MILE Working Group
Internet-Draft
Intended status: Informational
Expires: January 5, 2015

M. Suzuki
D. Inoue
M. Eto
K. Nakao
NICT

July 4, 2014

Incident Information Exchange in Darknet Monitoring System
draft-suzuki-mile-darknet-00.txt

Abstract

A darknet is a set of routable but unused IP addresses whose monitoring is an effective way of detecting malicious activities on the Internet. We have developed an alert system - called DAEDALUS - based-on a large-scale distributed darknet that consists of several organizations that mutually observe the malicious packets transmitted from the inside of the organizations. This draft shares the schema of an alert of the DAEDALUS to exchange incident information among organizations.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 5, 2015.

Copyright Notice

Table of Contents

1. Introduction

Recent epidemic of highly organized and sophisticated malwares like bots increases the necessity of techniques to detect, analyze and respond to them. Various commercial, academic, or government-backed projects are ongoing to research and develop the countermeasure technologies. As the prior step, many of these projects are concentrating on providing statistical data, such as rapid increase of accesses on certain port numbers, based on network events monitoring. In course of these activities, it is a popular approach to monitor a dark address space, which is a set of globally announced unused IP addresses. One method of these monitoring approaches is black hole monitoring that listen quietly to the incoming packets, which often contain great amount of malware scans, DDoS backscatter, etc.

We have been developing the nicter1 system[nicter] that consists of a large-scale darknet monitoring facility. There, however, have been a gap between the darknet monitoring and actual security operations on the live network (hereafter referred to as livenet), which comprises legitimate hosts, servers and network devices. For instance, although darknet monitoring can be used to inform network operators about a global increase in scan on 80/tcp, it may not ensure that any concrete security operations are carried out. This means that

darknet monitoring does not significantly contribute to the protection of the livenet.

Therefore, we propose a novel application of large-scale darknet monitoring that significantly contributes to the security of the livenet. In contrast to the conventional method wherein the packets received from the outside are observed, we employ a large-scale distributed darknet that consists of several organizations that mutually observe the malicious packets transmitted from the inside of the organizations. Based on this approach, we have developed an alert system called DAEDALUS (direct alert environment for darknet and livenet unified security)[DAEDALUS-VIZ].

DAEDALUS consists of an analysis center and several organizations. Each organization (hereafter referred to as org) establishes a secure channel with the analysis center and continuously forwards darknet traffic toward the center. In addition, each org registers the IP address range of its livenet to the center beforehand. We divide the darknet into two types - internal and external darknet. From the viewpoint of an org, the darknet within the org is an internal darknet, and the darknets in other orgs are external darknets.

When a malware infection occurs, and the infected host starts scanning the inside of the org, including the internal darknet, the analysis center can detect the infection on the basis of the match between the source IP address of darknet traffic from the org G and the preregistered livenet IP address. The analysis center then sends an internal darknet alert to org G. When the infected host starts scanning the outside, including the external darknet in org A, the analysis center can detect the infection in the same above-mentioned manner. The analysis center then sends an external darknet alert to org G. The alerts include information on the IP address of the infected host, protocol, source/destination ports, duration of attack, and analysis results, if any.

This draft describes the schemata of the alert in detail

2. Terminology

The terminology used in this document follows the terminology defined in RFC 5070.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

3. DAEDALUS alert data model

The DAEDALUS data model is used for sharing alert data among parties about darknet monitoring. The XML Schema of this data model is shown in the next section.

3.1. NicterEvent class

The NicterEvent class is the top level class in the DAEDALUS data model. This class and following Header class is commonly used in the other model of our nicter project. The EventType class in the Header class indicates the type of event in our nicter project. Fixed value "DaedalusAlert" is used in case of this draft. CreateTime class shows the time when this event occured.

3.2. DaedalusAlertHeader class

The DaedalusAlertHeader class contains general information of the alert. The AlertID class indicates unique ID throughout all alerts. The OrgID class shows unique ID of each organization that monitors its own darknet. The Trigger class shows the cause of issued alert. Currently, DAEDALUS has one of "Urgent" or "Periodic" in the Trigger class. The "Urgent" means the alert needs immediate attention. The "Periodic" means the alert is issued periodically, and is not urgent. The Duration class indicates the duration of monitoring until this alert issued.

3.3. AlertData class

The AlertData class contains packet data summarized by each source IP address. The following Packet class shows actual packet data. The EventTime attribute shows the time when the last packet in this AlertData class is monitored. The EventID attribute indicates unique ID throughout all AlertData class. The SrcIP attribute shows the monitored source IP address. The SrcCC attribute indicates the country code where the source IP address is allocated. The TotalPacketCount attribute shows the number of whole monitored packets. The DisplayedPacketCount shows the number of sampled packets when large number of packets is monitored. The Type attribute shows the type of the AlertData class. The string "New" means that the source IP address hasn’t been monitored for a certain period. While, the "Continued" means the source IP address has been monitored continuously.

3.4. Packet class

The Packet class shows a series of packets received from the source IP address indicated on the upper AlertData class. One Packet class contains layer 3 and layer 4 information of one packet. The DstIP attribute shows the destination IP address of the packet, and the DstCC shows the country code of that address. The Protocol attribute shows the protocol number of the packet. The DstPort attribute and the SrcPort attribute indicate the destination port number and the source port number of the packet. These attributes of port numbers appear only when the protocol number of the packet is 6 (TCP) or 17 (UDP). The Flag attribute shows both the flag of TCP header and the number of ICMP type field, which depends on the protocol of the packet. The DarknetType attribute shows where the packet comes from. The "internal" means that the packet comes from internal IP address of the monitored organization. In contrast, the "external" packets come from external IP address outside of its monitored organization.

4. DAEDALUS alert schemata

The XML schema of the DAEDALUS alert is as shown below.

```
<?xml version="1.0" encoding="shift_jis"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified" xml
ns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="NicterEvent">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Header">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="EventType" type="xs:string" />
              <xs:element name="CreateTime" type="xs:dateTime" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="DaedalusAlertHeader">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="AlertID" type="xs:unsignedInt" />
              <xs:element name="OrgID" type="xs:unsignedInt" />
              <xs:element name="Trigger" type="xs:string" />
              <xs:element name="Duration" type="xs:unsignedInt" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element maxOccurs="unbounded" name="AlertData">
          <xs:complexType>
            <xs:sequence>
```

```
              <xs:element maxOccurs="unbounded" name="Packet">
                <xs:complexType>
                  <xs:attribute name="PacketTime" type="xs:dateTime" use="requir
ed" />
                  <xs:attribute name="DstIP" type="xs:string" use="required" />
                  <xs:attribute name="DstCC" type="xs:string" use="required" />
                  <xs:attribute name="DstPort" type="xs:unsignedShort" use="requ
ired" />
                  <xs:attribute name="SrcPort" type="xs:unsignedShort" use="requ
ired" />
                  <xs:attribute name="Protocol" type="xs:unsignedShort" use="req
uired" />
                  <xs:attribute name="Flag" type="xs:string" use="required" />
                  <xs:attribute name="DarknetType" type="xs:string" use="require
d" />
                </xs:complexType>
              </xs:element>
            </xs:sequence>
            <xs:attribute name="EventTime" type="xs:dateTime" use="required" />
            <xs:attribute name="EventID" type="xs:unsignedInt" use="required" />
            <xs:attribute name="SrcIP" type="xs:string" use="required" />
            <xs:attribute name="SrcCC" type="xs:string" use="required" />
            <xs:attribute name="TotalPacketCount" type="xs:unsignedInt" use="req
uired" />
            <xs:attribute name="DisplayedPacketCount" type="xs:unsignedInt" use=
"required" />
            <xs:attribute name="Type" type="xs:string" use="required" />
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

5. An example XML document

An example XML document of the DAEDALUS alert is shown below. The source IP address and destination IP address are masked as xxx.yyy on this example.

```
<?xml version="1.0"?>
<NicterEvent>
  <Header>
    <EventType>DaedalusAlert</EventType>
    <CreateTime>2011-12-19 11:00:45</CreateTime>
  </Header>
  <DaedalusAlertHeader>
    <AlertID>277761</AlertID>
    <OrgID>2</OrgID>
    <Trigger>Periodic</Trigger>
    <Duration>3600</Duration>
  </DaedalusAlertHeader>
  <AlertData EventTime="2011-12-19 11:00:39" EventID="1096117" SrcIP="xxx.yyy.23
6.116" SrcCC="JP" TotalPacketCount="878" DisplayedPacketCount="878" Type="Contin
ued">
    <Packet PacketTime="2011-12-19 10:01:21" DstIP="xxx.yyy.241.101" DstCC="JP"
DstPort="" SrcPort="" Protocol="1" Flag="8" DarknetType="internal"/>
    <Packet PacketTime="2011-12-19 10:01:31" DstIP="xxx.yyy.241.101" DstCC="JP"
DstPort="" SrcPort="" Protocol="1" Flag="8" DarknetType="internal"/>
    <Packet PacketTime="2011-12-19 10:01:33" DstIP="xxx.yyy.241.101" DstCC="JP"
DstPort="" SrcPort="" Protocol="1" Flag="8" DarknetType="internal"/>
    <Packet PacketTime="2011-12-19 10:01:35" DstIP="xxx.yyy.241.101" DstCC="JP"
DstPort="445" SrcPort="3580" Protocol="6" Flag="2" DarknetType="internal"/>
    <Packet PacketTime="2011-12-19 10:01:38" DstIP="xxx.yyy.241.101" DstCC="JP"
DstPort="445" SrcPort="3580" Protocol="6" Flag="2" DarknetType="internal"/>
    <Packet PacketTime="2011-12-19 10:01:42" DstIP="xxx.yyy.241.101" DstCC="JP"
DstPort="" SrcPort="" Protocol="1" Flag="8" DarknetType="internal"/>
    <Packet PacketTime="2011-12-19 10:01:44" DstIP="xxx.yyy.241.101" DstCC="JP"
DstPort="" SrcPort="" Protocol="1" Flag="8" DarknetType="internal"/>
    <Packet PacketTime="2011-12-19 10:01:45" DstIP="xxx.yyy.241.101" DstCC="JP"
DstPort="445" SrcPort="3580" Protocol="6" Flag="2" DarknetType="internal"/>
    <Packet PacketTime="2011-12-19 10:01:47" DstIP="xxx.yyy.241.101" DstCC="JP"
DstPort="137" SrcPort="137" Protocol="17" Flag="" DarknetType="internal"/>
    <Packet PacketTime="2011-12-19 10:01:48" DstIP="xxx.yyy.241.101" DstCC="JP"
DstPort="137" SrcPort="137" Protocol="17" Flag="" DarknetType="internal"/>
  <!-- SNIP -->
  </AlertData>
</NicterEvent>
```

6. Use Cases

6.1. Finding Scans of Infected Hosts

When the infected host in a organization(Org. A) starts scanning outside the organization, including the external darknet in other organization(Org. B), Org. B detects the scanning. It then shares the monitored information with Org. A using this schema.

6.2. Observing Backscatter of DDoS

When a host in a organization(Org. A) is under a distributed denial of service (DDoS) attack from many spoofed IP addresses, the host sends backscatter (TCP SYN-ACK) packets to a wide area, including the external darknets in some of other organizations(Org. B and C). In this example case, sharing monitored information of Org. B and C with Org. A using this schema helps to defence against the DDoS attack.

7. Security Considerations

TBD

8. Acknowledgments

TBD

9. Informative References

[DAEDALUS-VIZ]
Inoue, D., "DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System", October 2012, <http://dl.acm.org/citation.cfm?id=2379700>.

[nicter] Inoue, D., "nicter: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis", April 2008, <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4627315>.

Authors' Addresses

Mio Suzuki
National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi Koganei
184-8795 Tokyo
Japan

Phone: +80 423 27 6277
EMail: mio@nict.go.jp

Daisuke Inoue
National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi Koganei
184-8795 Tokyo
Japan

Phone: +80 423 27 6243
EMail: dai@nict.go.jp

Masashi Eto
National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi Koganei
184-8795 Tokyo
Japan

Phone: +80 423 27 5573
EMail: eto@nict.go.jp

Koji Nakao
National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi Koganei
184-8795 Tokyo
Japan

Phone: +80 423 27 6826
EMail: ko-nakao@nict.go.jp