

Doppelganger Domains

September 6, 2011

Summary

Domain typo-squatting is commonly used to spread malware to users whom accidentally misspell a legitimate domain in their web browser.¹ A new type of domain typo-squatting takes advantage of an omission instead of a misspelling. A Doppelganger Domain is a domain spelled identical to a legitimate fully qualified domain name (FQDN) but missing the dot between host/subdomain and domain, to be used for malicious purposes. Doppelganger Domains have a potent impact via email as attackers could gather information such as trade secrets, user names and passwords, and other employee information.

Each company in the Fortune 500 was profiled for susceptibility to Doppelganger Domains and 151 companies (or 30%) were found to be susceptible. In large corporations, email usage is extremely high which dramatically increases the likelihood of mis-sent emails and data leakage.

Email Based Attack Vectors

There are two types of email based attacks that are possible with a Doppelganger Domain.

The first attack vector is completely passive. Once the attacker purchases the Doppelganger Domain, they will configure an email server to receive all email addressed to that domain, regardless of the user it was destined to. This type of configuration is also known as a catch-all email account. As email is a high-volume, primary communication mechanism for many corporations, a small percentage of those emails will be sent to the wrong destination because of user error (a typo by the email's sender). The attacker relies on this fact and will start collecting emails from both internal and external users.

The second attack vector involves social engineering and is likely to be only used on specific individuals. As a Doppelganger Domain can be very similar to the legitimate email domain, an attacker will impersonate a person and attempt to obtain sensitive information via social engineering.

¹ <http://en.wikipedia.org/wiki/Typosquatting>

Passive Email Attack

During a six-month span, over 120,000 individual emails (or 20 gigabytes of data) were collected which included trade secrets, business invoices, employee PII, network diagrams, usernames and passwords, etc. Essentially, a simple mistype of the destination domain could send anything that is sent over email to an unintended destination.

Keyword	Count
Investigation	350
Secret	425
Unclassified	106
Credit Card	402
Private	394
UserID	225
Password	405
Login	495
Confidentiality	374
VPN	75
Router	163
Contract	417
Affidavits	34
Invoice	323
Resume	275

Figure 1. List of how many emails contained interesting keywords.

Active Email Attack

The term Man-in-the-MailBox has been used to describe the exploiting of the natural trust and relation between trusted people or organizations.² Leveraging Doppelganger Domains, an attacker could take it one step further by creating a full man-in-the-middle scenario. Figure 2

² <http://www.nytimes.com/2010/02/19/technology/19china.html>

below describes an example scenario between two factitious domains, us.company.com and ru.bank.com.

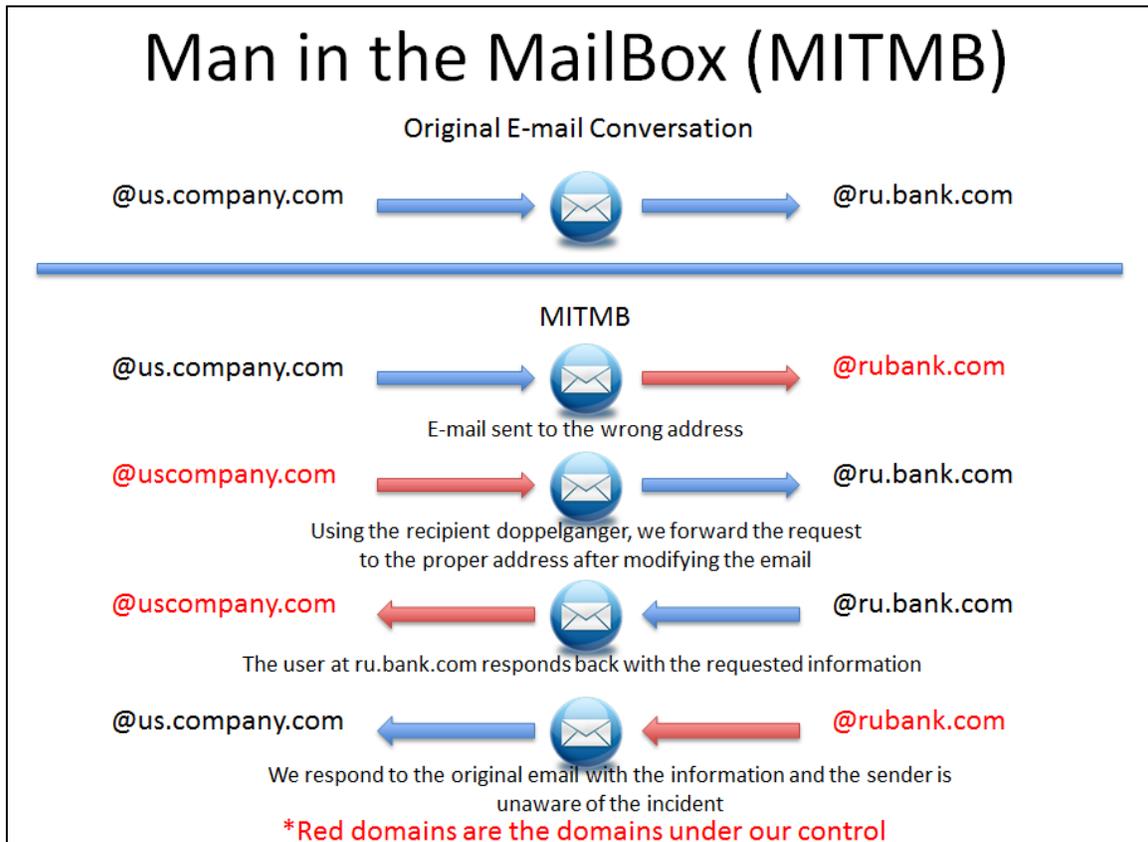


Figure 2: Man in the MailBox example scenario.

An attacker, if available, could purchase both uscompany.com and rubank.com allowing him to capture the mistyped email domains. When an email is mis-sent from us.company.com to rubank.com, the email arrives instead in the attacker's mailbox. The attacker creates a script to auto-forward those emails from his uscompany.com address to the legitimate ru.bank.com address.

Most likely, the recipient at the ru.bank.com address will be unaware that the email sourced from a Doppelganger Domain. The ru.bank.com user will then reply to the Doppelganger Domain email address, with the pertinent information we requested. As seen in Figure 2, the ru.bank.com user replies to the wrong email address, instead sending it to the uscompany.com address. When that response comes in to the attacker's uscompany.com mailserver, the attacker again creates a script to auto-forward that email out of our rubank.com email address to the valid us.company.com.

If both parties are unaware of the mistyped address, the attacker now has a full Man-in-the-MailBox scenario.

Other Network Based Attack Vectors

While our focus of research was on email attack vectors, we noticed other network services being requested from external and internal users during the six-month span.

The hit rate for administration ports such as 22 (SSH) and 3389 (RDP) was much lower than email, but an attacker could setup a fake server and harvest usernames and passwords.

Vulnerability Prevalence

Each company in the Fortune 500 was profiled for susceptibility to Doppelganger Domains and 151 companies (or 30%) were found to be susceptible. Figure 3 below shows the number of companies susceptible to Doppelganger Domains by industry.

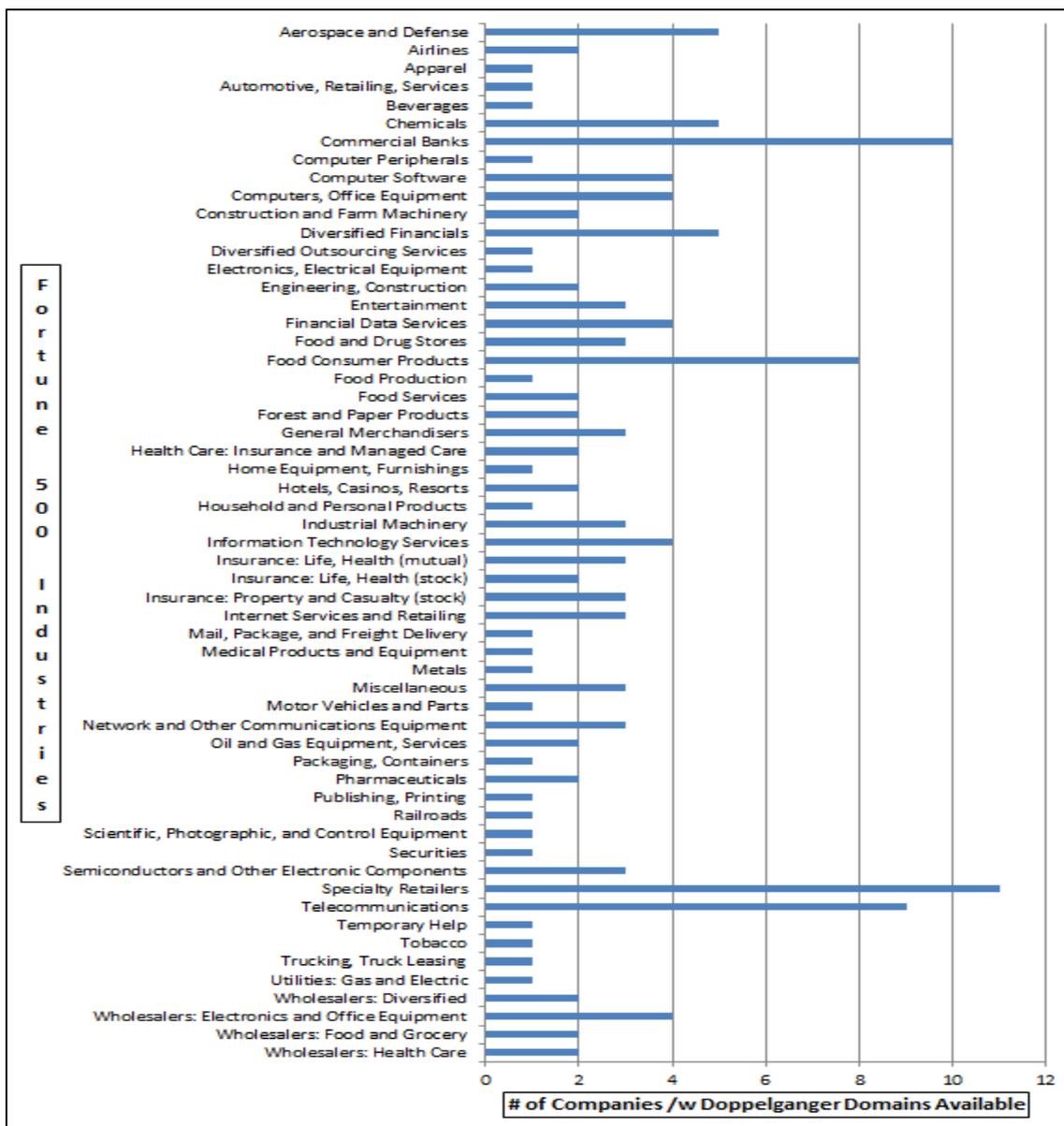


Figure 3. Number of companies /w Doppelganger Domains available by Industry.

Exploitation in the Wild?

After reviewing the WHOIS information from all Fortune 500 companies, we noticed some of the largest companies were already registered to locations in China and to domains associated with malware and phishing.³

While it is unknown if these domains are used in a malicious fashion, it is apparent that some targeting is happening here. If in six months we were able to collect 20 gigabytes of data, imagine what a malicious attacker could gain.

Target Company	Doppelganger Domain	Domain Registrant Email
adp.com	cnadp.com	adp@vip.163.com
cisco.com	kscisco.com	domainadm@hichina.com
dell.com	chndell.com	gdguy@163.com
dupont.com	sydupont.com	syxxhw@163.com
gm.com	ucgm.com	zydoor@126.com
hp.com	chehp.com	59031894@qq.com
ibm.com	caibm.com	604732486@qq.com
ibm.com	seibm.com	fjjclaw@263.net
intel.com	ausintel.com	nheras@gmail.com
itt.com	cnitt.com	dulingqun@sina.com
kohls.com	emailkohls.com	bridgeportltd@gmail.com
manpower.com	demanpower.com	tzstudent@163.com
mcd.com	cnmcd.com	617388068@qq.com
yahoo.com	nayahoo.com	xxxxxx_vip@yahoo.com.cn
unisys.com	caunisys.com	domainadm@hichina.com

Table 3. Example Doppelganger Domains owned by Chinese companies.

³ <http://www.malwareurl.com/listing.php?as=AS21327&active=off>

Mitigation Strategies

There are several methods of defending against Doppelganger Domains and the two email-based attacks that stem from them.

- Purchase and register the Doppelganger Domains. On the external DNS, configure those domains to not resolve anywhere so that the sender would receive a bounced email notification.
- Identify if attackers are already using a Doppelganger Domain against your company, and file a Uniform Domain Dispute Resolution Policy (UDRP) if they are.
- Internally configure the DNS to not resolve any Doppelganger Domains, even if your company does not own them. This will protect internal only email from being accidentally sent to a Doppelganger Domain.
- An alternative to configuring the internal DNS for Doppelganger Domains is to configure the mail server to not allow any outbound email destinations to Doppelganger Domains.
- Communicate the attack vector to your internal users, customers, and business partners. The more awareness they have on social engineering attacks, the less susceptible they will be.

Detection

Godai Group can scan your domain free of cost to determine if it is susceptible to Doppelganger Domains. For more information, visit <http://godaigroup.net/free-doppelganger-domain-scan/>

Authors

- Garrett Gee
- Peter Kim

About Godai Group

Godai Group is a professional services firm passionate about information security. Our area of focus is researching new threats, developing new tools, and providing services to ultimately make networked environments more secure. For more information, visit <http://godaigroup.net>

Copyright © 2011 Godai Group LLC. All rights reserved.