Parameter Tuning for Domain Name System Covert Channels

Evaluating Signature-Based Intrusion Detection System Evasion

Vilhelm Prytz Filip Dimitrijevic

EECS
KTH Royal Institute of Technology

DA150X Student Conference

Introduction

- **What is DNS?**

Introduction

- **What is DNS?**
- Phonebook of the internet: DNS translates domain names to IP addresses. It can also associate other types of data with a domain name.

Introduction

- **What is DNS?**
- Phonebook of the internet: DNS translates domain names to IP addresses. It can also associate other types of data with a domain name.
- Essential for internet to work.

Example Scenario

- **Imagine a computer system that controls a nuclear reactor**

Example Scenario

- **Imagine a computer system that controls a nuclear reactor**
- Assume an attacker has access to this system.

Example Scenario

- **Imagine a computer system that controls a nuclear reactor**
- Assume an attacker has access to this system.
- They want to exfiltrate a sensitive file but they cannot, because a firewall is limiting outgoing internet access.

Example Scenario

- **Imagine a computer system that controls a nuclear reactor**
- Assume an attacker has access to this system.
- They want to exfiltrate a sensitive file but they cannot, because a firewall is limiting outgoing internet access.
- But DNS is left unfiltered! Previous research indicates this is often the case. Using a **DNS covert channel**, they can send the sensitive file over DNS.

Example Scenario

- **Imagine a computer system that controls a nuclear reactor**
- Assume an attacker has access to this system.
- They want to exfiltrate a sensitive file but they cannot, because a firewall is limiting outgoing internet access.
- But DNS is left unfiltered! Previous research indicates this is often the case. Using a **DNS covert channel**, they can send the sensitive file over DNS.
- How can we detect this covert channel? **Intrusion Detection System (IDS)**.

Research Questions

- Can *Snort* (the IDS software) detect *Iodine* (the covert channel software) covert channels?

Research Questions

- Can *Snort* (the IDS software) detect *Iodine* (the covert channel software) covert channels?
- If so, how can the configuration or source code of *Iodine* be altered to avoid detection by *Snort* using established detection rules?

Research Questions

- Can *Snort* (the IDS software) detect *Iodine* (the covert channel software) covert channels?
- If so, how can the configuration or source code of *Iodine* be altered to avoid detection by *Snort* using established detection rules?
- What generalized conclusions can be drawn about how IDSs detect covert channels?

How are we answering these questions?

- Using an experimental setup that runs *Iodine* and *Snort*.

How are we answering these questions?

- Using an experimental setup that runs *Iodine* and *Snort*.
- Mixing *Iodine* traffic with legitimate traffic to see if *Snort* falsely detects this.

How are we answering these questions?

- Using an experimental setup that runs *Iodine* and *Snort*.
- Mixing *Iodine* traffic with legitimate traffic to see if *Snort* falsely detects this.
- Using established detection rules from previous research.

How are we answering these questions?

- Using an experimental setup that runs *Iodine* and *Snort*.
- Mixing *Iodine* traffic with legitimate traffic to see if *Snort* falsely detects this.
- Using established detection rules from previous research.
- Modifying *Iodine* to try to avoid these rules.

What are we modifying?

- **Record Type**: Iodine employs the NULL record type by default.

What are we modifying?

- **Record Type**: Iodine employs the NULL record type by default.
- **EDNS(0) Parameter**: Iodine also makes use of EDNS(0), an extension to DNS.

What scenarios are we comparing?

- **Baseline**: No parameters modified.

What scenarios are we comparing?

- **Baseline**: No parameters modified.
- **Record Type Parameter**: EDNS(0) Parameter remains unchanged.

What scenarios are we comparing?

- **Baseline**: No parameters modified.
- **Record Type Parameter**: EDNS(0) Parameter remains unchanged.
- **EDNS(0) Parameter**: Record Type Parameter remains unchanged.

What scenarios are we comparing?

- **Baseline**: No parameters modified.
- **Record Type Parameter**: EDNS(0) Parameter remains unchanged.
- **EDNS(0) Parameter**: Record Type Parameter remains unchanged.
- **Both Parameters**: Both parameters are modified.

What parameters are we looking at?

- **False Negative Rate (FNR)** $= \frac{FN}{FN+TP}$: The proportion of iodine's covert traffic that Snort fails to detect. A low FNR indicates poor stealth for iodine.

What parameters are we looking at?

- **False Negative Rate (FNR)** $= \frac{FN}{FN+TP}$: The proportion of iodine's covert traffic that Snort fails to detect. A low FNR indicates poor stealth for iodine.
- **False Positive Rate (FPR)** $= \frac{FP}{FP+FN}$: The proportion of normal (non-tunneled) DNS traffic incorrectly flagged by Snort as covert.

What parameters are we looking at?

- **False Negative Rate (FNR)** $= \frac{FN}{FN+TP}$: The proportion of iodine's covert traffic that Snort fails to detect. A low FNR indicates poor stealth for iodine.
- **False Positive Rate (FPR)** $= \frac{FP}{FP+FN}$: The proportion of normal (non-tunneled) DNS traffic incorrectly flagged by Snort as covert.
- **Bandwidth**: The achieved throughput. That the tunnel is able to send data from the client to the server during the bandwidth test.

What is the result?

Metric	Scenario 1	Scenario 2.1	Scenario 2.2	Scenario 3	Scenario 4
False Negative Rate (FNR)	0.82%	100%	50.36%	50.45%	100.0%
False Positive Rate (FPR)	0.0%	0.0%	0.0%	0.0%	0.0%
Bandwidth	775 Kbits/sec	879 Kbits/sec	584 Kbits/sec	894 Kbits/sec	961 Kbits/sec

What is the result?

Metric	Scenario 1	Scenario 2.1	Scenario 2.2	Scenario 3	Scenario 4
False Negative Rate (FNR)	0.82%	100%	50.36%	50.45%	100.0%
False Positive Rate (FPR)	0.0%	0.0%	0.0%	0.0%	0.0%
Bandwidth	775 Kbits/sec	879 Kbits/sec	584 Kbits/sec	894 Kbits/sec	961 Kbits/sec

What does this mean?

What is the result?

Metric	Scenario 1	Scenario 2.1	Scenario 2.2	Scenario 3	Scenario 4
False Negative Rate (FNR)	0.82%	100%	50.36%	50.45%	100.0%
False Positive Rate (FPR)	0.0%	0.0%	0.0%	0.0%	0.0%
Bandwidth	775 Kbits/sec	879 Kbits/sec	584 Kbits/sec	894 Kbits/sec	961 Kbits/sec

What does this mean?

- *Iodine* can be modified to evade *Snort*.

What is the result?

Metric	Scenario 1	Scenario 2.1	Scenario 2.2	Scenario 3	Scenario 4
False Negative Rate (FNR)	0.82%	100%	50.36%	50.45%	100.0%
False Positive Rate (FPR)	0.0%	0.0%	0.0%	0.0%	0.0%
Bandwidth	775 Kbits/sec	879 Kbits/sec	584 Kbits/sec	894 Kbits/sec	961 Kbits/sec

What does this mean?

- *Iodine* can be modified to evade *Snort*.
- Scenario 2.1 evades *Snort* by simply using another record type.

What is the result?

Metric	Scenario 1	Scenario 2.1	Scenario 2.2	Scenario 3	Scenario 4
False Negative Rate (FNR)	0.82%	100%	50.36%	50.45%	100.0%
False Positive Rate (FPR)	0.0%	0.0%	0.0%	0.0%	0.0%
Bandwidth	775 Kbits/sec	879 Kbits/sec	584 Kbits/sec	894 Kbits/sec	961 Kbits/sec

What does this mean?

- *Iodine* can be modified to evade *Snort*.
- Scenario 2.1 evades *Snort* by simply using another record type.
- The bandwidth remains virtually unchanged across scenarios.

Answering our Research Questions

- **Can Snort detect Iodine covert channels?**

Answering our Research Questions

- **Can Snort detect Iodine covert channels?**
- Yes, using well-defined Snort rules.

Answering our Research Questions

- **Can Snort detect Iodine covert channels?**
- Yes, using well-defined Snort rules.
- **If so, how can the configuration or source code of Iodine be altered to avoid detection by Snort using established detection rules?**

Answering our Research Questions

- **Can Snort detect Iodine covert channels?**
- Yes, using well-defined Snort rules.
- **If so, how can the configuration or source code of Iodine be altered to avoid detection by Snort using established detection rules?**
- By modifying the Record Type parameter and the EDNS(0) parameter.

Answering our Research Questions

- **Can Snort detect Iodine covert channels?**
- Yes, using well-defined Snort rules.
- **If so, how can the configuration or source code of Iodine be altered to avoid detection by Snort using established detection rules?**
- By modifying the Record Type parameter and the EDNS(0) parameter.
- **What generalized conclusions can be drawn about how IDSs detect covert channels?**

Answering our Research Questions

- **Can Snort detect Iodine covert channels?**
- Yes, using well-defined Snort rules.
- **If so, how can the configuration or source code of Iodine be altered to avoid detection by Snort using established detection rules?**
- By modifying the Record Type parameter and the EDNS(0) parameter.
- **What generalized conclusions can be drawn about how IDSs detect covert channels?**
- How easy it is to detect *Iodine* depends heavily on the selected ruleset.

Discussion

- **Selection of parameter values**: Limited scope to include parameter values relevant in typical DNS usage.

Discussion

- **Selection of parameter values**: Limited scope to include parameter values relevant in typical DNS usage.
- **Selection of Snort rules**: Use more than two rules.

Discussion

- **Selection of parameter values**: Limited scope to include parameter values relevant in typical DNS usage.
- **Selection of Snort rules**: Use more than two rules.
- **Signature-based**: We only look at signatures, adopt statistical-based.

Discussion

- **Selection of parameter values**: Limited scope to include parameter values relevant in typical DNS usage.
- **Selection of Snort rules**: Use more than two rules.
- **Signature-based**: We only look at signatures, adopt statistical-based.
- **Experimental Setup**: Simplified experimental setup that doesn't include a resolver.

Thank you!

Thank you for listening!

Acknowledgments

Jana Tumova, Roberto Guanciale and Fredrik Lindeberg.