On the use of name server log data as input for security measurements

Christian Frühwirth  
SBL, Aalto University, Finland  
christian.fruehwirth@tkk.fi

Christian Proschinger  
CERT.at, Austria  
proschinger@cert.at

Otmar Lendl  
CERT.at, Austria  
lendl@cert.at
Austrian national Computer Emergency Response Team

- **Mission Statement**
  “The purpose of CERT.at is to coordinate security efforts and incident response for IT-security problems on a national level in Austria. “

- **Constituency**
  “The constituency are IT-security teams and local CERTs in Austria. Pro-active and educational material will be provided for SMEs and the general public as well.”

- **Initiative from Nic.at – the Austrian registry**
Motivation

• National CERT’s **mission is to inform** its constituency about security issues and facilitate communication between its partners (ISPs, companies, universities, end-users, other CERTs)

• **DNS logs are a rich, and readily available, data source** for security measurement (from large organizations->companies -> end users).

→ **Individual analysis of DNS Logs proved useful in the past**, but without **cooperation** between organizations, our (CERT’s) **field of view** is limited.

→ **We wanted an overview** of how and where the Analysis of DNS logs for security measurement purposes is already **working well**, and **where we should focus** our improvement (i.e. cooperation) efforts.
Goal

• Give a high-level overview of how DNS is & can be used for practical security measurement by members of CERTs’ constituency

• Help CERT stakeholders understand where cooperation is beneficial.

→ Encourage more companies & organizations to partner with CERTs and improve security trend monitoring
Quick DNS 101
DNS hierarchy

**gTLDs**

- .com
- .org
- ...

**ccTLDs**

- .at
- .fi
- ...

- .co
- .ac
- .gv

ICANN and/or sponsor

Local Policies

**gTLD**...generic Top Level Domain

**ccTLD**...country-code Top Level Domain
Passive DNS

• Passive collection of DNS server replies
  – Allows to determine
    • Change of IP addresses behind domains
    • Change of nameservers
    • Domains hosted at the same IP
  – Major **limitation**: Passive DNS requires sensors in different networks
Approach
How to structure a high-level overview of DNS use in sec. measurement?

Our approach:
• DNS log analysis is used for security measurement by
  – different entities (stakeholders) with
  – different measurement capabilities (fields of view) on
  – different measurement elements in the security vulnerability-threat-incident chain of events.

➔ We organize the use of DNS for sec. measurement by
  1.) Stakeholder type & field of view
1.) Create matrix for stakeholders and security chain / measurements
2.) Fill cells with color-coded description of possible DNS log data use
3.) Add field of view:

Field of view in DNS hierarchy

![Diagram of DNS hierarchy with TLD 1 and TLD 2, including NS and Client nodes.]

- CERT
- Large Comp.
- SME
- User
- Vulnerability
- Exploit
- Threat
- Risk
- Countermeasure
- Incident
3.) Add field of view:

- CERT
- Large Comp.
- SME
- User

- Vulnerability
- Exploit
- Threat
- Risk
- Countermeasure
- Incident

Client

NS

Client

Client
3.) Add field of view:

- Vulnerability
- Exploit
- Threat
- Risk
- Countermeasure
- Incident

![Diagram showing the field of view with CERT, Large Comp., SME, and User layers, and a network structure with TLD 1 and TLD 2.](image-url)
3.) Add field of view:

- Vulnerability
- Exploit
- Threat
- Risk
- Countermeasure
- Incident

Diagram:

- TLD 1
- TLD 2
- NS
- Client
- ...
3.) Add field of view:

- Vulnerability
- Exploit
- Threat
- Risk
- Countermeasure
- Incident

Diagram:

- TLD 1
  - NS
  - Client

- TLD 2
  - NS
  - NS
  - ...
  - ...

User

SME

CERT

Large Comp.
4.) Apply to use cases:

We applied the categorization to 4 cases where DNS played an important role in understanding and measuring the security issue at hand.

- Targeted Attack: Aurora
- Worm: Conficker
- Technology issue: DNS Kaminsky Bug
- Industrial Malware: Stuxnet
DNS log analysis use cases
Experiences - Results
Aurora

• 12.1.2010 – Google announced attack
  - over 30 other organization affected too

• Infection by
  – drive-by download
  – Zero day exploit

• CnC Server
  – Based on DynamicDNS
## Aurora

<table>
<thead>
<tr>
<th>Stage</th>
<th>Measure</th>
<th>CERT</th>
<th>Large Company</th>
<th>SME</th>
<th>EndUser</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability</strong></td>
<td># of vulnerable Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Signs of exploited vulnerabilities</td>
<td>A (if info from DDNS providers is available)</td>
<td>info delivered FROM 3rd party</td>
<td>info delivered FROM 3rd party</td>
<td>info delivered FROM 3rd party</td>
</tr>
<tr>
<td><strong>Exploit</strong></td>
<td>Severity of threat (based on V, E)</td>
<td>A (if info from DDNS providers is available)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Threat</strong></td>
<td>Risk for group of stakeholders</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td># of countermeasures deployed / Vuln. Fixed</td>
<td>A *</td>
<td>A *</td>
<td>A (*)</td>
<td>A (*)</td>
</tr>
<tr>
<td><strong>Countermeasure</strong></td>
<td># of incidents that occurred</td>
<td>A (if info from DDNS providers or victims is available)</td>
<td>A (visible in NS and local cache)</td>
<td>A (visible in local cache)</td>
<td>A (visible in local cache)</td>
</tr>
<tr>
<td><strong>Incident</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Conficker and DNS

• Pseudorandom domains
  – Conficker.B: 250 / day
  – Conficker.C: 450 .at domains / day

• Large Scale
  – Aconet CERT runs nameservers and a sinkhole
  – CERT.at uses Data to generate Warnings
  – nic.at is sponsoring the domain costs
  – Cooperation with the international Conficker Working Group

• Small Scale
  – By looking at DNS Queries
  – Manipulation local DNS Cache
Conficker measurement example:
Unique infected IPs in Austria over time
Conficker measurement example:
Infected IPs Worldwide by location
## Conficker

<table>
<thead>
<tr>
<th>Stage</th>
<th>Measure</th>
<th>CERT</th>
<th>Large Company</th>
<th>SME</th>
<th>EndUser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability</td>
<td># of vulnerable Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Signs of exploited vulnerabilities</td>
<td>C, Quality improvement through 3rd party info</td>
<td>info delivered FROM 3rd party</td>
<td>info delivered FROM 3rd party</td>
<td>info delivered FROM 3rd party</td>
</tr>
<tr>
<td>Exploit</td>
<td>Severity of threat (based on V, E)</td>
<td>S, cooperation with Large ISPs required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat</td>
<td>Risk for group of stakeholders</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td># of countermeasures deployed / Vuln. Fixed</td>
<td>C *</td>
<td>C *</td>
<td>C*</td>
<td>C*</td>
</tr>
<tr>
<td>Countermeasure</td>
<td># of incidents that occurred</td>
<td>C (visible in NS cache)</td>
<td>C (visible in NS cache)</td>
<td>C (visible in local cache)</td>
<td>C (visible in local cache + ability to access antivir domains)</td>
</tr>
</tbody>
</table>

**Incident**
„Kaminsky“ DNS Bug

- VU#800113
- Dire Warning: Insufficient entropy in ID
- Recommendation were
  - Update Software
  - Implement Source Port Randomization
  - Restrict Recursion
  - Filter spoofed IP traffic

16 bits of entropy might have been enough in 1987, but not in 2008.
Scoring Resolvers

\[
\text{score} = \frac{\text{portchanges}}{\text{queries}} \times \frac{\text{ports}}{\min(\text{queries}, 65536)}
\]
Patching by Server (short term)

By request, not by server:

<table>
<thead>
<tr>
<th>Stage</th>
<th>Measure</th>
<th>CERT</th>
<th>Large Company</th>
<th>SME</th>
<th>EndUser</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability</strong></td>
<td># of vulnerable Systems</td>
<td>K</td>
<td>K</td>
<td>K</td>
<td>K</td>
</tr>
<tr>
<td></td>
<td>Signs of exploited vulnerabilities</td>
<td>info delivered FROM 3rd party</td>
<td>info delivered FROM 3rd party</td>
<td>info delivered FROM 3rd party</td>
<td>info delivered FROM 3rd party</td>
</tr>
<tr>
<td><strong>Exploit</strong></td>
<td>Severity of threat ( based on V, E)</td>
<td>K (if info from 3rd party is available)</td>
<td>K (given V+E is known)</td>
<td>info delivered FROM 3rd party</td>
<td>info delivered FROM 3rd party</td>
</tr>
<tr>
<td><strong>Threat</strong></td>
<td>Risk for group of stakeholders</td>
<td>K (if info from 3rd party is available)</td>
<td>K (given V+E+T is known)</td>
<td>info delivered FROM 3rd party</td>
<td>info delivered FROM 3rd party</td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td># of countermeasures deployed / Vuln. Fixed</td>
<td>K</td>
<td>K (on known NS)</td>
<td>K</td>
<td>K</td>
</tr>
<tr>
<td><strong>Countermeasure</strong></td>
<td># of incidents that occurred</td>
<td>K (if info from 3rd party is available)</td>
<td>K (access to cache + passive DNS)</td>
<td>K (access to cache + passive DNS)</td>
<td>K (access to cache + passive DNS)</td>
</tr>
</tbody>
</table>
Stuxnet

• Targeted Siemens Simatic industrial control systems
  – Point of entry Windows Systems

• CnC connection attempts visible in DNS logs:
  • mypremierfutbol.com
  • todaysfutbol.com
## Stuxnet

<table>
<thead>
<tr>
<th>Stage</th>
<th>Measure</th>
<th>CERT</th>
<th>Large Company</th>
<th>SME</th>
<th>EndUser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability</td>
<td># of vulnerable Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Signs of exploited vulnerabilities</td>
<td>S, cooperation with Large ISPs required</td>
<td>info delivered FROM 3rd party</td>
<td>info delivered FROM 3rd party</td>
<td>info delivered FROM 3rd party</td>
</tr>
<tr>
<td>Exploit</td>
<td>Severity of threat (based on V, E)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat</td>
<td>Risk for group of stakeholders</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td># of countermeasures deployed / Vuln. Fixed</td>
<td>S *</td>
<td>S *</td>
<td>S *</td>
<td>S *</td>
</tr>
<tr>
<td>Countermeasure</td>
<td># of incidents that occured</td>
<td>S, cooperation with Large ISPs required</td>
<td>S (visible in NS cache)</td>
<td>S (visible in local cache)</td>
<td>S (visible in local cache)</td>
</tr>
<tr>
<td>Incident</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Conclusions
<table>
<thead>
<tr>
<th>Stage</th>
<th>Measure</th>
<th>CERT</th>
<th>CERT</th>
<th>CERT</th>
<th>CERT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability</td>
<td># of vulnerable Systems</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploit</td>
<td>Signs of exploited vulnerabilities (info from CDNS providers is available)</td>
<td>info delivered from 3rd party</td>
<td>info delivered from 3rd party</td>
<td>info delivered from 3rd party</td>
<td>info delivered from 3rd party</td>
</tr>
<tr>
<td>Threat</td>
<td>Severity of threat (based on V, E)</td>
<td>K</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td>Risk for group of stakeholders</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Countermeasure</td>
<td># of countermeasures deployed / Vun. Fixed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident</td>
<td># of incidents that occurred</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Lack of visibility due to top-down view.**

**Focus on information exchange on signs of exploited vulnerabilities**

**Focus on information exchange on local incidents**
Conclusions

• National CERTs
  – can gain large scale view - but need cooperation
  – Able to compile/distribute information for other organizations
  – Top-Down view – only information from „victims“ allows detailed observation
  – Special Situation @ DNS Technical issues – possibility of countermeasure control
• Large Scale Companies
  – DNS is a good possibility for the detection and analysis (patient 0) of security incidents and control of countermeasures
  – They can benefit from CERT information
  – National CERTs can benefit from their nameserver logs
• SME, EndUser
  – Strength in local DNS cache analysis
  – Can benefit from CERT Incident Reports (Technical Guides)
Thank you!
Comments, Questions!

proschinger@cert.at - christian.fruewirth@tkk.fi - lendl@cert.fi

Special credit to:
Reijo Savola (VTT)
Aaron Kaplan
Florian Weimar
AcoNet CERT
Sources

Patching Nameservers: Austria reacts to VU#800113

Detecting Conficker in your Network

Erkennung von Stuxnet im eigenen Unternehmen

The Command Structure of the Aurora Botnet,

W32.Stuxnet Dossier, Symantec

Passive DNS Replication