

# DNS Abuse: how Kaspersky can help to counteract it

---

Alexey Shulmin  
Malware Expert,  
Threat Exploration

kaspersky

# Agenda

What DNS Abuse consists of

Malwares abused DNS

Takedown service

DNS Tunneling

Botnets abused DNS

The Bot farm Project

Three main groups of attacks on DNS

Q&A Session

---

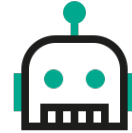
## DNS Abuse

According to DNS Abuse Framework [ 1], “DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS”:



---

Malware



---

Botnets



---

Spam



---

Phishing



---

Pharming

---

[ 1] [https:// dnsabuseframework.org/ media/ files/ 2020-05-29\\_ DNSAbuseFramework.pdf](https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf)

# Malware

is malicious software, installed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/ or gains access to private computer systems [1].

URL Reputation, IDS, WEB- AV, Snort/ Suricata



Malicious domains / malicious URLs (resources where the malicious software is hosted)

**273,033,368** unique malicious URLs were blocked in Q2 2022



Drive-by attacks (web-exploits)  
Almost disappeared now



DNS as a covert channel (DNS Tunneling)  
DNS backdoors (dnscat2)

---

[1] <https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf>

# Takedown Service



# Takedown Service



---

## Challenge

Cybercriminals create malicious and phishing domains which are used to attack companies and brands. The inability to quickly mitigate these threats, once identified, can lead to the loss of revenue, brand damage, loss of customer trust, data leaks, and more.

---

But managing takedowns of these domains is a complex process that requires expertise and time.

---

## Solution

Our many years of experience in analyzing malicious and phishing domains mean we know how to collect all the necessary evidence to prove that they are malicious. We'll take care of a takedown management and enable swift action to minimize digital risks.

# Takedown Service



---

## How it works

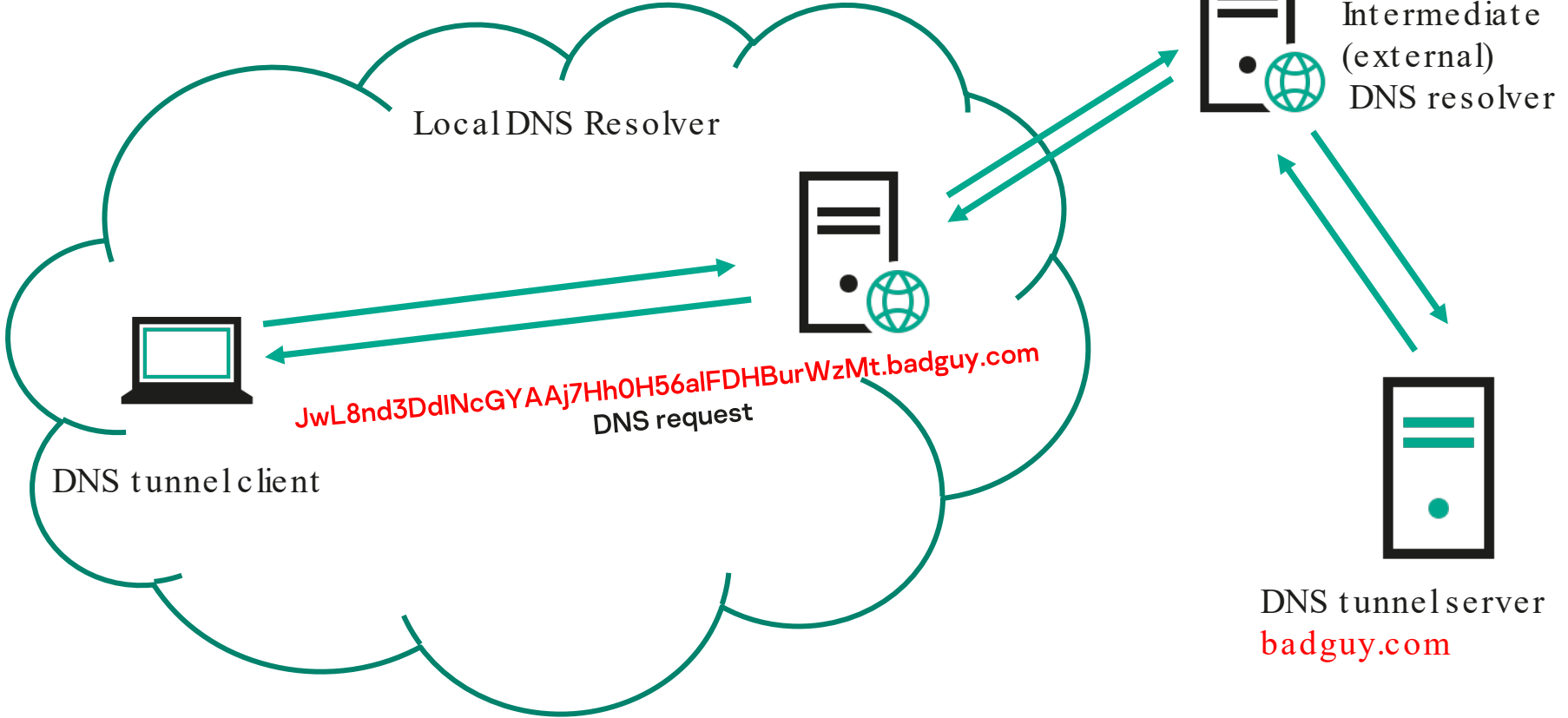
Our clients can submit their requests via our corporate customer support portal. We will prepare all the necessary documentation and will send the request for takedown to the relevant local/ regional authority (CERT, registrar, etc.) that has the necessary legal rights to shut down the domain. They will receive notifications at every step of the way until the requested resource is successfully taken down

# DNS Tunneling





# DNS Tunneling



# Backdoor.Win32.Denis

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.stream eq 5

Wireless controls are not supported in this version of Wireshark.

No.	Time	Source	Destina	Protoc	Len	Info
12	1.3133...	10.14...	8.8...	DNS	322	Standard query 0x042c NULL AAAAAAAAAAAAAAAAAAAAAAAAAAHNL.z.teriava.com
14	1.5391...	8.8...	10.1...	DNS	165	Standard query response 0x042c NULL AAAAAAAAAAAAAAAAAAAAAAAAAAHNL.z.teriava.com
15	1.5436...	10.14...	8.8...	DNS	322	Standard query 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAHoP.AAAAADwAAAA0AAAEJwL8nd5...
16	1.7455...	8.8...	10.1...	DNS	226	Standard query response 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAHoP.AAAAADwAAAA0AAAEJwL8nd5...
19	3.2475...	10.14...	8.8...	DNS	322	Standard query 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAHra.z.teriava.com
20	3.4389...	8.8...	10.1...	DNS	138	Standard query response 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAHra.z.teriava.com
23	4.9480...	10.14...	8.8...	DNS	322	Standard query 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAIF-.z.teriava.com
24	5.1387...	8.8...	10.1...	DNS	138	Standard query response 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAIF-.z.teriava.com
46	6.6488...	10.14...	8.8...	DNS	322	Standard query 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAIgi.z.teriava.com
47	6.8415...	8.8...	10.1...	DNS	138	Standard query response 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAIgi.z.teriava.com
48	8.3487...	10.14...	8.8...	DNS	322	Standard query 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAI7H.z.teriava.com
49	8.5393...	8.8...	10.1...	DNS	138	Standard query response 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAI7H.z.teriava.com
56	10.049...	10.14...	8.8...	DNS	322	Standard query 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAJvr.z.teriava.com
57	10.240...	8.8...	10.1...	DNS	138	Standard query response 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAJvr.z.teriava.com
61	11.749...	10.14...	8.8...	DNS	322	Standard query 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAJwQ.z.teriava.com
62	11.942...	8.8...	10.1...	DNS	138	Standard query response 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAJwQ.z.teriava.com
75	13.449...	10.14...	8.8...	DNS	322	Standard query 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAK0.z.teriava.com
76	13.640...	8.8...	10.1...	DNS	138	Standard query response 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAK0.z.teriava.com
78	15.150...	10.14...	8.8...	DNS	322	Standard query 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAK1Z.z.teriava.com
79	15.344...	8.8...	10.1...	DNS	138	Standard query response 0x042c NULL ktCrkqAAAAAAAAAAAAAAAAAAAAAAK1Z.z.teriava.com

> Frame 15: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits)  
> Ethernet II, Src: IntelCor\_e4:ce:4d (00:07:e9:e4:ce:4d), Dst: e2:4e:ce:30:b5:ec (e2:4e:ce:30:b5:ec)  
> Internet Protocol Version 4, Src: 10.14.0.2, Dst: 8.8.8.8  
> User Datagram Protocol, Src Port: 49579 (49579), Dst Port: 53 (53)

```
0000 e2 4e ce 30 b5 ec 00 07 e9 e4 ce 4d 08 00 45 00 .N.0.... .M..E.
0010 01 34 00 b8 00 00 80 11 1e e2 0a 0e 00 02 08 08 .4.....
0020 00 08 c1 ab 00 35 01 20 17 99 04 2c 01 00 00 01 .....5. ....
0030 00 00 00 00 00 00 20 6b 74 43 72 6b 67 51 41 41 ..... k tCrkqQAA
0040 41 41 41 41 41 45 41 41 41 41 41 41 41 41 41 41 AAAAAEAA AAAAAAAA
0050 41 41 41 41 48 6f 50 3e 41 41 41 41 44 77 41 AAAAHO> AAAAADwA
```

Packets: 97 · Displayed: 36 (37.1%) · Load time: 0:0.17 | Profile

Wireshark · Follow UDP Stream (udp.stream eq 5) · 1a4d58e281103fea2a4ccbfb93f74d2

```
00000000 04 2c 01 00 00 01 00 00 00 00 00 20 41 41 41 ..... AAA
00000010 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00000020 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 48 4e 4c 01 7a 07 AAAAAAAA AAHNL.z.
00000030 74 65 72 69 61 76 61 03 63 6f 6d 00 00 0a 00 01 teriava. com.....
00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000120 04 2c 81 80 00 01 00 01 00 00 00 20 41 41 41 ..... AAA
00000130 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00000140 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 48 4e 4c 01 7a 07 AAAAAAAA AAHNL.z.
00000150 74 65 72 69 61 76 61 03 63 6f 6d 00 00 0a 00 01 teriava. com....
00000160 c0 0c 00 0a 00 01 00 00 00 00 00 2f 00 00 00 ..... /./...
00000170 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 .....
00000180 10 00 00 13 00 00 00 78 9c 63 61 60 60 98 74 ..... x.ca`t
00000190 6f 24 06 28 00 00 1b e8 02 a4 ..... a.$.(...
000001a0 04 2c 01 00 00 01 00 00 00 00 00 20 6b 74 43 ..... k tC
000001b0 72 6b 67 51 41 41 41 41 41 41 41 41 45 41 41 41 41 rkgQAAAA AAAAAAAA
000001c0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 48 6f 50 3e 41 07 AAAAAAAA AAHoP>AA
000001d0 41 41 41 44 77 41 41 41 41 30 41 41 41 41 65 4a AAADwAAA A0AAAAEj
000001e0 77 4c 38 6e 64 33 44 64 49 4e 63 47 59 41 41 6a wL8nd3DD INcGYAAj
000001f0 37 48 68 30 48 35 36 61 6c 46 44 48 42 75 72 57 7Hh056a lFDHburW
00000200 7a 4d 74 62 77 4a 38 78 32 76 52 77 18 6d 46 35 zMtbwJ8x 2vRw.mf5
00000210 69 5a 47 4e 6b 5a 47 42 6b 59 47 4b 41 41 77 44 iZGnkZGB kYGKAAwD
00000220 57 49 67 30 65 01 7a 07 74 65 72 69 61 76 61 03 Wlg0e.z. teriava.
00000230 63 6f 6d 00 00 0a 00 01 00 00 00 00 00 00 00 00 00 .....
00000240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
18 client pkt(s), 18 server pkt(s), 35 turn(s).
```

Entire cor Show data as Hex Dump Stream 5

Find: Find Next

Hide this stream Print Save as... Close Help

## Response from C&C

11

```
00000160: 00 00 00 00-00 00 00 00-00 00 D2 51-D2 58 1B 98
00000170: 0A 00 A5 00-00 00 A5 00-00 00 00 07-E9 E4 CE 4D
00000180: A6 A0 15 16-6B F8 08 00-45 00 00 97-C4 D5 00 00
00000190: 38 11 A3 61-08 08 08 08-0A 0E 00 02-00 35 F5 0E
000001A0: 00 83 D8 16-02 14 81 80-00 01 00 01-00 00 00 00
000001B0: 20 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41
000001C0: 41 41 41 41-41 41 41 41-41 41 41 41-41 41 48 4D
000001D0: 38 01 7A 07-74 65 72 69-61 76 61 03-63 6F 6D 00
000001E0: 00 0A 00 01-C0 0C 00 0A-00 01 00 00-00 00 00 2F
000001F0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000200: 0B 00 00 00-10 00 00 00-13 00 00 00-78 9C 63 61
00000210: 60 60 D8 B3-57 74 17 03-14 00 00 18-9B 02 4D D2
```

```
FFFFFFFF ; enum CMDS, mappedto_64
FFFFFFFF CMD_API_RUN = 1
FFFFFFFF CMD_FREE_LIB = 2
FFFFFFFF CMD_PROC_START = 3
FFFFFFFF CMD_READ_FILE = 4
FFFFFFFF CMD_SHELL_RES = 5
FFFFFFFF CMD_NONE = 6
FFFFFFFF CMD_WRITE = 7
FFFFFFFF CMD_ENUM_WINDOWS = 0Ah
FFFFFFFF CMD_GET_COM_INFO = 0Bh
FFFFFFFF CMD_REG = 0Ch
FFFFFFFF CMD_FIND = 0Fh
FFFFFFFF CMDS_MOVE = 10h
FFFFFFFF CMD_DELETE = 11h
FFFFFFFF CMD_DRUS_INF = 12h
FFFFFFFF CMD_CREATE_DIR = 13h
FFFFFFFF CMD_REMOVE = 14h
FFFFFFFF
```

```
case CMD_SET_CFG:
    v26 = (int *)Src;
    if ( (unsigned __int8)set_config(Src) )
        dword_B6BE7C = *v26;
    v13 = collectPCInfo(&lpAddress);
    *(_DWORD *)a2 = 4;
    goto clean;
case CMD_REG:
    v13 = collectPCInfo(&lpAddress);
    *(_DWORD *)a2 = 3;
    goto clean;
```

```
ktCrkgQAAAAAAAAEAAAAAAAAAAAAAAHoP>AAAAADwAAAA0AAAAeJwL8nd3DdINcGYAAj7Hh0H56a1FDHBurWzMtbwJ8x2vRw.mF5iZGNkZGBkYGKAawDWIge==
```

↓ BASE 64 decoding

```
00000000: 92 D0 AB 92 04 00 00 00-00 00 01 00-00 00 00 00  |лТ◆  ⊕  
00000010: 00 00 00 00-00 00 7A 0F-00 00 00 00-3C 00 00 00  | z* <  
00000020: 34 00 00 00-78 9C 0B F2-77 77 0D D2-0D 70 66 00  | 4 хbσЄwwлТлpf  
00000030: 02 3E C7 87-41 F9 E9 A9-45 0C 70 6E-AD 6C CC B5  | ⊕>||3А-щйЕ♀рпн||н  
00000040: BC 09 F3 1D-AF 47 09 85-E6 26 46 36-46 46 06 46  | ♪oe↗пGoEц&F6FF♣F  
00000050: 06 28 00 30-0D 62 20 D1- - - - | ♣( 0)Ь Т
```

↓ Zlib unpacking

```
ROGER-PC AcRoger PC Ac}↗\пнРЯА||Z↓UmaYBYQYP
```

- **DNS request's length**

- alert udp any any -> any 53 (msg:"Large DNS Query, possible cover channel"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; **dsize:>40**; sid:192830182903; rev:1;)
- alert udp \$HOME\_NET any -> any 53 (msg:"Long dns sub-level domains"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; pcre:"/[\\x30-\\xFF]{1} [\\dA-Za-z\\/+]=]{48,} (?:[\\x02-\\xFF]\\S{2,})+\\x00/"; sid:3843858;)

- **Typical view of the DNS requests**

- alert udp \$HOME\_NET any -> any 53 (msg:"Not many numbers"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; pcre:"/\\x00[\\x30-\\xFF]{1} (?:\\S+[^\\-\\d]\\d){5,} (?:[\\x02-\\xFF]\\S{2,})+\\x00/"; sid:3858858;)

# Dnscat2<sup>[1]</sup>

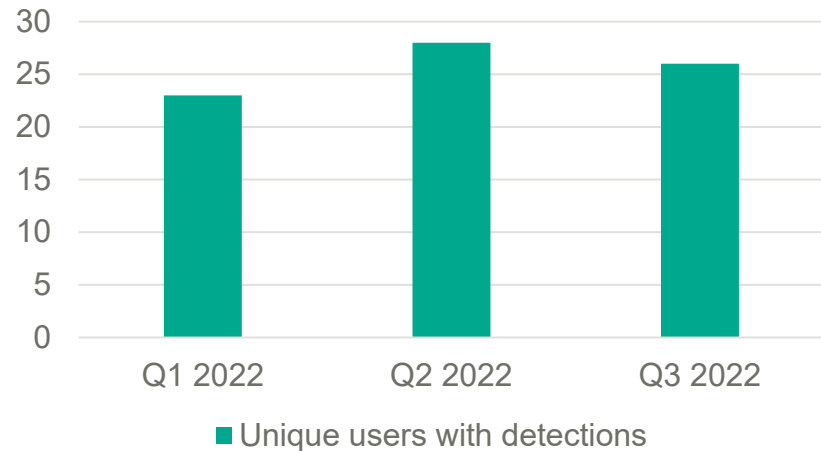
## Introduction

Welcome to dnscat2, a DNS tunnel that WON'T make you sick and kill you!

This tool is designed to create an encrypted command-and-control (C&C) channel over the DNS protocol, which is an effective tunnel out of almost every network.

This README file should contain everything you need to get up and running! If you're interested in digging deeper into the protocol, how the code is structured, future plans, or other esoteric stuff, check out the doc/ folder.

## Unique users with detections



[1] <https://github.com/iagox86/dnscat2>

# Botnets

are collections of Internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator [ 1].



Malicious domains / malicious URLs (**command and control servers** and other auxiliary resources)

**118** active botnet families are monitored by our botfarm system (more than **229k** bots)



DDoS-attacks (at DNS servers)

Sometimes they happen even suddenly



Spoof.dns attacks  
(Not a classic DNS spoofing attack, but sort of)

---

[ 1] <https://nices.cisa.gov/cybersecurity-career-resources/glossary#B>

---

## DNS DDoS Story (fun fact)

- several years ago a huge number of requests to non-existent domains 2-nd and 3-d levels were registered; it created enormous load at DNS-servers RU zone;
- there was a new version of well-known spam-bot Lethic behind that attack;
- we researched that version of trojan and discovered that the trojan, while was working in a multi-thread mode, created a lot of DNS-requests to non-existent subdomains;
- that trojan tried to hide the original CnC-communication that way;
- despite this story is interesting because it led to events that the developer, probably, had not expected, DDoS-attacks on DNS servers are not something new or highly-sophisticated, we are faced with such attacks on DNS-servers of our clients a lot of times.



- Bot tracking system
- Bot communication emulation
- Bot commands logging
- It can be used to:
  - to extract malicious domains from samples;
  - to predict newly registered malicious domains;

# The Bot farm project

2022-09-28T18:40:10.346003+03:00	<a href="#">spooof.dns on</a>	<a href="#">to.com</a>
fake	209.85.229.104	
2022-09-28T18:40:10.565766+03:00	<a href="#">spooof.dns on www.a</a>	<a href="#">s.ru</a>
fake	209.85.229.104	
2022-09-28T18:40:10.777209+03:00	<a href="#">spooof.dns on forum</a>	<a href="#">.com</a>
fake	209.85.229.104	
2022-09-28T18:40:10.988942+03:00	<a href="#">spooof.dns on www.ant</a>	<a href="#">t.com</a>
fake	209.85.229.104	
2022-09-28T18:40:11.201511+03:00	<a href="#">spooof.dns on www.</a>	<a href="#">.com.au</a>
fake	209.85.229.104	

<a href="#">2022.09.28 18:42:16</a>	attack.start	spooof.dns on	<a href="#">.de</a>	<a href="#">config_decrypted(text)</a> <a href="#">config_json(text)</a> <a href="#">config_raw(text)</a>
<a href="#">2022.09.28 18:42:16</a>	attack.start	spooof.dns on ant:	<a href="#">.com</a>	<a href="#">config_decrypted(text)</a> <a href="#">config_json(text)</a> <a href="#">config_raw(text)</a>
<a href="#">2022.09.28 18:42:16</a>	attack.start	spooof.dns on ru.:	<a href="#">com</a>	<a href="#">config_decrypted(text)</a> <a href="#">config_json(text)</a> <a href="#">config_raw(text)</a>
<a href="#">2022.09.28 18:42:16</a>	attack.start	spooof.dns on www.person:	<a href="#">.com</a>	<a href="#">config_decrypted(text)</a> <a href="#">config_json(text)</a> <a href="#">config_raw(text)</a>
<a href="#">2022.09.28 18:42:15</a>	attack.start	spooof.dns on pct	<a href="#">.com</a>	<a href="#">config_decrypted(text)</a> <a href="#">config_json(text)</a> <a href="#">config_raw(text)</a>
<a href="#">2022.09.28 18:42:15</a>	attack.start	spooof.dns on	<a href="#">guide.com</a>	<a href="#">config_decrypted(text)</a> <a href="#">config_json(text)</a> <a href="#">config_raw(text)</a>
<a href="#">2022.09.28 18:42:15</a>	attack.start	spooof.dns on	<a href="#">bs.com</a>	<a href="#">config_decrypted(text)</a> <a href="#">config_json(text)</a> <a href="#">config_raw(text)</a>

# Summarize



- **Attacks on DNS**
- **Attacks, performed by using DNS**
- **Attacks on DNS clients**

- **Attacks on DNS infrastructure (not DNS -specific):**
  - To scale DNS infrastructure
  - To use a special anti-DDoS solution or service, like Kaspersky DDoS Prevention
- **DNS request flood**
  - To scale DNS infrastructure
  - Fine tuning of service
  - To use a special anti-DDoS solution or service, like Kaspersky DDoS Prevention
- **NSXDOMAIN flood (a subset of DNS request flood attack)**
  - Mitigation measures are the same as for DNS request flood attack



- **DNS amplification DDoS:**

- To tune your DNS-server correctly (if it is vulnerable to this attack, most likely it does not tune correctly)

- **DNS tunneling**

- To use the complex of measures and settings and a special product or service, like, for example, Kaspersky Anti Targeted Attack Platform



Kaspersky  
Anti Targeted  
Attack Platform

- **DNS cache poisoning:**
  - To set TTL as lower as possible (our Kaspersky DDOS Prevention Service team recommends to our clients to set TTL=300).
  - To use DNSSEC protocol (it was especially developed to prevent this attack).

# Thank you!

Q&A session

Alexey Shulmin

Malware Expert

[Alexey.Shulmin@Kaspersky.com](mailto:Alexey.Shulmin@Kaspersky.com)

kaspersky