Severity:
High

CTM360®
Powered by EDX LABS
Subsidiaries: PENTEST360 | DMARC360 | MG360

MISLEADING "COM-" DOMAIN REGISTRATIONS

By Team CTM360

Reference: CTM-ADV-0517-02
Date: Date: 24TH May 2017
Category: Domain Spoofing

THREAT TARGETS:	POSSIBLE IMPACTS:	TARGET AUDIENCE FOR CIRCULATION:
• All sectors	• Financial, Reputational, Data Loss	• Executive Management • IT Department

Threat Description

URL obfuscation has long been a tactic of cybercriminals in their attempt to trick their potential victims. Yet again, another obfuscation technique has been observed by Team CTM360 to be on the rise – domain names being registered starting with "com-", due to the ease of setting up a subdomain. An example of this would be **"facebook.com- newstrending.co",** where the domain name is in fact **"com-newstrending.co".**

Normally, such websites imitate the design of a legitimate URL and alter it by adding special characters and/or misspelled words making it closely resemble the original website. Preliminary analysis has revealed that approximately 68,000 domains have been registered matching this pattern. Domains beginning with 'com-' were mostly found to be either phishing websites, fake news websites, or were being used to send out spoofed emails.

Following are some examples of websites detected by Team CTM360 which were found to be hosting fake news starting with 'com-

be hosting fake news starting with 'com- ':

http://businessinsider.com-newsbulletin.co/ananda-malaysia- businessinsider.html

http://businessinsider.com-newsbulletin.co/generic-qatar-businessinsider.html

http://businessinsider.com-newsbulletin.co/generic-uae-businessinsider.html

http://businessinsider.com-newsbulletin.co/wassim-qatar-businessinsider.html

http://facebook.com-newsbulletin.co/ananda-malayasia-facebook.html

http://facebook.com-newsbulletin.co/ananda-malaysia-facebook.html

http://facebook.com-newsbulletin.co/wassim-qatar-facebook.html

http://businessinsider.com-digitalmedia.com/alwaweed-saudi-businessinsider.html

http://businessinsider.com-digitalmedia.com/ananda-malaysia-businessinsider.html

http://businessinsider.com-digitalmedia.com/generic-uae-businessinsider.html

http://facebook.com-digitalmedia.com/wassim-qatar-facebook.html

http://facebook.com-digitalmedia.com/wissam-qatar-facebook.html

http://businessinsider.com-digitaldigest.co/alwaweed-saudi-businessinsider.html

http://facebook.com-digitaldigest.co/ananda-malayasia-facebook.html

Sample domains starting with 'com-'

com-article2.info
com-update-info.com
com-intl-service.info
com-recovery-i.cloud
com-reservations98412.info
com-getcoupon.us
com-mediastorage095.us
com-rate.info
com-winner12.net
com-freegiftcoupon.us
com-freeticket.us
com-iphone-locate.com
com-2freecuponfor.us
com-appleid-locate.com
com-freegifts.us
com-offer.world
com-websappsignin.info
com-avignon.com
com-chamonix-mont-blanc.com
com-couponsfreefor.us
com-activation-accounts.info
com-read.top
com-report.men
com-signin.email
com-winner10.info
com--news.com
com-accessecure.com
com-secureinformations.com
com-verifyissues.com
com-accountsuser.info
com-i.social
com-secureinformation.biz
com-service-lnc.site
com-shopping.info
com-findiphone.link
com-icloudlost.info
com-msoft302.info

Recommended Preventative Measures

- Quarantine emails from domains that begin with 'com-' in your email gateway
- Define firewall rules to detect and block access to websites that have domain names beginning with 'com-'

References:

http://www.phishing.org/phishing-and-spoofing
http://www.articsoftpgp.com/web_spoofing.htm

For more information:
Email: monitor@ctm360.com | Tel: (+973) 77 360 360

Follow us: