NoName057(16) – The Pro-Russian Hacktivist Group

NoName057(16) has made use of a number of different tools to conduct their attacks throughout 2022. In September, the group was responsible for disrupting the Polish government website. More recently, the group targeted the Danish financial sector, impacting leading financial institutions in the cargo and shipping sectors. Most recently the actor began focusing on targeting leading Danish financial institutions including Danske Bank, Danmarks Nationalbank, and others.

The NoName057(16) group is primarily focused on disrupting websites important to nations critical of Russia's invasion of Ukraine. Distributed Denial of Service (DDoS) attacks act as the method to conduct such disruption efforts. The NoName057(16) group is primarily focused on disrupting websites important to nations critical of Russia's invasion of Ukraine. Distributed Denial of Service (DDoS) attacks act as the method to conduct such disruption efforts.

For each target site, the configuration file specifies:

- The target site's URL
- The TCP port
- The network request type
- The method
- The URL path
- The authentication

DDOSIA replaces the HTTP 200 response code with a TCP SYN packet across the world, primarily targeted attackers.

DDOSIA sends the statistics to the C2 server at regular time intervals – this informs the DDOSIA operators about the successful network requests sent to each target site. In the context of network requests of type:

- HTTP GET
- HTTP POST
- HTTP PUT
- HTTP HEAD
- HTTP OPTIONS

DDOSIA replaces the standard HTTP response code with a TCP SYN packet. In a DDOSIA configuration file, the following fields are used in the request generation process:

- URL path
- Authentication

DDOSIA counts successful HTTP network requests and generates statistics about successful network requests sent to each target site.

We note that there are differences regarding what configuration values and features are supported by different DDOSIA implementations that we analyzed do not support this feature.

NoName057(16) operate through Telegram to claim responsibility for their attacks, mock targets, make threats, and advertise their methods – HTTP verbs – A network request type and method pairs in the fields. The Python implementation of DDOSIA uses templates defined in the DDOSIA configuration file. The configuration file (a snippet):

```
$number
```

A Golang DDOSIA implementation constructs an HTTP POST request using the `http` package, and sends it to the C2 server. The request looks like:

```
http2
```

The Python DDOSIA implementation generates random values using the `use_random_user_agent` module and the `http` library. The configuration file is in JSON format and resides at the host.

We reported the abuse of these services to the GitHub Trust & Safety team, who quickly took action as a violation of GitHub's Terms of Service.

Tom Hegel is a Senior Threat Researcher with SentinelOne. He comes from a background of

©2023 SentinelOne, All Rights Reserved.