



CHƯƠNG 3

Phát hiện xâm nhập

Nội dung

- 1. Giới thiệu về phát hiện xâm nhập
- 2. Phát hiện xâm nhập dựa trên danh tiếng
- 3. Phát hiện xâm nhập dựa trên chữ ký với Snort và Suricata
- 4. Phát hiện xâm nhập dựa trên bất thường với dữ liệu thống kê

1. Giới thiệu phát hiện xâm nhập

- ☐ Phân loại kỹ thuật phát hiện xâm nhập
- ☐ Dấu hiệu xâm nhập và chữ ký
- ☐ Quản lý dấu hiệu tấn công và chữ ký
- ☐ Các khung làm việc cho dấu hiệu tấn công và chữ ký



Kỹ thuật phát hiện xâm nhập

- ❑ Phát hiện xâm nhập: là một chức năng của phần mềm thực hiện phân tích các dữ liệu thu thập được để tạo ra dữ liệu cảnh báo
- ❑ Cơ chế phát hiện xâm nhập gồm hai loại chính là:
 - Dựa trên chữ ký
 - Dựa trên bất thường

Kỹ thuật phát hiện xâm nhập

- ❑ Cơ chế phát hiện dựa trên chữ ký
 - Là hình thức lâu đời nhất của phát hiện xâm nhập
 - Bằng cách duyệt qua dữ liệu để tìm các ra các kết quả khớp với các mẫu đã biết
 - Các mẫu được chia thành các mẫu nhỏ độc lập với nền tảng hoạt động → là dấu hiệu của tấn công
 - Mẫu được mô tả bằng ngôn ngữ cụ thể trong nền tảng của một cơ chế phát hiện xâm nhập, chúng trở thành chữ ký
 - Công cụ phát hiện dựa trên chữ ký phổ biến là Snort và Suricata

Kỹ thuật phát hiện xâm nhập

- Phát hiện dựa trên danh tiếng
 - Là một tập con của phát hiện dựa trên chữ ký
 - Phát hiện thông tin liên lạc giữa các máy tính được bảo vệ trong mạng và các máy tính trên Internet có thể bị nhiễm độc do đã từng tham gia vào các hành động độc hại trước đó
 - Kết quả phát hiện dựa trên các chữ ký đơn giản như địa chỉ IP hoặc tên miền

Kỹ thuật phát hiện xâm nhập

❑ Phát hiện dựa trên bất thường

- Là một hình thức mới của phát hiện xâm nhập
 - Phổ biến với công cụ Zeek
- Dựa vào quan sát sự cố mạng và nhận biết lưu lượng bất thường thông qua các chẩn đoán và thống kê
- Có khả năng nhận ra các mẫu tấn công khác biệt với hành vi mạng thông thường
- Đây là cơ chế phát hiện rất tốt nhưng khó thực hiện
 - Zeek là một cơ chế phát hiện bất thường, và thực hiện phát hiện bất thường dựa trên thống kê

Kỹ thuật phát hiện xâm nhập

- Phát hiện dựa trên Honeypot
 - Là tập con mới được phát triển của phát hiện dựa trên bất thường
 - Honeypot đã được sử dụng trong nhiều năm để thu thập phần mềm độc hại và các mẫu tấn công cho mục đích nghiên cứu
 - Honeypot có thể được ứng dụng tốt trong phát hiện xâm nhập bằng cách cấu hình hệ thống
 - Được cấu hình cho việc ghi lại dữ liệu, và thường được kết hợp với các loại khác của NIDS hoặc HIDS

Dấu hiệu xâm nhập và chữ ký

- ❑ Indicators of Compromise – IOC: là những thông tin được sử dụng để mô tả khách quan một xâm nhập mạng, độc lập về nền tảng
 - Ví dụ: địa chỉ IP của máy chủ C&C, hay tập các hành vi cho thấy email server là SMTP relay độc hại
- ❑ Được trình bày theo nhiều cách thức và định dạng khác nhau để có thể được sử dụng bởi các cơ chế phát hiện khác nhau
- ❑ Nếu được sử dụng trong một ngôn ngữ hoặc định dạng cụ thể → trở thành một phần của một chữ ký.
- ❑ Một chữ ký có thể chứa một hoặc nhiều IOC.

IOC cho mạng và máy tính

❑ IOC cho mạng:

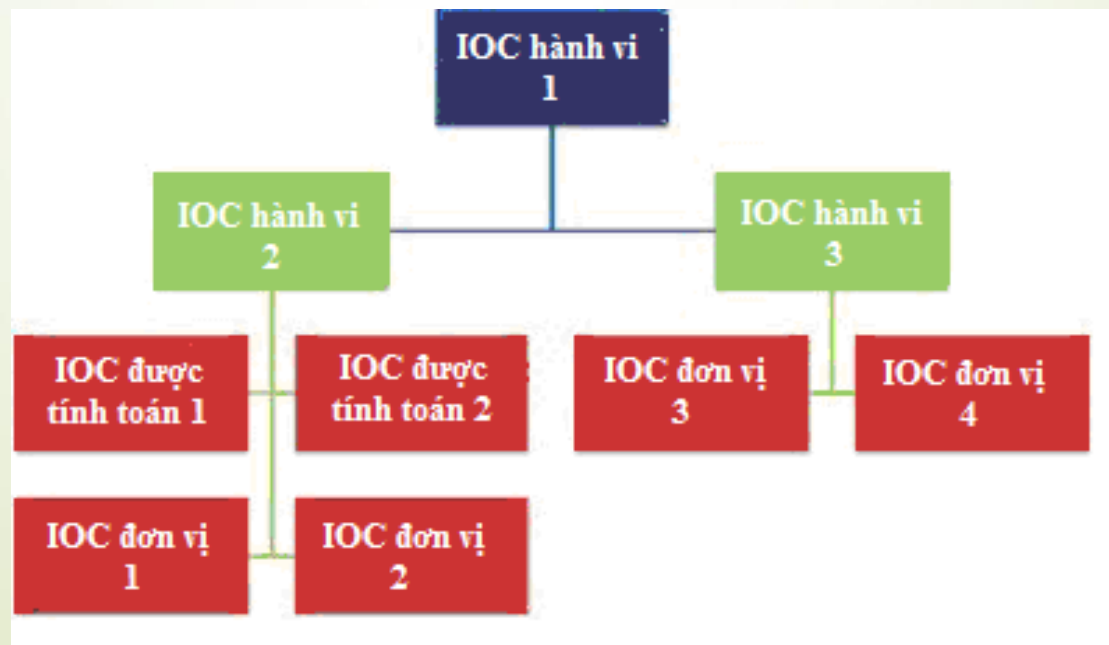
- Là một mẫu thông tin có thể được bắt trên kết nối mạng giữa các máy chủ, mô tả khách quan một xâm nhập.
- Ví dụ: địa chỉ IPv4, địa chỉ IPv6, tên miền, chuỗi văn bản, giao thức truyền thông,...

❑ IOC cho máy tính:

- Là một mẫu thông tin được tìm thấy trên một máy tính, mô tả khách quan một xâm nhập
- Ví dụ: tài khoản người dùng, đường dẫn thư mục, tên tiến trình, tên tệp tin, khóa đăng ký (registry), ...

IOC tĩnh

- ❑ Là những IOC mà giá trị được định nghĩa một cách rõ ràng
- ❑ Có ba biến thể của IOC tĩnh: đơn vị (hay còn gọi là nguyên tố), được tính toán, và hành vi



IOC tĩnh

❑ IOC đơn vị:

- Là các IOC cụ thể và nhỏ mà không thể chia được tiếp thành các thành phần nhỏ hơn nữa, nhưng vẫn có ý nghĩa trong tình huống một xâm nhập
- Ví dụ: địa chỉ IP, chuỗi văn bản, tên máy, địa chỉ thư điện tử, và tên tệp tin

❑ IOC được tính toán:

- Có nguồn gốc từ dữ liệu sự cố, bao gồm giá trị băm, các biểu thức thông thường, và các thống kê

❑ IOC hành vi:

- Là tập các IOC đơn vị và IOC được tính toán được kết hợp với nhau theo một số hình thức logic, dùng để cung cấp cho một số tình huống hữu dụng

Ví dụ

- 1. Người dùng nhận được một e-mail từ chris@appliednsm.com với chủ đề "Thông tin tiền lương" và một tệp PDF đính kèm là "Payroll.pdf". Tệp PDF có một giá trị băm MD5 là e0b359e171288512501f4c18ee64a6bd.

Vấn đề: sự kiện có mô tả quá phức tạp
→ gây khó khăn cho ứng dụng vào các cơ chế phát hiện

- 4. Ma trong DLL được thực thi, và một kết nối SSH được thiết lập tới một máy chủ có địa chỉ IP là 192.0.2.75 trên cổng 9966.
- 5. Khi kết nối này được thiết lập, phần mềm độc hại tìm kiếm mọi tệp DOC, DOCX, hoặc PDF từ máy nạn nhân và truyền nó qua kết nối SSH đến máy chủ nguy hiểm.

Ví dụ

- ❑ Phân tích các dấu hiệu thành các phần nhỏ có ích hơn, như các IOC hành vi (B) như sau:
 - B-1: Người dùng nhận được một e-mail từ chris@appliednsm.com với chủ đề "Thông tin tiền lương" và một tệp PDF đính kèm là "Payroll.pdf", có một giá trị băm MD5 là e0b359e171288512501f4c18ee64a6bd.
 - B-2: Tệp tin kernel32.dll với hàm băm MD5 da7140584983eccde51ab82404ba40db được tải về từ <http://www.appliednsm.com/kernel32.dll>.
 - B-3: Tệp tin C:/Windows/System32/Kernel32.dll bị ghi đè bởi một tệp tin độc hại cùng tên với giá trị hàm băm MD5 da7140584983eccde51ab82404ba40db.
 - B-4: Máy tính nạn nhân cố gắng kết nối qua SSH tới máy tính nguy hiểm bên ngoài 192.0.2.75 trên cổng 9966.
 - B-5: Các tệp tin DOC, DOCX, và PDF được truyền tới 192.0.2.75 trên cổng 9966 thông qua một kết nối được mã hóa.

Ví dụ

- ❑ Tiếp tục phân tích IOC hành vi thành các IOC đơn vị (A) và IOC được tính toán (C):
 - C-1: MD5 Hash e0b359e171288512501f4c18ee64a6bd
 - C-2: MD5 Hash da7140584983eccde51ab82404ba40db
 - A-1: Tên miền nguy hiểm: appliednsm.com
 - A-2: Địa chỉ e-mail địa chỉ: chris@appliednsm.com
 - A-3: Tiêu đề thư: "Thông tin tiền lương"
 - A-4: Tên file: Payroll.pdf
 - A-5: Tên file: Kernel32.dll
 - A-6: IP nguy hiểm 192.0.2.75
 - A-7: Cổng 9966
 - A-8: Giao thức SSH
 - A-9: Kiểu file DOC, DOCX, PDF
 - A-10: Tên file Kernel32.dll

Ví dụ

- ❑ IOC được chuyển đổi thành các chữ ký để sử dụng trong một loạt các cơ chế phát hiện:
 - C-1/2: Chữ ký chống vi-rút để phát hiện sự tồn tại của giá trị băm
 - A-1: Chữ ký Snort/Suricata để phát hiện kết nối với tên miền nguy hiểm
 - A-2: Chữ ký Snort/Suricata để phát hiện thư nhận được từ địa chỉ e-mail nguy hiểm
 - A-3: Chữ ký Snort/Suricata để phát hiện dòng chủ đề
 - A-3: Bro script để phát hiện dòng chủ đề
 - A-4/C-1: Bro script để phát hiện tên tệp tin hay giá trị băm MD5 được truyền trên mạng
 - A-5/C-2: Bro script để dò tìm tệp tin có tên là Kernel32.dll hoặc tệp tin với giá trị băm MD5 truyền qua mạng
 - A-6: Chữ ký Snort/Suricata để phát hiện thông tin liên lạc với địa chỉ IP
 - A-7/A-8: Chữ ký Snort/Suricata để phát hiện thông tin liên lạc SSH đến cổng 9966
 - A-10: Luật HIDS để phát hiện những thay đổi của Kernel32.dll



Biến IOC

- ☐ Cần phải coi IOC là các biến, trong đó có những dấu hiệu chưa biết giá trị → để tổng quát hóa cuộc tấn công
- ☐ Biến IOC hữu ích trong các giải pháp phát hiện bất thường như Bro

Ví dụ

❑ Kịch bản tấn công lý thuyết:

- 1. Người dùng nhận được một e-mail với một tệp tin đính kèm độc hại.
- 2. Người dùng mở tệp tin đính kèm, kích hoạt việc tải tệp tin từ một tên miền độc hại.
- 3. Tệp tin được dùng để ghi đè lên một tệp tin hệ thống với phiên bản mã độc của tệp tin đó.
- 4. Mã trong các tệp tin độc hại thực thi, gây ra một kết nối mã hóa đến một máy chủ độc hại.
- 5. Sau khi kết nối được thiết lập, một số lượng lớn dữ liệu sẽ bị rò rỉ từ hệ thống.

❑ Một số biến IOC:

- VB-1: Một người dùng nhận được một e-mail với một tệp tin đính kèm độc hại.
- VA-1: Địa chỉ e-mail
- VA-2: Tiêu đề e-mail
- VA-3: Tên miền nguồn của e-mail độc hại
- VA-4: Địa chỉ IP nguồn của e-mail
- VA-5: Tên tệp tin đính kèm độc hại
- VC-1: Tệp tin đính kèm độc hại với giá trị băm MD5
- VB-2: Người dùng mở tệp tin đính kèm, kích hoạt việc tải một tệp tin từ một tên miền độc hại.
- VA-6: Tên miền/IP chuyển hướng độc hại
- VA-7: Tên tệp tin độc hại đã tải
- VC-2: Giá trị băm MD5 của tệp tin độc hại đã tải
- VB-3: Tệp tin được sử dụng để ghi đè lên một tệp tin hệ thống với phiên bản mã độc của tệp tin đó.
- VB-4: Thực thi mã trong tệp tin độc hại, tạo ra một kết nối mã hóa đến một máy chủ độc hại trên một cổng không chuẩn.
- VA-8: Địa chỉ IP C2 ngoài
- VA-9: Cổng C2 ngoài
- VA-10: Giao thức C2 ngoài
- VB-5: Sau khi kết nối được thiết lập, một số lượng lớn các dữ liệu đã bị rò rỉ từ hệ thống.

❑ Kết hợp các IOC đơn vị, tính toán và hành vi để tạo thành chữ ký:

- VB-1 (VA-3/VA-4) VB-2 (VA-6) VB-4 (VA-8) VB-5 (VA-8): Luật Snort/Suricata để phát hiện các liên lạc với danh tiếng xấu theo địa chỉ IP và tên miền.
- VB-1 (VA-5/VC-1) VB-2 (VA-7/VC-2): Bro script để kéo các tệp tin từ đường truyền và so sánh tên của chúng và các giá trị băm MD5 với một danh sách các tên tệp tin danh tiếng xấu được biết đến và các giá trị băm MD5.
- VB-1 (VA-5/VC-1) VB-2 (VA-7/VC-2): Bro script để lấy các tệp tin từ đường truyền và đặt chúng vào trong thử nghiệm phân tích phần mềm độc hại sơ bộ.
- VB-2 (VA-6/VA-7/VC-2): chữ ký HIDS để phát hiện các trình duyệt đang được gọi từ một tài liệu.
- VB-3: chữ ký HIDS để phát hiện một tệp tin hệ thống đang bị ghi đè
- VB-4 (VA-9/VA-10) VB-5: Bro script để phát hiện mã hóa lưu lượng đang xảy ra trên một cổng không chuẩn
- VB-4 (VA-9/VA-10) VB-5: một luật Snort/Suricata để phát hiện mã hóa lưu lượng đang xảy ra trên một cổng không chuẩn
- VB-5: script tự viết sử dụng thông kê dữ liệu phiên để phát hiện khối lượng lớn lưu lượng gửi đi từ máy trạm.

Quản lý dấu hiệu tấn công và chữ ký

- ❑ Số lượng các IOC và chữ ký có thể phát triển nhanh trong một thời gian ngắn
- ❑ Cần phải có chiến lược lưu trữ, truy cập và chia sẻ chúng
- ❑ Hầu hết lưu trữ IOC và chữ ký trong cơ chế phát hiện đang sử dụng
 - Ví dụ: sử dụng Snort thì IOC sẽ được lưu thành chữ ký Snort, được truy cập trực tiếp bởi Snort
 - Hạn chế khả năng tương tác và tham khảo chúng

Quản lý dấu hiệu tấn công và chữ ký

□ Các nguyên tắc để quản lý IOC và chữ ký tốt nhất:

- Định dạng dữ liệu thô:
- Dễ tiếp cận: chuyên gia có thể truy cập và chỉnh sửa IOC và chữ ký dễ dàng
- Dễ tìm kiếm: nên tồn tại trong một định dạng dễ tìm kiếm
- Dễ theo dõi sửa đổi
- Theo dõi việc triển khai
- Sao lưu dữ liệu

Quản lý dấu hiệu tấn công và chữ ký

GUID	Tác giả	Ngày tạo	Ngày sửa đổi	Phiên bản	Nguồn	Phân loại	Loại	Giai đoạn trong chu kỳ sống	Độ tin tưởng	IOC	Triển khai
10001	Sanders	3/17/2013	3/20/2013	2	Case # 1492	MD5	Computed/Static	Mature	Very High	e0b359e171288512501f4c18ee64a6bd	Antivirus Signature 42039
10002	Smith	3/18/2013	3/18/2013	1	Malware Domain List	Domain	Atomic/Static	Mature	Moderate	appliednsm.com	Snort Signature 7100031
10003	Sanders	3/18/2013	3/18/2013	1	Case # 1498	E-Mail Address	Atomic/Static	Mature	Very High	chris@appliednsm.com	Snort Signature 7100032
10004	Sanders	3/19/2013	3/19/2013	1	Zeus Tracker	IP	Atomic/Static	Mature	High	192.0.2.99	Custom SiLK Script
10005	Randall	3/20/2013	3/24/2013	4	Analyst	Protocol/Port	Behavioral/Variable	Immature	Moderate	Encrypted Traffic over Non-Standard Port	Bro Script
10006	Sanders	3/20/2013	3/20/2013	1	RSS Feed	Protocol/Port	Behavioral/Static	Mature	Moderate	SSH/9966	Suricata Signature 7100038
10007	Sanders	3/21/2013	3/24/2013	3	Internal Discussion	Statistical	Behavioral/Variable	Immature	Low	Outbound Traffic Volume Ratio Greater than 4:1	Custom SiLK Script

Các framework cho IOC và chữ ký

❑ Vấn đề:

- Cộng đồng thiếu một framework chung để tạo lập, quản lý và phân phối cho IOC và chữ ký
- Dữ liệu thường lưu trữ theo định dạng cá nhân và khó chia sẻ
- Thông tin theo ngữ cảnh khó chia sẻ nhất

❑ Một số framework phổ biến nhất:

- OpenIOC của Mandiant
- STIX (Structured Threat Information eXpression) – phát triển bởi MITRE cho US Department of Homeland Security

Các framework cho IOC và chữ ký

❑ OpenIOC của Mandiant

- là một lược đồ XML được sử dụng để mô tả các đặc điểm kỹ thuật xác định các hoạt động tấn công
- cho phép quản lý các IOC với rất nhiều các thông tin theo ngữ cảnh cần thiết để sử dụng hiệu quả các IOC



```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="9ad0ddec-dc4e-4432-9687-
b7002806dcf8" last-modified="2013-02-20T02:07:40" xmlns="http://
schemas.mandiant.com/2010/ioc">
  <short_description>PHISH-UPS-218934</short_description>
  <description>Part of the UPS Phishing scheme reported on 12/4.</
description>
  <authored_by>Chris Sanders</authored_by>
  <authored_date>2013-02-20T02:02:00</authored_date>
  <links>
    <link rel="Source">http://www.appliednsm.com</link>
    <link rel="Stage">Nature</link>
  </links>
  <definition>
```

Các framework cho IOC và chữ ký

❑ STIX

- Mã nguồn mở
- Kiến trúc STIX dựa trên cấu trúc độc lập và các mối liên quan:
 - Gồm các đối tượng quan sát được, được định nghĩa là các thuộc tính có trạng thái hoặc các sự kiện đo được, thích hợp cho các hoạt động của máy tính và mạng
 - Có thể là một dịch vụ đang dừng, tên tệp tin, một sự kiện khởi động lại hệ thống, hoặc một thiết lập kết nối
 - Được lưu trong định dạng XML, và được mô tả bằng cách sử dụng ngôn ngữ CybOX

Full Sample

STIX Package

```
<stix:STIX_Package
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:indicator="http://stix.mitre.org/Indicator-2"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
  xmlns:example="http://example.com/"
  xsi:schemaLocation="
    http://stix.mitre.org/stix-1 ../stix_core.xsd
    http://stix.mitre.org/Indicator-2 ../indicator.xsd
    http://cybox.mitre.org/default_vocabularies-2 ../cybox/cybox_default_vocabularies.xsd
    http://stix.mitre.org/default_vocabularies-1 ../stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 ../cybox/objects/Address_Object.xsd"
  id="example:STIXPackage-33fe3b22-0201-47cf-85d0-97c02164528d"
  timestamp="2014-02-20T09:00:00.000000Z"
  version="1.1"
  >
```

Namespaces & Schemalocations

STIX Header

```
<stix:STIX_Header>
  <stix:Title>Example watchlist that contains IP information.</stix:Title>
  <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators - Watchlist</stix:Package_Intent>
</stix:STIX_Header>
<stix:Indicators>
```

```
  <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-33fe3b22-0201-47cf-85d0-97c02164528d"
    timestamp="2014-02-20T09:00:00.000000Z">
    <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">IP Watchlist</indicator:Type>
    <indicator:Description>Sample IP Address Indicator for this watchlist.
    This contains one indicator with a set of three IP addresses in the watchlist.</indicator:Description>
    <indicator:Observable id="example:Observable-1c798262-a4cd-434d-a958-884d6980c459">
      <cybox:Object id="example:Object-1980ce43-8e03-490b-863a-ea404d12242e">
        <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
          <AddressObject:Address_Value condition="Equals"
            apply_condition="ANY">10.0.0.0##comma##10.0.0.1##comma##10.0.0.2</AddressObject:Address_Value>
          </cybox:Properties>
        </cybox:Object>
      </indicator:Observable>
    </stix:Indicator>
  </stix:Indicators>
</stix:STIX_Package>
```

STIX Data (Indicators)



Tìm hiểu về openioc

➤ Chương 3. (Them) openioc.pdf

2. Phát hiện xâm nhập dựa trên danh tiếng

□ Danh sách danh tiếng công khai:

- Dựa trên danh sách công khai của các IOC đơn vị
 - Ví dụ: địa chỉ IP và tên miền ~ danh sách đen
- Bao gồm:
 - Danh sách tên miền có mã độc - Malware Domain List – MDL: được sử dụng nhiều nhất hiện nay, cung cấp các truy vấn, RSS, CSV ...
 - Abuse.ch Zeus và SpyEye Trackers
 - Có khoảng thời gian Zeus là botnet lớn nhất thế giới, tiếp đó là SpyEye
 - PhishTank: của OpenDNS chia sẻ các dữ liệu liên quan tới lừa đảo

Phát hiện xâm nhập dựa trên danh tiếng

Zeus Tracker :: Monitor

Below is a list of all Zeus C&Cs as well as Fake URLs which are currently known to Zeus Tracker. You can browse the Zeus Tracker to get a list of Zeus C&Cs and FakeURLs for a specified country or AS. Additionally, Zeus Tracker provides a feature which allows to filter the Zeus C&Cs for specified nameservers, level, status and many more.

Each Zeus C&C or FakeURL is tagged with a level. The level indicates which kind of IP the Host is hosted on. Here is an overview about the levels and its meaning:

Level	Description
Level 1	Bulletproof hosted
Level 2	Hacked webserver
Level 3	Free hosting service
Level 4	Unknown
Level 5	Hosted on a FastFlux botnet

Additionally, every host is at least in one of the following category:

- Hosts which are tagged as **CC** are Zeus Command&Control servers
- Hosts which are tagged as **FU** are referenced by Zeus as FakeURLs

You can also search the Zeus Tracker for domains, IPs, urls, MD5 hashes or FakeURLs:

Browse: [Zeus BinaryURLs](#) | [Zeus ConfigURLs](#) | [Zeus Dropones](#)
Malware family filter: [Zeus](#) | [Ice IX](#) | [Citadel](#)
Set a filter for the list below: [Remove filter \(Show all\)](#) | [online Zeus hosts](#) | [offline Zeus hosts](#) | [Zeus hosts with files online](#) | [order by lastupdated](#)
Filter C&C server tagged with level: [Level 1 \(Bulletproof\)](#) | [Level 2 \(Hijacked sites\)](#) | [Level 3 \(Free webhosting\)](#) | [Level 4 \(Unknown\)](#) | [Level 5 \(FastFlux hosted\)](#)

Dateadded	Malware	Host	IP address	Level	Status	Files Online	SBL	Country	AS number	Uptime
2013-06-28	Zeus	shanghairegistry.com	173.208.107.195	2	online	2	SBL100000000		AS15003	00:14:28
2013-06-28	Citadel	gnerisicnywvno.ru	FastFlux Botnet	5	online	1	Not listed	-	-	05:49:16
2013-06-26	Citadel	astarta.ru	FastFlux Botnet	5	online	1	Not listed	-	-	00:41:36
2013-06-26	Citadel	centos.ru	FastFlux Botnet	5	online	1	Not listed	-	-	00:43:03
2013-06-26	Citadel	pekin34.ru	31.31.199.159	2	online	1	SBL100000000		AS39792	00:43:03
2013-06-26	Zeus	cardpalcoza.su	FastFlux Botnet	5	online	1	Not listed	-	-	00:46:22
2013-06-26	Citadel	volgopromotion.su	FastFlux Botnet	5	online	2	Not listed	-	-	00:49:48
2013-06-26	Citadel	lomamo.com	46.119.217.55	4	online	2	Not listed		AS15895	01:00:09
2013-06-26	Zeus	eltriunfo.com.mx	216.139.244.210	2	online	2	SBL100000000		AS32400	03:24:53

Phát hiện xâm nhập dựa trên danh tiếng

❑ Danh sách danh tiếng công khai:

- Một số danh sách khác:

- Tor Exit Node

- Spamhaus

- AlienVault Labs IP Reputation Database:

- <http://labs.alienvault.com/labs/index.php/projects/open-source-ip-reputation-portal/>

- MalC0de Database: <http://malc0de.com/database/>

- SRI Malware Threat Center

- http://www.mtc.sri.com/live_data/attackers/

- Project Honeypot: https://www.projecthoneypot.org/list_of_ips.php

- Emerging Threats Rules: <http://www.emergingthreats.net/open-source/etopen-ruleset/>

Phát hiện xâm nhập dựa trên danh tiếng

- ❑ Tự động phát hiện xâm nhập dựa trên danh tiếng
 - Phát hiện danh tiếng IP với Snort
 - Sử dụng tiền xử lý danh tiếng
 - Cần tạo ra một tệp tin gọi là `preprocessor_rules` trong `/etc/NSM/rules` của bộ cảm biến SO

```
alert ( msg: "REPUTATION_EVENT_BLACKLIST"; sid: 1;  
gid: 136; rev: 1; metadata: rule-type preproc ;  
classtype:bad-unknown; )  
include $PREPROC_RULE_PATH/preprocessor.rules
```

- Chỉnh sửa: `/etc/nsm/sensor_name/snort.conf`
- Bổ sung IP vào: `/etc/nsm/rules/black_list.rules`

Phát hiện xâm nhập dựa trên danh tiếng

- ❑ Tự động phát hiện xâm nhập dựa trên danh tiếng

The screenshot displays the Snorby web interface for listing events. The browser address bar shows <https://172.16.16.10:444/events>. The main content area shows details for a specific event:

- Event Signature:** reputation: Packet is blacklisted
- IP Header Information:**

Source	Destination	Ver	Len	Tos	Len	ID	Flags	Off	TTL	Proto	Count
192.168.1.254	192.0.2.75	4	5	0	84	0	0	0	63	1	46775
- Signature Information:**

Generator ID	Sig. ID	Sig. Revision	Activity (19184038)	Category	Sig Info
136	1	1	0.23%	bad-unknown	Query Signature Database View Rule
- ICMP Header Information:**

Type	Code	Count	ID	SEQ
8	0	40547	8859	4
- Payload:** Hex and ASCII view of the packet data.
- Notes:** This event currently has zero notes - You can add a note by clicking the button below.

Phát hiện xâm nhập dựa trên danh tiếng

❑ Tự động phát hiện xâm nhập dựa trên danh tiếng

- Phát hiện danh tiếng với Suricata:
 - Sửa đổi file cấu hình Suricata.yaml , dựa trên danh sách thủ công giống Snort
- Phát hiện danh tiếng với Bro:
 - Thích hợp cho việc phát hiện một số loại IOC, chẳng hạn như địa chỉ IP, tên miền, địa chỉ thư điện tử và chứng chỉ SSL nhờ sử dụng các tính năng xử lý thông minh có sẵn được gọi là intel framework

3. Phát hiện xâm nhập dựa trên chữ ký với Snort và Suricata

☐ Snort:

- Phổ biến nhất trong thế giới do có nhiều tính năng mạnh mẽ và linh hoạt
- Nhiều tính năng trở thành tiêu chuẩn cho ngành công nghiệp IDS

☐ Suricata:

- Thay thế cho Snort trong việc phát hiện xâm nhập dựa trên chữ ký.
- Khả năng kiểm tra lưu lượng truy cập đa luồng, thích hợp hơn khi giám sát kết nối thông lượng cao
- Sử dụng cú pháp luật tương tự như Snort



ên chữ ký

Dashboard

LAST 24 TODAY 10

223 HIGH SEV

3,156 - 41,500

Sensors

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	so-suricat...	3.1556	2013-08-07 22:06:05	192.168.2.9	50503	74.125.134.125	5222	6	ET CHAT Google IM traffi...
RT	1	so-suricat...	4.89	2013-08-07 22:07:44	192.168.2.9	50557	50.19.105.233	30022	6	PADS New Asset - ssh O...
RT	1	so-suricat...	4.91	2013-08-28 17:42:20	172.16.16.139	53733	199.7.57.72	80	6	PADS New Asset - http o...
RT	1	so-suricat...	3.1560	2013-08-28 17:44:15	172.16.16.139	59932	62.231.75.133	6667	6	ET CNC Shadowserver R...
RT	2	so-suricat...	3.1956	2013-08-29 08:02:51	91.189.91.14	80	172.16.16.123	53487	6	SURICATA STREAM ESTA...
RT	554	so-suricat...	3.2432	2013-08-30 18:51:39	172.16.16.139	57517	67.205.2.30	21	6	IPREP Malware Domain ...
RT	1	so-suricat...	4.98	2013-08-30 19:41:44	172.16.16.139	57778	67.205.2.30	21	6	PADS New Asset - unkno...
RT	7	so-suricat...	3.2504	2013-08-31 07:01:17	96.43.137.98	443	172.16.16.123	51664	6	SURICATA STREAM ESTA...
RT	1	so-suricat...	4.104	2013-09-01 12:53:37	172.16.16.139	62539	172.16.16.20	22	6	PADS New Asset - unkno...
RT	1	so-suricat...	4.109	2013-09-04 12:20:18	172.16.16.139	65340	46.4.223.210	80	6	PADS New Asset - http Li...
RT	2	so-suricat...	3.3682	2013-09-05 12:12:20	172.16.16.138	60135	224.0.0.252	5355	17	ET P2P ThunderNetwork...
RT	126	so-suricat...	3.3948	2013-09-06 13:32:04	172.16.16.139	63211	67.215.242.139	6881	17	ET P2P BitTorrent DHT pl...
RT	20	so-suricat...	3.3949	2013-09-06 13:32:13	172.16.16.139	63211	31.172.124.29	80	17	ET P2P Vuze BT UDP Con...

IP Resolution Agent Status Snort Statistics System Mx

☐ Reverse DNS ☒ Enable External DNS

Src IP:

Src Name:

Dst IP:

Dst Name:

Whois Query: ☒ None ☐ Src IP ☐ Dst IP

☒ Show Packet Data ☒ Show Rule

alert top \$HOME_NET any -> \$EXTERNAL_NET 5222 (msg:"ET CHAT Google IM traffic Jabber client sign-on" flow:to server:content:"email.com":nocase:content:"jabber.org":nocase:

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	hSize
IP	192.168.2.9	74.125.134.125	4	5	0	182	7165	2	0	64	354

U A P R S F

TCP	Source	Dest	R R R C S S Y I	Port	Port	1 0 G K H T N N	Seq #	Ack #	Offset	Res	Window	Urp	hSize
TCP	50503	5222	. . . X X . . .	2111450131	1663122639	8	0	8242	0	159			

DATA

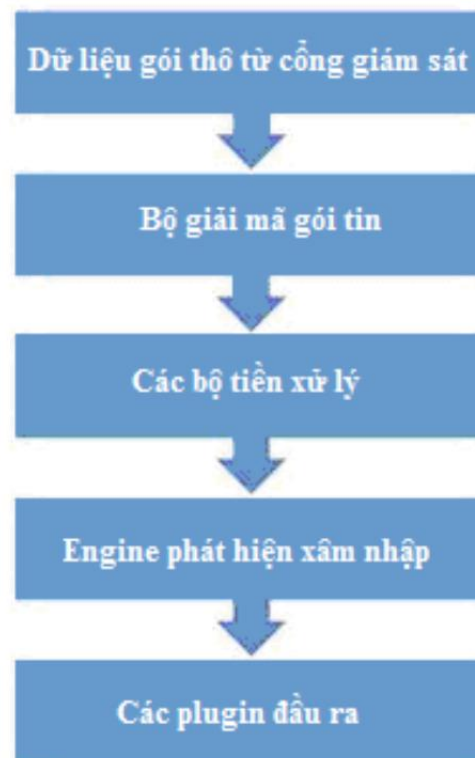
3C 73 74 72 65 61 6D 3A 73 74 72 65 61 6D 20 74 <stream:stream
6F 3D 22 67 6D 61 69 6C 2E 63 6F 6D 22 20 78 6D t
6C 3A 6C 61 6E 67 3D 22 65 6E 22 20 76 65 72 73 o="gmail.com" x
69 6E 6E 3D 73 31 7E 3D 73 7D 6D 6E 6E 73 74 =

Search Packet Payload ☐ Hex ☒ Text ☐ NoCase

Phát hiện xâm nhập dựa trên chữ ký

➤ Snort

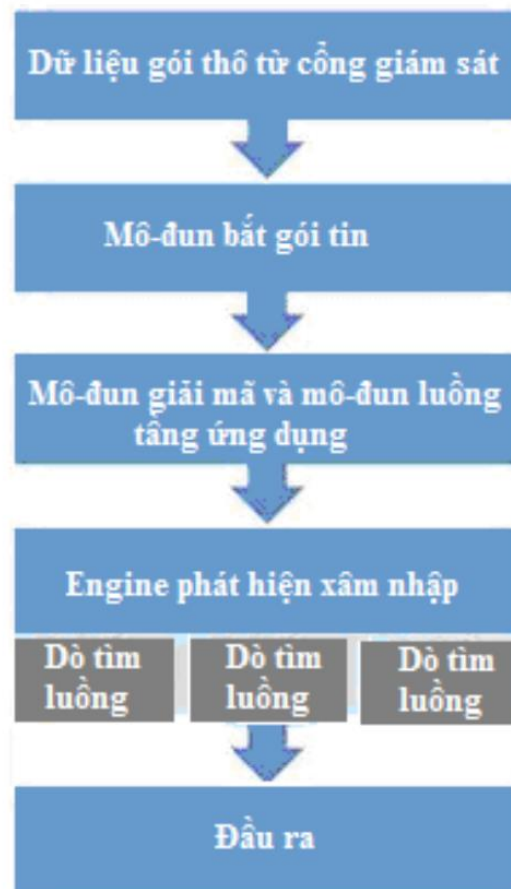
- chế độ sniffer
 - `snort -i <interface>`
- chế độ log gói tin
 - `snort -i <interface>`
- chế độ NIDS.



Hình 3.11 Kiến trúc Snort NIDS

Phát hiện xâm nhập dựa trên chữ ký

➤ Suricata



Hình 3.13 Runmode mặc định của Suricata

Phát hiện xâm nhập dựa trên chữ ký

- Làm báo cáo theo nhóm 4-5 sinh viên và báo cáo bằng slide trên lớp
- Đăng ký nhóm: <https://forms.gle/o3okgKPGajHFKp666>
- Nội dung báo cáo
 - Bộ công cụ Security Onion
 - Snort/Suricata: Lý thuyết và demo
- Thời gian báo cáo: Buổi học tiếp theo

4. Phát hiện xâm nhập dựa trên bất thường với dữ liệu thống kê

- ☐ Danh sách thống kê
- ☐ Khám phá dịch vụ
- ☐ Tìm hiểu thêm về phát hiện xâm nhập dựa trên thống kê
- ☐ Một số công cụ hiển thị thống kê

Danh sách thống kê

❑ Dữ liệu thống kê:

- Ví dụ: danh sách các máy tính giao tiếp trên mạng nội bộ có lưu lượng dữ liệu liên lạc lớn nhất
- Xác định được các thiết bị có lưu lượng gửi đi đến máy chủ bên ngoài lớn đáng ngờ, hoặc có thể là máy tính được bảo vệ nhưng bị nhiễm phần mềm độc hại kết nối với một số lượng lớn các địa chỉ IP bên ngoài đáng ngờ
- Đây là một bất thường thật sự của mạng, không thể phát hiện bằng chữ ký
- Sử dụng các công cụ phân tích dữ liệu về phiên như SiLK và Argus



Tạo danh sách thống kê với SiLK

- ☐ SiLK là công cụ được sử dụng hiệu quả cho việc thu thập, lưu trữ và phân tích dữ liệu luồng
- ☐ Đồng thời có thể tạo ra các số liệu thống kê và số liệu cho nhiều tình huống
- ☐ `rwstats` và `rwcount` dùng để tạo ra một danh sách thống kê lưu lượng

Tạo danh sách thống kê với SiLK

- ❑ rfilter tập hợp tất cả các bản ghi lưu lượng thu thập trong 1400 giờ ngày 8 tháng 8, và chỉ kiểm tra lưu lượng trong phạm vi IP 102.123.0.0/16. Dữ liệu đó được chuyển tới rwstats, để tạo ra một danh sách top 20 (--count = 20) kết hợp địa chỉ IP nguồn và đích (--fields = sip, dip) cho dữ liệu trong bộ lọc, sắp xếp theo byte (--value = bytes).

```
rwfilter --start-date = 2013/08/26:14 --any-  
address = 102.123.0.0/16 --type = all --  
pass = stdout | rwstats --top --count = 20 --  
fields = sip,dip --value = bytes
```

Tạo danh sách thống kê với SiLK

```
INPUT: 14258883 Records for 1442095 Bins and 359838834159 Total Bytes
OUTPUT: Top 28 Bins by Bytes
```

sIP	dIP	Bytes	%Bytes	cumul_%
182.123.222.245	168.59.76.107	38038339439	8.347739	8.347739
173.221.197.93	182.123.155.234	29118445814	8.092098	16.439837
173.221.45.238	182.123.168.43	6201468707	1.723403	18.163240
182.123.170.162	119.104.73.89	6196314721	1.721973	19.885213
182.123.242.126	79.86.35.244	6001882411	1.667718	21.552931
173.12.240.132	182.123.168.43	5633491224	1.565563	23.118494
182.123.73.19	173.184.168.79	4815223824	1.338164	24.456658
182.123.73.19	173.184.168.42	4791526426	1.331579	25.788237
182.123.168.248	182.123.112.7	3817497327	1.060893	26.849130
182.123.142.81	182.123.155.160	2335601387	0.649070	27.498200
168.59.73.160	182.123.25.93	2329652425	0.647417	28.145617
173.184.210.142	182.123.73.31	2119689249	0.589068	28.734685
71.9.97.121	182.123.175.66	2102937605	0.584412	29.319097
182.123.168.169	168.59.121.15	1950040136	0.541922	29.861019
168.59.73.132	182.123.25.53	1903135121	0.528887	30.389905
182.123.142.136	184.201.124.129	1890621864	0.525409	30.915314
182.123.142.203	182.123.155.160	1845292902	0.512812	31.428127
182.123.155.25	119.104.73.49	1831162761	0.508885	31.937012
168.59.73.160	182.123.25.53	1795540049	0.498986	32.435997
182.123.142.79	184.201.124.129	1756983560	0.488271	32.924268

Tạo danh sách thống kê với SiLK

- `rwfilter --start-date = 2013/08/26:14 --any-address = 102.123.222.245 --type = all --pass = stdout | rwstats --top --count = 5 --fields = sip,dip --value = bytes`

```
INPUT: 128837 Records for 8511 Bins and 32059683554 Total Bytes
OUTPUT: Top 5 Bins by Bytes
```

sIP	dIP	Bytes	%Bytes	cumul_%
102.123.222.245	168.59.76.107	30038339439	93.695059	93.695059
168.59.76.107	102.123.222.245	418907922	1.306650	95.001709
102.123.222.245	102.123.231.154	81795975	0.255137	95.256846
102.123.222.245	102.123.168.62	60875215	0.189881	95.446727
102.123.168.62	102.123.222.245	24694805	0.077028	95.523754

Tập trung vào nhóm các đối tác liên lạc thường xuyên của một máy tính đơn lẻ

Tạo danh sách thống kê với SiLK

- `rwfilter --start-date = 2013/08/26:14 --any-address = 102.123.222.245 --type = all --pass = stdout | rwstats --top --count = 5 --fields = sip, sport, dip --value = bytes`

```
INPUT: 128837 Records for 32092 Bins and 32059683554 Total Bytes
OUTPUT: Top 5 Bins by Bytes
      sip|sPort|      dIP|      Bytes|      %Bytes|      cumul_%|
102.123.222.245|  22| 168.59.76.107|    15257159577|  47.589863|  47.589863|
maverick:ch11 chris$
```

Sử dụng thống kê để xác định lượng sử dụng dịch vụ

Tạo danh sách thống kê với SiLK

➤ `rwfilter --start-date = 2013/08/26:14 --any-address = 102.123.222.245 --sport = 22 --type = all --pass = stdout | rwcount --bin-size = 600`

Date	Records	Bytes	Packets
2013/08/26T14:30:00	0.26	405758958.97	271885.01
2013/08/26T14:40:00	1.00	1553551544.63	1040980.97
2013/08/26T14:50:00	1.00	1553551544.63	1040980.97
2013/08/26T15:00:00	1.00	1516348807.05	1016170.31
2013/08/26T15:10:00	1.00	1411920652.04	946529.39
2013/08/26T15:20:00	1.00	1411920652.04	946529.39
2013/08/26T15:30:00	1.00	1596803663.96	1070176.01
2013/08/26T15:40:00	1.00	2120740976.27	1420577.00
2013/08/26T15:50:00	1.00	2120740976.27	1420577.00
2013/08/26T16:00:00	0.74	1565821801.15	1040865.34

rwcount để xác định khoảng thời gian giao tiếp diễn ra

Tạo danh sách thống kê với SiLK

❑ Nhận xét:

- Việc truyền dữ liệu tương đối nhất quán theo thời gian
- Đường hầm SSH có thể được sử dụng để chuyển một lượng lớn dữ liệu.
- Đây có thể là một nguy cơ như rò rỉ dữ liệu, hoặc một cái gì đó đơn giản như một người sử dụng công cụ SCP để chuyển một cái gì đó tới hệ thống khác với mục đích sao lưu.

Khám phá dịch vụ với SiLK

- ❑ Tạo ra một rfilter để thu thập tập dữ liệu để từ đó tạo ra số liệu thống kê

```
rwfilter --start-date = 2013/08/28:00 --end-date = 2013/08/28:23 --type = all --  
protocol = 0- --pass = sample.rw
```

- ❑ Các thiết bị trong mạng nội bộ trao đổi cái gì nhiều nhất tại các cổng phổ biến, 1-1024?

```
rwfilter sample.rw --type = out,outweb --sport  
= 1-1024 --pass = stdout | rwstats --fields =  
sip,sport --count = 20 --value = dip-distinct
```

```
INPUT: 893306 Records for 30815 Bins  
OUTPUT: Top 20 Bins by dIP-Distinct
```

sIP	sPort	dIP-Distin	%dIP-Disti	cumul_%
219.15.129.211	53	41806	?	?
184.226.35.112	25	28637	?	?
184.226.79.198	25	16328	?	?
184.226.79.199	53	6155	?	?
184.226.79.216	53	6134	?	?
219.15.128.211	53	4066	?	?
219.15.128.242	53	4062	?	?
219.15.165.211	25	1458	?	?
184.226.19.89	25	387	?	?
184.226.60.116	25	357	?	?
184.226.60.145	25	318	?	?
184.226.60.43	25	315	?	?
219.15.4.152	25	233	?	?
219.15.178.3	992	194	?	?
184.226.35.215	25	113	?	?
120.140.239.134	500	100	?	?
184.226.127.254	500	95	?	?
219.15.155.69	21	88	?	?
219.15.156.80	25	86	?	?
184.226.94.102	500	65	?	?

```
maverick:ch11 chris$
```

Tìm hiểu thêm về phát hiện xâm nhập dựa trên thống kê

- ❑ Xem xét cảnh báo về Zeus tạo ra bởi Snort

The screenshot displays the Snort GUI interface with the following sections:

- IP Header Information:** A table showing network header details.

Source	Destination	Ver	Ilen	Tos	Len	ID	Flags	Off	TTL	Proto	Checksum
[redacted]	[redacted]	4	5	0	76	440	0	0	120	17	27221
- Signature Information:** A table showing the detected signature details.

Generator ID	Sig. ID	Sig. Revision	Activity (316/358255)	Category	Sig Info
1	2404108	3169	0.09%	trojan-activity	Query Signature Database View Rule
- UDP Header Information:** A table showing UDP header details.

Src Port	Dst Port	Len	Checksum
60031	123	56	13039
- References:** A list of URLs related to the event.

Type	Value
url	doc.emergingthreats.net/bin/view/Main/BotCC
url	zeustracker.abuse.ch
url	palevotracker.abuse.ch
url	spyeyetracker.abuse.ch
- Payload:** A section showing the raw data of the event in hexadecimal and ASCII format.

Tìm hiểu thêm về phát hiện xâm nhập dựa trên thống kê

- ❑ Dễ nhầm với lưu lượng NTP do các kết nối giống lưu lượng UDP qua cổng 123
- ❑ Cần phải xem thêm các liên lạc khác của máy tính, xác định xem máy tính đang liên lạc với "các máy chủ NTP" khác nữa mà có thể có dấu hiệu đáng ngờ nhờ trường mã quốc gia

```
rwfilter --start-date = 2013/09/02 --end-date = 2013/09/02 --any-address = 192.168.1.17 --  
aport = 123 --proto = 17 --type = all --pass = stdout  
| rwstats --top --fields = dip,dcc,dport --count = 20
```

- ❑ Máy tính được bảo vệ giao tiếp với nhiều máy tính khác trên cổng 123


INPUT: 2042 Records for 44 Bins and 2042 Total Records						
OUTPUT: Top 28 Bins by Records						
dIP dco dPort	Records	NRecords	cumul_%			
192.5.xxxxxx us 123	128	6.268364	6.268364			
192.36.xxxxxx se 123	86	4.211557	10.479922			
192.36.xxxxxx se 123	85	4.162586	14.642507			
192.36.xxxxxx se 123	84	4.113614	18.756121			
150.254.xxxxxx pl 123	84	4.113614	22.869736			
129.242xxxxxx no 123	83	4.064643	26.934378			
192.36.xxxxxx se 123	81	3.966699	30.901077			
62.119xxxxxx se 123	81	3.966699	34.867777			
62.119xxxxxx se 123	80	3.917728	38.785504			
192.36.xxxxxx se 123	77	3.770813	42.556317			
192.36.1xxxxxx se 123	75	3.672870	46.229187			
203.117.xxxxxx sq 123	75	3.672870	49.902057			
192.36.xxxxxx se 123	73	3.574927	53.476983			
193xxxxxx sl 123	72	3.525955	57.002938			
204.11xxxxxx vg 123	67	3.281097	60.284035			
192.36.1xxxxxx se 123	67	3.281097	63.565132			
128.9.xxxxxx us 123	64	3.134182	66.699314			
192.16xxxxxx us 60059	60	2.938296	69.637610			
193.62xxxxxx gb 123	59	2.889324	72.526934			
192.16xxxxxx us 60060	58	2.840353	75.367287			

❑ Hiện thị nhiều thiết bị có các mẫu liên lạc tương tự

```
rwfilter --start-date = 2013/09/02 --end-date = 2013/09/02 --not-dipset = local.set --dport = 123 --proto = 17 --type = all --pass = stdout | rwstats --top --fields = sip --count = 20 --value = dip-distinct
```

```
INPUT: 19279 Records for 95 Bins
OUTPUT: Top 20 Bins by dIP-Distinct
```

sIP	dIP-Distin	%dIP-Disti	cumul_%
192.16.xxxxxx	596	?	?
192.16xxxxxx	500	?	?
192.16.1xxxxxx	471	?	?
192.16.xxxxxxx	130	?	?
192.26xxxxxx	93	?	?
10.20.xxxxxxx	46	?	?
192.16xxxxxx	22	?	?
10.49xxxxxx	21	?	?
10.49xxxxxx	21	?	?
205.204xxxxxx	12	?	?
192.24.1xxxxxx	10	?	?
192.25xxxxxx	7	?	?
10.242.xxxxxxx	5	?	?
10.240.xxxxxxx	5	?	?
192.16xxxxxx	3	?	?
192.24.xxxxxxx	3	?	?
192.24.xxxxxxx	3	?	?
192.24.1xxxxxx	3	?	?
10.240.xxxxxxx	3	?	?
10.43.1xxxxxx	3	?	?



Một số công cụ hiển thị thống kê

- ☐ Gnuplot
- ☐ Google Chart
- ☐ Afterglow

Một số công cụ hiển thị thống kê

❑ Hiển thị thống kê với Gnuplot

- ❑ Các đầu ra của lệnh `rwcount` được gửi thông qua một số dòng lệnh sửa đổi để tạo ra một tệp tin CSV chỉ chứa các dấu thời gian và giá trị byte cho mỗi dấu thời gian

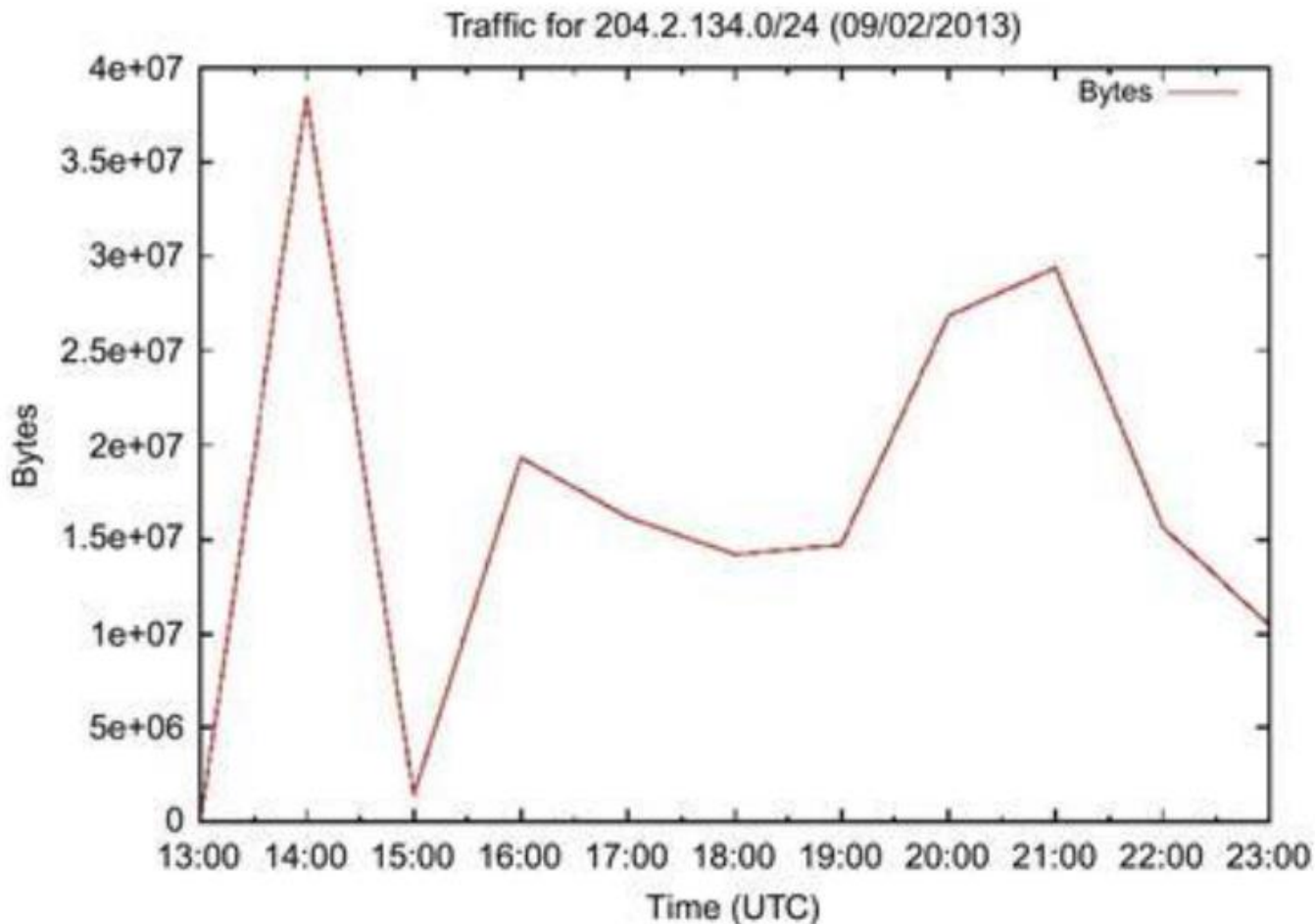
```
rwfilter --start-date = 2013/09/02 --any-address =  
204.2.134.0/24 --proto = 0- --pass = stdout --type =  
all | rwcount --bin-size = 3600 -delimited =, --no-  
titles| cut -d "," -f1,3 > hourly.csv
```

➤ Kết quả dữ liệu như sau:

```
2013/09 / 02T13: 00: 00,146847.07  
118  
2013/09 / 02T14: 00: 00,38546884.51  
2013/09 / 02T15: 00: 00,1420679.53  
...
```

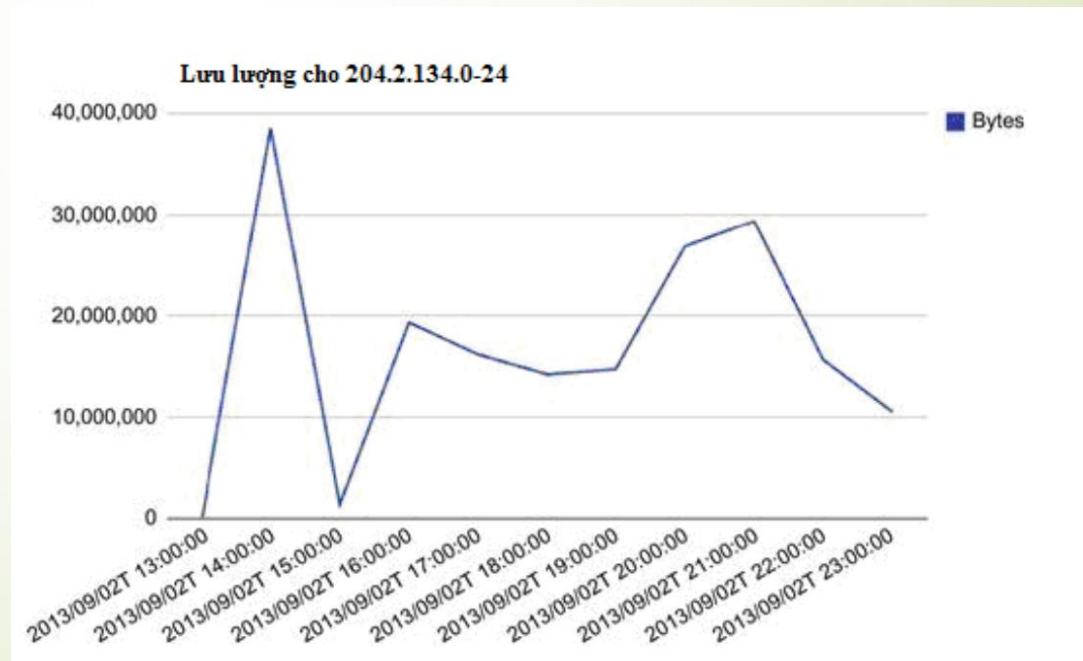
Một số công cụ hiển thị thống kê

- Hiển thị thống kê với Gnuplot



Một số công cụ hiển thị thống kê

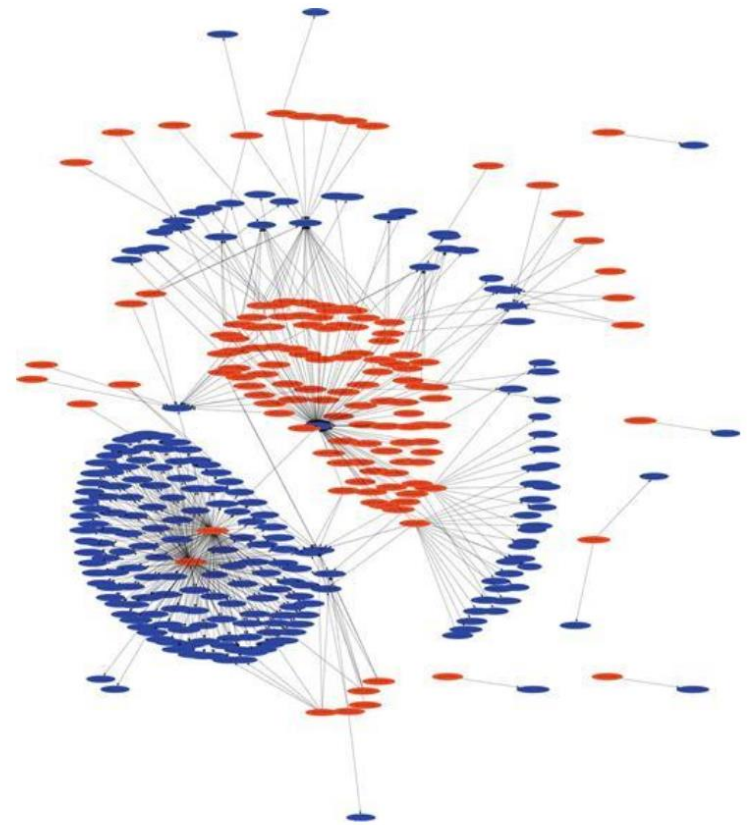
- ❑ Hiển thị thống kê với Google Chart
 - ❑ Google Chart API của Google
(<https://developers.google.com/chart/>)
 - ❑ Tương thích với các trình duyệt và 100% miễn phí
 - ❑ Cú pháp đơn giản



Một số công cụ hiển thị thống kê

❑ Hiển thị thống kê với Afterglow

- ❑ là một công cụ Perl cho phép tạo ra một đồ thị các liên kết để có thể thấy được mô tả toàn cảnh về các thành phần liên kết
- ❑ Afterglow nhận tệp tin CSV có định dạng sau
- ❑ tạo ra tệp tin ngôn ngữ đồ thị có định dạng sau hoặc một tệp tin GDF có thể được hiển thị bằng Gephi



Hình 3.35 Một đồ thị liên kết tạo từ dữ liệu NetFlow



Một số công cụ hiển thị thống kê

- Bộ công cụ ELK stack