УДК 004.056.5(045) **С.В. Толюпа, М.В. Розум'як**

ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ В МАСШТАБАХ ОРГАНІЗАЦІЇ ЗА ДОПОМОГОЮ ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ НА ПРИКЛАДІ CISCO

Із врахуванням зростаючої кількості способів та методів несанкціонованого отримання інформації яка оброблюється та зберігається в межах організації, доцільним стає питання про організацію системи стійкої до різного роду спроб проникнення, та раннього попередження можливих проблем.

Ключові слова: несанкціонований доступ до інформації, мережева інфраструктура, система захисту інформації.

Постановка проблеми

Архітектура системи обробки даних і технологія її функціонування дозволяє зловмисникам знаходити або спеціально створювати лазівки для прихованого доступу до інформації, причому різноманіття і різноманітність навіть відомих фактів злочинних дій дає достатні підстави припускати, що таких лазівок існує або може бути створено багато. Тому протидія таким загрозам є і буде актуальною.

Мета статті

Метою даної статті є розгляд можливостей попередження несанкціонованого доступу та використання програмних та апаратних можливостей захисту та безпеки мережевої інфраструктури Cisco.

Основні матеріали дослідження

З розвитком інформаційних технологій збільшується різноманіття пристроїв і засобів зберігання, обробки та передачі інформації, хмарні технології та Інтернет речей. Це відкриває широкі можливості мобільності співробітників компанії та гнучкості у вирішенні бізнес завдань, хоча з іншого боку ускладнює відстеження за використанням важливих для бізнесу даних. Відповідно причинами несанкціонованого доступу до інформації та корпоративної мережі можуть бути такі фактори як: необережність чи неграмотність співробітників, навмисна крадіжка інформації як своїми співробітниками так і зловмисниками, які використовують різноманітні засоби для проникнення в корпоративну мережу. Таким чином, слабким місцем може стати будь-який елемент, що підключений до мережі організації, як в апаратній, так і в програмній частині.

Багато організацій досі будують свою систему захисту спираючись на застарілий периметровий підхід, зосереджуючи всі засоби безпеки в кількох контрольних точках мережі, повністю забуваючи про наявність обхідних каналів – WiFi, USB flash носів, інформації, 3G, ActiveSync і т.д., а також про внутрішнього порушника, який вже знаходиться всередині мережі і може виконувати свою ”чорну справу”, не боячись бути виявленим периметровими засобами захисту.

Що ж відбувається в сучасних мережах? Розглянемо часовий розподіл подій у відсотках від загального числа зломів [1] (рис. 1).

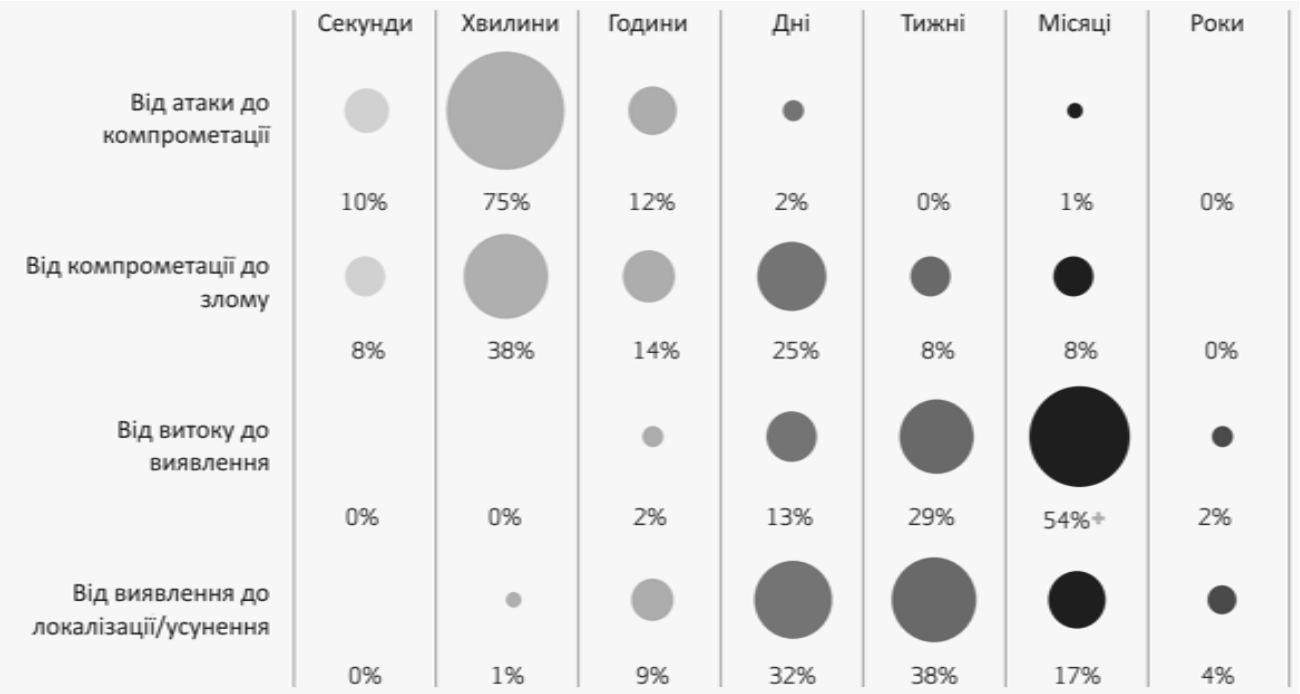

Рис.1. Часові затрати на злом та його виявлення

Можна виділити три варіанти вирішення проблеми. [2]

Перший – побудувати у внутрішній мережі ще одну, створену із міркувань засобів безпеки. Багато виробників засобів захисту надають пропозиції для даного варіанту, включаючи в нього багато IPS сенсорів та мережевих екранів які будуть контролювати внутрішні мережеві потоки та виявляти шкідливий код та заборонені додатки. Але такий варіант стикається з рядом складностей. Не завжди існуючий дизайн мережі дозволяє реалізувати таке підключення. Мережа може працювати на швидкостях недоступних засобам безпеки. Або організація активно використовує віртуалізацію і засоби захисту не можуть ефективно контролювати трафік що не виходить за межі фізичного серверу. Також встановлення додаткових пристроїв потребує немалих фінансових затрат, що також не завжди можливо реалізувати.

Другий часто рекомендований варіант – встановлення засобів захисту на сервери та робочі станції, виявляючи і блокуючи несанкціоновану активність користувачів чи проти користувачів. Це правильно, але виникає питання що робити з рештою пристроїв, як то принтери, сканери, промислові контролери, IP-системи відеоспостереження і контролю доступу. За ними користувачі не працюють (та їх не можна аутентифікувати традиційними методами) і на них не можна встановити ні антивірус, ні HIPS чи інші засоби захисту. Так склалось що часто ці пристрої, а їх може бути навіть більше ніж комп'ютерів користувачів, стають мішенню для зловмисників чи площею для подальшого просування по внутрішній мережі організації. На такого роду пристроях можна встановити перехоплення трафіку і він буде сканувати все що в зоні досяжності. І ніякі засоби захисту ПК і серверів таке порушення політики безпеки не помітять в принципі. А наявність обхідних каналів у вигляді незахищеного WiFi чи 3G модему призведуть до того, що конфіденційні дані можуть витекти минаючи засоби захисту корпоративного периметра.

Третій варіант – перенести рішення на те у що вже інвестовано кошти, а саме на мережеву інфраструктуру. Маршрутизатори, комутатори і точки доступу, які можуть не лише передавати трафік з точки А в точку Б але й ефективно захищати цей трафік, виконуючи одночасно роль сенсору, захисної стіни та інструменту реагування на інциденти безпеки. Адже по суті кожен мережевий пристрій представляє собою сенсор системи захисту мережі – трафік проходить через нього, ідентифікується та класифікується, направляється в

точку призначення. Можна поставити питання розгляду кожного з цих пунктів з точки зору політики інформаційної безпеки. Ідентифікувати додаток на рівні маршрутизатора чи комутатора, не доводячи трафік до міжмережевих екранів на периметрі. Ідентифікувати атаки не комутуючи трафік через span-порт на IDS, а користуватись можливостями інфраструктурного обладнання. Блокувати трафік на порту комутатора, до котрого підключений порушник а не чекати, коли трафік дойде до міжмережевого екрану. Динамічно змінювати списки контролю доступу в залежності від місця знаходження користувача або пристрою, а не закривати очі на неконтрольоване проходження трафіку всередині мережі і необмежений доступ користувачів до внутрішніх ресурсів.

Власне всі ці можливості надає Cisco в своїй мережевій інфраструктурі, виступаючи не лише як сенсор системи захисту (Network as a Sensor), але і як система захисту (Network as a Enforcer) і система розслідування інцидентів ІБ (Інформаційної Безпеки). В якості вихідних даних використовується протокол Netflow [3], який дає нам всі потрібні дані про що проходить трафіку, відповідають на всі важливі для політики ІБ питання – хто, що, коли, куди/звідки, як. За допомогою NetFlow можна класифікувати трафік, розпізнавати додатки, ідентифікувати атаки і витоки, виявляти використання недозволених додатків або появу сторонніх вузлів, проводити розслідування інцидентів та ідентифікувати точку входу зловмисників в мережу. Все це дозволяє зробити NetFlow, на який накладається аналітика ІБ, закладена в рішеннях Cisco Cyber Threat Defense. Розмежування і блокування несанкціонованого доступу реалізується з допомогою списків контролю доступу і міток безпеки SGT (Security Group Tag), що закладають основи для технології Cisco TrustSec, а ефективно управляти всіма параметрами безпеки на десятках тисяч пристроїв допомагає Cisco Identity Service Engine (ISE).

Мережева інфраструктура в ролі "Мережа як сенсор" дозволяє проактивно виявляти загрози по наступних категоріях:

Пристрої:

- Виявлення чужих пристроїв (Wireless Security Module).
- Виявлення невідповідних політик пристроїв (Device Sensor, Identity Service Engine).
- Виявлення зміни репутації зовнішніх і внутрішніх пристроїв (NetFlow, Lancope).

Трафік:

- Виявлення аномалій в трафіку (NetFlow, Lancope, NBAR2).
- Виявлення DDoS-атак (Control Plane Policing, Clean Air).
- Виявленняджерелішляхурозповсюдження APT (NetFlow, Identity Service Engine, Lancope).
- ВиявленякеруванняіроботишкідливогоПЗ (NetFlow, Lancope).

Додатки:

- Виявлення аномальної поведінки додатків (NBAR2).

Користувачі:

- Виявлення порушення користувацького доступу (Identity Service Engine, TrustSec).

Зловмисне програмне забезпечення:

- Виявлення зловмисного ПЗ в пошті та Web (ISR, Cisco Cloud Web Security).
- Виявлення вторгнень, ботнетів, цільових атак, SQL Injection, зловмисного ПЗ (IPS Module, Wireless IPS (wIPS), Sourcefire NGIPS).
- Виявлення розповсюдження зловмисного ПЗ всередині мережі (NetFlow, Lancope).
- Виявлення витоку даних (NetFlow, Lancope).
- Системараннього попередження (Cisco Security Intelligence Operations).

Завдяки охопленню всієї мережі можна бачити більш цілісну картину поведінки ніж на окремих точках контролю (котрі можуть стояти на периметрі, в ЦОД чи ще десь, але вони не бачать все в цілісності), можна використовувати мережеву інфраструктуру як систему раннього попередження, яка не може точно сказати що тут точно атака, але по деяких

індикаторах можна сказати що мережа скомпрометована, що вузол починає себе вести нестандартно, користувач або додаток починає здійснювати нестандартні операції та дії. За рахунок більшого охоплення мережі, трафік будь-якого вузла, додатку чи користувача і навіть зловмисного коду завжди проходить через мережу, і можна бачити все що відбувається в мережі. Відповідно з цим ми можемо пропускати, дозволяти, блокувати, розміщувати в карантин, обмежувати чи виконувати інші дії.

Нижче наведено приклад роботи системи Cisco Identity Service Engine, яка дозволяє розпізнавати пристрої в середині мережі (рис. 2). Це можна використовувати як інструмент інвентаризації, і можна використовувати цю інформацію в рамках політик, наприклад заборонивши роботу застарілих пристроїв, які можуть становити загрозу з точки зору безпеки. Різноманітні варіанти за рахунок класифікації та профілювання пристроїв що розпізнаються за допомогою Cisco ISE.

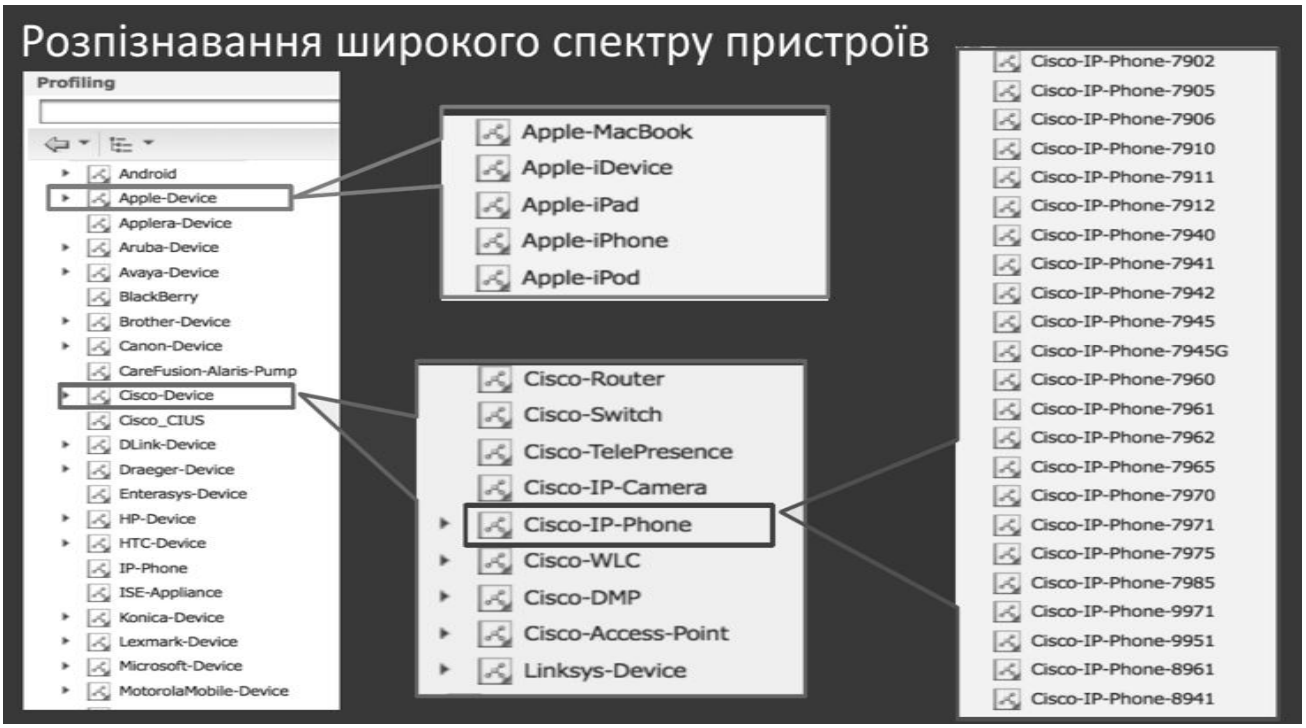

Рис. 2. Cisco Identity Service Engine

Нижче наведено приклад, як можна здійснити ідентифікацію та блокування сторонніх безпровідних пристроїв.

Cisco Wireless Controller / Cisco Wireless Adaptive IPS / Cisco Wireless Location Services. Це частина функціоналу платформи Cisco Mobility Services Engine.

За рахунок вбудованого в безпровідну інфраструктуру функціоналу (рис. 3), можна на фізичній карті будови відмічати з точністю до 1-2-х метрів місцеположення несанкціонованих точок доступу, несанкціонованих безпровідних клієнтів і при необхідності їх подавляти.

Розпізнавання додатків та їх функцій на прикладі Skype (рис. 4).

Приклад технології Cisco Firepower, NBAR2. Можна відповідні дії додатків дозволяти, чи забороняти в визначений час, чи для визначених облікових записів користувачів в певних напрямках з певних вузлів, тобто використовувати будь-які комбінації в політиках безпеки.

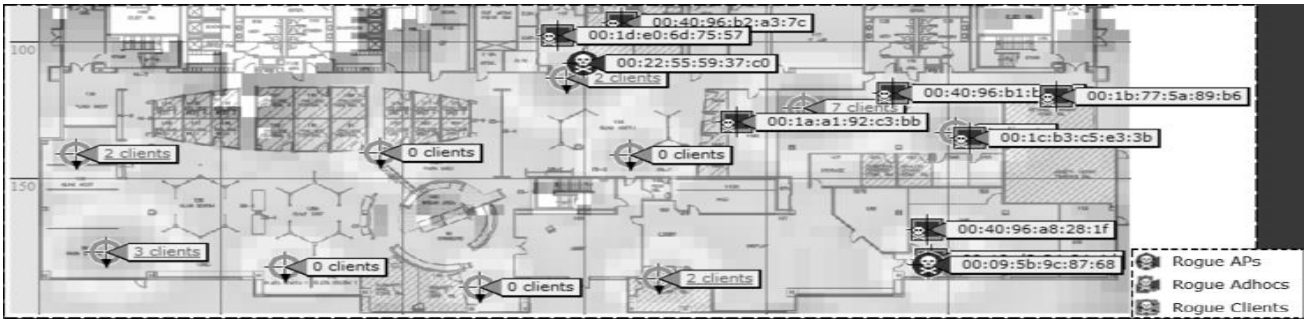

Рис. 3. Cisco Wireless Location Services

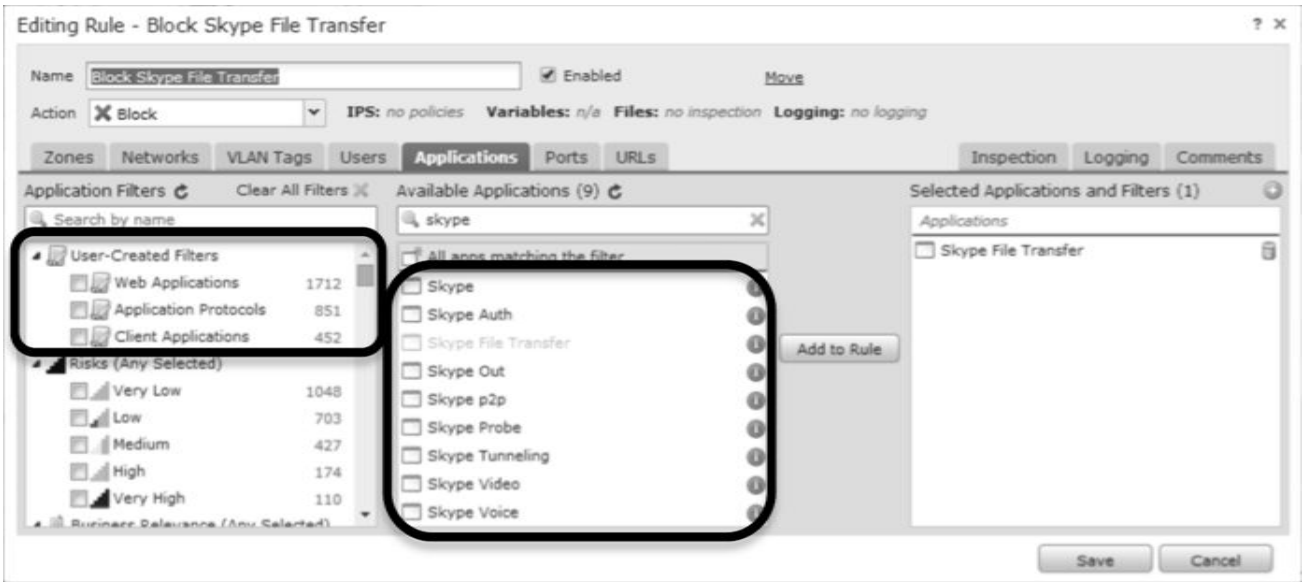

Рис. 4. Налаштування правил в Cisco Firepower

За рахунок доступу до мережевого трафіку можна створювати білі та чорні списки того, що можна робити в мережі. Наприклад білий список – це профіль вузла, який включає в себе опис. Профіль хосту включає всю необхідну для аналізу інформацію: IP-, NetBIOS-, MAC- адреса; операційні системи; використовувані додаткі; зареєстровані користувачі; мережевий протокол; транспортний протокол; прикладний протокол; і т.д.

Ідентифікація і профілювання мобільних пристроїв.

Будь-які відхилення від профілю будуть викликати спрацювання сигналу тривоги.

Ще один елемент мережевої інфраструктури NetFlow [4] (рис. 5, 6) – з самого початку призначався для визначення проблем в мережі. За рахунок того, що NetFlow являється потужним джерелом інформації для кожного мережевого з'єднання, ми можем його використовувати для ідентифікації атак, зломів, витоків даних, тощо.

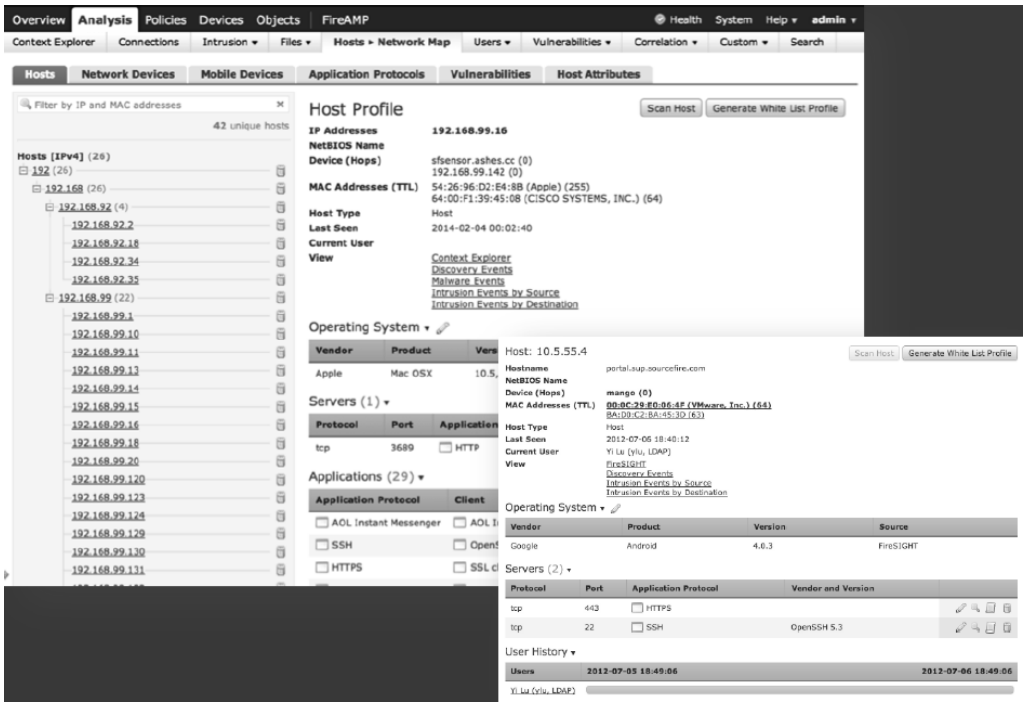

Рис. 5. Приклад інформації з NetFlow

Рис. 6. Інформація з NetFlow

Приклад: NetFlow Alerts з Lancope StealthWatch може відстежувати:

- Сканування мережі: Сканування TCP, UDP, портів по множині вузлів.
- Відмова в обслуговувані DDoS: SYN Half Open; ICMP/UDP/Port Flood.
- Зміну репутації вузла: Потенційно скомпрометовані внутрішні вузли чи отримання сканування чи інші аномалії.
- Знаходження ботнетів: Коли внутрішній вузол спілкується із зовнішнім сервером C&C протягом великого періоду часу.

- Фрагментовані атаки: Вузол відправляє незвичайний фрагментований трафік.
- Розповсюдження червів: Інфікований вузол сканує мережу і з'єднується з вузлами по мережі; Інші вузли починають повторювати ці дії;
- Витоки даних: Великий об'єм вихідного трафіку VS, перевищення денної квоти.

NetFlow може використовуватись на всіх стадіях атаки:

Таблиця 1

Стадії виявлення атак компонентом NetFlow

	Стадія атаки	**Виявлення**
1	Використання вразливостей: Зловмисник сканує IP-адреси та порти для пошуку вразливостей (ОС, користувачі, додатки)	- NetFlow може виявити сканування діапазонів IP - NetFlow може виявити сканування портів на кожному IP-адресі
2	Встановлення зловмисного ПЗ на перший вузол: Хакер встановлює ПЗ для отримання доступу	- NetFlow може виявити вхідний керуючий трафік з неочікуваного місця розташування
3	З'єднанняз "Command and Control": Зловмисне ПЗ з'єднується з C&C сервером для отримання інструкцій	- NetFlow може виявити вихідний трафік до відомих адрес серверів C&C
4	Розповсюдження зловмисного ПО на інші вузли: Атака інших систем в мережі через використання вразливостей	- NetFlow може виявити сканування діапазонів IP - NetFlow може виявити сканування портів на кожному IP-адресі внутрішнього вузла
5	Витік даних: Відправка даних на зовнішні сервери	- NetFlow може виявити розширені потоки (HTTP, FTP, GETMAIL, MAPIGET та інші) і передачу даних на зовнішні вузли

Візуалізацію результатів роботи і аналізу NetFlow можна отримати в StealthWatch, як частині Cisco Cyber Threat Defense.

Платформа виявлення зловмисного коду Advanced Malware Protection (рис. 7), включає в себе емуляцію атак, пісочницю, а також :

- Репутаційний аналіз (Ідентична сигнатура; Нечіткі ідентифікуючі мітки; Машинне навчання;).
- Поведінковий аналіз (Ознаки компрометації; Динамічний аналіз; розширена аналітика; Співставлення потоків пристроїв;).

Платформа AMP може встановлюватись на маршрутизатори, сервери, міжмережеві екрани, IPS, WSA/ESA, персональні комп'ютери, мобільні пристрої.

Підхід базується на виділенні і правильному описанні "Що значить нормально", і будь-які відхилення від "нормально" сприймаються як аномалії з послідуючим реагуванням, блокуванням, розміщенням в карантин чи іншими діями.

Мережа як захисна стіна.

Це надає наступні можливості [5]:

- Сегментувати мережу для локалізації атак (TrustSec – Secure Group Tagging, VLAN/VRF/EVN, ACL, ISE та інші).
- Шифрувати трафік для захисту даних в процесі передачі (MACsec for Wired, DTLS for Wireless, IPSec/SSL for WAN та інші).
- Захистити філіали при прямому доступі в Інтернет (IWAN, Cloud Web Security та інші).

Сегментація мережі важлива для контролю доступу і локалізації атак.

Рис. 7. Інтерфейс платформи виявлення зловмисного коду Advanced Malware Protection

Таблиця 2

Сегментація мережі

Сегментація мережі	**Контроль доступу**
для локалізації атак	**для виконання політик**
- Ролевий контроль доступу на базі топології, способу доступу (TrustSec/SGT, ISE) - Сегментація мережі (VLAN, TrustSec/SGT, VRF/EVN)	- Контроль доступу користувачівна базі пристрою, місця знаходження, типу мережі, часу та інших параметрів (ISE) - Фізичні і віртуальні дозволи і заборони (Access Control Lists) - Єдина політика для провідного/безпровідного віддаленого доступу (ISE, Unified Access Switches)

Складність виникає, коли в мережі є багато контрольних точок, і тоді вручну кожну налаштувати досить складно. Наприклад, в мережі Cisco більше 40 000 маршрутизаторів. Через це в багатьох організаціях/компаніях не бажають займатись контролем у внутрішній мережі.

Для цього спеціально розроблено інструмент Cisco Identity Service Engine, який автоматизує процес ролевого доступу і технологію TrustSec [5] котра реалізується над всією інфраструктурою мережі.

В ньому можна налаштувати наступні політики:

- Хто може з’єднуватись і з ким.
- Хто може отримати доступ до активів.
- Як система може спілкуватись з іншими системами.

Ми задаємо політики, що користувачі з такої групи можуть отримати доступ до вузлів з такої групи, далі ISE сам транслює високорівневі політики в конкретні налаштування конкретного обладнання.

Це дозволяє з плоскої мережі, яка являє собою єдиний сегмент, зробити набір сегментів, тим самим локалізуючи загрозу чи зловмисника в межах одного вузла не дозволяючи йому розповсюджувати загрозу далі. Це дозволяє задовольняти вимоги законодавства, як міжнародного (наприклад PCI DSS) так і українського.

Таким чином ISE надає керування політиками в масштабах всієї мережі (рис. 8), завдяки ідентифікації пристроїв і користувачів, визначенню контексту(хто, що, звідки, коли, як). Комбінуючи ці параметри ми можемо дозволяти чи забороняти користувачу чи пристрою доступ до запитуваного ресурсу.

Рис. 8. Cisco Identity Service Engine – налаштування політик

Таблиця 3

Шифрування і попередження перехоплення даних.

Шифрування даних	**Захист від перехоплення**
Реалізація багаторівневого шифрування: LANLink (Wired) Encryption: MACsec LAN Link (Wireless) Encruption: DTLS WAN Link Encryption: IPSec, SSL Mobile Device Encryption: ISE with MDM	Захиствідвідслідковування: Catalyst Integrated Security Feature Set (Port Security, DHCP Snooping, IP Source Guard, Dynamic ARP Inspection), IPv6 First Hop Security Попередження атак на WiFi-спектр: CleanAir

Таблиця 4

Захист філіалів з допомогою Intelligent WAN.

Масштабований WAN та Інтернет-доступ	**Захищені з'єднання**
Покращена продуктивність додатків Один для будь-яких транспортів АвтоматичнітунеліSite-to-SiteIPsec Zero-touch Hub Configuration Інкапсуляціятрафіку	Інтеграціяз Cloud Web Security, фільтрація Web вреальномучасізконтролемдодатків Масштабованабезпекачерез Dynamic Multipoint VPN (DMVPN) Масштабована криптографія Інтегрований міжмережевий екран/IPS Надійна аутентифікація

Мережа як інструмент реагування. Мережа може:

- Зменшити час відновлення і прискорити реагування. Наприклад, аналіз траєкторії зловмисного коду, інтеграція з AD на рівні мережі.
- Автоматизувати налаштування і динамічно його змінювати виходячи з ситуації вмережі. Наприклад ACL, QoS, динамічні політики, кореляція подій.
- Інтеграція з іншими рішеннями для захисту інвестицій і росту якості захисту. Наприклад, RESTful API, eStreamer API і т.д.

Для покращення реагування потрібно автоматизувати багато функцій. Для цього також розроблено APIC Enterprise Module. Він дозволяє автоматизувати ACL:

- Виявлення дублікатів політик
- Виявлення конфліктів політик
- Оцінка відповідності політик
- Follow-Me ACL. Автоматизація ACLs для мобільності

Інтеграція з FirePower, Network-Wide Rapid Threat Detection and Migration.

Автоматизація захисту філіалів.Performance Routing (PfR) Config (IWAN). Оцінка відповідності політик WAN (IWAN).

Вбудована система кореляції подій FireSIGHT дозволяє збирати дані по всій мережі. (рис. 9):

- Події виявлення зловмисників
  - Бекдор.
  - Підключення до серверів керування и контролю ботнетів.
  - Набори експлоїтів.
  - Отримання адміністраторських прав.
  - Атаки на веб-додатки.
- Події аналізу ІБ
  - Підключення до відомих IP серверів керування і контролю ботнетів.
- Події пов'язані із зловмисним кодом
  - Виявлення зловмисного коду.
  - Виконання зловмисного коду.
  - Компрометація Office/PDF/Java.
  - Виявлення дропера.

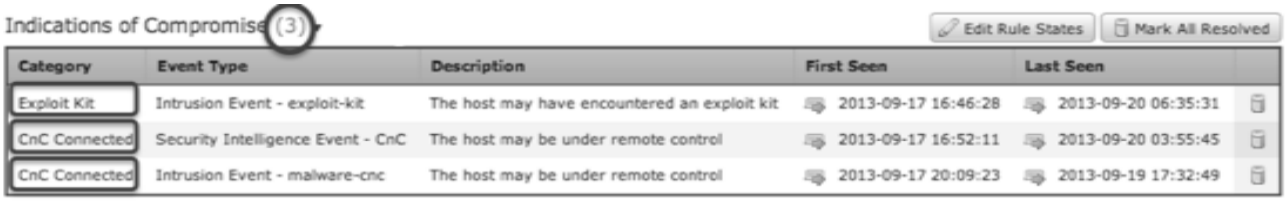

Рис. 9. FireSIGHT - виявлені проблеми в мережі

Можливість відслідковувати рух шкідливого ПО і зловмисника по мережі (рис. 10):

- Які системи були інфіковані.
- Хто був інфікований.
- Коли це відбулось.
- Який процес був відправною точкою.
- Чому це трапилось.
- Що ще трапилось.
-

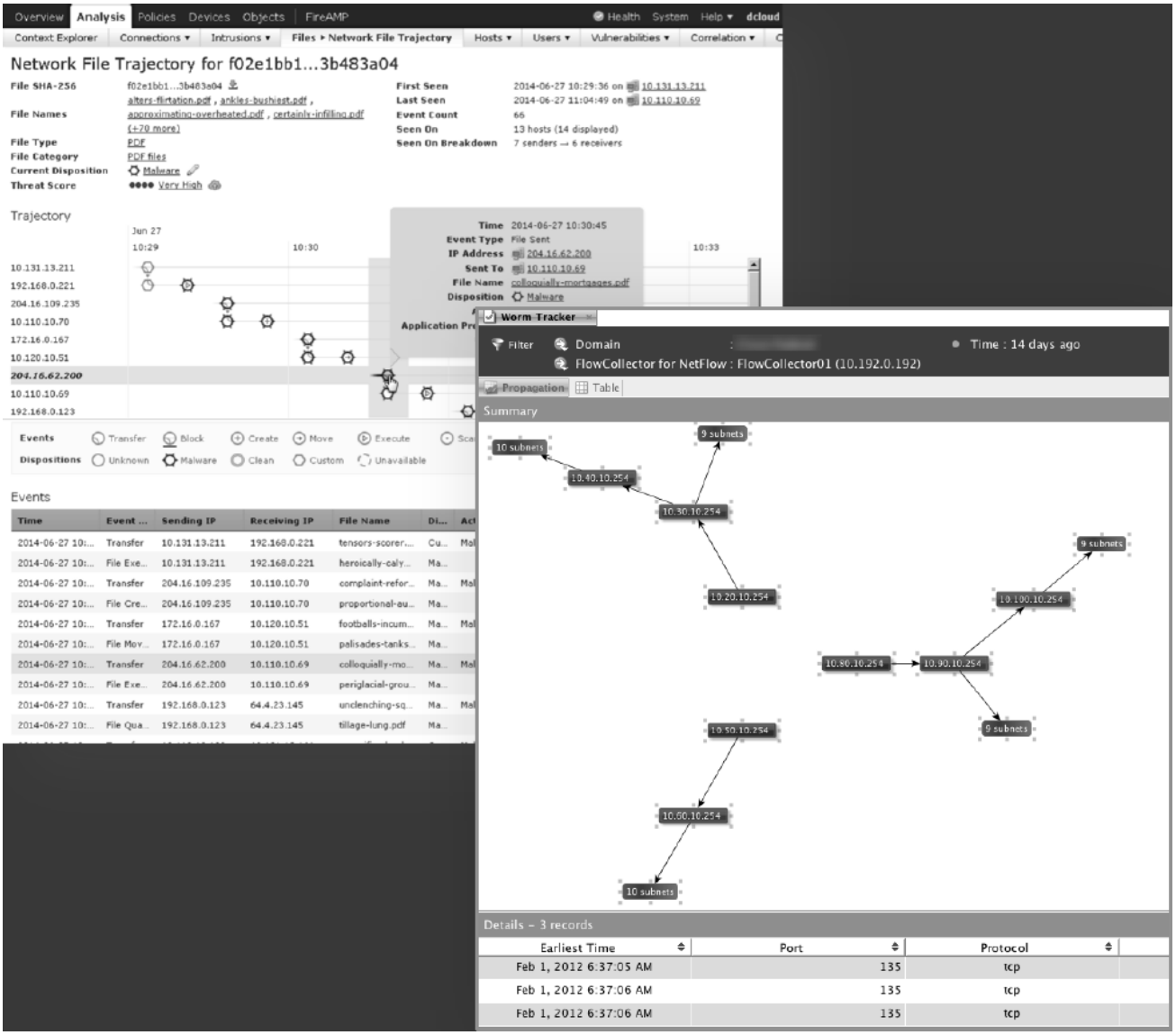

Рис. 10. FireSIGHT – аналіз поширення у мережі

Висновки

Можна виділити 5 принципів для побудови справжньої захищеної мережі:

- Увімкнення NetFlow. Виділення ознак нормального функціонування мережі.
- Впровадження TrustSec/сегментації. Локалізує атаки. Надає ролеве керування, що не залежить від топології чи типу доступу.
- Шифрування трафіку і увімкнення CISF.
- Впровадження IntelligentWAN. Захист філіалів, додаткових офісів, тощо.

- Впровадження APIC-EM. Прискорення конфігурування і усунення проблем.

Таким чином, користуючись наявною інфраструктурою мережі можна перетворити її в систему захисту. Мережа виступатиме в наступних ролях:

- Мережа як сенсор. Виявлення аномального трафіку. Виявлення порушень користувачами політик. Виявлення чужих пристроїв, точок доступу та ін..
- Мережа як захисна стіна. Сегментація мережі для локалізації атак. Шифрування даних для захисту від людини посередині. Захист філіалів для Direct Internet Access.
- Мережа як інструмент реагування. Автоматизоване, близьке до реального часу відхилення атак.

Література

1. 2012 DATA BREACH INVESTIGATIONS REPORT [Електронний ресурс] // - Режим доступу: http://www.verizonenterprise.com/ - (25.03.2016).

2. Лукацкий А. Как превратить саму сеть в полноценную систему защиты? [Електронний ресурс] // - Режим доступу: https://habrahabr.ru/ (23.03.2016).

3. Jesse Russell, Ronald Cohn. Netflow, pages 75-81.

4. Introduction to Cisco IOS NetFlow - A Technical Overview, pages 101-110.

5. Казаков Д. Управление доступом в архитектуре CiscoTrustSec. [Електронний ресурс] // - Режим доступу: http://gblogs.cisco.com/ (29.03.2016).

6. Cisco TrustSec Configuration Guide, Cisco IOS Release 15M&T, pages 45-47.

Надійшла 11.05.2016 р. Рецензент: д.т.н., проф. Єрохін В.Ф.