George Kirikos <ceo@leap.com>

Is it ok to blog about this CERT issue? (was Re: VU#928700 - .mil vulnerability)

1 message

George Kirikos <ceo@leap.com> Thu, Sep 18, 2014 at 4:44 AM
To: soc@us-cert.gov

Hello,

I submitted a report to CERT (VU#928700) more than a month ago about an entity that is typosquatting a large number of US Military domain names (via mass registrations of corresponding Mali .ml top-level domain names, which is a typo of the .mil US military top-level domain). As I've pointed out, unlike most typosquatters, this one is unusual because:

1. the target -- it's the US military
2. breadth -- they're targeting a large number of .mil domains, via registration of the .ml (Mali) counterparts, and
3. apparent non-commercial focus -- instead of trying to monetize the typos via pay-per-click, etc., they're instead playing a "long game", quietly harvesting large amounts of email, and not activating any website. As I pointed in the initial report, that amount of email can be significant (researchers were able to gather 20 Gigabytes of email in 6 months targeting typos of Fortune 500 companies, e.g. see http://www.cnn.com/2011/TECH/web/09/09/email.typos.stolen.data.wired/).

Anyhow, I thought it would be appropriate to report this, lest some malevolent entity with interests counter to those of the US military was behind this (e.g. a foreign government, foreign intelligence agency, terrorists, etc.)...i.e. someone who doesn't care about short-term "profit" in terms of parking the domains with ads, but instead wants to gather up lots of misdirected US military email messages, to gather intelligence.

I wanted to eventually blog about this to raise awareness, since the same kind of attack can target companies (as per that CNN article). However, since I believe in "responsible disclosure", I thought it wise to make sure that by blogging on this I wasn't interfering with any official investigation that might be taking place (i.e. the "attacker", if this is truly an attack -- it's certainly unusual and suspicious given the above), since whoever is doing this might cover their tracks if they know that others are aware of their behaviour.

Thus, it was suggested I write to you, to check if there's any concerns (i.e. whether I should hold off on blogging for a reasonable amount of time, if the matter is being investigated), or if instead it's ok to blog about this matter (the emails exchanges with CERT are below).

Sincerely,

George

George Kirikos
CEO

Leap of Faith Financial Services Inc.
34 Burnfield Avenue, Toronto, Ontario M6G 1Y5 Canada
Tel: +1 (416) 588-0269 Fax: +1 (416) 588-5641
E-mail: ceo@leap.com Website: www.leap.com

This email and any attachments are for the sole use of the intended
recipients and may be privileged or confidential. Any distribution,
printing or other use by anyone else is prohibited. If you are not an
intended recipient, please contact the sender immediately, and
permanently delete this email and attachments.

To stop receiving commercial electronic messages, visit http://optout.loffs.com/

On Thu, Sep 18, 2014 at 4:22 AM, George Kirikos <ceo@leap.com> wrote:
> Hello,
>
> Thanks for your email. Yes, that's exactly what the issue is, namely
> typosquatting in order to harvest the misdirected email messages. It's
> not a "buffer overflow" or something that's more easily
> fixable....it's a different type of "attack."
>
> In this case, I thought perhaps the US military might want a "heads
> up", because obviously the attacker isn't doing the "usual" kind of
> thing, namely putting up parked pages, or making phishing attacks in
> order to make quick case. They're playing the "long game", just
> quietly harvesting US MILITARY emails -- and, as per that CNN article
> I mentioned in the initial report:
>
> http://www.cnn.com/2011/TECH/web/09/09/email.typos.stolen.data.wired/
>
> there can be quite a lot of data (those researchers were able to get
> 20 Gigabytes of emails in just 6 months.
>
> Not many people would have the resources or the patience to be
> targeting a large number of typos of US military domains, all with
> hidden WHOIS, and for an obscure country-code domain like .ml (Mali).
> If it turns out the 'attacker' has interests that are counter to US
> interests, isn't that something they should investigate or would wants
> to be aware of??
>
> Anyhow, I'll drop them a line, and see if they care about whether I
> blog about it.
>
> Sincerely,
>
> George
>
>
>
>
>
>
>
>
> ---

> George Kirikos
> CEO
>
> Leap of Faith Financial Services Inc.
> 34 Burnfield Avenue, Toronto, Ontario M6G 1Y5 Canada
> Tel: +1 (416) 588-0269 Fax: +1 (416) 588-5641
> E-mail: ceo@leap.com Website: www.leap.com
>
> This email and any attachments are for the sole use of the intended
> recipients and may be privileged or confidential. Any distribution,
> printing or other use by anyone else is prohibited. If you are not an
> intended recipient, please contact the sender immediately, and
> permanently delete this email and attachments.
>
> To stop receiving commercial electronic messages, visit http://optout.loffs.com/
>
>
> On Wed, Sep 17, 2014 at 1:24 PM, CERT(R) Coordination Center
> <cert@cert.org> wrote:
>> -----BEGIN PGP SIGNED MESSAGE-----
>> Hash: SHA1
>>
>> George,
>>
>> Try emailing them at soc@us-cert.gov and see if you get a response.
>>
>> Otherwise, this sort of typosquatting is fairly well known, http://en.wikipedia.org/wiki/Typosquatting . We generally handle responsible
>> disclosure for vulnerabilities, and this particular issue is not a vulnerability as we define it. If you feel that this needs to be disclosed,
>> we usually recommend that you speak to the affected party first (which you've done).
>>
>> Regards,
>>
>> - ---
>> Vulnerability Analysis Team
>> ==
>> CERT(R) Coordination Center | cert@cert.org
>> Software Engineering Institute | Hotline : +1 412.268.7090
>> Carnegie Mellon University | FAX : +1 412.268.6989
>> Pittsburgh, PA 15213-3890 | http://www.cert.org/
>> ==
>>
>>
>> George Kirikos <ceo@leap.com> writes:
>>>Hi again,
>>>
>>>I still never heard back from anyone at US-CERT. Perhaps they're not
>>>investigating? Or they've completed their work?? Or they've determined
>>>it's not an issue? With silence, I don't know what to think.
>>>
>>>Since my initial report, it seems that whoever is operating the
>>>handle.catchemail.ml inbound email servers (which is still associated
>>>with the MX records of the .ml (Mali) domains that correspond to the
>>>various .mil (Military) domains) has changed the IP addresses of the
>>>server. As per my initial report, the email servers were at
>>>69.160.33.74 and 38.101.213.200, which were both within the
>>>NameCheap.com network in the USA.
>>>
>>>But, as of today, if you do a "dig handle.catchemail.ml" to view the
>>>IP address, it's instead going to 46.137.119.181, which is hosted by

>>>Amazon AWS in Ireland:
>>>
>>>https://whois.domaintools.com/46.137.119.181
>>>
>>>according to DomainTools (i.e. outside the USA, and thus harder for
>>>security investigators to perhaps figure out what's going on!
>>>Although, Amazon is a US company, so they might cooperate, despite the
>>>server being outside of the USA) The TTL has also changed from 1800
>>>seconds to 300 seconds (although, that might not mean anything; there
>>>could be good or bad reasons for doing this; e.g. higher uptime for
>>>resiliency; or faster redirection to a new server in case an older
>>>server gets detected/compromised if there's an investigation, etc.)
>>>
>>>As I said before, I believe in responsible disclosure. This same kind
>>>of behaviour might be done to corporate users, by acquiring typos of
>>>their domain names, and quietly intercepting misdirected emails over a
>>>long period. As per the 2011 CNN article I mentioned in the initial
>>>report, researchers were able to suck up 20 Gigabytes of corporate
>>>emails in only 6 months.
>>>
>>>I imagine .mil has a huge amount of email daily, so just a tiny
>>>fraction of typos/misdirected emails could generate large volumes of
>>>potentially sensitive email, which might be of interest to foreign
>>>intelligence agencies, foreign companies, or others with malevolent
>>>intentions towards the US military. There was a news story just last
>>>week about fake cell phone towers near US military bases, e.g.
>>>
>>>http://blackbag.gawker.com/rogue-interceptor-cell-phone-towers-discovered-near-u-1630079351
>>>http://www.al.com/news/index.ssf/2014/09/who_is_listening_17_fake_cellp.html
>>>http://www.popsci.com/article/technology/mysterious-phony-cell-towers-could-be-intercepting-your-calls
>>>
>>>so, this technique of passive interception isn't just limited to
>>>email, obviously. (I have no special insights about the cell phone
>>>stuff, though)
>>>
>>>So, I'd like to be able to blog about this domain name issue, to raise
>>>awareness, so that security-conscious companies can take appropriate
>>>counter-measures. e.g. if I was running .mil mail servers, I would
>>>consider a blacklist of the entire .ml (Mali) ccTLD for all outgoing
>>>emails (with perhaps a "white-list" for appropriate addresses). If I
>>>was running a corporation on a .com domain name, I might implement a
>>>similar policy for .co (Colombia) and .cm (Cameroon) ccTLD to reduce
>>>the risk of misdirect emails being intercepted. There are other
>>>counter-measures one can take, beyond just these. Of course, such
>>>policies require that individuals in those organizations only send
>>>email through their organizational servers (e.g. if one made a typo
>>>and sent to a .ml or .co or .cm domain from Gmail or Hotmail,
>>>obviously it's not going to be caught by the organization's email
>>>blacklisting rules/policies).
>>>
>>>However, if I did blog about this, it might interfere with any
>>>investigation that US-CERT might be conducting, allowing the potential
>>>attacker (if there's an attack; as I made clear before, I'm not 100%
>>>sure, but I can see no good reason why all those .ml domains are being
>>>registered with hidden WHOIS, inactive websites, but active incoming
>>>email servers, all corresponding to .mil domains) to destroy evidence,
>>>cover their tracks, etc. Given that it involves .mil, I'm sensitive to
>>>the military aspect, that they might be a bit slower with their
>>>bureaucracy, etc.
>>>
>>>So, I'm put into an ethical dilemma. While I remain silent, more

>>>corporations remain vulnerable. However, if I blog, it might hamper an
>>>investigation over who is operating these .ml domains, and whether
>>>they are malevolent or not.
>>>
>>>Since I have no actual "official word" that anyone from US-CERT is
>>>even investigating the issue, or cares whether I blog about it or not,
>>>that inclines me towards blogging about it. But, I wanted to give yet
>>>another opportunity for someone to say "Hey, we think something's
>>>worth investigating, please give us more time to look into this. We'll
>>>need a reasonable amount of time....etc."
>>>
>>>I don't want to stay silent indefinitely, but it's been over a month
>>>already. If you have some guidance or advice on responsible disclosure
>>>for this particular incident, I'd appreciate it.
>>>
>>>Sincerely,
>>>
>>>George
>>>
>>>---
>>>George Kirikos
>>>CEO
>>>
>>>Leap of Faith Financial Services Inc.
>>>34 Burnfield Avenue, Toronto, Ontario M6G 1Y5 Canada
>>>Tel: +1 (416) 588-0269 Fax: +1 (416) 588-5641
>>>E-mail: ceo@leap.com Website: www.leap.com
>>>
>>>This email and any attachments are for the sole use of the intended
>>>recipients and may be privileged or confidential. Any distribution,
>>>printing or other use by anyone else is prohibited. If you are not an
>>>intended recipient, please contact the sender immediately, and
>>>permanently delete this email and attachments.
>>>
>>>To stop receiving commercial electronic messages, visit http://optout.loffs.com/
>>>
>>>
>>>On Wed, Sep 10, 2014 at 12:17 PM, CERT(R) Coordination Center
>>><cert@cert.org> wrote:
>>>> -----BEGIN PGP SIGNED MESSAGE-----
>>>> Hash: SHA1
>>>>
>>>> Hi George,
>>>>
>>>> I'll put you in touch with US-CERT shortly. I'm not sure why they didn't respond to you yet.
>>>>
>>>> Regards,
>>>>
>>>> - ---
>>>> Vulnerability Analysis Team
>>>> ==
>>>> CERT(R) Coordination Center | cert@cert.org
>>>> Software Engineering Institute | Hotline : +1 412.268.7090
>>>> Carnegie Mellon University | FAX : +1 412.268.6989
>>>> Pittsburgh, PA 15213-3890 | http://www.cert.org/
>>>> ==
>>>>
>>>>
>>>> George Kirikos <ceo@leap.com> writes:
>>>>>Hello,
>>>>>

>>>>>It's been about a month now since the initial report, and no one from
>>>>>US CERT communicated with me. It appears all the .ml catch-all mail
>>>>>servers are still active, from what I can ascertain.
>>>>>
>>>>>I was thinking of blogging about this, to draw attention to the broad
>>>>>vulnerability (since it affects corporations too, as I noted before),
>>>>>but wanted to ensure that I gave US CERT sufficient time to do a
>>>>>thorough investigation (i.e. the principle of "responsible
>>>>>disclosure"). If someone can provide a time-frame on their work, or if
>>>>>there would be any objections to blogging about this, please advise.
>>>>>
>>>>>I'm particularly sensitive due to it being related to US military, so
>>>>>I wouldn't want to tip off the attackers before US CERT had a chance
>>>>>to gather all the information they required.
>>>>>
>>>>>A response would be greatly appreciated.
>>>>>
>>>>>Sincerely,
>>>>>
>>>>>George
>>>>>
>>>>>---
>>>>>George Kirikos
>>>>>CEO
>>>>>
>>>>>Leap of Faith Financial Services Inc.
>>>>>34 Burnfield Avenue, Toronto, Ontario M6G 1Y5 Canada
>>>>>Tel: +1 (416) 588-0269 Fax: +1 (416) 588-5641
>>>>>E-mail: ceo@leap.com Website: www.leap.com
>>>>>
>>>>>This email and any attachments are for the sole use of the intended
>>>>>recipients and may be privileged or confidential. Any distribution,
>>>>>printing or other use by anyone else is prohibited. If you are not an
>>>>>intended recipient, please contact the sender immediately, and
>>>>>permanently delete this email and attachments.
>>>>>
>>>>>To stop receiving commercial electronic messages, visit http://optout.loffs.com/
>>>>>
>>>>>
>>>>>On Sat, Aug 9, 2014 at 3:16 PM, George Kirikos <ceo@leap.com> wrote:
>>>>>> Thanks for acknowledging receipt of my report. I did some further
>>>>>> analysis identifying additional domain names within .mil that have the
>>>>>> corresponding .ml (Mali) domains activated for email. I can send those
>>>>>> along separately if/when someone from US-CERT contacts me.
>>>>>>
>>>>>> Also, applications for new top-level domain names like .army and .navy
>>>>>> might create opportunities for similar attacks. If one examines the
>>>>>> "name collision" reports published by ICANN for .army, for example:
>>>>>>
>>>>>> https://www.icann.org/sites/default/files/tlds/army/army-apd-list-12nov13-en.csv
>>>>>>
>>>>>> many of the strings correspond to various active subdomains in the
>>>>>> army.mil space. For instance, the string "ftmeade" in the collision
>>>>>> report indicates that ftmeade.army is getting DNS traffic. That domain
>>>>>> name corresponds to the existing ftmeade.army.mil domain run by the US
>>>>>> military. Same story for tardec.army, imcom.army, jackson.army,
>>>>>> knox.army, chapnet.army, aec.army, tradoc.army detrick.army and
>>>>>> goordnance.army, to name a few others. Almost every domain name I
>>>>>> checked that is used by the US military within the .army.mil space can
>>>>>> be found in that name collision list.
>>>>>>

```
>>>>>> This demonstrates that people/systems do mistakenly type in or use
>>>>>> incorrect domain names (either for web surfing, email, or other uses),
>>>>>> and thus information/data can and does "leak" to these non-military
>>>>>> systems. The potential for malicious use and security issues if these
>>>>>> sensitive domains are controlled by bad actors should be obvious.
>>>>>>
>>>>>> Sincerely,
>>>>>>
>>>>>> George
>>>>>>
>>>>>> -----------------------------------------------
>>>>>> George Kirikos
>>>>>> CEO
>>>>>>
>>>>>> Leap of Faith Financial Services Inc.
>>>>>> 34 Burnfield Avenue, Toronto, Ontario M6G 1Y5 Canada
>>>>>> Tel: +1 (416) 588-0269 Fax: +1 (416) 588-5641
>>>>>> E-mail: ceo@leap.com  Website: www.leap.com
>>>>>>
>>>>>> This email and any attachments are for the sole use of the intended
>>>>>> recipients and may be privileged or confidential. Any distribution,
>>>>>> printing or other use by anyone else is prohibited. If you are not an
>>>>>> intended recipient, please contact the sender immediately, and
>>>>>> permanently delete this email and attachments.
>>>>>>
>>>>>> To stop receiving commercial electronic messages, visit http://optout.loffs.com/
>>>>>>
>>>>>>
>>>>>> On Sat, Aug 9, 2014 at 10:40 AM, CERT(R) Coordination Center
>>>>>> <cert@cert.org> wrote:
>>>>>>> -----BEGIN PGP SIGNED MESSAGE-----
>>>>>>> Hash: SHA1
>>>>>>>
>>>>>>> Greetings,
>>>>>>>
>>>>>>> As per our policy, this was forwarded directly to US-CERT for action.
>>>>>>> They will handle further communication on this issue.
>>>>>>>
>>>>>>> Regards,
>>>>>>> Vulnerability Analysis Team
>>>>>>> ==================================================================
>>>>>>> CERT Coordination Center
>>>>>>> www.cert.org / cert@cert.org / Hotline: 1-412-268-7090
>>>>>>> ==================================================================
>>>>>>>
>>>>>>> -----BEGIN PGP SIGNATURE-----
>>>>>>> Version: GnuPG v1.4.5 (GNU/Linux)
>>>>>>>
>>>>>>> iQEVAwUBU+YzL74NbsoIhRIZAQKCfwf5AbjaAausUhZMXIBhZwopq94CxafLTlEH
>>>>>>> 5IRZl8st7RJHLUGSGW+bamSgneQ0A34Z2JjMjcYft+elQahK3LmVOIy/PEqWfKRB
>>>>>>> VkollnKMEHW2twUm3fx76lQQ2c66iAkKdzT3+Smkbx8N5xjI7umkDy9911JSvl5g
>>>>>>> 8JOBb+uwcoARvfljB0ba+A0Z6b3zIY91dpA3dwrrFKh82qFhOo819+j/0G5THdyA
>>>>>>> QOu8r2A9LIweHGZUWpw9f1UoV2iotZKjlAuhILVrQbencl302b8CBGL3AtTp6dYE
>>>>>>> 7OKl03KTSMWHQ0rnAlY2U4jfAXpTm/C1r90WchvPSqGxgDEVn+K2YQ==
>>>>>>> =xpCu
>>>>>>> -----END PGP SIGNATURE-----
>>>> -----BEGIN PGP SIGNATURE-----
>>>> Version: GnuPG v1.4.5 (GNU/Linux)
>>>>
>>>> iQEVAwUBVBB6fL4NbsoIhRIZAQLxyAgAgQktxb6pFk1dRubVIXHr8mHNCwzT+WtV
>>>> bal3CFJlc04N1BVXsjLF9LMl3L6lTII+QeyRYeUKEbbqDM+7zQqFWxqB2llja+4p
```

```
>>>> O323ApeEj2hhgxwqpF3+HX+RLaLKMoZTwF1AOZVUehDgVp06S7TPNRp5qMmQdMBJ
>>>> hxAERojnNdS8wV2kznyQXjtT6696PV4Hl08iO6CTwYWs8obnHUesL59hqx0MkX5P
>>>> wpgssANmczRnmmTCMPDCebq3hcrauqbOPlGllN+fyVCOcy++JbpEHSdBKDC7vbGI
>>>> y6RGinkXeUGevcWN8HPZ3rXRb2EeJB+FqYoBsEL6Hc0kbG+squauaA==
>>>> =3OXQ
>>>> -----END PGP SIGNATURE-----
>> -----BEGIN PGP SIGNATURE-----
>> Version: GnuPG v1.4.5 (GNU/Linux)
>>
>> iQEVAwUBVBnFaL4NbsoIhRIZAQKKbQgAjyTLgS+u5oSi15W5K1qY2d/FWgg5eVIe
>> NhfsRz6+YuNuMHIOwkjfbmhuEhoaNvnwqIhLMQjIZryoogeAufwepKIG4KHz1oGM
>> JnODBnkFCS1450cgl88OxYJkgrhKX1sOp2jJdSh3YUBGKVuEtOsqP2Pkx4IA0Xwz
>> q+rWpsIECG7YrZ1ld3HH/NixT7CMfvUqFKc+NDbGTVTZI0UgJP1bmBVMxAu0gxWW
>> LZAT4EuRQR9wjop1/j7VEj4MejvjKn6Ca4ikipkdK3deBe9Ik6d5Ml1EYYcVOlb6
>> iuze8HCMS6nHFjMKLL/Yuz4Mt6f3pvgJ48owaYDnsJkkVOlX4xj1kQ==
>> =ddtw
>> -----END PGP SIGNATURE-----
```