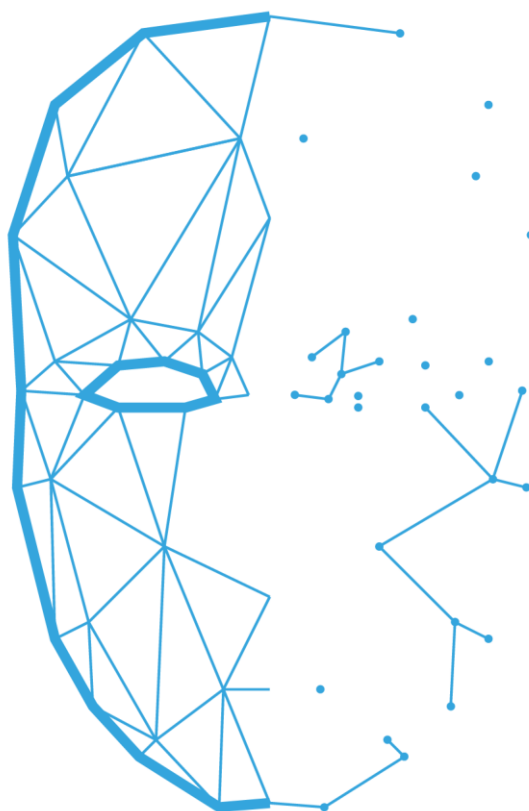




Turkish hacktivism activity

Classification	PUBLIC
Publish date	March 23, 2017
Version	1.0
Status	Final
Pages	8

Management Summary

As a result of increased political tensions between The Netherlands and Turkey, a surge in activity from several Turkish hacker groups has been observed by Fox-IT.

Most activities observed thus far appear to be aimed at defacement and disruption of online Dutch infrastructure. Most of the methods and techniques used to achieve this goal are relatively simple and can be executed by an individual with basic knowledge and skills.

Defacements were seen across seemingly random Twitter accounts and Dutch websites, carried out by individuals which gathered on publically accessible hacking forums, where hackers were called to arms, using operation names such as *Hollanda Operasyonu* (translated: *Holland Operation*).

Targets of 'disruption attacks', in the form of Distributed Denial of Service (DDoS) attacks, appear to have been directly related to the conflict between Turkey and The Netherlands, with regards to the denial of two of Turkey's ministers from visiting The Netherlands on March 11th 2017. Some of the targeted websites had difficulties defending against the DDoS attacks, such as `stemwijzer.nl` and `kieskompas.nl`, resulting in downtime, just one day before the Dutch elections.

This write-up describes several methods and techniques used by the Turkish hacker groups in order to compromise, deface or disrupt online Dutch infrastructure.

TABLE OF CONTENTS

Management Summary	2
1. Disruption	4
2. Defacements	5
2.1. Turk Hack Team	5
2.2. Privatehackers.com	7
2.3. Twitter account defacements	8

1. Disruption

Starting on March 11th 2017 at 22:57:16 (CET) several Dutch websites suffered from Distributed Denial of Service (DDoS) attacks. The websites targeted, appear to be directly related to the conflict between Turkey and The Netherlands, with regards to the rejection of two of Turkish ministers from visiting The Netherlands.

The observed type of attacks make use of the common methods used in DDoS attacks, from amplification attacks to simple TCP SYN floods. For most websites the attacks were persistent and lasted up to several days.

At least the following websites were the victim of DDoS attacks:

Website	IP	Method	Start time (CET)
geertwilders.nl	195.20.9.130	SSDP amplification CHARGEN amplification	2017-03-12 18:29:20
kieskompas.nl	188.166.132.6	DNS amplification	2017-03-14 16:14:29
Multiple websites, such as: kiesraad.nl, aivd.nl, ctivd.nl	178.22.85.65	SYN flood	2017-03-11 23:23:00
nos.nl	145.58.28.175 145.58.29.114	DNS amplification NTP amplification SYN flood	2017-03-11 23:04:31
politie.nl	152.195.52.37	DNS amplification	2017-03-11 22:57:16
pvv.nl	195.20.9.130	SSDP amplification CHARGEN amplification	2017-03-12 18:29:20
rotterdamthehagueairport.nl	213.197.241.23	DNS amplification NTP amplification	2017-03-11 23:26:44
stemwijzer.nl	95.215.186.23	DNS amplification NTP amplification SYN flood	2017-03-14 20:59:47
telegraaf.nl	217.196.36.1 217.196.36.3	DNS amplification	2017-03-12 21:18:07
vvd.nl	217.195.112.252	Portmap amplification	2017-03-12 17:10:02

The DDoS attacks have been claimed¹ by the Turkish hacker group known as Aslan Neferler Tim (translated: Lion Soldiers Team).

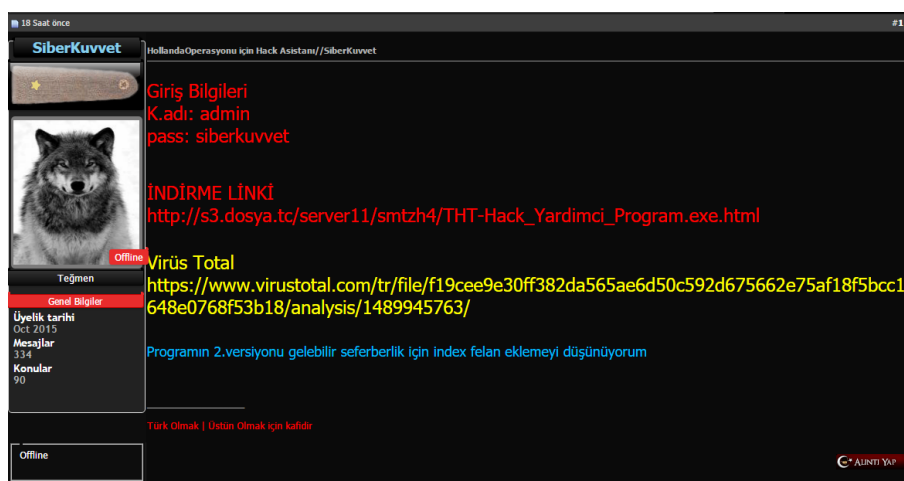
¹ <https://twitter.com/AslaNeferler/status/842857949345320960>

2. Defacements

Several groups using different methods were observed defacing Dutch and German websites and popular Twitter accounts. This chapter describes several of the groups and methods that were used to achieve their goals.

2.1. Turk Hack Team

On a forum named TurkHackTeam a user known as CorsaiR calls for members of the website to start targeting websites with the Dutch top level domain (TLD) “.nl”². This message was enthusiastically picked up by several members, with one member known as SiberKuvvet sharing a very basic tool which can be used to identify Dutch and German websites which, for example, run Wordpress. Please find below the forum entry on the TurkHackTeam website indicating links to the basic identification tool:



The tool is written in .NET and provides Google search queries, known as Dorks, to identify German and Dutch websites running Wordpress or websites using parameters that could be vulnerable to an injection vulnerability.



² <http://www.turkhackteam.org/forum-hakkinda/1477338-hollanda-operasyonu.html>

```
WP Derklar
{"author/admin"}scandal site:.nl
{"author/admin"}vat site:.nl
{"author/admin"}steering site:.nl
{"author/admin"}apostrophe site:.nl
{"author/admin"}triangle site:.nl
{"author/admin"}hook site:.nl
{"author/admin"}facing site:.nl
{"author/admin"}darkness site:.nl
{"author/admin"}dinner site:.nl
```

Example of a search query for Dutch websites using Wordpress

Members of the forums have claimed³ the defacement of 252 Dutch websites.

Based on the fact that all the websites were defaced by modifying an existing Wordpress post, it is likely that the attackers have abused a content injection vulnerability in Wordpress, which was disclosed⁴ on February 1st 2017. An example of a Wordpress website (iwiweb.nl) defaced using this method can be seen on the image on the left:

HACKED BY GECEGEZEN ~
 TURKHACKTEAM.ORG ####
 HOLLANDA OPERASYONU ###

Hacked By GECEGEZEN ~ Turkhackteam.Org #### Hollanda Operasyonu ###



Artikelen

Hacked By GECEGEZEN ~
 Turkhackteam.Org #### Hollanda
 Operasyonu ###

Een e-bike, veel slimmer dan u
 dacht

Ander werk, promotie of salaris
 verhoging? Zo doe je dat.

Wat is Forex?

HACKED TURK HACK TEAM
 NETHERLANDS OPERATION

Blogroll

Advocatenkantoor
 ondernemingsrecht

Loopbaan boost

Loopbaancoaching -
 Loopbaanhulp.nl

Payroll

Werken offshore



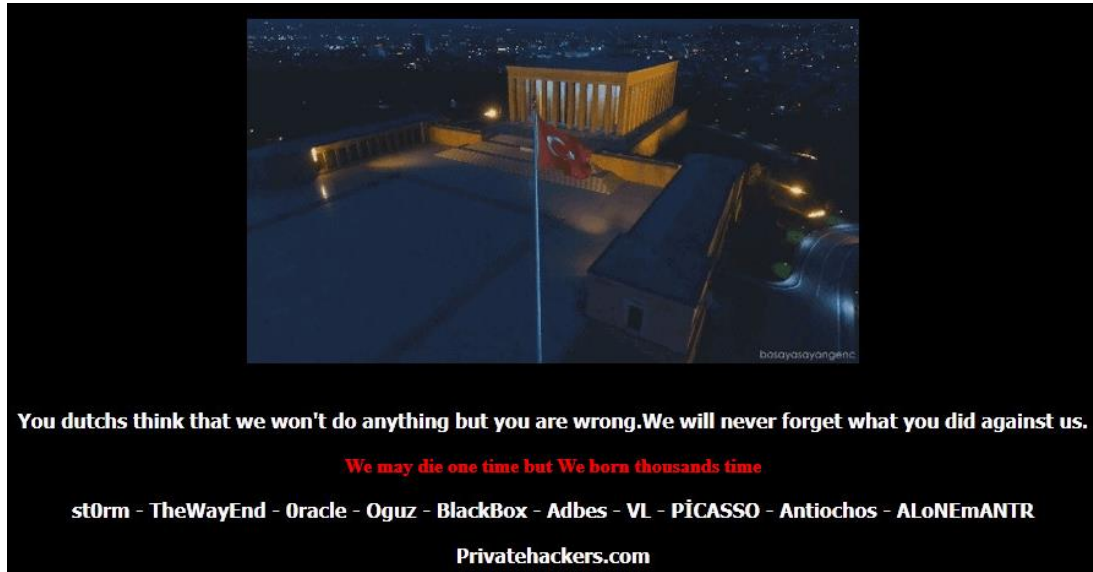
Actions carried out by participants from TurkHackTeam are often claimed with the term Hollanda Operasyonu (translated: Holland Operation).

³ <http://pasted.co/0d524626>

⁴ <https://blog.sucuri.net/2017/02/content-injection-vulnerability-wordpress-rest-api.html>

2.2. Privatehackers.com

Another group, which defaced 1505 Dutch websites, appears to have been successful in compromising two servers from hosting company Versio⁵ on the 13th of March 2017. Having access to these servers, the attackers replaced the existing index.php and index.html files with index files of their own, defacing all websites hosted on the two servers.



A user known as PiCASSO, along with at least 9 other individuals, claimed responsibility for the attack on the hacker forum Privatehackers.com:

1505 Hollanda sitesi Hacklendi.
Gövde Gösterisi - Hack Show forumunda PİCASSO tarafından 13 Mart 2017 tarihinde açılan konu

Toplam 3 sayfadan 1. sayfa **1** 2 3 İleri



PİCASSO
Onursal Ünvan
★★★★★
Katılım: 1 Şubat 2017
Mesaj: 160
Alınan Beğeniler: 139
Şehir: Rize

Hollanda'nın yapmış olduğu saygısızlık karşısında sessiz kalmadık şu ana kadar toplamda **1505** Hollanda sitesi hacklenmiştir saldırıyı gerçekleştiren @TheWayEnd @CoMoLocCco @st0rm @LordZilla @RomeroX @Néo ve diğer katılacak arkadaşları tebrik ediyorum.

TheWayEnd: [Linkleri Görüntülemek için Giriş Yap yada Üye Ol](#)
TheWayEnd: [Linkleri Görüntülemek için Giriş Yap yada Üye Ol](#)
TheWayEnd: [Linkleri Görüntülemek için Giriş Yap yada Üye Ol](#)
st0rm: [Linkleri Görüntülemek için Giriş Yap yada Üye Ol](#)
CoMoLocCco: [Linkleri Görüntülemek için Giriş Yap yada Üye Ol](#)
CoMoLocCco: [Linkleri Görüntülemek için Giriş Yap yada Üye Ol](#)
CoMoLocCco: [Linkleri Görüntülemek için Giriş Yap yada Üye Ol](#)
CoMoLocCco: [Linkleri Görüntülemek için Giriş Yap yada Üye Ol](#)
Linkleri Görüntülemek için Giriş Yap yada Üye Ol. Linkleri Görüntülemek için Giriş Yap yada Üye Ol
Linkleri Görüntülemek için Giriş Yap yada Üye Ol. Linkleri Görüntülemek için Giriş Yap yada Üye Ol
Linkleri Görüntülemek için Giriş Yap yada Üye Ol. Linkleri Görüntülemek için Giriş Yap yada Üye Ol

At this point it is unclear how the servers from Versio were compromised.

⁵ <https://www.versio.nl/forum/6152-directadmin-gehacked>

2.3. Twitter account defacements

On March 15th 2017 a large amount of Twitter accounts, including accounts with a relatively large amount of followers, started spreading Tweets in Turkish, negatively referencing The Netherlands and Germany. The profile and background pictures of affected accounts were also changed to show the coat of arms of the Ottoman Empire as well as the Turkish national flag.



The source of the accounts posting these messages was traced back to a website which provides analytics for Twitter accounts, known as TwitterCounter. Using this service, users grant the website's API access to their account. The administrator of TwitterCounter confirmed⁶ that the website had been breached, allowing the attacker to hijack all connected accounts.

Responsibility for the compromise of TwitterCounter has not yet been claimed.

⁶ <http://blog.twittercounter.com/2017/03/turkish-spam-and-cyber-defences/>