬ У СТАНДАРТАХ ШИФРУВАННЯ – І ЦЕ ГЛОБАЛЬНА ПРОБЛЕМА

На думку експерта у галузі високопродуктивних обчислень, зберігання та безпеки Генрі Ньюмана, Національний інститут стандартів і технологій США (NIST) дуже відстає у питаннях валідації FIPS 140-3 і розробки постквантової криптографії, і це може перетворитися на кризу глобального масштабу. У своїй колонці для eSecurity Planet він привертає увагу до цієї проблеми та пояснює її значення і висловлює сподівання, що її можна вирішити в рамках імплементації Національної стратегії кібербезпеки США.

FraudGPT: ЗЛОВМИСНИЙ АВАТАР ChatGPT

Netenrich повідомила 25 липня, що у дарквеб з'явився ще один шкідливий генеративний інструмент ШІ. Бот під назвою FraudGPT призначений для написання шкідливого коду, створення фішингових сторінок, написання шахрайських електронних листів тощо. Інструмент був запущений 23 липня і є доступним для використання за 200 доларів на місяць або 1700 доларів на рік.

Про запуск подібного інструменту WormGPT 13 липня повідомляла Slashnext. Його зловмисники використовують для компрометації корпоративних листів.

5. КРИТИЧНА ІНФРАСТРУКТУРА

ВЕЛИКІ ВИРОБНИКИ ІТ-ОБЛАДНАННЯ СТВОРЮЮТЬ NETWORK RESILIENCE COALITION

27 липня було повідомлено, що 11 членів-засновників (включаючи Cisco, Intel, AT&T, Broadcom і Fortinet) створили Network Resilience Coalition – коаліцію, що має на меті об'єднати постачальників технологій, експертів із безпеки та мережевих операторів, аби розв'язати проблему впровадження оновлень програмного та апаратного забезпечення. Майбутній Закон ЄС «Про кіберстійкість» вимагатиме від постачальників таких продуктів чіткого визначення очікуваної «тривалості життя» їх продукту, протягом якого компанія зобов'язана підтримувати його протягом всього життєво циклу, випускаючи оновлення безпеки весь цей час.

НЕВІДОМА APT ГРУПА НАЦІЛИЛАСЬ НА ВИКОРИСТАННЯ ДВОХ ВРАЗЛИВОСТЕЙ В ПРОДУКТАХ ROCKWELL AUTOMATION

13 липня було повідомлено, що ще невідома APT група намагається використати дві вразливості в продуктах Rockwell Automation, що може дозволити зловмиснику блокувати або викрадати дані, що проходять через певні пристрої виробництва Rockwell – 1756 EN2, EN3 та EN4.

В ПРОДУКТІ GE CIMPLICITY ВИЯВЛЕНО ВРАЗЛИВІСТЬ, СХОЖУ НА ТУ, ЯКОЮ КОРИСТУВАЛАСЯ ГРУПА SANDWORM

19 липня стало відомо про виявлення понад 10 вразливостей у продукті Cimplicity компанії GE. Кожну з вразливостей можна використати для виконання довільного коду, змусивши законного користувача відкрити спеціально створений файл проєкту .cim. Атака схожого типу нагадує експертам атаки, здійснені десять років тому російською Sandworm проти енергетичного сектору України.

КРИТИЧНА ІНФРАСТРУКТУРА ТА ХМАРА: ДЕРЖАВНА ПОЛІТИКА ЩОДО НОВИХ РИЗИКІВ – ЗВІТ DFRLAB

У звіті, опублікованому 10 липня, DFRLab розглядає ризики, які в собі несе широке використання хмарних технологій з боку об'єктів критичної інфраструктури та пропонує створити урядові структури нагляду, відповідні новій ключовій ролі хмари, а саме офіси управління хмарою.

Дослідники пропонують розмістити згадані вище офіси в секторальних агентствах з управління ризиками (SRMA), які наразі керують ризиками кібербезпеки в рамках критичної інфраструктури. А також наділити їх повноваженнями досліджувати та оцінювати залежність сектора від хмарних обчислень, визначати найкращі практики для їх впровадження та розглядати секторальні ризики та потреби. Офіси також матимуть користь від розвитку професійних знань у галузі хмарної безпеки на базі SRMA без необхідності створювати нові установи з нуля.

Окрім офісів управління хмарою, у звіті також висувається ідея створення нового органу для безпосереднього нагляду за самим хмарним сектором.

6. АНАЛІТИЧНІ ОЦІНКИ

ДОСЛІДНИКИ З TREND MICRO ПРЕДСТАВИЛИ ДЕТАЛЬНИЙ АНАЛІЗ НОВОГО RANSOMWARE BIG HEAD

7 липня дослідники з Trend Micro оприлюднили детальний аналіз нового ransomware Big Head, який з'явився на початку травня 2023 року. Наразі дослідники не змогли ідентифікувати зловмисного актора, який стоїть за цим ransomware, але Big Head демонструє унікальну поведінку під час процесу шифрування. Наприклад, відображає екран оновлення Windows, коли він шифрує файли, щоб ввести користувачів в оману та фактично блокувати їх на їхніх машинах, перейменовуючи зашифровані файли за допомогою кодування Base64, щоб забезпечити додатковий рівень обфускації.

РІЗНЕ РОЗУМІННЯ «ДЕЛІКАТНОЇ ІНФОРМАЦІЇ» УСКЛАДНЮЮТЬ ДЛЯ США ТА ЇЇ СОЮЗНИКІВ СПІВПРАЦЮ У СФЕРІ КІБЕРБЕЗПЕКИ – RAND

5 липня RAND Corporation опублікувало результати дослідження про ті перешкоди, які постають перед Міністерством оборони США (Департаментом повітряних сил) при налагоджені взаємодії із союзниками. У сфері кібербезпеки однією з важливих перешкод названо різне розуміння США та союзниками «делікатної інформації», якою сторони готові ділитись, а також те, що і в США, і у союзників не завжди вдається визначити центральну точку взаємодії з цього питання.

ІДЕЯ ДОДАТИ ХМАРНІ СЕРВІСИ ДО КАТЕГОРІЇ КРИТИЧНОЇ ІНФРАСТРУКТУРИ Є СУМНІВНОЮ З ТОЧКИ ЗОРУ РЕАЛЬНОЇ КІБЕРБЕЗПЕКИ – CSIS

17 липня аналітичний центр CSIS оприлюднив матеріал щодо оцінки ідеї додати операторів хмарних послуг як окремого сектору критичної інфраструктури в США. Авторка матеріалу (Їнуо Генг) вважає, що таке «просте» рішення може мати низку негативних наслідків для індустрії та не розв'яже ті задачі, задля яких може бути прийнято. На її думку, зусилля уряду мають бути спрямовані не так на більші вимоги до хмарних сервісів, як на підвищення навичок громадян правильно користуватись хмарними сервісами безпечно. При цьому підкреслюється, що громадяни дійсно зацікавлені в тому, аби бути впевнені, що самі хмарні сервіси захищені належним чином.

США МАЮТЬ ПЕРЕЙТИ ДО ПРАКТИЧНОГО ВПРОВАДЖЕННЯ КОНЦЕПЦІЇ СТІЙКОСТІ – CSIS

11 липня аналітики CSIS Емілі Гардінг та Сюзанна Сполдінг оприлюднили свої оцінки поточної кібербезпекової політики США. Вони вказують, що попри те, що у нових стратегічних документах концепція стійкості згадується все частіше, але практичні кроки по її впровадженню все ще не достатні, а базовий кібербезпековий підхід переважно залишається старим: блокування актуальних загроз замість розбудови спроможностей для продовження виконання функцій.

УЧАСТЬ ГРОМАДЯН ТА БІЗНЕСУ Є КРИТИЧНО ВАЖЛИВИМ ДЛЯ КІБЕРБЕЗПЕКИ БРИТАНІЇ – ЗВІТ NCSC UK

6 липня NCSC UK оприлюднив 6-й звіт Active Cyber Defense (ACD) (програма NCSC, яка складається із сукупності різних безкоштовних сервісів для громадян та бізнесу і яка має допомогти поліпшити кібербезпеку широких верст суспільства від найбільш типових загроз), в якому підкреслено, що роль громадян та бізнесу у звітуванні про кіберінциденти є ключовою для успішної мінімізації загроз. За даними звіту у 2022 році громадяни повідомили NCSC про 7,1 млн підозрілих листів. Завдяки цьому вдалось видалити майже чверть мільйона (235 000) шкідливих URL-адрес.

54% ЗАГРОЗ КІБЕРБЕЗПЕЦІ У СЕКТОРІ ОХОРОНИ ЗДОРОВ'Я СПРИЧИНЯЄ RANSOMWARE – ENISA

5 липня ENISA оприлюднило свій перший огляд кіберзагроз для сектору охорони здоров'я. Серед висновків звіту:

- програми-вимагачі становлять 54% загроз кібербезпеці у секторі охорони здоров'я;
- 53% всіх великих кіберінцидентів в ЄС припадають на сектор охорони здоров'я;
- російсько-українська війна призвела до сплеску DDoS-атак проросійських груп хактивістів на лікарні та органи охорони здоров'я на початку 2023 року;
- 43% інциденти призводять до значних наслідків для організацій охорони здоров'я, головним чином – до крадіжки даних.

NSA ТА CISA ПОПЕРЕДЖАЮТЬ ПРО ВРАЗЛИВІСТЬ ВЕБЗАСТОСУНКІВ

27 липня NSA та CISA оприлюднили безпековий бюлетень, в якому звертають увагу на проблему вразливості вебзастосунків. Звіт містить технічні відомості про вразливості IDOR (вразливості контролю доступу у вебдодатках, які дозволяють зловмисникам змінювати, видаляти або отримувати доступ до конфіденційних даних) і рекомендовані засоби пом'якшення загроз. Використання цих вразливостей може потенційно вплинути на будь-яку вебпрограму, включно з тими, які розгорнуті:

- локально в організації;
- програмне забезпечення як послуга (SaaS);
- інфраструктура як послуга (IaaS);
- приватних хмарах.

КІБЕРЗЛОЧИНЦІ ВСЕ БІЛЬШЕ СХОЖІ НА ТЕХНОЛОГІЧНІ СТАРТАПИ, НІЖ НА ХАКЕРІВ-ОДИНАКІВ

В статті для Infosecurity Magazine директорка Endpoint Security Research Меліса Бішопінг розглядає тривожну тенденцію, що формується у кіберзлочинному середовищі – дії суб'єктів загроз стають все більше схожими на професійні підприємства. В результаті організованого підходу і співпраці з іншими групами, вони стають більше схожими на технологічні стартапи, ніж на хакерів-одинаків, якими їх часто зображують. Результатом стають атаки, які обходять найдосконаліші служби безпеки та захисні дії урядів. Крім того, фінансовий вплив лише зростає – згідно з нещодавнім дослідженням IBM, середня вартість атаки програм-вимагачів у 2022 році становила 4,35 мільйона доларів, що на 2,6% більше, ніж у 2021 році, і майже на 13% з 2020 року, коли вона становила 3,86 мільйона доларів.

ЗВІТ BLACKFOG ПРО СТАН ПРОГРАМ-ВИМАГАЧІВ

Згідно з даними компанії BlackFrog, червень став другим за активністю місяцем 2023 року, під час якого було оприлюднено інформацію про 46 атак програм-вимагачів, не враховуючи жертв атаки MOVEit. Освіта та охорона здоров'я і надалі залишаються основними об'єктами нападу, з одинадцятьма та дев'ятьма атаками відповідно. Викрадення даних залишається обраною тактикою, оскільки кіберзлочинці продовжують зосереджуватися на вимаганні. Пластична хірургія Беверлі-Хіллз, Манчестерський університет і Reddit потрапили в заголовки, коли зловмисники погрожували опублікувати особисту інформацію, викрадену під час атак. Основним актором, у червні став Clop через атаку на MOVEit.

58% СІМЕЙСТВ ШКІДЛИВИХ ПРОГРАМ, ЯКІ ПРОДАЮТЬСЯ ЯК ПОСЛУГИ, Є ПРОГРАМАМИ-ВИМАГАЧАМИ

15 липня команда Kaspersky Digital Footprint Intelligence представила дослідження, яке показало, що програми-вимагачі є найпоширенішою шкідливою програмою як послуга (MaaS) за останні сім років.

Фахівці Касперського вивчили обсяги продажу різних сімей шкідливих програм, а також згадки, обговорення, публікації та пошукові оголошення в даркнеті та інших ресурсах щодо MaaS, щоб визначити найпопулярніші типи. Лідером виявилося програмне забезпечення вимагач або рансомвер. На нього припадало 58% усіх сімей, розповсюджених за моделлю MaaS між 2015 і 2022 роками.

НОВИЙ ПЛАН РЕАЛІЗАЦІЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ, ПРИЙНЯТИЙ БІЛИМ ДОМОМ, ПІДВИЩИТЬ КІБЕРСТІЙКІСТЬ

Стаття на NextGov містить короткий виклад змісту плану реалізації Стратегії кібербезпеки з коментарями аналітиків та посадовців. В ній підіймається питання відсутності постійного очільника Офісу національного кібердиректора та можливого впливу цього фактору на імплементацію Стратегії.

Серед перших кроків, про які заявила Кемба Волден, звернення до представників приватного сектору з проханням надати інформацію про суперечності у регуляторних нормах з метою їх усунення. Вона наголосила, що перш ніж запроваджувати зміни, необхідно почути голос стейкхолдерів. «Ми, уряд і приватний сектор, повинні нести відповідальність один перед одним, щоб досягти наших спільних цілей і спільної відповідальності за безпеку американців в Інтернеті», наголосила вона.

ПЛАН РЕАЛІЗАЦІЇ НАЦІОНАЛЬНОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ: ПОГЛЯД CYBER SECURITY INITIATIVE АТЛАНТИЧНОЇ РАДИ.

Аналізуючи план реалізації Національної стратегії кібербезпеки, Cyber Security Initiative Атлантичної ради відмічає три таких тенденції:

1. План містить конкретніший перелік дій, ніж сама стратегія, з корисним визначенням провідних і допоміжних агенцій, а також великою кількістю часових рамок. Призначаючи кожній дії визначений напрямок і строк виконання, а також включаючи новий номінальний розділ, який повністю присвячений оцінці ефективності та постійному повторенню, ONCD говорить про те, що План реалізації не стільки окремий текст, скільки основа для щорічного, повторюваного політичного процесу. Те, що багато віх лишаються нечітко визначеними, може бути менш важливим, ніж зобов'язання адміністрації переглядати план щороку, дозволяючи команді ONCD використовувати унікальне поєднання тематичної глибини та повноважень щодо перегляду бюджету.

2. Є явні перемоги. Значна увага приділяється програмному забезпеченню з відкритим вихідним кодом (OSS) і підтримці кібербезпеки в енергетичному секторі, і існує підсилений бюджетний стимул як для модернізації технологій, так і для досліджень у сфері кібербезпеки. Але є й втрачені можливості. Багато з найскладніших і революційних цілей стратегії були скорочені або повністю пропущені. Існує тривожна відсутність дій, спрямованих на зміну стимулів, що є однією з найважливіших цілей початкової стратегії.

3. Багато цілей, встановлених планом реалізації, мають часові рамки, що розтягуються до 2025 року. Через період невизначеності, викликаний переходом до наступної адміністрації, буде важко впоратися за найкращих обставин. Це ставить під загрозу ще більше найсміливіших ідей, які містяться у цьому плані, та викликає питання, як найкраще визначити пріоритети чи прискорити імплементацію перелічених.

ОЦІНКА ПОЛІТИЧНИХ МОТИВІВ АТАК ПРОГРАМ-ВИМАГАЧІВ

Дослідники зі Стенфордського університету Карен Нерші (Karen Nershi) та Шелбі Гроссман (Shelby Grossman) оприлюднили нове дослідження. Попри те, що атаки рансомвер традиційно вважаються аполітичними, нещодавні події свідчать про наявність зв'язків між деякими групами програм-вимагачів і російським урядом. Щоб краще зрозуміти цей зв'язок, дослідники створили набір даних про 4194 жертви програм-вимагачів, опублікованих у дарквеб з травня 2019 року по травень 2022 року.

У статті встановлено, що російські групи збільшували кількість атак перед виборами в кількох великих демократичних країнах. Також компанії, які згорнули діяльність у росії після вторгнення в Україну, частіше ставали цілями. Ці висновки свідчать про потенційну політичну мотивацію цих нападів. Аналіз витоку внутрішньої комунікації великої групи програм-вимагачів також показує зв'язки з кремлем. Автори стверджують, що російський уряд підтримує неформальну співпрацю з групами, забезпечуючи безпечну гавань від судового переслідування та отримуючи правдоподібне заперечення атак і доступ до кваліфікованих кіберакторів. Висновки свідчать про те, що рансомвер становить загрозу міжнародній безпеці, крім того, що функціонує як форма злочину.

КРИПТОЗЛОЧИННІСТЬ ЗАГАЛОМ ВПАЛА НА 65%, АЛЕ РЕНСОМВЕР МАТИМЕ ДУЖЕ УСПІШНИЙ РІК – CHINALYSIS

Згідно зі звітом Chainalysis, опублікованим 12 липня, злочинність, пов'язана з криптовалютою, знижується, але прибутки від застосування рансомвер зростають. Надходження від різноманітних форм злочинів, пов'язаних із криптовалютою, таких як хакерство та інше зловмисне програмне забезпечення, ринки даркнету, шахрайські магазини та шахрайство, зменшилися порівняно з аналогічним періодом минулого року. Лише програми-вимагачі збільшили дохід. Криптовалютні гаманці, пов'язані з групами програм-вимагачів, отримали майже 450 мільйонів доларів, що приблизно на 176 мільйонів доларів більше, ніж за той самий період минулого року.

СИСТЕМА ПІДРИВНИХ ДІЙ ГРУ – ДОСЛІДЖЕННЯ MANDIANT

У звіті, опублікованому 12 липня, Mandiant описує діяльність російського гру від початку повномасштабного вторгнення в Україну. З моменту вторгнення в лютому минулого року Mandiant відстежував підривні операції російської військової розвідки проти України, дотримуючись стандартної схеми з п'яти етапів.

Mandiant оцінює з помірною впевненістю, що ця стандартна оперативна концепція навмисно спрямована на те, щоб збільшити швидкість, масштаб та інтенсивність, з якою гру може проводити наступальні кібероперації, мінімізуючи при цьому ймовірність виявлення.

Тактичні та стратегічні переваги, які надає цей підхід, ймовірно, створені для застосування у швидкоплинному та жорсткому операційному середовищі. Mandiant вважає, що цей оперативний підхід може бути відображений у сценаріях майбутніх криз і конфліктів, коли існують вимоги щодо підтримки великих обсягів руйнівних кібероперацій.

КІБЕРОПЕРАЦІЇ ПІД ЧАС РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

13 липня Center for Strategic and International Studies опублікував дослідження щодо російської агресії в Україні, у якому дійшов трьох основних висновків:

«Кібероперації відіграватимуть допоміжну, а не вирішальну роль у великих війнах». Збір розвідувальних даних та оперативний обман, ймовірно, стануть найвидатнішим внеском кібербезпеки після початку військових дій.

«Війна залишатиметься продовженням політики іншими засобами і покладатиметься на більш відчутні наслідки насильства, ніж на невловимі наслідки компрометації інформаційних мереж». Оскільки боротьба загострюється вздовж спектру конфлікту, впевнені кінетичні ефекти матимуть перевагу перед невизначеними результатами кібероперацій.

«Переваги кібероперацій продовжують полягати в тому, що вони корисні як інструмент політичної війни, оскільки вони сприяють допороговим діям, які покладаються на приховану діяльність, пропаганду та стеження, але таким чином, що створює фундаментальну загрозу свободам людини».

CLOUDFLARE ПОВІДОМЛЯЄ ПРО СПЛЕСК СКЛАДНИХ DDOS-АТАК

Згідно з нещодавнім дослідженням, оприлюдненим Cloudflare 18 липня, хакерські групи, багато з яких розташовані в росії, завдали шкоди компаніям у другому кварталі цього року добре спланованими DDoS атаками.

Звіт Cloudflare показує, що загальна кількість DDoS-запитів з квітня по червень досягла 5,4 трильйона, що на 15% більше, ніж у першому кварталі цього року.

Попри зростання кількості атак у 2023 році, інциденти DDoS зменшилися порівняно з другим кварталом 2022 року, коли Cloudflare зафіксувала 8,3 трильйона запитів. За даними Cloudflare, кількість запитів вказує не на кількість «унікальних» атак, а на загальний обсяг DDoS-атак.

ОГЛЯД ПРОГРАМИ-ВИМАГАЧА CL0P

21 липня Fortinet опублікувала блог, в якому описує діяльність групи програм-вимагачів Cl0p, яка привернула значну увагу ЗМІ через злам великої кількості організацій, використовуючи донедавна невиправлену вразливість у MOVEit Transfer (CVE-2023-34362), яка використовується для керованої передачі файлів (MFT). Хоча немає доказів того, що зловмисник використовував шифрувальник у цьому конкретному інциденті, група викрала дані жертв і вимагала у них викуп в обмін на нерозкриття викраденої інформації.

Блог містить інформацію про діяльність групи програм-вимагачів Cl0p за останні кілька років.

ДОСЛІДЖЕННЯ COHESITY ПОКАЗУЄ, ЩО КОМПАНІЇ ГОТОВІ СПЛАЧУВАТИ ВИКУПИ ЧЕРЕЗ ПРОГАЛИНИ У КІБЕРСТІЙКОСТІ ТА ВІДНОВЛЕННІ ДАНИХ

25 липня Cohesity опублікувала звіт про ставлення компаній до ренсомвер. Під час дослідження було опитано 3409 спеціалістів з IT та безпеки з шести континентів відносно здатності їхніх організацій захистити себе від атак програм-вимагачів.

Порівнюючи прогноз кібербезпеки на 2023 рік і 2022 рік, 93% респондентів сказали, що вважають, що загроза атак програм-вимагачів для їхньої галузі зросла в 2023 році. Тривожно те, що майже половина респондентів (45%) підтвердили, що їхній бізнес став жертвою нападу вимагачів протягом останніх шести місяців. Респонденти також виявили, що можливості їхнього бізнесу щодо кібервідмовостійкості та безпеки даних відстають, причому 80% висловили занепокоєння щодо стратегії кіберстійкості їхньої організації та того, чи зможе вона «дати відповідь на сучасну ескалацію кібервикликів і загроз». Результати дослідження також показують, що 74% респондентів заплатили б викуп за відновлення своїх даних.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

ПОГЛИБЛЮЄМО СПІВПРАЦЮ З НАТО: УКРАЇНСЬКА ДЕЛЕГАЦІЯ ПІД ГОЛОВУВАННЯМ СЕКРЕТАРЯ НКЦК ВІДВІДАЛА ШТАБ-КВАРТИРУ АЛЬЯНСУ

Делегація представників основних суб'єктів забезпечення кібербезпеки України на чолі з секретарем Національного координаційного центру кібербезпеки, керівником служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталією Ткачук 6-7 липня 2023 року відвідала штаб-квартиру НАТО, Командування НАТО з операцій та Агенцію НАТО зі зв'язку та інформації у рамках проєкту з обміну знаннями С4 Трастового фонду Комплексного пакету допомоги НАТО – Україна. Українська делегація виступила з оглядовою презентацією про систему кібербезпеки України та уроки кібервійни, що триває, а також представила потреби та пропозиції щодо майбутньої співпраці з НАТО у сфері кібербезпеки.

Партнери відзначили злагоджену роботу усіх суб'єктів кібербезпеки України під час війни та наголосили на готовності розширювати підтримку та взаємодію з Україною у сфері кібербезпеки.

НА ЗАСІДАННІ НКЦК ОБГОВОРЕНО ПИТАННЯ ЩОДО РОЗБУДОВИ КІБЕРДИПЛОМАТІЇ ТА СТАНУ ВИКОНАННЯ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ

Заступник Секретаря Ради національної безпеки і оборони України Сергій Демедюк провів 22 засідання Національного координаційного центру кібербезпеки. Учасники засідання обговорили питання щодо розбудови кібердипломатії, стану виконання Стратегії кібербезпеки України та підвищення ефективності щорічного планування реалізації її завдань, а також про додаткові заходи кібербезпеки систем управління технологічними процесами на об'єктах критичної інфраструктури.

Учасники засідання підтримали пропозицію заступника Секретаря РНБО України щодо необхідності формування підходів до реалізації заходів у сфері кібердипломатії Міністерством закордонних справ України, а комунікації з міжнародними партнерами - за участю НКЦК та основних суб'єктів національної системи кібербезпеки для забезпечення узгодженої позиції. У цьому контексті обговорено питання щодо створення міжвідомчої робочої групи та відповідної цифрової платформи.

АПАРАТ РНБО УКРАЇНИ ЗАПОЧАТКУВАВ НАЦІОНАЛЬНИЙ КЛАСТЕР З ІНФОРМАЦІЙНОЇ СТІЙКОСТІ

З метою зміцнення стратегічних ресурсів державних органів у боротьбі з російською інформаційною агресією та протидії дезінформації Апарат РНБО України за підтримки Держдепартаменту США, Офісу зі спільного зменшення загрози, CRDF Global та за сприяння Міністерства закордонних справ України та Міністерства культури та інформаційної політики України започаткували Національний кластер з інформаційної стійкості.

Національний кластер з інформаційної стійкості – стратегічна координаційна платформа, покликана допомагати зацікавленим сторонам українського державного та приватного секторів визначати інструменти та методи, які росія використовує для поширення дезінформації, розробляти плани координації спільних дій, спрямованих на протидію шкідливим наративам, а також сприяти в організації тренінгів з інформаційної стійкості за підтримки міжнародних донорів та партнерів.

Під час першого засідання було обговорено ряд питань, які потребують детальнішої уваги та комунікації в їх втіленні. Зокрема розпочато публічну дискусію щодо методів протидії використання країною-агресором месенджера Telegram в інформаційній війні проти України. Адже сьогодні Telegram-канали стали одним з інструментів поширення російських фейків та дезінформації з-поміж українського населення.

УКРАЇНА ТА ЄВРОПЕЙСЬКИЙ СОЮЗ ЗМІЦНЮЮТЬ СПІВПРАЦЮ В БОРОТЬБІ З КІБЕРАГРЕСІЄЮ

Делегація представників основних суб'єктів забезпечення кібербезпеки України на чолі з секретарем Національного координаційного центру кібербезпеки 7 липня 2023 року в Брюсселі зустрілася з представниками Європейської служби зовнішньої діяльності (ЄСЗД), Генерального директорату з комунікаційних мереж, контенту і технологій (DG CONNECT) та ENISA. Українська делегація поділилася досвідом у протидії кіберагресії рф. Також обговорено питання збільшення рівня міжнародної кіберзлочинності через активне долучення зловмисних акторів з боку рф. У цьому контексті міжнародним партнерам було представлено ефективні заходи протидії, що вживаються Україною, зокрема поінформовано про впровадження системи фільтрації фішингових доменів Protective DNS.

Зустріч також стала платформою для обговорення організації третього раунду кібердіалогу між Україною та Європейським Союзом. Обговорено успіхи України та напрями подальшої гармонізації законодавства України із законодавством ЄС у сфері кібербезпеки.

НКЦК ПОГЛИБЛЮЄ СПІВПРАЦЮ З ЄС ТА США ЩОДО ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШІ У СФЕРІ КІБЕРБЕЗПЕКИ

Керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталія Ткачук та керівник Управління забезпечення діяльності НКЦК Сергій Прокопенко провели робочу зустріч з директором Інституту національної безпеки та протидії тероризму США, колишнім радником Президента США Джеймсом Бейкером,керівником департаменту національної та державної безпеки Консультативної місії Європейського Союзу в Україні Сеппо Рутсалененом та радником КМЄС з національної безпеки Максимом Будаковим.

Під час зустрічі обговорено питання використання технологій штучного інтелекту в інтересах національної безпеки. Сторони обмінялися думками щодо перспектив використання ШІ у сфері кібербезпеки, а також обговорили пріоритети і виклики, з якими стикається Україна у сфері кібербезпеки.

МІНЦИФРА І CYBERFAME GMBH СПІВПРАЦЮВАТИМУТЬ У СФЕРІ ЦИФРОВОЇ БЕЗПЕКИ

Міністерство цифрової трансформації та німецька компанія Cyberfame GmbH підписали меморандум про співпрацю у сферах цифровізації, цифрової безпеки, створення та функціонування програмного забезпечення, професійного розвитку із цифрової та кібербезпеки. Меморандум передбачає обмін досвідом, знаннями та напрацюваннями для підвищення цифрової стійкості й кіберзахисту. У межах взаємодії з Cyberfame GmbH планується проведення тренінгів як для технічних спеціалістів, так і для менеджерів державних установ.

Співпраця Мінцифри з Cyberfame GmbH дозволить значно посилити захищеність вебресурсів, забезпечити стійкість до спроб блокування або неавторизованого отримання доступу до даних.

ДЕРЖСПЕЦЗВ'ЯЗКУ РОЗПОЧАЛА СПІВПРАЦЮ З ІСПАНСЬКИМ НАЦІОНАЛЬНИМ ІНСТИТУТОМ КІБЕРБЕЗПЕКИ

Делегація Іспанського національного інституту кібербезпеки (INCIBE), підпорядкованого Міністерству економіки та цифрової трансформації через Державного секретаря з цифровізації та штучного інтелекту, на чолі з Генеральним директором Феліксом Барріо відвідала з офіційним візитом Держспецзв'язку.

Ключовим результатом візиту стало підписання Меморандуму про взаєморозуміння у сфері кіберзахисту та визначення перших кроків подальшої роботи. Співробітництво між органами буде зосереджене на обміні інформацією про кіберзагрози, а також рекомендаціями та передовими практиками з метою вдосконалення відповідних систем управління інцидентами, систем реагування на інциденти та відновлення після кіберінцидентів. Водночас особливу увагу приділятимуть законодавчим аспектам, інформаційно-комунікаційним технологіям стратегічного, технічного і наукового характеру.

УКРАЇНА ВКОТРЕ ВИСТУПИЛА НА ЩОРІЧНИХ НАВЧАННЯХ НАТО ІЗ ВЗАЄМОСУМІСНОСТІ – CWIX

У м. Бидгощ проходило щорічне навчання НАТО CWIX – Coalition Warrior Interoperability Exercise. Україна бере участь у CWIX як повноправний учасник та тестує свої спроможності на взаємосумісність з державами-членами НАТО з 2018 року. У цьому році Україну під час навчання представляли Центр інновацій Міноборони та представники Збройних Сил України.

Команда Центру інновацій змогла перевірити на взаємосумісність 4 протоколи обміну та частково виконати цілі 12 фокус-груп з 19 наявних на навчанні. Також під час навчань команда Центру інновацій успішно відпрацювала спільні тести на досягнення взаємосумісності із 12 системами з 10 країн та 3 системами, розробленими безпосередньо НАТО, в тому числі в різних комбінаціях передачі між ними даних.

Загалом цього року у навчання взяли участь 2200 учасників із 43 країн, було протестовано 406 унікальних спроможностей та проведено 22 тисячі тестів.

НКЦК ПРОВІВ ДВОДЕННИЙ CYBER COMMUNICATIONS WORKSHOP ДЛЯ КОМУНІКАЦІЙНИКІВ ДЕРЖАВНОГО СЕКТОРУ

Національний координаційний центр кібербезпеки при РНБО України за підтримки Державного департаменту США і Фонду цивільних досліджень та розвитку США 27-28 липня 2023 року провів тренінг для комунікаційників державного сектору Cyber Communications Workshop: комунікації для посилення національної кіберстійкості.

Cyber Communications Workshop спрямований на підвищення рівня професійних навичок комунікаційників державного сектору. У заході у форматі офлайн та онлайн взяли участь понад 150 представників суб'єктів кібербезпеки України, міністерств, державних установ, об'єктів критичної інфраструктури, ОВА та міських адміністрацій регіонів. Проведено лекції щодо кібергігієни, комунікації кіберінцидентів, фактчекінгу та протидії дезінформації, репутаційних та антикризових комунікацій та співпраці з медіа.

ФАХІВЦІ ДЕРЖСПЕЦЗВ'ЯЗКУ ПРОЙШЛИ НАВЧАННЯ В CYBERSECURITY SUMMER BOOTCAMP У ЛЕОНІ

Фахівці Держспецзв'язку взяли участь у навчальному таборі з кібербезпеки Cybersecurity Summer BootCamp 2023, який відбувся в місті Леон (Іспанія). Українські фахівці долучилися до семінарів та технічних воркшопів з теми кіберзахисту, зокрема, протидії сучасним кіберзагрозам, їх пошуку та своєчасного виявлення, а також моніторингу та підтримки безпеки критичної інформаційної інфраструктури. Значну увагу було приділено темі NIST CyberSecurity Framework та його компонентам.

Навчання допомогли фахівцям Держспецзв'язку здобути нові знання та на практичних кейсах розглянути роботу кращих європейських фахівців, вивчити європейський досвід та поділитися своїм. Цього року в CSBC взяли участь понад 300 учасників з 24 країн світу.

СБУ ЗНЕШКОДИЛА ПОТУЖНЕ ХАКЕРСЬКЕ УГРУПОВАННЯ, ЯКЕ «ЗЛАМУВАЛО» БАНКІВСЬКІ РАХУНКИ УКРАЇНЦІВ

Кіберфахівці Служби безпеки нейтралізували у Києві злочинну організацію, яка крала гроші з банківських рахунків українців. Задокументовано, що лише в одному з епізодів вони вкрали понад 10 млн грн з депозитного рахунку столичного нотаріуса. Ці гроші належали Фонду гарантування вкладів фізичних осіб та призначались для виплат потерпілим вкладникам ліквідованих банків.

За даними слідства, зловмисники створили шкідливе програмне забезпечення, яке давало їм доступ до електронних кабінетів вкладників одного з київських банків. Зловмисники перебувають під вартою. Їм загрожує до 12 років ув'язнення.

СБУ ПРИПИНИЛА РОБОТУ НЕЗАКОННОГО СЕРВІСУ, ЯКИЙ ДОЗВОЛЯВ РОСІЯНАМ АНОНІМНО ТЕЛЕФОНУВАТИ В УКРАЇНУ

Кіберфахівці Служби безпеки викрили ділків, які здійснювали перемаршрутизацію міжнародних дзвінків в Україну. Їхні послуги дозволяли будь-кому із-за кордону анонімно телефонувати в нашу державу. Цим каналом користувалися також росіяни, що створювало додаткову загрозу національній безпеці України.

За матеріалами слідства, ділки використовували PROXY-сервери, новітні технології IP-телефонії та спеціалізоване програмне забезпечення. Це дозволяло обходити центри комутації українських операторів і робило всі дзвінки, що проходили через «сервіс», невидимими для українських правоохоронних органів. За наявними даними, щотижня ця незаконна діяльність приносила ділкам до 50 тис. доларів США. Зловмисникам загрожує до 15 років позбавлення волі.

КІБЕРПОЛІЦІЯ ВИКРИЛА ЗЛОВМИСНИКА, ЯКИЙ СТВОРЮВАВ ТА ПОШИРЮВАВ ДИТЯЧУ ПОРНОГРАФІЮ ЗА УЧАСТЮ МОЛОДШОЇ СЕСТРИ

Готові матеріали він публікував на форумах у DarkNet. Кіберполіцейські під час моніторингу інтернет-мережі виявили контент щодо сексуальної експлуатації дитини. 19-річний молодик створював протиправний контент за участю своєї 11-річної сестри. Надалі такі матеріали він розповсюджував на форумах анонімного сегмента мережі Інтернет – «DarkNet». Зловмисника затримано. За виготовлення і збут дитячої порнографії передбачено від восьми до дванадцяти років позбавлення волі.

КІБЕРПОЛІЦІЯ ВИКРИЛА ОРГАНІЗАТОРІВ БОТОФЕРМ, ЯКІ ПОШИРЮВАЛИ ВОРОЖУ ПРОПАГАНДУ ТА ЗАЙМАЛИСЯ ІНТЕРНЕТ-ШАХРАЙСТВАМИ

Фігуранти використовували фейкові акаунти у соцмережах для проведення інформаційно-психологічних операцій агресора, виправдання дій окупантів, розповсюдження протиправного контенту, поширення персональних даних і шахрайства тощо.

Кіберполіцейські встановили, що зловмисники використовували спеціальне обладнання та програмне забезпечення для реєстрації тисяч облікових записів ботів у різних соцмережах із подальшим запуском реклами, що порушувала норми та законодавство України.

Окрім поширення ворожої пропаганди, акаунти також використовувалися для несанкціонованого поширення в мережі Інтернет персональних даних громадян України, у схемах інтернет-шахрайства та для розсилки завідомо неправдивих повідомлень про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності.

GHOSTWRITER ПРОВОДИТЬ ЗЛОВМИСНУ КАМПАНІЮ ПРОТИ ДЕРЖАВНИХ, ВІЙСЬКОВИХ ТА ЦИВІЛЬНИХ ОРГАНІЗАЦІЙ В УКРАЇНІ ТА ПОЛЬЩІ – ДЕТАЛЬНИЙ АНАЛІЗ ВІД CISCO TALOS

Ухвалена постанова передбачає впровадження цифрових систем у держуправлінні та посилення кіберзахисту органів державної влади, фінансових установ, підприємств тощо.

Реалізація Національної програми інформатизації дасть змогу швидше впроваджувати цифрові технології, створювати, модернізувати й розвивати інформаційні та інформаційно-комунікаційні системи, засоби інформатизації, а також підвищувати кіберзахист критичної інформаційної інфраструктури. Це позитивно вплине на безпеку, результативність та ефективність роботи держорганів.

ДЕРЖСПЕЦЗВ'ЯЗКУ ЗАТВЕРДИЛА МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ЩОДО РЕАГУВАННЯ СУБ'ЄКТАМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ НА РІЗНІ ВИДИ ПОДІЙ У КІБЕРПРОСТОРІ

У межах реалізації Стратегії кібербезпеки України, на виконання постанови Уряду, Адміністрація Держспецзв'язку розробила та затвердила Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. Відповідний наказ від 03.07.2023 № 570 розміщений на сайті Служби.
Рекомендації визначають:

- необхідний перелік заходів із кіберзахисту, яких можуть вживати суб'єкти забезпечення кібербезпеки послідовно за етапами реагування на кіберінциденти / кібератаки;
- мету та цілі виконання заходів;
- механізм застосування критеріїв, за якими визначається категорія (рівень) критичності кіберінциденту / кібератаки;
- принципи пріоритезації кіберінцидентів / кібератак;
- типовий перелік заходів із реагування на кіберінциденти / кібератаки для одночасного відстеження заходів до їх завершення тощо.

Окрім того, Рекомендаціями затверджені Загальні правила обміну інформацією про кіберінциденти (Протокол TLP) версії 2.0, схвалені Національним координаційним центром кібербезпеки при РНБО, а також – Перелік категорій і типів кіберінцидентів.

УРЯД УХВАЛИВ ПОСТАНОВУ, ЯКА ДОЗВОЛЯЄ СТВОРИТИ ПРАВОВІ ОСНОВИ ДЛЯ МЕРЕЖІ СИТУАЦІЙНИХ ЦЕНТРІВ В УКРАЇНІ

Для оперативного ухвалення управлінських рішень під час виникнення кризових ситуацій та з метою визначення потенційних або реальних загроз національній безпеці України необхідно створювати відповідні ситуаційні центри. Ухвалена постанова «Питання мережі ситуаційних центрів» визначає склад, завдання та їх функції, вимоги до програмного й апаратного забезпечення ситуаційного центру, його підсистем та мереж. А також дозволить створити правові передумови для подальшого розширення й розвитку мережі ситуаційних центрів.

КІБЕРАТАКА НА ДЕРЖСТАТ УКРАЇНИ: ВОРОГ УКОТРЕ ПРОЗВІТУВАВ ПРО «ПЕРЕМОГУ», ЯКОЇ НЕ БУЛО

Так звані російські хактивісти, яких пов'язують із гу гш зс рф (раніше відомого як гру), продовжують здійснювати комплексні атаки проти України, поєднуючи кібератаки та інформаційно-психологічні операції. На офіційній сторінці Державної служби статистики України в соціальній мережі Facebook було опубліковане повідомлення про кібератаку, яка нібито унеможливила надання статистичних даних органам державної влади України.

Публікація про кібератаку та її «наслідки» з'явилася внаслідок компрометації офіційної сторінки Держстату в Facebook. Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA та Держстат підтверджують факт атаки зловмисників на інформаційні ресурси. Проте її результати значно перебільшені. Зокрема, зараз можна стверджувати, що внаслідок інциденту інформаційні ресурси Держстату не постраждали. Дані, що обробляються на ресурсах Служби, серверне обладнання Держстату, як і інформаційно-комунікаційна інфраструктура, не постраждали. Також у Служби є можливість подальшого надання статистичних даних.

ЗЛОВМИСНИКИ ВЧЕРГОВЕ ВИКОРИСТОВУЮТЬ ДЛЯ КІБЕРАТАК ПРОТИ ДЕРЖОРГАНІВ ЕЛЕКТРОННІ ЛИСТИ НА ТЕМУ «РАХУНКІВ» ТА «ПЕРЕКАЗІВ»

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA виявила та дослідила факт розповсюдження хакерським угрупуванням UAC-0057 електронних листів із використанням скомпрометованих облікових записів з темою, що стосується рахунків та переказів.

Зловмисники розповсюджують XLS-документи «PerekazF173_04072023.xls» та «Rahunok_05072023.xls». Вони містять макрос, який здійснює запуск шкідливої програми PicassoLoader. На момент дослідження PicassoLoader забезпечував завантаження, дешифрування та запуск шкідливої програми njRAT.

Як зазначають фахівці CERT-UA, якщо на комп'ютері застосовуються продукти Avast, FireEye, Fortinet, то шкідливу програму запущено не буде. Більш детальна інформація щодо невідкладних заходів кіберзахисту доступна за посиланням https://cert.gov.ua/article/1751036

CERT-UA ВИЯВИЛА КІБЕРАТАКУ, СПРЯМОВАНУ НА ВИКРАДЕННЯ ДАНИХ УКРАЇНЦІВ ДЛЯ ВХОДУ В ПОШТОВІ СЕРВІСИ

Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA виявила та дослідила факт розповсюдження хакерською групою APT28 фішингових атак з метою отримання аутентифікаційних даних українців, необхідних для входу до публічних поштових сервісів. Як зазначають фахівці, зловмисники розсилають HTML-файли, які імітують вебінтерфейс поштових сервісів (зокрема, UKR.NET, Yahoo.com) та реалізують технічну можливість передавання введених жертвою аутентифікаційних даних за допомогою HTTP POST-запитів. Водночас передавання викрадених даних здійснюється за допомогою заздалегідь скомпрометованих пристроїв Ubiquiti (EdgeOS).

CERT-UA закликає відповідальних співробітників організацій не ігнорувати повідомлень про виявлення ознак аномальної активності та вживати невідкладних заходів зі зменшення «поверхні» атаки. Більш детальна інформація щодо невідкладних заходів кіберзахисту доступна за посиланням https://cert.gov.ua/article/1751036

РОСІЙСЬКЕ ХАКЕРСЬКЕ УГРУПОВАННЯ ARMAGEDDON НАРОЩУЄ АКТИВНІСТЬ В ІТ-СИСТЕМАХ ДЕРЖАВНИХ ОРГАНІВ УКРАЇНИ

Фахівці CERT-UA проаналізували актуальні тактики, техніки та процедури, що використовують хакери одного з найбільш активних та небезпечних російських хакерських угрупувань – UAC-0010 (Armageddon / Gamaredon). До нього належать колишні «офіцери» із СБУ в АР Крим, які у 2014 році зрадили Батьківщину і почали прислужувати фсб росії. Основним завданням угрупування є кібершпигунство щодо сил безпеки та оборони України. Також відомо щонайменше про один випадок здійснення деструктивної діяльності на об'єкті інформаційної інфраструктури.

За даними CERT-UA, кількість одночасно інфікованих комп'ютерів, які переважно функціонують в межах інформаційно-комунікаційних систем державних органів, може сягати кількох тисяч. Деталі щодо кібератак угрупування, рекомендації щодо захисту – на сайті CERT-UA за посиланням https://cert.gov.ua/article/5160737.

РОСІЙСЬКЕ УГРУПУВАННЯ TURLA СПРЯМОВУЄ АТАКИ ПРОТИ СИЛ ОБОРОНИ, ВИКОРИСТОВУЮЧИ ШКІДЛИВІ ПРОГРАМИ CAPIBAR ТА KAZUAR – ДОСЛІДЖЕННЯ CERT-UA

Фахівці CERT-UA від 2022 року за ідентифікатором UAC-0024 відстежують активність, що полягає у здійсненні цільових кібератак, спрямованих проти сил оборони з метою шпигунства із застосуванням шкідливої програми CAPIBAR (Microsoft: DeliveryCheck, Mandiant: GAMEDAY). За певних обставин на уражені комп'ютери може довантажуватися складний багатофункціональний бекдор KAZUAR, серед функцій якого – викрадення різноманітних автентифікаційних даних, баз даних / конфігураційних файлів різних програм, отримання даних із журналів операційної системи тощо.

З достатнім рівнем впевненості цю активність асоційовано з угрупуванням Turla (UAC-0003, KRYPTON, Secret Blizzard), діяльність якого скеровується фсб росії.

Детально про специфіку програм, процес ураження, а також індикатори кіберзагроз – у матеріалі CERT-UA за посиланням https://cert.gov.ua/article/5213167

КІЛЬКІСТЬ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У КАТЕГОРІЇ «ШКІДЛИВИЙ ПРОГРАМНИЙ КОД» ЗРОСЛА НА 95,8%: ЗВІТ ОПЕРАТИВНОГО ЦЕНТРУ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ДЦКЗ

Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку оприлюднив звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти у II кварталі 2023 року. Загалом було опрацьовано 3 млрд подій, зібраних за допомогою засобів моніторингу, аналізу та передання телеметричної інформації про кіберінциденти та кібератаки. Кількість зареєстрованих та опрацьованих кіберінцидентів зросла до 191.

Також було детектовано 122 мільйони підозрілих подій інформаційної безпеки (при первинному аналізі) та опрацьовано 55 тисяч критичних подій інформаційної безпеки (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій інформаційної безпеки та вторинного аналізу). Порівняно з I кварталом 2023 року кількість подій інформаційної безпеки (ІБ) зросла:

- у категорії «Шкідливий програмний код» – на 95,8%;
- у категорії «Збір інформації зловмисником» – на 35,8%;
- загальна кількість критичних подій ІБ – на 38,1%.

Серед сімейств шкідливого програмного забезпечення, детектованих у подіях ІБ категорії «02 Шкідливий програмний код» протягом звітного періоду, переважають Agent Tesla, Snake Keylogger, SmokeLoader, Formbook та Remcos.Повний текст звіту ДЦКЗ:

UA: https://cip.gov.ua/services/cm/api/attachment/download?id=54463
EN: https://cip.gov.ua/services/cm/api/attachment/download?id=54462

ІНТЕГРУЄМОСЯ ДО ЄВРОПЕЙСЬКОГО КІБЕРПРОСТОРУ – ДЕРЖНДІ ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ ПРИЄДНУЄТЬСЯ ДО ECSO

Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації здобув статус тимчасового члена Європейської організації з кібербезпеки (ECSO – European Cyber Security Organisation). Восени наглядова рада ECSO має розглянути питання щодо приєднання ДержНДІ технологій кібербезпеки до організації як постійного члена.

ECSO – європейська міжгалузева та незалежна організація з кібербезпеки, яка об'єднує європейських державних і приватних стейкхолдерів у сфері кібербезпеки та сприяє їхньому співробітництву. Серед майже 300 членів організації є великі компанії-розробники та постачальники рішень з кібербезпеки, дослідницькі центри, університети, кластери та асоціації, місцеві, регіональні та національні адміністрації держав-членів Європейського Союзу тощо.

АКАДЕМІЯ СБУ РОЗПОЧИНАЄ СПІВПРАЦЮ З ПАРТНЕРАМИ, ЯКІ ДОПОМАГАТИМУТЬ РОЗВИВАТИ ПІДГОТОВКУ КІБЕРФАХІВЦІВ

Безпечне функціонування кіберпростору, забезпечення кіберстійкості нашої держави, розробка ефективного нормативно-правового забезпечення, розвиток цифрової грамотності та кібергігієни – важливі безпекові питання сьогодення. Особливо в умовах кібервійни, яка ведеться росією проти нашої країни з 2014 року. Усі ці напрями під час робочої зустрічі обговорили ректор НА СБУ Андрій Черняк та співробітник кіберцентру НА СБУ Євген Владіміров із директорами ГО «Оперативна група з кібербезпеки» Ксенією Смірновою та ГО «Міжнародний університет кібербезпеки» Олексієм Хоменком.

Також учасники зустрічі підписали Меморандуми про співпрацю, які стануть початком обопільних проєктів та справжньою дорожньою картою партнерства.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

КІБЕРОПЕРАЦІЇ ВІДІГРАВАТИМУТЬ ДОПОМІЖНУ, А НЕ ВИРІШАЛЬНУ РОЛЬ У ВЕЛИКИХ ВІЙНАХ НА ТЕАТРІ – ЕКСПЕРТНА ДИСКУСІЯ CSIS

13 липня аналітичний центр CSIS оприлюднив результати експертної дискусії «Кібероперації під час російсько-української війни: від дивних моделей до альтернативного майбутнього». Дослідники вказують, що як в російсько-українській війні, так і у конвенційних конфліктах майбутнього кібероперації відіграватимуть допоміжну, а не вирішальну роль.

Хоча держави продовжуватимуть інвестувати у свій кіберпотенціал, після початку війни віддача від цих інвестицій зменшуватиметься поза розвідувальною діяльністю та зусиллями з введення в оману. Відтак війни все ще будуть реалізовуватись іншими засобами, а держави будуть покладатись на більш відчутні наслідки насильства, ніж на невловимі наслідки компрометації інформаційних мереж. Під час переходу до бойових дій військові командири нададуть перевагу впевненості в завдаванні смертоносних точних ударів по цілях високої цінності, ніж невизначеності генерації ефектів у кіберпросторі.

РОСІЙСЬКІ ХАКЕРИ СПРОБУВАЛИ АТАКУВАТИ ПРАЦІВНИКІВ ІНОЗЕМНИХ ПОСОЛЬСТВ В УКРАЇНІ РЕКЛАМОЮ ДЕШЕВИХ BMW

12 липня стало відомо, що хакери APT29 (Cozy Bear) спробували атакувати 22 іноземних представництва, які розташовані в Києві. Для цього вони перехопили повідомлення від дипломата Міністерства закордонних справ Польщі, який розіслав електронною поштою листівку до різних посольств із рекламою продажу вживаного седана BMW 5-серії. Хакери перехопили та скопіювали цей флаєр, вставили в нього шкідливе програмне забезпечення, а потім відправили його десяткам інших іноземних дипломатів. Наразі не відомо щодо яких посольств кібератака вдалась.

ПЕНТАГОН НАМАГАЄТЬСЯ ПЕРЕЙНЯТИ УКРАЇНСЬКИЙ ДОСВІД ШВИДКОГО ВПРОВАДЖЕННЯ ТА МАСШТАБУВАННЯ НОВИХ ТЕХНОЛОГІЙ У ВІЙСЬКОВІЙ СПРАВІ

23 липня новий керівник ключового підрозділу Пентагону по роботі з Кремнієвою долиною Дуг Бек заявив, що Пентагон продовжує вчитися на досвіді російсько-української війни. Його увага зосереджена на вивчені того, як Україна швидко впроваджує в тактичних цілях цивільні технології або технології подвійного призначення (як то невеликі безпілотні літальні апарати, комерційні супутникові знімки тощо). За його словами Україна продемонструвала чудові спроможності масштабувати таке використання технологій і це те, чого Пентагон все ще не вміє. І це створює перешкоди у його відносинах із Кремнієвою долиною.

КІБЕРАТАКА ВИВЕЛА З ЛАДУ СУПУТНИКОВИЙ ЗВ'ЯЗОК РОСІЙСЬКИХ ВІЙСЬКОВИХ

30 червня Washington Post повідомила, що 28 червня супутникова система зв'язку, яка обслуговує російську армію, була виведена з ладу через кібератаку і залишалася переважно неробочою протягом наступного дня. Оператор супутникової системи Dozor-Teleport під час збою перемкнув частину користувачів на наземні мережі. Одна мережа була покрита материнською компанією «Дозор», Амтел-Зв'язок, тоді як три інші залишалися неактивними. Принаймні дві групи взяли на себе відповідальність за атаку: одна назвала себе організацією хакерів, а інша – частиною Групи Вагнера. Компанія Dozor-Teleport обслуговує російську армію та інші федеральні служби. Серед її клієнтів є російські солдати в Україні. Разом з тим, аналітики висловлюють сумніви, що атака завдасть значної шкоди.

КОРПОРАЦІЯ MICROSOFT ЗАПЕРЕЧУЄ ЗЛАМ, ЯКИЙ НІБИТО СТОСУВАВСЯ 30 МІЛЬЙОНІВ КЛІЄНТІВ

Хакерська група Anonymous Sudan (зазвичай вважається російською організацією прикриття) 1 липня заявила у своїх Telegram-каналах, що зламала сервери Microsoft і викрала дані, що належать приблизно тридцяти мільйонам клієнтів. «Ми повідомляємо, що ми успішно зламали Microsoft і маємо доступ до великої бази даних, яка містить понад 30 мільйонів облікових записів Microsoft, електронну пошту та пароль. Ціна за повну базу даних: 50 000 доларів США», – повідомили в групі.

Microsoft каже, що ці заяви є безпідставними. «Зараз наш аналіз даних показує, що це оманлива заява, що стосується сукупності даних», – представник Microsoft повідомив виданню BleepingComputer. «Ми не бачили доказів того, що дані наших клієнтів були скомпрометовані або хтось отримав доступ до них».

ЯПОНСЬКИЙ ПОРТ НАГОЯ ПАРАЛІЗОВАНИЙ ВНАСЛІДОК ОСТАННЬОГО РОЗГУЛУ ПРОГРАМИ-ВИМАГАЧА LOCKBIT

Найбільша гавань Японії була паралізована зломом LockBit. Атаку виявили вранці 4 липня, коли припинила працювати система управління вантажними терміналами порту. Вимога викупу, надрукована офісним принтером, підтвердила, що порт став жертвою атаки російського вимагача LockBit 3.0. Сума викупу не розголошується.

Наступного дня в блозі жертв групи з'явилися назви трьох компаній, а саме MITRE, Euro Support в Нідерландах та іспанська організація Reclam Laser. Таким чином за п'ять днів кількість жертв угруповання сягнула 10.

Попереднього тижня LockBit також вразив провідну глобальну компанію з виробництва напівпровідників TSMC, розташовану на Тайвані. З TSMC вимагали викуп у розмірі 70 000 000 доларів США, а крайній термін виплати – 6 серпня.

ROMCOM RAT НАЦІЛЕНА НА ГРУПИ ПІДТРИМКИ НАТО ТА УКРАЇНИ

Згідно з дослідженням BlackBerry Threat Research and Intelligence, опублікованим 8 липня, зловмисники, які стоять за RomCom RAT, вірогідно здійснюють фішингові атаки, спрямовані на майбутній саміт НАТО у Вільнюсі, а також на організацію, яка підтримує Україну за кордоном.

BlackBerry Threat Research and Intelligence виявила два шкідливі документи, надіслані з угорської IP-адреси 4 липня 2023 року. У цих документах зловмисники видають себе за Світовий Конгрес українців.

RomCom, який також відстежується під іменами Tropical Scorpius, UNC2596 і Void Rabisu, нещодавно був помічений в організації кібератак на політиків в Україні, які тісно співпрацюють із західними країнами та медичною організацією в США, яка допомагає українським біженцям.

Ланцюжки атак, організованих групою, є геополітично вмотивованими та використовували фішингові електронні листи, щоб спрямовувати жертв на клоновані вебсайти, на яких розміщені троянські версії популярного програмного забезпечення. Цілі включають військові, ланцюжки постачання харчових продуктів та IT-компанії.

НОРВЕЗЬКА РАДА У СПРАВАХ БІЖЕНЦІВ ТА ІНШІ ГУМАНІТАРНІ ОРГАНІЗАЦІЇ ЗАЗНАЮТЬ КІБЕРАТАК

Норвезька рада у справах біженців (NRC) оголосила 13 липня, що виявила кібератаку на онлайн-базу даних, яка зберігає особисту інформацію учасників проєкту. NRC заявила, що негайно відключила базу від мережі, щоб захистити дані та запобігти подальшим атакам. Вони також розпочали зовнішнє розслідування, щоб визначити масштаби та наслідки кібератаки.

Це не перший випадок, коли хакери атакують гуманітарні організації. У лютому українські біженці в Польщі, Литві та Великій Британії стали об'єктами дезінформаційної кампанії, спрямованої на викрадення їхніх особистих даних. У січні 2022 року Міжнародний Комітет Червоного Хреста став жертвою кібератаки, під час якої хакери викрали дані понад 515 000 надзвичайно вразливих людей, у тому числі тих, хто розлучився зі своїми родинами через конфлікт, міграцію та катастрофи, зниклих безвісти та їхніх родин та людей, які перебувають під вартою.

ОЧІКУВАЛОСЯ, ЩО РОСІЯ ЗНИЩИТЬ УКРАЇНУ В КІБЕРВІЙНІ. ЦЬОГО НЕ СТАЛОСЯ.

У дописі від 17 липня Moonlock Lab аналізує причини, через які рф не вдалося знищити Україну у кіберпросторі. Серед причин – тривала російська агресія проти України у кіберпросторі, завдяки якій українські фахівці змогли здобути необхідні навички захисту та протидії.

У звіті також наголошується, що українські кіберфахівці часто не афішують свою діяльність, завдаючи шкоду здатності рф проводити операції у кіберпросторі без заяв про те, що відповідальними за конкретну атаку є вони. Також не афішуються плани та стратегії.

НОВИЙ БЕКДОР TURLA DELIVERYCHECK ЗАГРОЖУЄ УКРАЇНСЬКОМУ ОБОРОННОМУ СЕКТОРУ

Оборонний сектор в Україні та Східній Європі став мішенню нового бекдору на основі .NET під назвою DeliveryCheck (він же CAPIBAR або GAMEDAY), який здатний доставляти корисні навантаження наступного рівня.
Команда розвідки загроз Microsoft у співпраці з Групою реагування на надзвичайні ситуації в області комп'ютерних ситуацій України (CERT-UA) приписали атаки російському державному актору, відомому як Turla, який також відстежується під іменами Iron Hunter, Secret Blizzard (раніше Криптон), Уроборос, Venomous Bear, та Waterbug. Він пов'язаний з федеральною службою безпеки росії (фсб).

НАТО РОЗСЛІДУЄ ЙМОВІРНУ КРАДІЖКУ ДАНИХ ХАКЕРАМИ SIEGEDSEC

26 липня НАТО підтвердила, що її IT-команда розслідує заяви про ймовірну крадіжку даних на порталі Співпраці спільнот інтересів (Communities of Interest Cooperation (COI) хакерською групою, відомою як SiegedSec. Портал COI (dnbl.ncia.nato.int) – це несекретне середовище для обміну інформацією та співпраці, призначене для підтримки організацій НАТО та країн-членів.

Хакери заявили, що вони викрали сотні документів з порталу співпраці COI. Компанія з кібербезпеки CloudSEK проаналізувала витік даних і виявила, що вони містять 845 МБ файлів, 8000 рядків конфіденційної інформації, пов'язаної з користувачами, несекретні документи та деталі доступу до облікових записів користувачів. НАТО розслідує автентичність цієї інформації.

SiegedSec заявили, що атака не пов'язана з російсько-українською війною та є відповіддю на порушення прав людини з боку НАТО.

РОСІЙСЬКА BLUEBRAVO РОЗГОРТАЄ GRAPHICALPROTON BACKDOOR ПРОТИ ЄВРОПЕЙСЬКИХ ДИПЛОМАТИЧНИХ УСТАНОВ

російський державний актор, відомий як BlueBravo, був помічений у нападах на дипломатичні установи по всій Східній Європі з метою створення нового бекдора під назвою GraphicalProton, що є прикладом постійної еволюції загрози. Фішингова кампанія характеризується використанням законних інтернет-сервісів (LIS) для обфускації системи команди та контролю (C2), повідомляє Recorded Future у новому звіті, опублікованому 27 липня. Описана у ньому активність спостерігалася в період з березня по травень 2023 року.

УКРАЇНСЬКІ ХАКЕРИ ЗАПУСТИЛИ «ТРОЯН» НА ТЕЛЕФОНИ РОСІЙСЬКИХ ВІЙСЬКОВИХ МОРЯКІВ

30 липня пресслужба Головного управління розвідки Міноборони повідомила, що українські хакери «привітали» військових моряків рф з днем вмс рф, запустивши на їх телефони «троянську» програму, яка знімає інформацію і перенаправляє її на українські сервери.

9. РІЗНЕ

ОГЛЯД КОНКУРЕНЦІЇ США ТА КИТАЮ У СФЕРІ ВИРОБНИЦТВА МІКРОЧИПІВ

7 липня Liga.net розмістила короткий огляд конкуренції між США та Китаєм у сфері технологій, зокрема у сфері виробництва мікрочипів. На думку авторів тексту, проблема полягає у тому, що свій технологічний прогрес Китай хоче використовувати не тільки для посилення своєї частки на глобальному ринку, а й для нарощування військової сили. Саме цьому і намагаються завадити США, вступаючи у конкуренцію з Китаєм.

ЯПОНІЯ ОБМЕЖИЛА ЕКСПОРТ ДО КИТАЮ ОБЛАДНАННЯ ДЛЯ ВИРОБНИЦТВА МІКРОСХЕМ

Японія ввела обмеження на експорт передового обладнання для виробництва мікросхем, головною метою яких є завадити Китаю розробляти високоякісні напівпровідники, що можуть бути використані у військових цілях.

Наказ Міністерства торгівлі, що вимагає отримання компаніями-експортерами окремого дозволу на продаж такого обладнання за кордон, набув чинності 23 липня.

ЄВРОСОЮЗ УХВАЛИВ «ЗАКОН ПРО ЧИПИ» ДЛЯ ЗМЕНШЕННЯ ЗАЛЕЖНОСТІ ВІД ІМПОРТУ

Європейський Союз у вівторок, 25 липня, завершив ухвалення регламенту щодо зміцнення європейської напівпровідникової промисловості, спрямований на зменшення залежності від імпорту.

Мета цього документа – створення умов для розвитку європейської інноваційної промисловості та підготовка до будь-якої майбутньої кризи у сфері постачання мікросхем. Програма має мобілізувати 43 млрд євро державних та приватних інвестицій і подвоїти частку Євросоюзу на світовому ринку напівпровідників з нинішніх 10% щонайменше до 20% до 2030 року.

КЕРІВНИКА GROUP-IB ІЛЛЮ САЧКОВА ЗАСУДИЛИ ДО 14 РОКІВ УВ'ЯЗНЕННЯ ЗА ЗВИНУВАЧЕННЯМ У ДЕРЖАВНІЙ ЗРАДІ

26 липня стало відомо, що Іллю Сачкова – екс-керівника компанії Group-IB засуджено до 14 років колонії суворого режиму за звинуваченням у державній зраді. Він перебував під вартою з моменту арешту у вересні 2021 року. У 2003 році він став співзасновником фірми з мережевої безпеки. Його звинуватили у передачі ФБР інформації про підтримувану Кремлем команду APT28, також відому як Fancy Bear і інформацію про її втручання у вибори на Заході. Сама Group-IB підозрюється у тісній співпраці з російськими спецслужбами.