

Translating Saitama's DNS tunneling messages - SANS ISC

By SANS Internet Storm Center

Archived: 2026-04-05 14:47:24 UTC

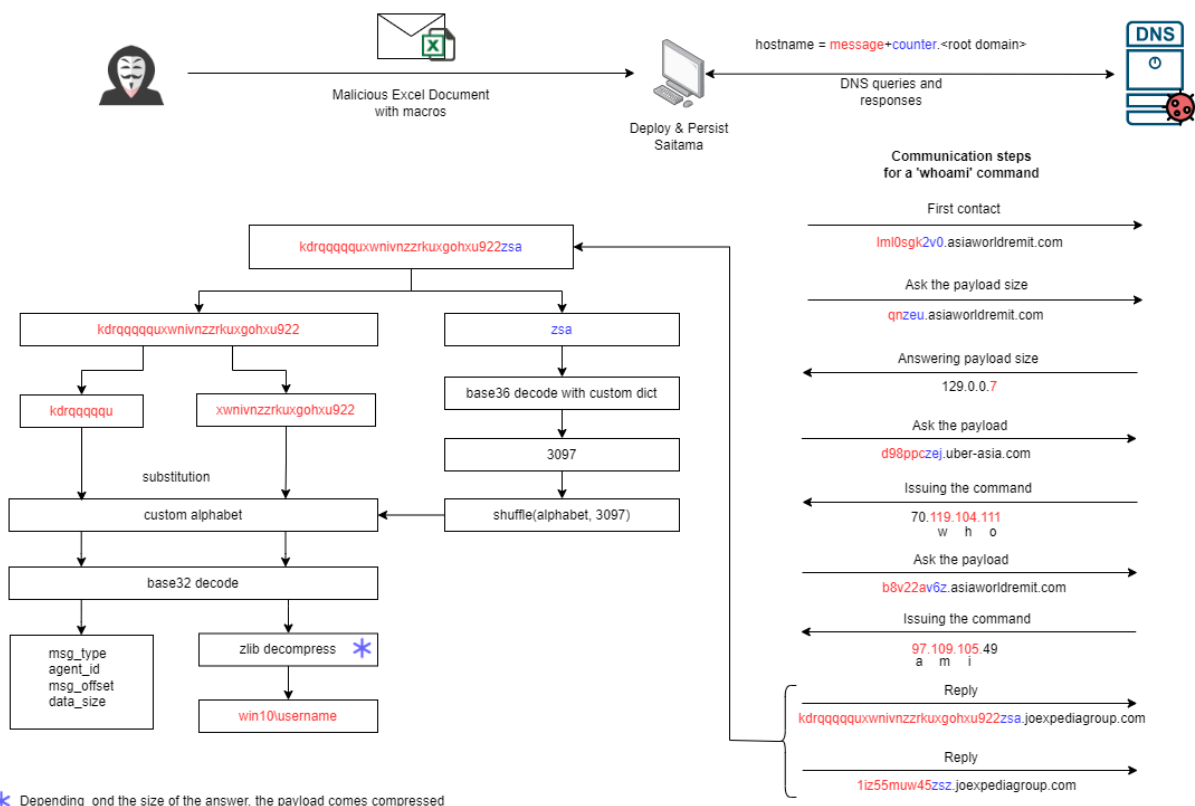
Saitama is a **backdoor** that uses the DNS protocol to encapsulate its **command and control** (C2) messages - a technique known as DNS Tunneling ([MITRE ATT&CK T1071](#)). Spotted and documented by MalwareBytes in two articles posted last month ([How the Saitama backdoor uses DNS tunneling](#) and [APT34 targets Jordan Government using new Saitama backdoor](#)), Saitama was used in a phishing e-mail targeted to a government official from Jordan's foreign ministry on an attack attributed to the Iranian group APT34.

Saitama caught my attention for two reasons: the stealth way the C2 messages are hidden in DNS protocol and the ease of access to malware implementation details by simply decompiling the .Net binary. Those points may increase the potential for other groups to use similar DNS tunneling techniques.

Saitama's DNS tunneling stealth strategy

Command and control (C2) over DNS is not new. It is common for a Victim <-> C2 communication occurs in the following way: data can be exfiltrated or answered from the victim to a C2 encoded in the hostname portion of the FQDN (i.e., oxn009lc7n5887k96c4zfckes6uif.rootdomain.com). In the other hand, commands or additional payloads can be downloaded from the C2 by the victim by querying TXT records to the attacker's controlled DNS server.

Saitama's implementation differs by not using TXT or other records able to store large data to encapsulate orders from the C2 to the victim. Instead, the orders are encapsulated in the IPV4 addresses themselves. For example, to issue the command '**whoami**', the server will answer two IP addresses: **70.119.104.111** and **97.109.105.49**. The first octet (70) has a special meaning to the Saitama (a command will be issued), and the following octets are the ASCII code of the 'whoami' characters: **w=119**, **h=104**, **o=111**, and so on until **i=105**. The remaining octet is discarded. Look at the image below the communication between a victim and the C2 by issuing the command 'whoami':



Saitama Translator

After analyzing Saitama's code, we developed a simple tool (available at https://github.com/morphuslabs/saitama_translator) capable of translating/decrypting the messages issued by the infected victim to the C2 server (the DNS queries). It may be helpful for those who face Saimanta or variants messages and need to try to discover what data is being sent to the C2.

Usage examples:

1. Passing one FQDN. In this case, the first response from Saitama do C2 after executing the command 'ver' on the infected system:

```
$ python translate.py vy5xxxxvzz650coacbsf03f2jkviwui9.joexpediagroup.com
agent_id: 114, msg_type: 1, msg_offset:0, msg_size:43, msg_content:b'9Microsoft W', requ
```

2. Passing multiple FQDN at once. In this case, all the responses from Saitama to C2 after executing 'ver' command:

```
$ python translate.py vy5xxxxvzz650coacbsf03f2jkviwui9.joexpediagroup.com oxn009lc7n5887k96c4zfckes6
agent_id: 114, msg_type: 1, msg_offset:0, msg_size:43, msg_content:b'9Microsoft W', requ
agent_id: 114, msg_type: 1, msg_offset:12, msg_size:None, msg_content:b'indows [Vers', requ
```

```
agent_id: 114, msg_type: 1, msg_offset:24, msg_size:None, msg_content:b'ion 10.0.183', requ  
agent_id: 114, msg_type: 1, msg_offset:36, msg_size:None, msg_content:b'63.418]', request:w7ir
```

Notice that the string "**Microsoft Windows [Version 10.0.18363.418]**" was sent to the C2 server in four requests.

Saitama sample

e0872958b8d3824089e5e1cfab03d9d98d22b9bcb294463818d721380075a52d

References

<https://attack.mitre.org/techniques/T1071/004>

<https://blog.malwarebytes.com/threat-intelligence/2022/05/how-the-saitama-backdoor-uses-dns-tunnelling/>

<https://blog.malwarebytes.com/threat-intelligence/2022/05/apt34-targets-jordan-government-using-new-saitama-backdoor/>

--

Renato Marinho

[Morphus Labs](#) | [LinkedIn](#) | [Twitter](#)

Source: <https://isc.sans.edu/diary/Translating+Saitama%27s+DNS+tunneling+messages/28738>