Observing attacks with the ARAKIS early warning system

Tomasz Grudziecki
Agenda

I. ARAKIS – what is it?
II. VoIP attacks
III. Massive traffic from Myanmar/Burma
IV. Sudden death of the Slammer...
V. ...and sudden resurrection :(
I About the ARAKIS (1)

- An early warning system
- Detects threats that propagate *actively* through network scanning
- Focuses on detection and *characterization* of current and new automated threats
- Focus primarily on exploits used in the wild, not malware.
I About the ARAKIS (2)

• Uses four types of sources:
  • Low-interaction Honeypots (main source)
  • Darknet (a.k.a. network telescope)
  • Firewall logs (minor)
  • AV logs from mail servers

• Data from these sources is aggregated and correlated
About the ARAKIS (3)

Sensor (honeypot + log parser, first analyses)

Darknet

Center (aggregation & correlation, next analyses, data mining)

Web GUI
I About the ARAKIS (4)

- Distributed network of sensors (data from multiple sensors are aggregated)
- Operates on national level (sensors are placed only in Polish networks)
- Techniques used in Analyses:
  - Sliding window mechanism (applied on the flows)
  - Rabin-Karp algorithm
  - Computing the Longest Common Substring (LCS)
  - Clusterization of the similar LCS-es
Recent observations
II VoIP attacks - SIP

- SIP: Session Initiation Protocol (RFC 3261)
- Control protocol used for establish, modify, and terminate multimedia sessions (conferences)
- SIP default port/protocol is 5060/UDP (and TCP)
- RFC defines 6 main methods used in SIP protocol:
  - REGISTER – registering contact information,
  - INVITE, ACK, and CANCEL – setting up sessions
  - BYE – terminating sessions
  - OPTIONS for querying servers about their capabilities
II VoIP attacks - SIP

• First massive scanning: July 2010
II VoIP attacks - SIP

Source: ISC SANS (http://isc.sans.org/)
II VoIP attacks - SIP

- Scanning sources

<table>
<thead>
<tr>
<th>Position</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>China</td>
</tr>
<tr>
<td>2</td>
<td>USA</td>
</tr>
<tr>
<td>3</td>
<td>France</td>
</tr>
<tr>
<td>4</td>
<td>Nigeria</td>
</tr>
<tr>
<td>5</td>
<td>Germany</td>
</tr>
<tr>
<td>6</td>
<td>Egypt</td>
</tr>
<tr>
<td>7</td>
<td>Russia</td>
</tr>
<tr>
<td>8</td>
<td>Korea</td>
</tr>
<tr>
<td>9</td>
<td>Ireland</td>
</tr>
<tr>
<td>10</td>
<td>Romania</td>
</tr>
</tbody>
</table>

SIP (VoIP) attack sources

- CN 60%
- US 11%
- FR 5%
- other world 24%
- CN 60%
II VoIP attacks - SIP

• SIP OPTIONS scanning:
  • CSeq (Command Sequence) number: 1
  • User-Agent:
    • `friendly-scanner` (80%) = Sipvicious scanner
    • or `sundayddr` (20%) = Sundayddr/sipsscuser scanner

Source: honeynet.org.au/?q=sunday_scanner
Session Initiation Protocol
Request-Line: OPTIONS sip:100@10.x.x.25 SIP/2.0
Method: OPTIONS
[Resent Packet: False]
Message Header
Via: SIP/2.0/UDP 10.x.x.203:5064;branch=z9hG4bK-4143939552;rport
Transport: UDP
Sent-by Address: 10.x.x.203
Sent-by port: 5064
Branch: z9hG4bK-4143939552
RPort: rport
Content-Length: 0
From: "sipvicious"; tag=3531303662623139313363340133393439363734343739
SIP Display info: "sipvicious"
SIP from address: sip:100@1.1.1.1
SIP tag: 3531303662623139313363340133393439363734343739
Accept: application/sdp
User-Agent: friendly-scanner
To: "sipvicious"
SIP Display info: "sipvicious"
SIP to address: sip:100@1.1.1.1
Contact: sip:100@10.x.x.203:5064
Contact Binding: sip:100@10.x.x.203:5064
URI: sip:100@10.x.x.203:5064\r
SIP contact address: sip:100@10.x.x.203:5064\r
CSeq: 1 OPTIONS
Sequence Number: 1
Method: OPTIONS
Call-ID: 693404165087465926103669
Max-Forwards: 70
II VoIP attacks - SIP

- SIP REGISTER scanning:
  - User-Agent: eyeBeam release 3006o stamp 17551
  - Call-ID: different in each packet
  - Branch: different in each packet
Session Initiation Protocol
Request-Line: REGISTER sip:82.x.x.121 SIP/2.0
Method: REGISTER
[Resnet Packet: False]
Message Header
To:
SIP to address: sip:500@82.x.x.121
From: ;tag=33742674
SIP from address: sip:500@82.x.x.121
SIP tag: 33742674
Via: SIP/2.0/UDP 192.x.x.3:6021;branch=z9hG4bK-d87543-944197934-1--d87543--;rport
Transport: UDP
Sent-by Address: 192.x.x.3
Sent-by port: 6021
Branch: z9hG4bK-d87543-944197934-1--d87543-
RPort: rport
Call-ID: 562d2c461a1f4626
CSeq: 1 REGISTER
Sequence Number: 1
Method: REGISTER
Contact:
Contact Binding:
URI:
SIP contact address: sip:500@192.x.x.3:6021
Expires: 3600
Max-Forwards: 70
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
User-Agent: eyeBeam release 30060 stamp 17551
Content-Length: 0
II VoIP attacks - SIP

- SIP INVITE + CANCEL scanning:
  - User-Agent: Asterisk PBX
  - SIP tag: as*
  - SIP Display info: "Shenzhou Morokoshi"
  - CSeq: 102
Session Initiation Protocol
Request-Line: INVITE sip:010863982164000@81.x.x.13 SIP/2.0
Method: INVITE
[Resent Packet: False]
Message Header
Via: SIP/2.0/UDP 188.x.x.46:5060;branch=z9hG4bK277d8087;rport
Transport: UDP
Sent-by Address: 188.x.x.46
Sent-by port: 5060
Branch: z9hG4bK277d8087
RPort: rport
From: "Shenzhou Morokoshi" ;tag=as7047c7fe
SIP Display info: "Shenzhou Morokoshi"
SIP from address: sip:01064442288@188.x.x.46
SIP tag: as7047c7fe
To:
SIP to address: sip:010863982164000@81.x.x.13
Contact:
Contact Binding:
URI:
SIP contact address: sip:01064442288@188.x.x.46
Call-ID: 7ba4b1815214a23b049486ca288812aa@188.x.x.46
CSeq: 102 INVITE
Sequence Number: 102
Method: INVITE
User-Agent: Asterisk PBX
Max-Forwards: 70
Date: Thu, 18 Nov 2010 22:35:43 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces
Content-Type: application/sdp
Content-Length: 264
Message body
Message body
Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator, Session Id (o): root 3506 3506 IN IP4 188.x.x.46
Owner Username: root
Session ID: 3506
Session Version: 3506
Owner Network Type: IN
Owner Address Type: IP4
Owner Address: 188.x.x.46
Session Name (s): session
Connection Information (c): IN IP4 188.x.x.46
Connection Network Type: IN
Connection Address Type: IP4
Connection Address: 188.x.x.46
Time Description, active time (t): 0 0
Session Start Time: 0
Session Stop Time: 0
Media Description, name and address (m): audio 17928 RTP/AVP 8 0 101
Media Type: audio
Media Port: 17928
Media Proto: RTP/AVP
Media Format: ITU-T G.711 PCMA
Media Format: ITU-T G.711 PCMU
Media Format: 101

Media Attribute (a): rtpmap:8 PCMA/8000
Media Attribute Fieldname: rtpmap
Media Format: 8
MIME Type: PCMA
Media Attribute (a): rtpmap:0 PCMU/8000
Media Attribute Fieldname: rtpmap
Media Format: 0
MIME Type: PCMU
Media Attribute (a): rtpmap:101 telephone-event/8000
Media Attribute Fieldname: rtpmap
Media Format: 101
MIME Type: telephone-event
Media Attribute (a): fmtp:101 0-16
Media Attribute Fieldname: fmtp
Media Format: 101 [telephone-event]
Media format specific parameters: 0-16
Media Attribute (a): silenceSupp:off - - -
Media Attribute Fieldname: silenceSupp
Media Attribute Value: off - - -
Media Attribute (a): ptime:20
Media Attribute Fieldname: ptime
Media Attribute Value: 20
Media Attribute (a): sendrecv
II VoIP attacks - SIP

- Current status

Honeynet:

Darknet:
III Massive traffic from Myanmar/Burma

• From 21st of February 2011 for a couple of months
• Traffic from the Union of Myanmar (Burma).
• At regular intervals from about 3AM to 12PM (UTC).
• Dst ports: 21/TCP, 22/TCP, 25/TCP, 80/TCP, 443/TCP and 179/TCP
• Most of flows did not contain any payloads
• All TCP headers have been malformed in the same manner
III Massive traffic from Myanmar/Burma

- Destination Port 21/tcp
  - Total Current: 278.00
  - Average: 102.60
  - Max: 578.00
  - Total Events: 0.00

- Destination Port 22/tcp
  - Total Current: 338.00
  - Average: 132.13
  - Max: 752.00
  - Total Events: 0.00

- Destination Port 25/tcp
  - Total Current: 235.00
  - Average: 92.54
  - Max: 537.00
  - Total Events: 0.00

- Destination Port 80/tcp
  - Total Current: 1.09 k
  - Average: 308.47
  - Max: 1.62 k
  - Total Events: 0.00

- Destination Port 443/tcp
  - Total Current: 569.00
  - Average: 109.49
  - Max: 720.00
  - Total Events: 0.00
III Massive traffic from Myanmar/Burma

- Other CERTs confirmed the attack:
  
  Source: Tsubame Working Group, APCERT
III Massive traffic from Myanmar/Burma

- Other CERTs confirmed the attack:
  Source: Tsubame Working Group, APCERT
III Massive traffic from Myanmar/Burma

• Other CERTs confirmed the attack:

Source: Tsubame Working Group, APCERT
III Massive traffic from Myanmar/Burma

- Other CERTs confirmed the attack:
  Source: Tsubame Working Group, APCERT
III Massive traffic from Myanmar/Burma

- Other CERTs confirmed the attack:
  Source: Tsubame Working Group, APCERT
IV Sudden death of the Slammer...

- SQL Slammer – well known computer worm, that targets MS SQL Server and Desktop products
- Propagation through 1434/UDP
- Sudden decline on the 10-03-2011
IV Sudden death of the Slammer...

Honeynet:

Darknet:
IV Sudden death of the Slammer...

Source: http://isc.sans.edu/diary.html?storyid=10576
V ...and sudden resurrection :( 

- Traffic is back since 08-04-2011

**Honeynet:**

**Darknet:**
LCS details

Id: a0a4a74b70cbca5a03960df1a3dc878

Name: 

First seen: 2007-06-14 17:00:43 


Last flow: 75.76.53.95:1044 -> xxx.xxx.133.244:1434 [UDP]

Seen on ports: 1434/UDP

Analysis: VLCS, HLCS

Cluster: [WORM] SQL Slammer (1434/UDP, MS02-039, MS02-061, CVE-2002-0649)

Matched Bleeding Snort rules:

MS-SQL Worm propagation attempt [1][2][3][4][5]
MS-SQL version overflow attempt [1]

Payload size: 376

Payload:

0x0000: 0401 0101 0101 0101 0101 0101 0101 0101 ................
0x0010: 0101 0101 0101 0101 0101 0101 0101 0101 ................
0x0020: 0101 0101 0101 0101 0101 0101 0101 0101 ................
0x0030: 0101 0101 0101 0101 0101 0101 0101 0101 ................
0x0040: 0101 0101 0101 0101 0101 0101 0101 0101 ................
0x0050: 0101 0101 0101 0101 0101 0101 0101 0101 ................
0x0060: 01dc c9b0 42eb 0e01 0101 0101 0101 70ae ............B........p.
0x0070: 4201 70ae 4290 9090 9090 9068 dcc9 B.p.B........h..
0x0080: b042 b801 0101 0131 c9b1 1850 e2fd 3501 .B.....l..P..5.
0x0090: 0101 0550 89e5 5168 2e64 6c6c 6865 6c33 ................P..Qh.dllhe13
0x00a0: 326b 6b65 726e 5168 6775 6e74 6869 636b 2hkernel0hountichk
0x00b0: 4368 4765 7454 66b9 6c6c 5168 3332 2e64 ChGetTf.11Qh32.d
0x00c0: 6877 7332 5f66 b965 7451 6873 6f63 6b66 Chs2.f.etQhssockf
0x00d0: b974 6f51 6873 656e 646e 1810 aa42 8d45 .toQhsend...B.E
0x00e0: d450 ff16 508d 45e0 508d 45f0 50ff 1650 .P..P.E.P.E.P.P
0x00f0: be10 10ae 4288 1e8b 033d 558b ec51 7405 ........B....U.Qt.
0x0100: be1c 10ae 42ff 1bff d031 c951 5150 81f1 ........B....1.QP..
0x0110: 0301 049b 81f1 0101 0101 518d 45cc 508b ...........Q.E.P.
0x0120: 45c0 50ff 166a 116a 026a 02ff d050 8445 E.P..j.j...P.E
0x0130: c450 8b45 c050 ff16 89c6 09db 81f3 3c61 .P.E.P.........<a
0x0140: d9ff 8b45 b4ad 0c40 8d14 8ec1 e204 01c2 ...........E.E.B.
0x0150: c1e2 0829 c28d 0490 01d8 8945 b46a 108d ).....E..j.
0x0160: f170 0151 8d45 0350 E.P.L.Qf.x.Q.E.P
0x0170: 8b45 ac50 ffdf ebca .E.P....
V ...and sudden resurrection :(

- Current status of the Slammer propagation

---

**Honeynet:**

**Darknet:**
ARAKIS in academic and research publications


Braun, Lothar; Dressler, Falko; Holz, Thorsten; Kirda, Engin; Kohlrausch, Jan; Krügel, Christopher; Limmer, Tobias; Rieck, Konrad; Sterbenz, James P G, "WG Requirements for network monitoring from an IDS perspective", Dagstuhl seminar on Network Attack Detection and Defense 2008, March 2-6, 2008, Dagstuhl, Germany
THANK YOU!

Any questions?

tomasz.grudziecki@cert.pl
www.arakis.pl