Vulnerability Report Confirmation - [VRF#HYIXW4Z4]

Your vulnerability report has been successfully received. You may save or print this page for your own records. The Report Tracking ID assigned to this report is VRF#HYIXW4Z4. Details of your report are listed below.

If you have any questions or require additional information, please call the CERT Hotline at +1 412-268-7090 or send email to cert@cert.org. Please reference this Report Tracking ID: VRF#HYIXW4Z4.

Do not use the back button to submit another report. Click here instead.

Vulnerability Report

Name	George Kirikos
Organization	Leap of Faith Financial Services Inc.
Email Address	ceo@leap.com
Telephone Number	416-588-0269
Vulnerability Description	I'm not 100% sure, but I believe that there *may* be a vulnerability in association with typos of the .mil (US Military) top-level domain name that might be actively exploited, particularly in association with the .ml (Mali) top-level domain name. In particular, by registering similar domain names in .ML and activating the mail records ("MX records"), an attacker could read emails that are intended for someone in the .MIL namespace. Given the sensitivity of .MIL for military use, an attacker could be reading all emails that are misdirected to the .ML domain name, instead of the .MIL domain name. This is particularly the case if the attacker sets up a "Catch All" email address. Since typos are very common (especially for mobile users inputting an address on a cell phone or tablet), an attacker can quietly intercept sensitive communications that were sent to an incorrect email address (on an unintended basis). I believe someone had done a research paper examining typos of corporate domain names, and the researchers were able to suck up 20 GB of corporate emails in only 6 months: http://www.cnn.com/2011/TECH/web/09/09/email.typos.stolen.data.wired/ These typos of the .mil domain name might have been going on for much longer. (see below)
Can we provide your name to the	Yes

vendor?	
Do you want to be publicly acknowledged?	Yes
Vendor Contact Status	will not contact
Vendor Name	
Vendor Contact Name	
Vendor Contact Email	
Vendor Contact Telephone Number	
Vendor Tracking ID	
Additional Vendor Information	I have not contacted anyone else within the US government or military regarding the above vulnerability, as the CERT system was listed on the DHS website: http://www.dhs.gov/report-incidents as the appropriate contact for cybersecurity activity. I'd appreciate an acknowledgement that this incident report was received, as I'm not sure whether I should report it to someone else if I don't hear back from you.
Affected System Configurations	Any system/user that sends email. Even encrypted mail is vulnerable, since encryption can be broken. An even more sophisticated attacker could start "conversations" with the person who sent the email to the wrong address, masquerading as the true intended recipient to gather even more information (until they're found out).

See below.

My company owns a number of elite websites and domain names (e.g. math.com, school.com, depot.com, leap.com, seeds.com, options.com, etc.), so I'm often researching and analyzing domain name issues. ICANN (the non-profit that manages global domain name policies) launched a process to increase the number of top-level domain names as alternatives to dot-com (e.g. new extensions like .guru or .club) a couple of years ago, and those new domain extensions have been launching over the past 6 months.

I read a story today that the City of Montreal might apply for the .MTL top-level domain name. I thought to myself that this might be confusingly similar to .MIL (the US military top-level domain), and it prompted me to check the IANA database of all existing top-level domains to see whether there were any TLDs that are already similar to .MIL. The existing .ML top-level domain name (for the country of Mali) stood out on the list:

https://www.iana.org/domains/root/db

Using Google to identify them, I manually checked some of the top .MIL domain names, to see whether anyone might have registered the matching .ML domain names. For example, nationalguard.mil is an active domain name.

Using the "WHOIS" tool at:

http://www.point.ml/en/whois.html

it displays full WHOIS information for some domain names (e.g. Google.ml shows the full public info for Google). However, for nationalguard.ml, the domain name *is* registered and paid for, but the WHOIS information is missing. Digging further, to check the email DNS Records, using the:

dig nationalguard.ml mx

command, it shows that the MX records *do* exist for that domain name, and that inbound email is being routed to the HANDLE.CATCHEMAIL.ml server. The person who registered the nationalguard.ml domain *doesn't* have active "A" records (often used for websites, etc.) for nationalguard.ml or www.nationalguard.ml, which might suggest to others that the domain name itself is inactive (which is not the case, since the MX records for inbound email *are* active).

If we examine where HANDLE.CATCHEMAIL.ml goes, by using another "dig" command, we see that it goes to 2 servers, namely:

dig handle.catchemail.ml

;; ANSWER SECTION:
handle.catchemail.ml. 1800 IN A 69.160.33.74
handle.catchemail.ml. 1800 IN A 38.101.213.200

How was this vulnerability found?

Thus, the inbound emails are being routed to:

69.160.33.74
38.101.213.200

Using DomainTools.com, we can lookup what network those IP addresses belong to:

https://whois.domaintools.com/69.160.33.74
https://whois.domaintools.com/38.101.213.200

and, scrolling to the bottom of those pages, one can see that the emails are being delivered to servers within the NameCheap.com network. NameCheap.com is a domain name registrar and hosting company, so conceivably one of their retail customers is receiving all the emails.

Note that the WHOIS for the catchemail.ml domain name is similarly not shown in the .ML WHOIS system (but is an active and paid account).

Other .mil domain names that I checked where the matching .ML (Mali) domain name has the

MX records activated and routed to handle.catchemail.ml include:

navy.ml
health.ml
transcom.ml
marines.ml
northcom.ml
army.ml
af.ml (i.e. matching the Air Force af.mil domain)
militaryonesource.ml
jcs.ml
disa.ml
stratcom.ml
eucom.ml
vaccines.ml
osd.ml
dia.ml
southcom.ml
dtic.ml
dsca.ml
darpa.ml

I've not checked every .MIL domain name, but the above is a good start, and shows that something unusual might be happening (i.e. actively in progress).

I also sent a test email to webmaster@navy.ml, to see whether the system would "bounce" the email as undeliverable. It didn't bounce (test email sent 1 hour ago).

Conceivably an authorized military contractor is "catching" these emails intentionally, given that the vulnerability might have been foreseen by the military. However, the fact that the IP address of the servers that are receiving the email are not located within US government IP address space might lead one to believe that this interception of email might be an active attack.

Is the vulnerability being exploited?	Yes
Is there a public exploit?	No
Vulnerability Impact	See above. In particular, an attacker can gather intelligence via emails that have been misdirected. The amount of information can be significant (i.e. see the article above re: 20 GB of corporate emails stolen over a 6 month period). Given the sensitivity of military data, and military personnel's emails, and the fact that this "attack" might have been taking place for a longer period, the impact can obviously be much bigger than one aimed at corporations.

I'd be glad to provide further assistance and analysis if it would help the Department of Homeland Security and/or the US military. My expertise is in domain names as I mentioned above.

My cell phone number is _____ (although the landline number of 416-588-0269 is a better first choice).

Comments	I've only spent about 1 hour delving into the issues above, but thought it was potentially serious enough to bring to your attention. Obviously CERT and the DHS have more advanced tools and resources available to investigate further, should it warrant an investigation. If I spent more time, I could probably help to determine the extent of the problem (if it's a real attack, as it's not 100% clear who is receiving the emails at this time and whether that entity is malicious), and appropriate responses or next steps.
Attached File	
Date	2014-08-06T13:38:26
Report Tracking ID	VRF#HYIXW4Z4
CERT Tracking IDs	