Герус В. А., ст. викладач
Національний університет водного господарства та природокористування

ХАКЕРСЬКІ УГРУПУВАННЯ

У всесвітньому кіберпросторі існує таємничий та нестабільний світ хакерських угруповань, які, наче тіні, переслідують власну мету та інтереси. Вони є віртуозами в галузі комп'ютерної безпеки, порушуючи закони та залишаючи за собою сліди хаосу та руйнування. У цій статті ми розглянемо хакерські угруповання як феномен сучасного інтернет-суспільства, розгадаємо їх мотивацію, методи та вплив на сучасний світовий ландшафт інформаційної безпеки. Від таємничих колективів, які виходять на світло лише під час великих кібератак, до постійно активних груп, які підірвали традиційні уявлення про безпеку.

Кіберзлочинці активно шукають способи застосування нейромереж в атаках. Штучний інтелект допомагає зловмисникам підтримувати ілюзію осмисленого діалогу з жертвою, генерувати переконливі фішингові листи, створювати дипфейки голосів, зображень та відео. Ми можемо тільки прогнозувати зростання кількості атак з використанням нейромереж, які поступово поповнюють арсенал зловмисників. Кіберзлочинці не лише прагнуть обійти цензуру ChatGPT на створення шкідливого контенту, а й створюють власні набори інструментів. Наприклад, WormGPT – генеративна нейромережа для проведення фішингових та BEC-атак – створена зловмисниками на основі мовної моделі JPT-J з відкритим вихідним кодом спеціально для незаконної діяльності.

Хакерські угруповання залишаються невід'ємною частиною динамічної кіберпросторової реальності. Спробуємо перерахувати їх, вказавши альтернативні назви та цілі:

APT31 – група, відома з 2016 року; їй приписують атаки на організації Франції, США, уряду Норвегії, Фінляндії, Німеччини.

Альтернативні назви: JudgmentPanda, Zirconium, APT 31, TEMP.Avengers, BronzeVinewood.

Атаковані галузі: Фінансовий сектор, Авіаційно-космічна промисловість, Телекомунікації, Будівництво, Дослідницькі компанії, Неурядові організації, Медіа.

APT32. Кібершпигунська група APT32 активна щонайменше з 2012 року. Націлена на урядові, громадські та торговельні організації країн Східної та Південно-Східної Азії. Має різнобічний інструментарій, що постійно змінюється.

Альтернативні назви: OceanLotus, APT-C-00, CobaltKitty, SeaLotus, OceanBuffalo, TinWoodlawn, SectorF01, PondLoach

Атаковані галузі: Військово-промисловий комплекс, Державний сектор, Фінансовий сектор, Промисловий сектор, Телекомунікації, Медіа.

BronzeUnion – APT- угруповання, активне як мінімум з 2010 року. На думку різних дослідників, має китайське походження. Широко використовує для початкового проникнення техніки «атаки на водопій» (wateringhole), зокрема зараження веб-сайтів, відвідуваних жертвами, а також фішинг та вразливість мережевих сервісів. Група спеціалізується на кібершпигунстві, переважно в мережах державних установ, оборонних підприємств та політичних організацій. У 2020 році деякі дослідники (включно зі спеціалістами PT ExpertSecutityCenter) припустили появу у групи фінансової мотивації.

Альтернативні назви: LuckyMouse, EmissaryPanda, APT27, IronTiger, TG-3390, TEMP.Hippo, Group 35, ZipToken

Атаковані галузі: Державний сектор, Промисловий сектор, Інформаційні технології, Авіаційно-космічна промисловість, Освіта, Військово-промисловий комплекс, Медіа, Аналітичні центри.

Calypso. Вперше активність групи Calypso була виявлена фахівцями PT ExpertSecurityCenter у березні 2019 року під час робіт з виявлення кіберзагроз. Група активна як мінімум із вересня 2016 року. Основною метою групи є крадіжка конфіденційних даних, основні жертви – державні установи Бразилії, Індії, Казахстану, Росії, Таїланду, Туреччини.

Атаковані галузі: Державний сектор.

ChamelGang. У другому кварталі 2021 року Експертний центр безпеки PositiveTechologies (PTESC) виявив діяльність невідомої раніше групи. Група була названа ChamelGang (від Chameleon) за вміння ефективно маскувати свою діяльність та оминати засоби захисту. Жертви цієї групи перебувають у світі навіть у Росії, де група скомпрометувала енергетичну організацію та організацію з авіаційно-промислового сектора.

Атаковані галузі: Державний сектор, Фінансовий сектор, Енергетика, Авіаційно-космічна промисловість, Телекомунікації.

Cobalt. Кіберзлочинна група Cobalt існує з 2016 року і атакує організації кредитно-фінансової сфери з метою крадіжки коштів через зламування банкоматів, картковий процесинг, різні платіжні системи (SWIFT, АРМ КБР). Імовірно, деякі її учасники були членами групи Carbanak, яка існувала раніше. За оцінками ФінЦЕРТ, збитки від атак групи Cobalt у Росії в 2017 році перевищили 1 млрд рублів. Після арешту одного з лідерів групи у 2018 році група продовжила свою активність. Один із гучних зломів, до яких була причетна група, – зламування системи швидких платежів Unistream.

Альтернативні назви: CobaltGang, CobaltSpider

Атаковані галузі: Фінансовий сектор

CozyDuke. Група CozyDuke – добре оснащена, організована та віддана своїй справі кібершпигунська група. На думку дослідників, група є російськомовною і існує щонайменше з 2008 року. Влада США інкримінує групі кібератаки на Білий Дім США, Держдепартамент США та Національний комітет Демократичної партії США.

Альтернативні назви: APT 29, TheDukes, Group 100, Yttrium, IronHemlock, Minidionis

Атаковані галузі: Державний сектор, Промисловий сектор, Телекомунікації, Освіта, Військово-промисловий комплекс, Дослідницькі компанії, Неурядові організації, Фармацевтика.

FancyBear – імовірно російськомовна група, що спеціалізується на шпигунстві. Група активна щонайменше з 2004 року. Має багатий інструментарій, що постійно змінюється.

Атаковані галузі: Державний сектор, Фінансовий сектор, Промисловий сектор, Інформаційні технології, Освіта, Військово-промисловий комплекс, Дослідницькі компанії, Неурядові організації, Медіа, Охорона здоров'я.

GoblinPanda вперше виявлена в 2013 році дослідниками з CrowdStrike і вважається групою, яка діє на користь Китаю. Група зосереджена на шпигунстві та має у своєму арсеналі ВПО здатне комунікувати у закритих мережах. У результаті аналізу ВПО було виявлено, що група має перетину з інструментами групи Calypso.

Альтернативні назви: Cycldek, Hellsing, Conimes

Атаковані галузі: Державний сектор

Higaisa. Кібершпигунський гурт Higaisa активний як мінімум з 2009 року. Націлена на державні, громадські та торгові організації у Північній Кореї. У списку атакованих країн також є Китай, Польща, Росія, Японія.

Атаковані галузі: Державний сектор.

Lazarus. Lazarus – APT-група, яку дослідники пов’язують з урядом Північної Кореї. Найбільш відома за шифрувальником WannaCry, від якого постраждали понад 150 країн, і злому SonyPictures. Група активна принаймні з 2009 року, організовує широкомасштабні кампанії кібершпигунства, операції із застосуванням програм-шифрувальників, а також атаки на криптовалютний ринок.

Альтернативні назви: Hidden cobra, Zinc, GuardiansofPeace, Group 77, Office 91, RedDot, Temp. -APT-15, NewRomanicCyberArmyTeam, Appleworm, SectorA01, ITG03

Атаковані галузі: Державний сектор, Фінансовий сектор, Інформаційні технології, Авіаційно-космічна промисловість, Військово-промисловий комплекс, Медіа, Фармацевтика, Охорона здоров'я, Криптовалютні біржі, Дослідники в галузі кібербезпеки.

RTM (ReadTheManual). Кіберзлочинна група RTM розпочала свою активність у 2015 році та атакує організації з різних галузей з метою крадіжки коштів з рахунків, крадіжки конфіденційних документів, облікових записів. Група використовує шкідливе ПЗ (ВПО) власної розробки. ВПО групи немає статичного контрольного сервера: воно отримує його через блокчейн.

Атаковані галузі: Державний сектор, Фінансовий сектор, Енергетика, Промисловий сектор, Інформаційні технології.

Silence. Кіберзлочинна група Silence з’явилася у 2016 році та атакувала організації кредитно-фінансової сфери, переважно в Росії. Метою групи є крадіжка коштів через зламані банкомати, картковий процесинг, АРМ КБР. З 2018 року група розширила географію атак та стала атакувати організації по всьому світу. У деяких атаках група використовувала інструменти групи TA505, що може говорити про їхню кооперацію. *Атаковані галузі:* Фінансовий сектор.

SpacePirates. Вперше угруповання SpacePirates було помічене фахівцями PT ExpertSecurityCenter наприкінці 2019 року під час робіт з виявлення кіберзагроз. Активна як мінімум із 2017 року. Основними цілями зловмисників є шпигунство та крадіжка конфіденційної інформації. Угруповання активно атакує різні галузі Росії. Крім цього, було виявлено жертви в Грузії, Узбекистані, Монголії, Китаї та Сербії.

Атаковані галузі: Фінансовий сектор, Інформаційні технології, Авіаційно-космічна промисловість, Освіта, Військово-промисловий комплекс, Охорона здоров'я, Сільське господарство, Паливно-енергетичний комплекс, Електроенергетика, Державні установи.

TA505. Одна з найнебезпечніших та найактивніших злочинних кібергруп, що діє більш ніж у 60 країнах. Основна мета групи – крадіжка або вимагання коштів.

Альтернативні назви: EvilCorp, ATK 103, SectorJ04, Hive0065, GRACEFUL SPIDER, GOLD TAHOE, Dudear, CHIMBORAZO.

Атаковані галузі: Фінансовий сектор, Державний сектор, Енергетика, Авіаційно-космічна промисловість, Дослідницькі компанії, Фармацевтика.

TaskMasters. Кібершпигунське угруповання TaskMasters виявлено у 2018 році фахівцями PT ExpertSecurityCenter. Група активна щонайменше з 2010 року. Серед атакованих організацій – великі промислові та енергетичні підприємства, державні структури, транспортні компанії. Угруповання атакує компанії з різних країн, але більшість жертв перебувають у Росії та країнах СНД.

Альтернативні назви: BlueTraveller.

Атаковані галузі: Державний сектор, Енергетика, Промисловий сектор, Транспортні компанії.

Turla – відома група кібершпигунства, що має величезну кількість інструментів, яка понад десять років пов'язана з операціями проти різних організацій по всьому світу. Особливістю групи є розробка своїх власних унікальних сучасних шкідливих програм та інструментів, а також нових методів атак та обфускації.

Альтернативні назви: Waterbug, WhiteBear, VenomousBear, Group 88, Snake, SIG23, IronHunter, Krypton, Pacifier APT

Атаковані галузі: Державний сектор, Енергетика, Освіта, Військово-промисловий комплекс, Дослідницькі компанії, Неурядові організації, Фармацевтика.

Winnti. Група активна з 2012 року, походить з Китаю і належить до класу спонсорованих урядом. Ключові інтереси – це шпигунство та отримання фінансової вигоди. Основний арсенал групи складається із власне розробленого ВПО. Winnti використовує складні методи атак серед яких supply-chain і wateringhole. Група точно знає хто їхня жертва, вона дуже обережно розвиває атаку і лише після детального аналізу зараженої системи

завантажує основний інструментарій. Атакує країни по всьому світу: Білорусь, Бразилію, Німеччину, Індію, Монголію, Росію, США, Південну Корею, Японію ін.

Альтернативні назви: APT41, AXIOM, BARIUM, LEAD, BlackFly.

Атаковані галузі: Державний та Фінансовий сектор, Енергетика, Ігрова індустрія, Розробка ПЗ, Авіаційно-космічна промисловість, Телекомунікації, Будівництво, Освіта, Фармацевтика.

Загалом, ситуація з хакерськими угрупованнями вимагає постійної уваги та стратегічного підходу до кібербезпеки. Завдяки спільним зусиллям ми можемо забезпечити безпеку та захист в інтернет-середовищі, де інформація стає все більш цінним ресурсом, а загрози – більш вдосконаленими та складними.

Нові технології, такі як штучний інтелект та блокчейн, також можуть виконувати важливу роль у покращенні кібербезпеки. Штучний інтелект може виявляти та відповідати на загрози в реальному часі, а блокчейн може забезпечити додатковий рівень захисту даних.