DOI: 10.18372/2410-7840.22.14977
УДК 654.071

АНАЛІЗ АТАК, ЩО ВИКОРИСТОВУЮТЬСЯ КІБЕРЗЛОЧИНЦЯМИ ПІД ЧАС ПАНДЕМІЇ COVID 19

Віталій Сусукайло, Іван Опірський, Андріян Піскозуб, Ростислав Волошин, Олег Друзюк

За даними Всесвітньої організації охорони здоров'я, пандемія визначається як „поширення нової хвороби у всьому світі ". З точки зору кібербезпеки це означає - катастрофа. Під час катастроф кількість кіберзлочинців зростає щодня. По мірі того як все більше висококваліфікованих фахівців з кібербезпеки долучається до блакитної команди, щодня запускається все більше шкідливих аплікацій, приблизно 230000 нових зразків шкідливих програм на день, згідно з інформацією дослідників з PandaLabs. Пандемію можна розглядати як подію, яка може призвести до виконання планів безперервності бізнесу або реалізації заходів з аварійного відновлення. Протягом цього часу слід аналізувати зростаючу кількість загроз кібербезпеки та визначати застосовні заходи безпеки. Існує також багато проблем з адміністративною інформаційною безпекою, які також слід враховувати. У цій статті розкрито основні питання щодо моніторингу інфраструктури, а також забезпечення високого рівня управління вразливостями та реагування на інциденти. Наведено заходи управління, які необхідно використовувати у SOC центрах, а також представлено поглиблений аналіз векторів атак та заходів безпеки, які можна застосувати для їх запобігання. Визначено, що віддалений моніторинг безпеки повинен бути зосереджений на аналізі подій з кінцевих точок за допомогою хост-систем виявлення вторгнень, рішень для виявлення і реагування на кінцеві точки, а також програмного забезпечення для забезпечення безпеки кінцевих точок, яке дозволяє дистанційно керувати і агрегувати події в центральній консолі.

***Ключові слова**: вектор атаки, шкідливе програмне забезпечення, реагування на інциденти, безперервність бізнесу, Cyber Kill Chain.*

Вступ. Ситуація з пандемією COVID-19 змінила принципи роботи. Люди були стурбовані, і з занепокоєнням вони хотіли отримати інформацію, відчуття безпеки та підтримки. У той же час організовані злочинні групи використовують страх, невпевненість і сумніви, пов'язані з COVID-19, роблячи вразливими людей та цілі компанії. Через цю ситуацію приватні організації та державні установи почали забезпечувати дистанційну оперативну діяльність, що спричиняє багато проблем із безпекою.

У той же час критично важливі об'єкти інфраструктури, такі як експлуатаційні, інфраструктурні стаціонарні активи та IoT, стали першочерговими об'єктами для суб'єктів загрози. Поглиблений аналіз поверхні атаки та стану кібербезпеки під час COVID-19 визначив чотири основні виклики кібербезпеки, описані нижче.

- Недостатній захист критичної інфраструктури. Наступна проблема може призвести до збільшення кількості приватних та державних SOC центрів. Крім того, це може вплинути на якість послуг, які надають SOC центри, експерти з кібербезпеки повинні забезпечити високий рівень моніторингу безпеки, управління вразливістю та реагування на інциденти, щоб гарантувати відсутність перебоїв у роботі критичної інфраструктури та захист персональних даних клієнтів.

- На сьогодні недостатня кількість фахівців з кібербезпеки є актуальною проблемою, і ситуація з пандемією показує, наскільки важливо мати кваліфікованих експертів, що забезпечує захист інформації в державних та приватних організаціях. Наступна проблема може призвести до вдосконалення системи освіти в галузі кібербезпеки та збільшення кількості закладів, які можуть підготувати кваліфікованих фахівців [2].

- Необхідно вдосконалити процеси безперервності бізнесу та заходи з аварійного відновлення. Ситуація з COVID-19 показала, що багато оперативних заходів з безпеки неможливо виконувати віддалено в організаціях, які будують свої рішення

щодо безпеки на локальних активах інфраструктури. Очікується, що кінцевим користувачам, що використовують ПЗ в якості моделі обслуговування, буде надаватися більше вирішень з кібербезпеки, а також буде застосовуватися більш агентоорієнтований підхід.

- Недостатній рівень обізнаності в галузі соціальної інженерії. Хакери озброїлись картою COVID-19, маніпулювали інформацією ВООЗ та інших медичних організацій, створили багато заражених фішинг-сайтів, що поставило під загрозу мільйони користувачів. Наступна проблема може призвести до збільшення кількості державних програм інформування про соціальну інженерію.

Аналіз векторів атак. Найпоширенішими та найпопулярнішими нападами під час пандемії є група атак соціальної інженерії, яка використовує страхи людей або співчуття (рис.1).

Для аналізу були відібрані атаки соціальної інженерії під час COVID-19, в яких використовувалося шкідливе програмне забезпечення Alozurt.

Рис. 1 Атаки з використанням соціальної інженерії

На етапі розвідки зловмисник досліджував найпоширеніші страхи кінцевих користувачів - необхідність інформації про COVID-19. Найпопулярнішими ресурсами, які користувачі відвідали під час пандемії, були інтерактивні карти COVID-19, які передавали інформацію про стан зараження в різних країнах.

Тож зловмисники використовували страхи людей і створили тисячі підроблених карт COVID 19 та веб-сайти з неправдивими новинами.

Після вибору способу зараження зловмисники вибирали шкідливе програмне забезпечення.

Популярним був Azolurt - це шкідливе програмне забезпечення для крадіжки інформації, яке націлене на викрадення облікових даних та облікових записів[5].

Для доставки Azolurt було використано зловмисне програмне забезпечення для підроблених онлайн-карт COVID-19 або фішинг-листів. Шкідливе програмне забезпечення було доставлено у вигляді документа Microsoft Office, що полегшило зловмисникам маніпуляції зі страхами кінцевих користувачів. Коли користувач відкрив файл, шкідливе програмне забезпечення використовує вразливість CVE-2017-11882 Microsoft Office Equation Editor і завантажує шкідливий файл. Потім зловмисний файл вносить зміни в реєстр, що відповідає за автозапуск.

На завершальному етапі зловмисне програмне забезпечення запускається самостійно, а потім приступає до викрадення персональних даних та підключення до серверів керування та управління. По-

тім зловмисний файл запускає cmd.exe, щоб видалити себе через 3-секундний тайм-аут.

Перший вектор атаки показує, як суб'єкти загрози використовують страхи кінцевих користувачів. Другий вектор атаки, який складається з методів соціальної інженерії під час пандемії, покладається на людське співчуття. Зловмисники створили кілька підроблених благодійних веб-сайтів, щоб обдурити людей та заробити кошти або скомпрометувати активи кінцевих користувачів шкідливим програмним забезпеченням.

Третім вектором атаки, який використовує методи соціальної інженерії, є неправдиві інтернет-магазини, які продають ліки або медичні товари. Метою таких веб-сайтів є фінансова вигода. Для запобігання цьому типу атак засоби управління інформаційною безпекою повинні посилатися на стратегію оборонного захисту інформації. Першим засобом контролю, який можна застосувати для уникнення атак соціальної інженерії, є сеанси інформування або тренінги, які містять приклади підроблених COVID 19 ресурсів, таких як coronavirus-map.com та офіційні ресурси, які необхідно використовувати, такі як www.who.int. Результати обізнаності можуть бути протестовані шляхом проведення фальшивої фішинг-атаки на вибрану групу осіб, які відвідували тренінг. Другим контролем може бути включення модулів виявлення фішингу та сканування зловмисного програмного забезпечення електронної пошти в програмному забезпеченні безпеки кінцевої точки та в налаштуваннях системи доставки електронної пошти - GSuite, Office 365 вже має можливості виявлення та запобігання фішингу [7]. Також, щоб уникнути цього типу атак, можна встановити розширення браузера VirusTotal, що забезпечить фільтрацію веб-сайтів.

Атаки, які переривають критично важливі бізнес-функції. Щоб забезпечити безперервність бізнесу під час пандемії, комерційним організаціям потрібно надати високоякісні можливості дистанційної роботи де це можливо. Ось чому найпоширенішими службами під час віддаленої роботи є послуги VPN, SaaS, хмарні технології, програмне забезпечення для проведення конференцій тощо. Для аналізу векторів атак на важливий бізнес були обрані функції атак на програмне забезпечення для конференцій Zoom.

Протягом березня-квітня 2020 року програмне забезпечення Zoom було основною ціллю зловмисників. Щодня джерела інформації про загрози інформували про проблеми безпеки та конфіденційності програмного забезпечення Zoom, близько 500000 облікових записів Zoom, проданих на хакерських форумах, у настільних додатках Zoom виявлялись численні критичні вразливості, хмарна служба, яка зберігала записані конференції, була скомпрометована. Але найпоширенішою проблемою було Zoombombing, яке дозволяє зловмисникам приєднуватися до незахищених зустрічей Zoom. Наступна проблема могла призвести до компрометації вмісту зустрічі, переривання критичної для бізнесу зустрічі, зараження кінцевих користувачів шкідливим програмним забезпеченням.

Найгірший сценарій, який може вплинути на організацію, - це зараження кінцевих користувачів шкідливим програмним забезпеченням через обмін ним в чаті Zoom. Коли зловмисне програмне забезпечення надається під законним псевдонімом користувача, інші користувачі можуть завантажити його та встановити на свої активи. На рис. 2. представлена атака через програмне забезпечення для проведення конференцій Zoom, що описує можливий вектор атаки, який використовується суб'єктом загрози для компрометації організації через незахищених користувачів.

Першим контролем інформаційної безпеки, щоб уникнути атак через програмне забезпечення для проведення конференцій Zoom, має бути встановлений захист паролем для конференц-залів. Постійні оновлення підписів шкідливого програмного забезпечення та глибоке сканування файлів можуть допомогти виявити шкідливі файли, якими користуються Zoom. Крім того, рекомендується використовувати програмне забезпечення виявлення та реагування на кінцеві точки, таке як

Wazuh, для виявлення аномалій потенційно зараженого активу.

Напади на критично важливу інфраструктуру. Ще однією основною мішенню для нападників під час пандемії стали лікарні та організації охорони здоров'я. Зловмисники використовували стандартні методи для компрометації інфраструктури та IoT-пристроїв через вразливості в програмному забезпеченні і службах рис.3. Початковий вектор атаки був здійснений через сторонні служби. У квітні 2020 року було зламано 25 000 акаунтів ВООЗ, Фонду Гейтса, NIH. Як повідомили наступні організації, атака проводилася на ресурси, не пов'язані з організаціями охорони здоров'я, а на сервіси, де ці облікові записи використовувалися для реєстрації. Щоб уникнути атак через сторонні сервіси, організації, які інтегрують кілька сервісів в одну інфраструктуру, повинні встановити процес перевірки безпеки постачальників послуг.

Профілактичні заходи. Пандемія ускладнює оперативну діяльність по забезпеченню безпеки. Фахівцям з кібербезпеки стає все важче виявляти загрози на ранній стадії і оперативно реагувати на них. Процеси забезпечення безпеки в організаціях під час пандемії повинні бути трансформовані. Для операційних центрів безпеки стало неможливим відслідковувати мережеві загрози, які можуть впливати на їх операційні активи і кінцевих користувачів. Ще одна проблема, викликана пандемічної ситуацією, контроль робочих станцій кінцевих користувачів. Для організацій, які використовують локальну інфраструктуру, стає неможливим управляти робочою станцією без активного VPN-з'єднання.

Під час епідемії необхідно забезпечити дистанційне керування кінцевими точками. Фахівці з кібербезпеки повинні мати можливість віддалено впроваджувати конфігурації безпеки. Повинні застосовуватися такі політики безпеки, як політика паролів, політика блокування облікових записів і тощо. Операційна система і служби повинні оновлюватися автоматично. Віддалене підключення до ресурсів кінцевого користувача також має бути забезпечено для виконання дій з діагностики системи. Необхідно вдосконалювати стратегії зміцнення кінцевих точок. Для забезпечення безпечних умов роботи користувачів, що виконують свої повсякденні обов'язки з домашнього кінцевого програмного забезпечення безпеки повинні бути налаштовані так, щоб ними можна було керувати з "хмари" або як програмне забезпечення через центр управління послугами. Додатки для захисту від шкідливого ПО повинні отримувати сигнатури безпосередньо від джерел інформації про загрози постачальників. Програмне забезпечення для виявлення кінцевих точок і реагування на них з "хмарним" центром управління повинно бути встановлено на кінцевих точках кінцевих користувачів. Правила брандмауера кінцевих точок повинні бути налаштовані на дозвіл віддалених підключень до робочих станцій тільки з IP-адресу організації; непотрібні порти повинні бути відключені. Необхідно встановити рішення веб-фільтрації та управління додатками, які можуть мінімізувати ризик компрометації кінцевого користувача невідомими ресурсами. Це дозволить фахівцям з кібербезпеки здійснювати постійний моніторинг безпеки і виявляти аномалії на робочих станціях кінцевих користувачів.

Пандемія є проблемою для державних і приватних організацій, яка може привести до активації плану забезпечення безперервності бізнесу. Цифрове перетворення і міграція в хмару повинні бути розглянуті організаціями, які покладаються на локальну інфраструктуру. Вектор атак, що описує дії, які ставлять під загрозу критично важливі бізнес-функції, показує, наскільки важливо застосовувати конфігурації безпеки, що надаються виробником. У випадку з додатком Zoom необхідно було застосувати захист паролем для зборів, застосувати конфігурацію, яка вимагає, щоб учасники зборів були прийняті хостом, тимчасово не зберігати записані відео в хмарі Zoom і застосувати MFA.

Рис. 2 Атака за допомогою програмного забезпечення для проведення конференцій Zoom.

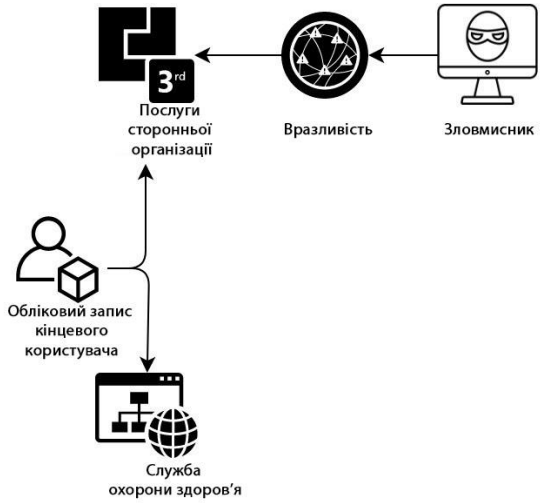

Рис.3 Атака на медичні сервіси

Ці прості заходи зміцнення захисту можуть бути використані для запобігання компрометації користувачів. Крім того, для захисту активів організації необхідно забезпечити безпечне підключення до локальних мереж організації. Щоб уникнути юридичних проблем, організаціям слід переглянути свої договірні угоди з клієнтами, які містять вимоги щодо інформаційної безпеки. Це дозволить організації запобігти порушенням контрактної угоди.

Віддалений моніторинг безпеки повинен бути зосереджений на аналізі подій з кінцевих точок за допомогою хост-систем виявлення вторгнень, рішень для виявлення і реагування на кінцеві точки, а також програмного забезпечення для забезпечення безпеки кінцевих точок, яке дозволяє дистанційно керувати і агрегувати події в центральній консолі. Крім того, аналітики з безпеки повинні звертати увагу на події та журнали, що надходять від служб організації і активів "хмарної" інфраструктури. Розподілена система управління інформацією про безпечність та подіями (SIEM), побудована на локальній інфраструктурі, є загальноприйнятим підходом.

Однак під час пандемічної ситуації було б більш доцільно проводити моніторинг безпеки з використанням SaaS SIEM, або SIEM, розгорнутої в "хмарній" інфраструктурі.

ЛІТЕРАТУРА

[1] *"Рекомендації щодо посилення боротьби за кібербезпеку під час COVID -19"* [Електронний ресурс] – Режим доступу до ресурсу: https://home.kpmg/ua/uk/home/insights/2020/04/covid-19-cyber-security.html.

[2] *Covid-19: основні тенденції в області кібер-безпеки* [Електронний ресурс] – Режим доступу до ресурсу: https://www.tandfonline.com/doi/full/10.1080/15265161.2020.1764136.

[3] John Wileym. Carbon Black Special Edition, *"Полювання на загрози для манекенів"*. Inc. 111 River St. Hoboken, 2017, pp. 9-10.

[4] O. Milov, A.Voitko, I. Husarova, I. Opirskyy, O. Fraze-Frazenko, Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems Eastern-European Journal of Enterprise Technologies, 2019. – pp. 55-66.

[5] "Alozurt - аналіз шкідливого ПЗ" [Електронний ресурс] – Режим доступу до ресурсу: https://any.run/malware-trends/azorult.

[6] *"Реагування на інциденти і усунення їх наслідків при віддаленій роботі"* [Електронний ресурс] – Режим доступу до ресурсу: https://www.crowdstrike.com/resources/crow dcasts/conducting-incident-response-and-reme diation-remotely.

[7] Іван Опірський, Андрій Винар. «Аналіз використання хмарних сервісів для фішингових атак»// *Кібербезпека: освіта, наука, техніка*, вип. 1, вип. 9, 2020. - С. 59-68.

АНАЛИЗ АТАК, ИСПОЛЬЗУЕМЫХ КИБЕРПРЕСТУПНИКАМИ ВО ВРЕМЯ COVID 19

По данным Всемирной организации здравоохранения, пандемия определяется как "распространение новой болезни во всем мире". С точки зрения кибербезопасности это значит - катастрофа. Во время катастроф количество киберпреступников растет каждый день. По мере того, как все больше высококвалифицированных специалистов по кибербезопасности вступает в голубый команды, ежедневно запускается все больше вредных аппликаций, примерно 230000 новых образцов вредоносных программ в день, по информации исследователей из PandaLabs. Пандемию можно рассматривать как событие, которое может привести к выполнению планов непрерывности бизнеса или реализации мер аварийного восстановления. В течение этого времени следует анализировать растущее количество угроз кибербезопасности и определять применимы меры безопасности. Существует также много проблем с административной информационной безопасностью, которые также следует учитывать. В этой статье раскрыты основные вопросы мониторинга инфраструктуры, а также обеспечения высокого уровня управления уязвимостями и реагирования на инциденты. Приведены меры управления, которые необходимо использовать в SOC центрах, а также представлено углубленный анализ векторов атак и мер безопасности, которые можно применить для их предотвращения. Представленная атака через программное обеспечение для проведения конференций Zoom, описывающая возможный вектор атаки, используемый субъектом угрозы для компрометации организации через незащищенных пользователей. Когда вредоносное программное обеспечение предоставляется под законным псевдонимом пользователя, другие пользователи могут скачать его и установить на свои активы. Определено, что первым средством контроля, которое можно применить во избежание атак социальной инженерии, является сеансы информирования или тренинги, которые содержат примеры поддельных COVID 19 ресурсов, а вторым - может быть включение модулей обнаружения фишинга и сканирования вредоносных программ электронной почты в программном обеспечении безопасности конечной точки и в настройках системы доставки электронной почты. Определено, что удаленный мониторинг безопасности должен быть сосредоточен на анализе событий из конечных точек с помощью хост-систем обнаружения вторжений, решений для выявления и реагирования на конечные точки, а также программного обеспечения для обеспечения безопасности конечных точек, которое позволяет дистанционно управлять и агрегировать события в центральной консоли. Кроме того, аналитики по безопасности должны обращать внимание на события и журналы, поступающих от служб организации и активов "облачной" инфраструктуры.

Ключевые слова: вектор атаки, вредоносное программное обеспечение, реагирование на инциденты, непрерывность бизнеса, Cyber Kill Chain.

ANALYSIS OF ATTACKS USED BY CYBER CRIMINALS DURING COVID 19

According to the World Health Organization, a pandemic is defined as "the spread of a new disease throughout the world." From a cybersecurity perspective, this means disaster. During disasters, the number of cybercriminals grows every day. As more and more highly qualified cybersecurity professionals join the blue team, more and more malicious applications are launched daily, with an estimated 230,000 new malware samples per day, according to researchers at PandaLabs. A pandemic can be viewed as an event that can lead to the fulfillment of business continuity plans or the implementation of disaster recovery measures. During this time, the growing number of cybersecurity threats should be analyzed and the applicable security measures determined. There are also considermany administrative information security issues. This article covers the main issues of infrastructure monitoring, as well as ensuring a high level of vulnerability management and incident response. Presented the management measures that must be used in SOC centers, as well as an in-depth analysis of attack vectors and security measures that can be applied to prevent them. A presented attack via Zoom conferencing software that describes the possible attack vector used by a threat actor to compromise an organization through unprotected users. When malware is provided under the user's legitimate pseudonym, other users can download it and install it on their assets. It has been determined that the first control that can be applied to avoid social engineering attacks is informative sessions or training sessions that contain examples of fake COVID 19 resources and the second could be the inclusion of phishing detection and email malware scanning modules in the endpoint security software and in the settings of the e-mail delivery system. It has been determined that remote security monitoring should focus on analyzing events from endpoints with host intrusion detection systems, endpoint detection and response solutions, and endpoint security software that allows remote control and aggregation of events across center console. In addition, security analysts should pay attention to events and logs from the organization's services and cloud infrastructure assets.

Keywords: attack vector, malware, incident response, business continuity, Cyber Kill Chain.

Сусукайло Віталій Андрійович аспірант кафедри захисту інформації Національного університету «Львівська політехніка».
E-mail: vitalii.a.susukailo@lpnu.ua.
Orcid ID: 0000-0003-4431-9964.
Сусукайло Виталий Андреевич аспирант кафедры защиты информации Национального университета «Львовская политехника».
Vitalii Susukailo, Postgraduate Student of the Department of Information Protection of the National University "Lviv Polytechnic".

Опірський Іван Романович, д.т.н., доц., професор кафедри захисту інформації Національного університету «Львівська політехніка».
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.
Опирский Иван Романович, д.т.н., доц., профессор кафедры защиты информации Национального университета «Львовская политехника».
Opirskyy Ivan, Doctor of Technical Sciences, Associate Professor, Professor of the Department of Information Protection of the National University "Lviv Polytechnic".

Піскозуб Андріян Збігнєвич, к.т.н., доц., доцент кафедри захисту інформації Національного університету «Львівська політехніка».
E-mail: azpiskozub@gmail.com.
Orcid ID: 0000-0002-3582-2835.
Пискозуб Андриян Збигневич, к.т.н., доц., доцент кафедры защиты информации Национального университета «Львовская политехника».
Piskozub Andrian Zbignievycz, Ph.D., Associate Professor, Associate Professor of the Department of Information Protection of the National University "Lviv Polytechnic".

Волошин Ростислав Ярославович студент кафедри захисту інформації Національного університету «Львівська політехніка».
E-mail: rostyslav.voloshyn.kb.2017@lpnu.ua.
Orcid ID: 0000-0002-1357-1334.
Волошин Ростислав Ярославович студент кафедры защиты информации Национального университета «Львовская политехника».
Voloshyn Rostyslav, Student of the Department of Information Protection of the National University "Lviv Polytechnic".

Друзюк Олег Сергійович студент кафедри захисту інформації Національного університету «Львівська політехніка».E-mail: oleh.druziuk.kb.2017@lpnu.ua.
Orcid ID: 0000-0001-9852-2680.
Друзюк Олег Сергеевич студент кафедры защиты информации Национального университета «Львовская политехника».
Druziuk Oleg, Student of the Department of Information Protection of the National University "Lviv Polytechnic".