КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.24.172184
УДК 004.056

Опанович Максим Юрійович
аспірант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-2748-2965
maksym.y.opanovych@lpnu.ua

АНАЛІЗ КІБЕРАТАК ТА ДІЯЛЬНОСТІ APT ГРУП В УКРАЇНІ

Анотація. Стаття присвячена аналізу кібератак та діяльності APT(Advanced Persistent Threat) груп в Україні, яка значно активізувалася протягом останнього десятиліття у контексті зростаючої глобалізації інформаційної війни та політичних конфліктів. В роботі поглиблено розглядаються методи, тактики та процедури (TTP), які використовуються відомими APT групами, такими як Sandworm, Fancy Bear (APT28), та Gamaredon, для здійснення цілеспрямованих кібератак проти України. Основною метою статті є виявлення закономірностей у діяльності APT груп і формування рекомендацій для розробки ефективних стратегій кіберзахисту. В роботі використані дані з відкритих джерел, звіти CERT-UA, та аналітичні матеріали міжнародних компаній для оцінки сучасного стану кібербезпеки та ідентифікації потенційних вразливостей, які можуть бути використані зловмисниками. В статті детально описано різні методи кібератак, що включають використання поліморфних і метаморфічних шкідливих програм, атаки на ланцюги поставок та методи, тактики та процедури відповідно до фреймворку Mitre. Значну увагу приділено стратегіям захисту від APT атак, з особливим фокусом на архітектурі нульової довіри (Zero Trust) та поглибленому захисті (Defence in Depth), що включає застосування багаторівневих систем захисту для мінімізації ризиків та забезпечення відновлення після інцидентів. Також обговорюються тактики протидії зловмисникам, використання передових рішень для захисту мережі та кінцевих точок, і широке впровадження багатофакторної автентифікації та методів захисту проти фішингових атак. Стаття наголошує на важливості комплексного підходу до побудови системи захисту, який включає як технічні, так і організаційні аспекти. Результати дослідження підкреслюють необхідність постійної оновленості технологій та методів аналізу загроз для адекватного реагування на сучасні та майбутні кібератаки.

Ключові слова: APT; кіберзагрози; кібервійна; Mitre; Zero Trust; Defence in Depth.

ВСТУП

За останнє десятиліття кібервійна та діяльність APT(Advanced Persistent Threat) груп значно розвинулася. Ситуація визначається зростаючою витонченістю кібератак, зростанням діяльності, що фінансується державою, і розширенням масштабу цілей.

За останнє десятиліття помітно зросла кількість кібератак, спонсорованих національними державами або здійснених за підтримки держави. Ці операції часто спрямовані на досягнення геополітичних цілей, включаючи шпигунство, порушення роботи критичної інфраструктури та вплив на політичні, економічні та військові можливості інших країн. Групи APT, пов’язані з різними країнами, були причетні до численних кампаній, націлених на державні установи, критичну інфраструктуру та приватний сектор по всьому світу.

Методи кібератак стали більш досконалими, що ускладнює виявлення та захист. Це включає використання:

– Поліморфних та метаморфічних шкідливих програм, які можуть змінювати свій код, щоб уникнути виявлення;

- Атаки на ланцюги поставок, коли зловмисники націлюються на менш захищені елементи в ланцюзі поставок, щоб скомпрометувати кінцеву ціль.
- Атаки Living off the land (LotL), коли зловмисники використовують легітимні інструменти, наявні в системі жертви, для виконання своїх операцій, що ускладнює виявлення;
- Атаки програм-вимагачів розвинулися, коли зловмисники не просто шифрують дані, а й викрадають їх і погрожують оприлюднити, якщо не буде сплачено викуп (подвійне вимагання).

Атаки програм-вимагачів різко зросли, націлені на уряди, заклади охорони здоров'я, навчальні заклади та корпорації. Ці атаки стали більш витонченими, зловмисники проводять ретельну розвідку, щоб ідентифікувати та зашифрувати критично важливі системи та дані, щоб максимізувати свій вплив.

В останнє десятиліття спостерігається зростання ринку «кібернайманців», де держави та приватні компанії наймають сторонніх хакерів для шпигунства, диверсій або операцій впливу. Поширення найманих послуг кіберзлочинців, таких як програми-вимагачі як послуга (RaaS), знизило вхідний бар'єр для проведення складних кібератак.

Зараз кібероперації регулярно поширюються на сферу інформаційної війни, коли групи APT використовують платформи соціальних мереж для поширення дезінформації, маніпулювання громадською думкою та втручання в політичні процеси в різних країнах.

У той час як уряди, військові та критично важлива інфраструктура завжди були основними цілями, за останнє десятиліття стало очевидним значне розширення сфери цілей. Це включає фінансовий сектор, охорону здоров'я, освіту та навіть малі та середні підприємства, що підкреслює той факт, що жоден сектор не застрахований від кіберзагроз.

Ландшафт кібервійни в Україні суттєво сформувався під впливом геополітичної ситуації, зокрема через вторгнення Росії. За останнє десятиліття Україна зіткнулася з численними складними кібератаками, спрямованими на критичну інфраструктуру, державні установи та компанії приватного сектору. Ці інциденти часто розглядаються як безпосередньо пов'язані з війною з Росією, що робить Україну центром для розуміння еволюції кібервійни та діяльності груп APT.

Україна є об'єктом постійних кампаній кібершпигунства та дезінформації, спрямованих на підрив уряду, військового потенціалу та соціальної єдності. Ці кампанії часто включають складні фішингові атаки, зловмисне програмне забезпечення та використання соціальних мереж для поширення неправдивої інформації.

APT групи, що часто є підозрюваними у зв'язках із російськими спецслужбами були особливо активними в Україні. Наприклад:

- Sandworm: пов'язана з російською військовою розвідкою ГРУ, Sandworm була причетна до різних атак на Україну, включно з інцидентами BlackEnergy та NotPetya;
- Fancy Bear (APT28): ще одна група, пов'язана з ГРУ, Fancy Bear, займалася кібершпигунством проти українських урядовців і військових, часто з метою отримання доступу до конфіденційної інформації;
- Gamaredon: група вважається пов'язаною із ФСБ Росії, зосереджувалась на постійних атаках на українські служби безпеки, військові та державні структури, головним чином за допомогою фішингових кампаній для доставки зловмисного програмного забезпечення.

Ландшафт кібервійни в Україні ілюструє статус країни як важливої лінії фронту в сфері кіберконфлікту, що розвивається. Витонченість і частота кібератак проти України підкреслюють стратегічне використання кібероперацій у сучасному конфлікті, зокрема

суб'єктами, які фінансуються державою. Досвід України підкреслює важливість надійного кіберзахисту, міжнародного співробітництва, а також необхідність постійної пильності та адаптації для протидії цим загрозам.

Постановка проблеми. Останнє десятиліття кібервійни та розвиток кіберзагроз в загальному демонструють дедалі складніше середовище, де атаки, що фінансується державою, відіграють визначну роль. Еволюція методів кібератак і розширення цільових секторів підкреслюють необхідність постійного вдосконалення стратегій кібербезпеки та міжнародного співробітництва. За допомогою аналізу діяльності APT груп можна визначити мотиви, патерни та закономірності в їхніх атаках, що дає змогу визначити слабкі місця в захисті, наявні вразливості, методи атак та розуміння як працюють використовувані ними інструменти.

Аналіз останніх досліджень і публікацій. У роботі Оллі Хоньо [1] було досліджено як оперують APT групи, що пов'язані з Росією, а саме APT28, APT29, і Turla. В цій роботі було визначено які техніки, тактики та процедури (TTP) ці групи використовують, а також які інструменти були задіяні в їхніх операціях. В роботі було визначено, що групи пов'язані з РФ маю схожі риси у свої діях та використаних інструментах.

Ключовими мотивами наступного дослідження [2] були аналіз трьох конкретних груп APT — APT28, Red October і Regin, які в основному спрямовані на критичну національну інфраструктуру, і розробка виявлення активності цих груп. Це дослідження визначило методи, які використовують ці групи, а також те, як вони атакують і реалізують усі процеси від розвідки до дій на кінцевих точках. У цьому дослідженні визначено потенційні цілі досліджуваних груп APT і те, як ці групи можуть використовувати свої можливості для компрометації цільової інфраструктури. В контексті даного дослідження нас цікавить саме дослідження APT28, оскільки ця група є одним з найпомітніших фігурантів в атаках націлених на Україну.

У досліджені Вей Хань [3] була запропонована нова структура виявлення зловмисного програмного забезпечення APT під назвою APTMalInsight, спрямована на ідентифікацію та розпізнавання зловмисного програмного забезпечення яке використовується APT групами шляхом використання інформації про системні виклики та знань онтології. Було виявлено, що зі огляду на встановлені вектори функцій, зловмисне програмне забезпечення APT може бути точно виявлено та згруповано у відповідні родини.

У дослідженні Нахаата Мохамеда [4] представлено анатомію груп APT і використані техніки та тактики, а також зловмисне програмне забезпечення, яке використовується для атак на уряди та приватні установи по всьому світу. У цьому ж контексті ця стаття підкреслює важливість аналізу загроз у процесі передбачення та протидій атакам шляхом розуміння методів, які використовують APT групи під час атаки.

Метою статті є аналіз кібератак та діяльності APT груп націлених на Україну, виявлення їх патернів та закономірностей для отримання даних про методи атак та розуміння як працюють використовувані ними інструменти, щоб на основі цих даних розробити рекомендації для протидії.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Досліджуючи звіти про атаки націлені на Україну від Cert-UA та низки закордонних джерел [5] – [23] можна помітити, що в Україні діє щонайменше 8 APT груп, хоча їх кількість може бути більшою. Серед цих груп були помічені такі групи, як: Winter Vivern, Turla, Sandworm, Fancy Bear (APT28), Scarab, TrickBot, GhostWriter,

Gamaredon. Діяльність деяких з них була помітна з 2014 року, але найбільший сплеск їхньої активності був помічений з 2022 року. Варто зазначити, що усі групи окрім Scarab є напряму пов'язані з Росією.

Далі наведений аналіз атак цих APT груп на українську інфраструктуру.

Winter Vivern. Для розповсюдження зловмисного програмного забезпечення ця група використовує фішингові ресурси, що імітують офіційні веб-сторінки державних установ, з яких викачується програмне забезпечення. Шкідлива програма у вигляді BAT-файлу виконує PowerShell скрипти, що викачують файли та знімки екрану на підконтрольні зловмисникам домени. Для закріплення в системі жертв передбачений механізм створення запланованих завдань. Однією з характерних ознак групи є використання трояну APERITIF, який був помічений в попередніх кампаніях цієї групи. Основним мотивом групи є викрадання даних.

Turla. Для первинної компрометації ця група надсилала фішингові листи, що містили документи з шкідливим макросом, який містив PowerShell скрипти, що встановлює бекдор KAZUAR, який може збирати журнали подій з системи, викрадати облікові дані, файли, конфігурації програмного забезпечення. Помічено використання легітимних інструментів, таких як Rclone для викрадання даних. Також група використовує зловмисне програмне забезпечення CAPIBAR, що використовується для компрометації серверів MS Exchange, що дозволяє зловмисникам перетворити сервер на інструмент для дистанційного керування зловмисним програмним забезпеченням. Основним мотивом є викрадення даних.

Sandworm. Ця група помічне в масштабних атаках на енергетичну інфраструктуру України. Ще до 2022 року ця група була помічена в атаках з використанням трояну BlackEnergy та вірусом-вимагачем NotPetya. За звітами про останні атаки відомо, що вони були залучені для виведення з ладу високовольтних електричних підстанцій. Окрім цього, за ними була помічена компрометація систем на базі ОС WINDOWS за допомогою CANDDYWIPER, розповсюдження якого відбувалось за допомогою групових політик, що означає попередню компрометацію доменного контролера Виконання команд виконувалось за допомогою PowerShell, а горизонтальне переміщення забезпечувалось створенням ланцюгів SSH-тунелів. А також, ними була здійснена компрометація серверного обладнання під управлінням операційної систем Linux — за допомогою шкідливих скриптів-деструкторів ORCSHRED, SOLOSHRED, AWFULSHRED.

Fancy Bear (APT28). Ця група є однією з найбільш помітних в Україні та світі. За ними була помічена серія атак з використанням фішингових листів, які містили документи з шкідливими макросами. Ці макроси встановлювали різні шкідливі програми, наприклад програми сімейства CredoMap, головна мета яких — це викрадання файлів, даних автентифікації та надсилання їх, на підконтрольні зловмисникам, домени. Окрім цього, в деяких атаках, було помічено шкідливі вкладення в листах, що створювали фільтр «default filter» для перенаправлення вхідних електронних листів на сторонню електронну адресу, а також здійснювали вивантаження: адресної книги, файли cookie та електронних повідомлень жертви. Враховуючи активність цієї групи в інших атаках, це можна сприймати як першу стадію атаки, в якій вони збирають дані для планування подальших дій. Також в одній з атак було помічено використання більш розвинутих технік з використання вразливості прикладного протоколу «search» («ms-search») в операційній системі Windows. Завдяки цій вразливості встановлювався інтерпретатор мови програмування Python за допомогою якого довантажується та запускається OPENSSH для завантаження і вивантаження файлів та виконання віддалених команд. Окрім цього використовувалась OCEANMAP — шкідлива програма, розроблена з використанням мови програмування C#. Основний функціонал полягає у виконанні команд за допомогою cmd.exe та STEELHOOK — програми, яка представлена у вигляді PowerShell скрипту, що

забезпечує викрадення даних Інтернет-браузерів. Слід зауважити, що команди та дані, що вивантажувались були закодовані за допомогою base64.

GhostWriter. Група розповсюджувала PPT-документ, який містить шкідливий макрос, на систему жертви встановлювався Cobalt Strike Beacon, який надає можливість віддалено виконувати команди. Встановлення відбувалось через розшифрування контенту картинки в середині документу, що містив скрипти для його встановлення.

Gamaredon (Primitive Bear). За даними Cert-UA ця група спромоглась скомпрометувати декілька тисяч кінцевих точок в Україні. Для первинної компрометації використовувались месенджери та фішингові листи. Способами первинної компрометації були змінні носії інформації та документи Microsoft Office Word. В середині інфікованих файлів містились HTM або HTA-файли, запуск яких починав ланцюг компрометації. Для виконання команд використовувався PowerShell та VBScript. За потреби здійснення інтерактивного віддаленого доступу за допомогою PowerShell може бути встановлено Anydesk. Слід зауважити, що угрупування постійно підлаштовується до вживаних засобів та методів захисту. Зокрема, з метою обходу двофакторної автентифікації реалізовано PowerShell-сценарій, який забезпечує викрадення даних сесії (Cookie). Як правило, для забезпечення персистентності та запуску пейлоадів використовуються заплановані завдання, гілка реєстру Run, а також змінні середовища. Результатом діяльності зловмисних програм було викрадення ряду даних через вивантаження файлів та знімків екрану на підконтрольні зловмисникам домени.

TrickBot. Група використовувала фішингові листи з ISO-файлом, що містив документ приманку який відкривався через LNK-файл. Для приховання зловмисної активності відкривався документ приманка, а тим часом PowerShell скрипт компрометував систему жертви, встановлюючи Meterpreter, який надає можливість виконання віддалених команд.

Scarab. Це група китайського походження і є єдиною напряму не пов’язаною з Росією. Група використовувала фішингові листи, які містили шкідливе програмне забезпечення HeaderTip. Основним функціоналом програми є завантаження та виконання DLL файлів, що містили інші модулі шкідливого програмного забезпечення, а також комунікація з сервером зловмисників для виконання віддалених команд. Постійна присутність на системі жертви забезпечувалась через модифікації реєстрів.

Підсумовуючи аналіз активності цих груп можна помітити наступні закономірності:

- Найбільш популярним способом розповсюдження шкідливого програмного забезпечення є надсилання фішингових листів. Рідше використовувались месенджери та веб-ресурси, що імітували справжні сторінки державних установ;
- Найпопулярнішим способом первинної компрометації документ, що інфікований зловмисним макросом, який встановлює інші компоненти зловмисного програмного забезпечення;
- Зловмисники часто використовують шкідливі програми які вони самі розробляють та постійно удосконалюють для обходу систем захисту;
- Найчастіше для виконання команд використовується мови PowerShell та Bat;
- Помічено використання легітимних інструментів, що ускладнює виявлення зловмисної активності;
- Основними мотивами атак були викрадання даних та отримання контролю на системою чи цілою мережею жертви.

Для кращого відображення тактик, технік та процедур, які використовували APT групи, вони відображенні у таблиці відповідно до фреймворку Mitre [24]. Таблиця містить усі техніки які використовувались відповідно до фази атаки.

Таблиця 1

Техніки використані APT групами

Фаза	Техніки
Reconnaissance	– Phishing for Information – Search Open Websites/Domains – Search Victim-Owned Websites
Initial Access	– Exploit Public-Facing Application – Drive-by Compromise – External Remote Services – Replication Through Removable Media – Trusted Relationship – Valid Accounts
Execution	– Cloud Administration Command – Exploitation for Client Execution – Native API – Software Deployment Tools – Windows Management Instrumentation
Persistence	– Account Manipulation – BITS Jobs – Boot or Logon Autostart Execution – Compromise Client Software Binary – Create Account – External Remote Services – Valid Accounts
Privilege Escalation	– Account Manipulation – Boot or Logon Autostart Execution – Exploitation for Privilege Escalation – Process Injection – Valid Accounts
Defense Evasion	– BITS Jobs – Deobfuscate/Decode Files or Information – Exploitation for Defense Evasion – Indicator Removal – Masquerading – Modify Registry – Obfuscated Files or Information – Process Injection – Rootkit – Template Injection – Use Alternate Authentication Material – Valid Accounts
Credential Access	– Brute Force – Credentials from Password Stores – Multi-Factor Authentication Request Generation – Network Sniffing – OS Credential Dumping – Steal Application Access Token – Steal or Forge Authentication Certificates – Steal Web Session Cookie
Discovery	– Account Discovery – Application Window Discovery – Domain Trust Discovery – File and Directory Discovery

	– Group Policy Discovery – Network Service Discovery – Network Share Discovery – Network Sniffing – Password Policy Discovery – Peripheral Device Discovery – Permission Groups Discovery – Process Discovery – Query Registry – Remote System Discovery – Software Discovery – System Information Discovery – System Network Configuration Discovery – System Network Connections Discovery – System Owner/User Discovery – System Service Discovery – System Time Discovery
Lateral Movement	– Exploitation of Remote Services – Lateral Tool Transfer – Remote Services – Replication Through Removable Media – Software Deployment Tools – Taint Shared Content – Use Alternate Authentication Material
Collection	– Archive Collected Data – Audio Capture – Automated Collection – Data from Information Repositories – Data from Local System – Data from Network Shared Drive – Data from Removable Media – Data Staged – Screen Capture – Video Capture
Command and Control	– Communication Through Removable Media – Dynamic Resolution – Encrypted Channel – Fallback Channels – Ingress Tool Transfer – Non-Application Layer Protocol – Non-Standard Port – Proxy – Remote Access Software – Web Service
Exfiltration	– Data Transfer Size Limits – Exfiltration Over C2 Channel – Exfiltration Over Web Service
Impact	– Data Destruction – Data Encrypted for Impact – Endpoint Denial of Service – Inhibit System Recovery – Network Denial of Service – Service Stop

Основні методи протидії атак APT груп

Так як фішингові листи є найпопулярнішим методом надсилання шкідливого програмного забезпечення, протидія фішингу вимагає комплексного підходу. В нього входять як технічні рішення, так і організаційні заходи.

До технічних заходів можна виділити:

- Фільтрація електронної пошти. Використання спеціалізованих сервісів для фільтрації пошти, які можуть виявляти і блокувати фішингові листи, спам та інші підозрілі повідомлення та налаштування SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) і DMARC (Domain-based Message Authentication, Reporting & Conformance) записів для зменшення кількості спаму та фальшивих листів;
- Запровадження 2FA для всіх корпоративних аккаунтів, щоб ускладнити зловмисникам доступ до ресурсів, навіть якщо вони отримали пароль;
- Обмежити використання сторонніх поштових сервісів на службовому обладнанні, що нівелює існуючий периметр безпеки (вміст і вкладення електронних листів не перевіряються засобами захисту).

До організаційних заходів можна виділити:

- Розробка та впровадження чіткої політики безпеки, яка включає правила користування електронною поштою та вимоги до обізнаності співробітників про фішинг. Регулярне оновлення цієї політики з огляду на нові загрози;
- Проведення регулярних тренінгів з кібербезпеки для співробітників для підвищення їх обізнаності про фішинг, методи розпізнавання підозрілих листів та дії при їх отриманні;
- Симуляції фішингових атак для практики розпізнавання та реагування на фішинг.

Також для кращого виявлення і протидії загроз слід впровадити концепції нульової довірити (Zero Trust) та поглибленого захисту (Defense in depth).

Архітектура нульової довіри — це концепція безпеки, яка передбачає відсутність довіри до будь-якого користувача або пристрою, незалежно від їхнього місцезнаходження або мережевого підключення. Вона спрямована на захист чутливих ресурсів, шляхом впровадження суворого контролю доступу та постійного моніторингу і перевірки поведінки користувачів і пристроїв [25].

Концепція полягає у наступному:

- Контроль доступу через впровадження принципу найменших привілеїв, контроль доступу на основі ролей для призначення дозволів користувачам і групам та жорстким контролем адміністративного доступу;
- Використанні багатофакторної автентифікації для всіх облікових записів користувачів, включаючи привілейовані облікові записи та в впровадженні адаптивної автентифікації, яка коригує рівень автентифікації на основі факторів ризику;
- Впровадження постійного моніторингу мережевого трафіку, сегментації мережі для ізоляції критично важливих активів та впровадження системи виявлення та запобігання вторгнень для виявлення та блокування зловмисної мережевої активності;
- Впровадження інструментів аналізу поведінки користувачів та організацій для виявлення аномальних моделей поведінки;

- Забезпечення безперервного моніторингу та захисту кінцевих точок, впроваджуючи передові рішення для захисту, які включають антивірусне програмне забезпечення, моніторинг цілісності файлів інструменти SIEM та EDR;
- Впровадження плану реагування на інциденти, встановлення чітких процедур для виявлення, локалізації та ліквідації загроз.

Поглиблений захист (Defence in Depth) — це стратегічний підхід до забезпечення безпеки, який використовує багаторівневу систему захисних механізмів для мінімізації ризиків та захисту ресурсів. Ця концепція базується на принципі, що захист повинен включати кілька рівнів оборони на різних етапах, так що якщо один захисний бар'єр не вдасться, інші продовжать забезпечувати захист. Цей підхід є комплексним і включає фізичну безпеку, технічні заходи, адміністративні контролі, правила поведінки та реагування на інциденти, щоб створити повноцінну оборону проти потенційних загроз. Багаторівневий підхід до безпеки в системі поглибленого захисту включає елементи з наступних областей:

- Фізичні засоби контролю: наприклад, ключ-картки для входу в будівлю або сканери для зчитування відбитків пальців;
- Контроль безпеки мережі: це програмне забезпечення, яке автентифікує співробітника для входу в мережу та використання пристрою чи програми;
- Адміністративний контроль: це дозволяє співробітникам після автентифікації отримувати доступ лише до певних програм або частин мережі;
- Захист кінцевих точок: набір інструментів, який запобігає проникненню та поширенню шкідливого програмного забезпечення в мережі;
- Аналіз поведінки: алгоритми та машинне навчання можуть виявляти аномалії в поведінці співробітників, а також у самих програмах і пристроях.

Впровадження згаданих концепцій, інструментів та підходів це тяжкий і тривалий процес, але він є життєво необхідним, оскільки атаки APT груп несуть велику загрозу та вимагають комплексного підходу до захисту.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

За останнє десятиліття, активність груп APT в Україні значно зросла, що виявляється в збільшенні кількості та складності кібератак. Основні цілі цих атак зосереджені на критичній інфраструктурі, державних інституціях, та військових об'єктах, які відображають геополітичні інтереси замовників цих операцій. Групи, що досліджувались у цій роботі, продемонстрували здатність використовувати витончені механізми для проведення спланованих кампаній, включаючи використання власноруч розроблених програм та інструментів, поліморфних та метаморфічних вірусів, атаки на ланцюги поставок, і використання легітимних інструментів в свої атаках.

Ці APT атаки виявляють значні проблеми в системах кіберзахисту, особливо з виявленням і блокуванням таких складних загроз, які часто маскуються під легітимні процеси та інструменти. Відповідь на такі загрози вимагає від урядів та організацій впровадження комплексних захисних стратегій, які поєднують технічні та організаційні заходи. Технічні заходи включають застосування фільтрації електронної пошти, багатофакторної автентифікації, сучасних рішень для моніторингу та протидії загрозам та систем виявлення аномалій, тоді як організаційні заходи мають включати чітке

формулювання політик безпеки, регулярне навчання співробітників, і симуляції фішингових атак для підвищення обізнаності і підготовки.

Ключовим елементом ефективної стратегії кіберзахисту є міжнародне співробітництво, особливо у світлі глобалізації кіберпростору та міжнародного характеру APT загроз. Співпраця може включати обмін розвідданими, спільні дослідження та розробку стандартів і технологій кіберзахисту. У цьому контексті, уряди повинні також активізувати законодавчі та нормативні ініціативи для створення правових основ захисту критичної інфраструктури та відповідального реагування на інциденти.

Завершуючи, необхідно відзначити, що успіх у протидії APT атакам залежить не тільки від технологій, але й від стратегічного підходу, що включає постійне оновлення методів захисту, адаптацію до нових загроз, та активну міжнародну взаємодію. Враховуючи постійно зростаючу загрозу від APT атак, кібербезпека повинна бути визначена як один з пріоритетів національної безпеки для держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hönö, O. (2023). From moonlight maze to solarwinds: how russian apt groups operate? *Master's Thesis. Jyväskylä.*
2. Mwiki, H., Dargahi, T., Dehghantanha, A., & Choo, K.-K. R. (2019). Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin. *Critical Infrastructure Security and Resilience,* 221–244. https://doi.org/10.1007/978-3-030-00024-0_12
3. Han, W. et al. (2021). APTMalInsight: Identify and cognize APT malware based on system call information and ontology knowledge framework. *Information Sciences, 546,* 633–664.
4. Mohamed, N. (2022). State-of-the-Art in Chinese APT Attack and Using Threat Intelligence for Detection. A Survey. *Journal of Positive School Psychology, 6(5),* 4419–4443.
5. *Активність групи UAC-0114 (Winter Vivern) у відношенні державних органів України та Польщі (CERT-UA#5909).* (б.д.). cert.gov.ua. https://cert.gov.ua/article/3761023
6. *Кібератака групи APT28 з використанням шкідливої програми CredoMap (CERT-UA#4843).* (б.д.). cert.gov.ua. https://cert.gov.ua/article/341128
7. *Кібератака групи APT28 із застосуванням шкідливої програми CredoMap_v2 (CERT-UA#4622).* (б.д.). cert.gov.ua. https://cert.gov.ua/article/40102
8. *Кібератака групи APT28: розповсюдження електронних листів з «інструкціями» щодо «оновлення операційної системи» (CERTUA#6562).* (б.д.). cert.gov.ua. https://cert.gov.ua/article/4492467
9. *Кібератака групи Sandworm (UAC-0082) на об'єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435).* (б.д.). cert.gov.ua. https://cert.gov.ua/article/39518
10. *Кібератака групи UAC-0026 з використанням шкідливої програми HeaderTip (CERT-UA#4244).* (б.д.). cert.gov.ua. https://cert.gov.ua/article/38097
11. *Кібератака групи UAC-0035 (InvisiMole) на державні організації України (CERT-UA#4213).* (б.д.). cert.gov.ua. https://cert.gov.ua/article/37829
12. *Кібератака групи UAC-0098 на державні органи України із застосуванням фреймворку Metasploit (CERT-UA#4560).* (б. д.). https://cert.gov.ua/article/39934
13. *Цільові атаки Turla (UAC-0024, UAC-0003) з використанням шкідливих програм CAPIBAR та KAZUAR (CERT-UA#6981).* (б.д.). cert.gov.ua. https://cert.gov.ua/article/5213167
14. *Cyber Operations during the Russo-Ukrainian War.* (n.d.). www.csis.org. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war
15. *2022 ICS Attacks: Fewer-Than-Expected on US Energy Sector, But Ransomware Surged.* (n.d.). SecurityWeek. https://www.securityweek.com/2022-ics-attacks-fewer-than-expected-on-us-energy-sector-but-ransomware-surged/
16. *Energy Provider in Ukraine Targeted With Industroyer2 ICS Malware.* (n.d.). SecurityWeek. https://www.securityweek.com/energy-provider-ukraine-targeted-industroyer2-ics-malware/
17. *Chinese threat actor Scarab targets Ukraine, CERT-UA warns.* (n.d.). Security Affairs. https://securityaffairs.com/129477/apt/chinese-threat-actor-scarab-targets-ukraine-cert-ua-warns.html

18. *Gamaredon APT Improves Toolset to Target Ukraine Government, Military.* (n.d.). Threatpost | The first stop for security news. https://threatpost.com/gamaredon-apt-toolsetukraine/152568/
19. *Possible APT attacks against Ukraine expand to target journalists, researchers say.* (n.d.). CyberScoop. https://cyberscoop.com/gamaredon-apt-ukraine-anomali-foritnet/
20. *Ukraine Targeted by Chinese Threat Actor Group, Scarab.* (n.d.). www.anvilogic.com. https://www.anvilogic.com/threat-reports/scarab-attacks-ukraine-china
21. *Pro-Russian CyberSpy Gamaredon Intensifies Ukrainian Security Targeting - SentinelLabs.* (n.d.). SentinelOne. https://www.sentinelone.com/labs/pro-russian-cyberspy-gamaredon-intensifies-ukrainian-security-targeting/
22. *Russian Cybercrime Trickbot Group is systematically attacking Ukraine.* (n.d.). Security Affairs. https://securityaffairs.com/132999/cyber-crime/trickbot-systematically-attacking-ukraine.html
23. *Unprecedented shift: The Trickbot group is systematically attacking Ukraine*. (n.d.). securityintelligence.com. https://securityintelligence.com/x-force/trickbot-group-systematically-attacking-ukraine/
24. *Enterprise Matrix.* (n.d.). attack.mitre.org. https://attack.mitre.org/matrices/enterprise/
25. Журавчак, Д., Глущенко, П., Опанович, М., Дудикевич, В., & Піскозуб, А. (2023). Концепція нульової довіри для захисту active directory для виявлення програм-вимагачів. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22),* 179–190. https://doi.org/10.28925/2663-4023.2023.22.179190

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023

Maksym Opanovych
Postgraduate student of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-2748-2965
maksym.y.opanovych@lpnu.ua

ANALYSIS OF CYBER ATTACKS AND THE ACTIVITIES OF APT GROUPS IN UKRAINE

Abstract. The article is devoted to the analysis of cyberattacks and the activities of the APT (Advanced Persistent Threat) group in Ukraine, which significantly intensified the trend of the last decade in the context of the growing globalization of information warfare and political conflicts. The paper takes an in-depth look at the methods, tactics, and procedures (TTP) used by known APT groups such as Sandworm, Fancy Bear (APT28), and Gamaredon to carry out targeted cyber-attacks against Ukraine. The main focus of the article is the identification of patterns in the activities of APT groups and the formation of recommendations for the development of effective cyber protection strategies. The work uses data from open sources, CERT-UA reports, and analytical materials of international companies to assess the current state of cyber security and identify existing vulnerabilities that can be used by attackers. The article details various cyber-attack techniques that include the use of polymorphic and metamorphic malware, supply chain attacks, and methods, tactics, and procedures according to the Mitre framework. Considerable attention is paid to strategies for protection against APT attacks, with a special focus on zero trust architecture (Zero Trust) and defense in depth (Defense in Depth), which includes the application of multi-level protection systems to minimize risks and ensure recovery after incidents. Also discussed are tactics to counter attackers, the use of advanced network and endpoint security solutions, and the widespread adoption of multi-factor authentication and methods to protect against phishing attacks. The article emphasizes the importance of a comprehensive approach to the construction of a protection system, which includes both technical and organizational aspects. The results of the study emphasize ensuring the constant updating of technologies and methods of threat analysis for an adequate response to modern and future cyber-attacks.

Keywords: APT; cyber threats; cyber war; Mitre; Zero Trust; Defence in Depth.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Hönö, O. (2023). From moonlight maze to solarwinds: how russian apt groups operate? *Master's Thesis. Jyväskylä.*
2. Mwiki, H., Dargahi, T., Dehghantanha, A., & Choo, K.-K. R. (2019). Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin. *Critical Infrastructure Security and Resilience*, 221–244. https://doi.org/10.1007/978-3-030-00024-0_12
3. Han, W. et al. (2021). APTMalInsight: Identify and cognize APT malware based on system call information and ontology knowledge framework. *Information Sciences, 546,* 633–664.
4. Mohamed, N. (2022). State-of-the-Art in Chinese APT Attack and Using Threat Intelligence for Detection. A Survey. *Journal of Positive School Psychology, 6(5),* 4419–4443.
5. *Activity of the UAC-0114 (Winter Vivern) group in relation to the state bodies of Ukraine and Poland (CERT-UA#5909).* (n.d.). cert.gov.ua. https://cert.gov.ua/article/3761023
6. *Cyber attack by the APT28 group using the CredoMap malicious program (CERT-UA#4843).* (n.d.). cert.gov.ua. https://cert.gov.ua/article/341128
7. *Cyberattack by the APT28 group using the CredoMap_v2 malicious program (CERT-UA#4622).* (n.d.). cert.gov.ua. https://cert.gov.ua/article/40102
8. *APT28 cyberattack: distribution of emails with "instructions" for "updating the operating system" (CERTUA#6562).* (n.d.). cert.gov.ua. https://cert.gov.ua/article/4492467

9. *Cyber attack of the Sandworm group (UAC-0082) on the energy facilities of Ukraine using malicious programs INDUSTROYER2 and CADDYWIPER (CERT-UA#4435).* (n.d.). cert.gov.ua. https://cert.gov.ua/article/39518
10. *Cyber attack of the UAC-0026 group using the HeaderTip malware (CERT-UA#4244).* (n.d.). cert.gov.ua. https://cert.gov.ua/article/38097
11. *Cyber attack of the UAC-0035 group (InvisiMole) on state organizations of Ukraine (CERT-UA#4213).* (n.d.). cert.gov.ua. https://cert.gov.ua/article/37829
12. *Cyber attack of the UAC-0098 group on the state bodies of Ukraine using the Metasploit framework (CERT-UA#4560).* (n.d.). https://cert.gov.ua/article/39934
13. *Targeted Turla attacks (UAC-0024, UAC-0003) using CAPIBAR and KAZUAR malware (CERT-UA#6981).* (n.d.). cert.gov.ua. https://cert.gov.ua/article/5213167
14. *Cyber Operations during the Russo-Ukrainian War.* (n.d.). www.csis.org. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war
15. *2022 ICS Attacks: Fewer-Than-Expected on US Energy Sector, But Ransomware Surged.* (n.d.). SecurityWeek. https://www.securityweek.com/2022-ics-attacks-fewer-than-expected-on-us-energy-sector-but-ransomware-surged/
16. *Energy Provider in Ukraine Targeted With Industroyer2 ICS Malware*. (n.d.). SecurityWeek. https://www.securityweek.com/energy-provider-ukraine-targeted-industroyer2-ics-malware/
17. *Chinese threat actor Scarab targets Ukraine, CERT-UA warns.* (n.d.). Security Affairs. https://securityaffairs.com/129477/apt/chinese-threat-actor-scarab-targets-ukraine-cert-ua-warns.html
18. *Gamaredon APT Improves Toolset to Target Ukraine Government, Military.* (n.d.). Threatpost | The first stop for security news. https://threatpost.com/gamaredon-apt-toolsetukraine/152568/
19. *Possible APT attacks against Ukraine expand to target journalists, researchers say.* (n.d.). CyberScoop. https://cyberscoop.com/gamaredon-apt-ukraine-anomali-foritnet/
20. *Ukraine Targeted by Chinese Threat Actor Group, Scarab.* (n.d.). www.anvilogic.com. https://www.anvilogic.com/threat-reports/scarab-attacks-ukraine-china
21. *Pro-Russian CyberSpy Gamaredon Intensifies Ukrainian Security Targeting - SentinelLabs.* (n.d.). SentinelOne. https://www.sentinelone.com/labs/pro-russian-cyberspy-gamaredon-intensifies-ukrainian-security-targeting/
22. *Russian Cybercrime Trickbot Group is systematically attacking Ukraine.* (n.d.). Security Affairs. https://securityaffairs.com/132999/cyber-crime/trickbot-systematically-attacking-ukraine.html
23. *Unprecedented shift: The Trickbot group is systematically attacking Ukraine.* (n.d.). securityintelligence.com. https://securityintelligence.com/x-force/trickbot-group-systematically-attacking-ukraine/
24. *Enterprise Matrix.* (n.d.). attack.mitre.org. https://attack.mitre.org/matrices/enterprise/
25. Zhuravchak, D., Glushchenko, P., Opanovych, M., Dudykevych, V., & Piskozub, A. (2023). A zero-trust concept for active directory protection to detect ransomware. *Electronic specialized scientific publication "Cybersecurity: education, science, technology", 2(22),* 179–190. https://doi.org/10.28925/2663-4023.2023.22.179190