Peter Sunde Kolmisoppi **@brokep** *Mon May 03 20:22:10 +0000 2021*

Maybe you heard that the domain **https://t.co/3lp8qhGgxd** (**@DarkDotFail**) got hijacked. Here's the story on how it happened. A thread! (I've pieced together the data I have so I might have some small errors in this thread, FYI.)

First, the domain was registered through a service I started, **@njal_la** (or transferred in, not sure here). Njalla in turn uses **@tucows** as a registrar for .FAIL domains.

On the 28th of April, Tucows receives a court order, from Amtsgericht Köln, the district court of Cologne, NRW, Germany. It contains a list of domain names that they want handed over. Two of three domains listed are registered through Njalla, the last one with **@hover**.

The PDF looks like a real court order, I've seen a lot of these (...) but this one is fake. It's without spelling errors, referring to a German paragraph that was previously used to get the domain **https://t.co/OnnqhgyRMf** suspended. So really looks legit.

I do not have a copy of the email and headers, but I'm assuming it is sent using a sender from the domain listed in the document, agkoeln-nrw[.]de. The official domain for Amtsgericht Köln is ag-koeln[.]nrw[.]de. I.e. Not the same.

If you go to the listed domain, agkoeln-nrw[.]de, you will be redirected to the correct domain. **https://t.co/BteCla1XmH**

```
1 - Connected to agkoeln-nrw.de (192.64.119.141) port 80 (#0)
2 > GET / HTTP/1.1
3 > Host: agkoeln-nrw.de
4
5 < Date: Sun, 02 May 2021 09:46:16 GMT
6 < Location: https://www.ag-koeln.nrw.de/
7 < X-Served-By: Namecheap URL Forward
```

If you look at the MX pointers for the domain, it points here: **https://t.co/WYERl4Dfk2**

```
;; ANSWER SECTION:
agkoeln-nrw.de.         1800    IN      MX      10 mx1.privateemail.com.
agkoeln-nrw.de.         1800    IN      MX      10 mx2.privateemail.com.
```

Whereas the correct MX pointers for the correct Amtsgericht Köln is: **https://t.co/ll4Gx927RE**

```
;; ANSWER SECTION:
ag-koeln.nrw.de.        7200    IN      MX      60 relay1v.it.nrw.de.
ag-koeln.nrw.de.        7200    IN      MX      20 relay5m.it.nrw.de.
```

The phishing domain is registered with **@Namecheap**, and is also using their web redirect service and their email service.

Now, Tucows probably deals with quite a load of court orders, and sloppily let's this one through. It looks convincing, the domain is almost correct and if they tried browsing they would have ended up on the correct site. It's a classic phishing expedition.

The fake court order also included a gag order, to not inform the registrant that this was happening. This means that neither Njalla nor Hover was informed about what was going to happen and had no possibility of stopping the transfer.

We presume that Tucows replied with the transfer codes for the domains to the phishing email. We have asked them for more information (like a full copy of the incoming email with SMTP headers etc) and hope to get that soon.

Very quickly after that happened, the domains were transferred out from Tucows. One of the Njalla-originated domains went to **@EpikDotCom** and another one to, you guessed it, **@Namecheap**.

It didn't take long until the websites of the domains (and their MX pointers) all of a sudden had new content. The new sites are now phishing sites, and most likely making a lot of money and collecting sensitive user data.

Njalla (and presumably Hover) informed Tucows very quickly and they were to their credit very quick to put a lot of effort into solving the situation, and they put (from our experience) their best people on it.

Now, I don't like **@EpikDotCom** from a personal and political standpoint. But credit due: when they were informed about the phishing situation, the domain that was transferred to them was handed back very quickly all things considered.

Now, the dark[.]fail domain is another story. There's been a lot of effort put in from the registrant, the reseller, the registrar and many others to return the hijacked domain. But the gaining registrar, **@Namecheap**, has still not done anything at all.

We've all asked if they could first of all suspend the domain so that the active phishing site (yes, it's insanely enough still active, visit with caution) would be stopped. And the domain should be returned, as per regulation that Namecheap has agreed to with ICANN/registry.

Njalla has even contacted **@DonutsInc** that operates the TLD .fail in order to actually get the site shut down and the domain returned. Hopefully this will amount to enough pressure to make **@Namecheap** actually rectify the situation.

(Personally I even contacted The **@NamecheapCEO** who has still not returned my e-mails.)

Now, here's the kicker. Today we got informed that **@Namecheap** doesn't agree that the court order is fake! Even though the domain listed on the court order is registered through them, the web redirect is hosted with them, and the incoming email is hosted by them.

So even though **@Namecheap** has all the evidence needed to stop not only one but two ongoing phishing attacks (the domain hijacked plus the domain used to do it) hosted by them, they refuse.

The past days has not been great for Tucows nor the people working with them. It was a human error, and unfortunately out of the hands of Njalla (& hover). If the court order would have ended up with Njalla, I'm 110% certain it would not have happened.

I've seen a few people very upset with Njalla for "shitty security". The way that domain names work (with this hierarchy) it's near impossible to optimise this flow. Believe me; I'm trying. I left **@njal_la** (I'm on the advisory team still) to work on a new registrar!

My registrar is focused on better technology, and a lot more security. However, ICANN refused me to do so. Ironic. **https://t.co/xOVjPO9bnF**

So if ICANN had not refused me - afraid that I would not follow their regulation - we would not have ended up in a situation where a domain was phished because of low opsec by one ICANN accredited registrar, and then not returned because another is breaking ICANN regulation.

Some of the privacy sensitive domains that used Njalla decided to move. All respect to that. Some have moved to other Tucows-partners (...) and some of them moved to, you guessed it, **@Namecheap**. Oh do I wish I would had an alternative for them for .fail domains.

Now, the phishing attack is still ongoing, and if enough people would push **@Namecheap** and their **@NamecheapCEO** on social media, maybe they will help **@DarkDotFail** out and get their domain back. Thanks.

BONUS 1: The court order PDF has no metadata. It's written in German with correct spelling, the person processing it at Tucows speaks German.

BONUS 2: The domains transferred to **@Namecheap** use their privacy service -- would say uncommon for a court to do.

BONUS 3: If **@Namecheap** is claiming the court order is correct, they must believe that the German court has themselves put up a phishing site.

BONUS 4: The domain transferred to **@EpikDotCom** listed NRW as the region of the registered name holder in the whois data. Most likely the account created there was registered to match the transfer in? Maybe you can update us Epik?

BONUS 5: The domain that was with **@hover** seems to also be stuck with **@Namecheap**.

BONUS 6: The court order makes me believe that the attacker is _very_ well versed in how these court orders usually look, and have directed it extremely well within Tucows. It's not someone without insight.

Resolved! **@Namecheap** finally agreed to return the domain, after a lot of pressure from many angles. Many thanks for all the support here, and now we're going into analysis and debriefing.