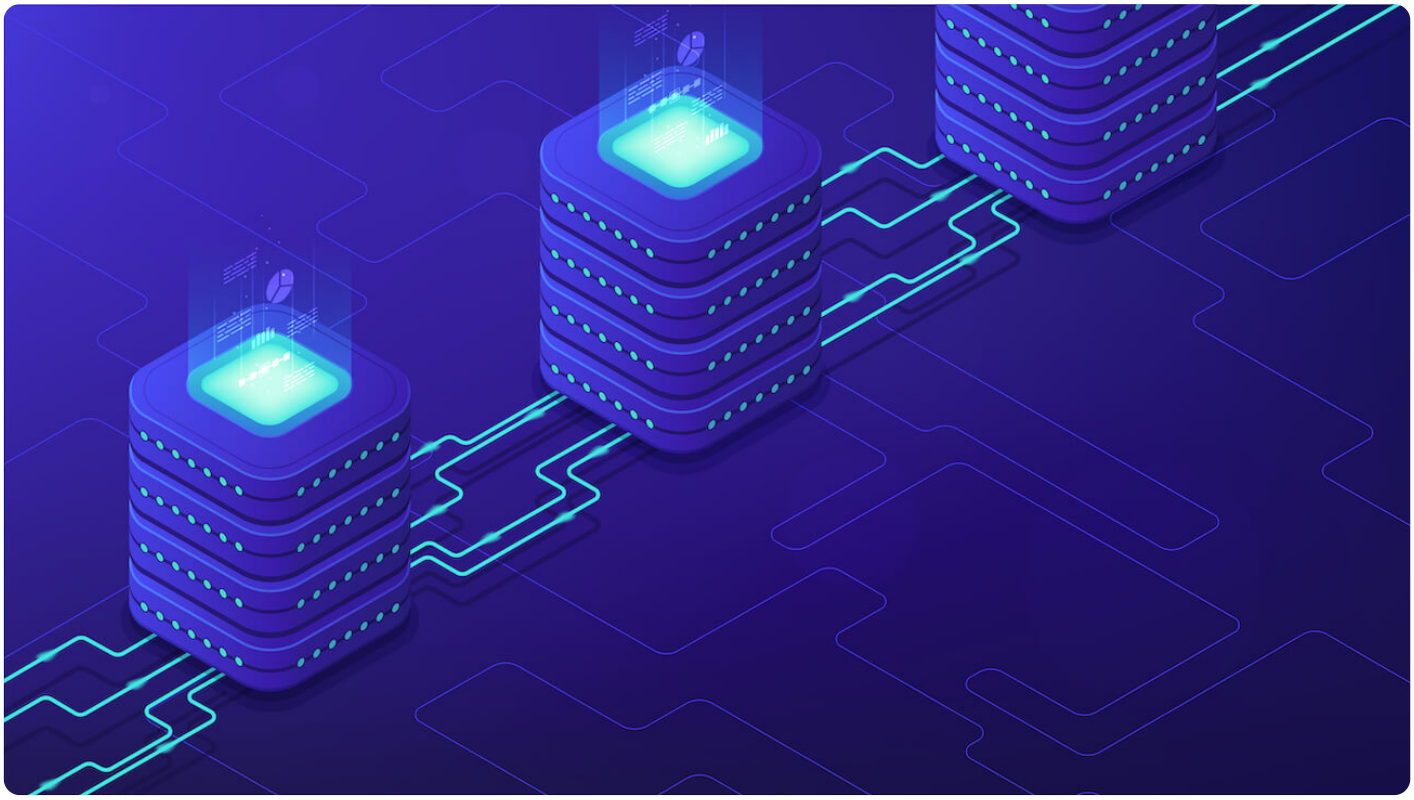
DNS Hijacking Prevention: How to Detect Suspicious Subdomains with Passive DNS

Posted on December 2, 2020



Earlier this year, we saw several cyberattacks target European and Middle Eastern governments and other organizations. Their modus operandi? DNS hijacking. The attackers intercepted Internet traffic going to the victimized websites, likely enabling them to obtain unauthorized access to the intended targets' networks.

That's just one of the many occasions when organizations fell prey to DNS hijacking attacks. More can succumb to the threat if we're to consider that 34% more companies in 2019 alone suffered from a DNS attack (not limited to DNS hijacking) compared to 2018, costing each victim an average of almost $1.1 million.

DNS hijacking notably occurs when hackers tamper with the Domain Name System (DNS) to redirect a target website's visitors to fake login pages designed to capture their passwords and other information they may unknowingly fill in.

But to what extent can DNS hijacking affect organizations with a widespread online presence?

This post aims to answer this question by looking into eBay's potential domain attack surface and the numerous subdomains that contain its brand aided by passive DNS and publicly accessible data.

The Numbers

We used three intelligence sources for this particular study, namely:

- **PhishTank:** Partial list of verified eBay-related phishing URLs (limited to online or active) between 6 January and 18 November 2020.
- **WhoisXML DNS Database Feed:** Large sample of subdomains that contain the text string "ebay."
- **AbuseIPDB:** List of IP addresses that 10% of the total number of subdomains obtained from DNS Database Download resolved to.

We collected a total of 204 confirmed active phishing URLs that contained the text string "ebay" or its misspelled iteration, reported between 6 January and 18 November 2020 from PhishTank. All

these could have figured in various scams throughout the year. Examples include:

- http[:]//ebay-diskussionsforen-clubs-de[.]aydinfidancilik[.]com/index[.]php reported on 3 November 2020
- https[:]//www[.]view-shop[.]net/ebay[.]co[.]uk/?REDACTED reported on 1 October 2020
- https[:]//pgmm[.]club/store[.]ebay[.]de/?REDACTED reported on 30 September 2020
- https[:]//itms-4[.]co[.]uk/eBay-items-48718632/ reported on 25 September 2020
- https[:]//ebay[.]dll[.]singin[.]pms-mingkee[.]com/edy/ reported on 14 September 2020
- https[:]//drrosu[.]ro/store[.]ebay[.]es/ reported on 4 September 2020

DNS Database Download, meanwhile, provided us with a list of 4,330 subdomains containing the text string “ebay.” These subdomains resolved to 6,013 IP addresses.

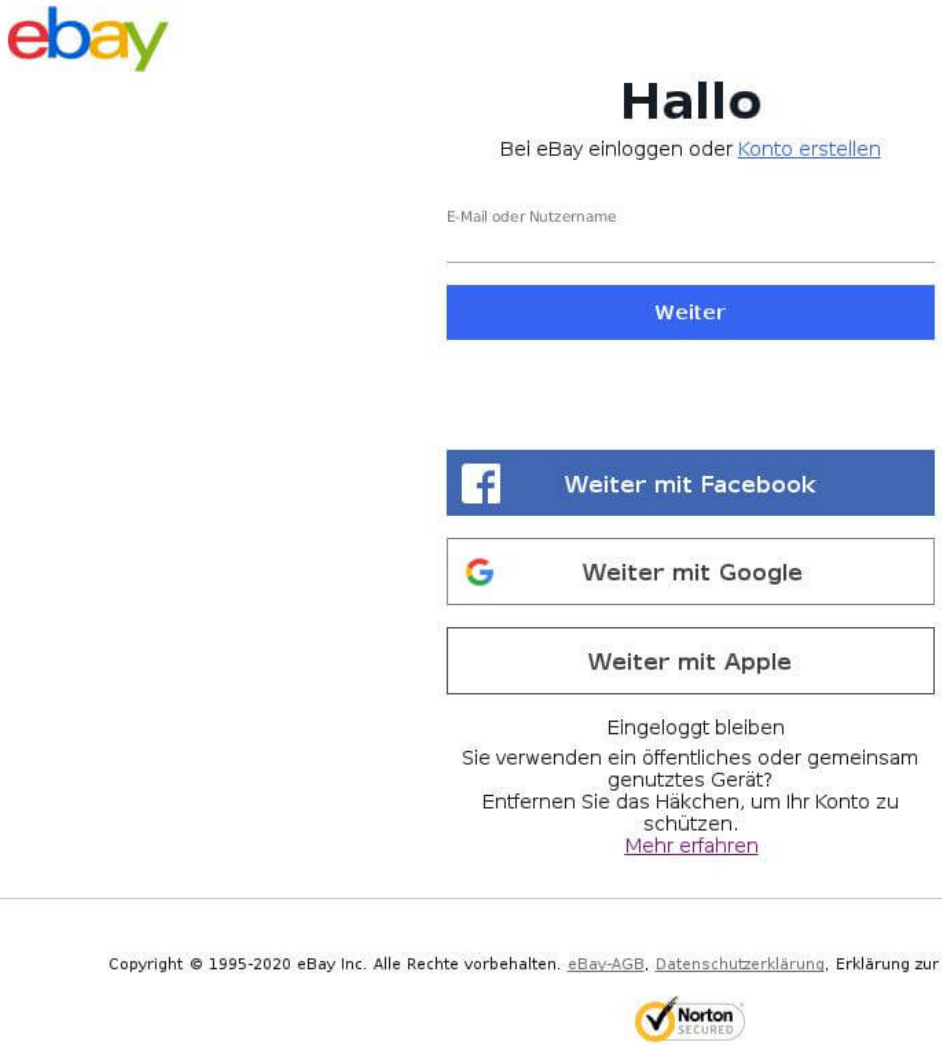
The Lowdown

No blacklist is fully comprehensive, and some may contain more or different indicators of compromise (IoCs) than others based on how their data was collected. That is why it is advisable to obtain information from as many threat intelligence sources as possible, both internal and external alike.

External Data: From a Publicly Accessible Threat Intelligence Source

Without subscribing to or constantly monitoring phishing blacklist sites like PhishTank, organizations and users may think they are liaising with eBay through the 204 confirmed phishing URLs when they’re actually dealing with pages specially crafted by threat actors to scam them.

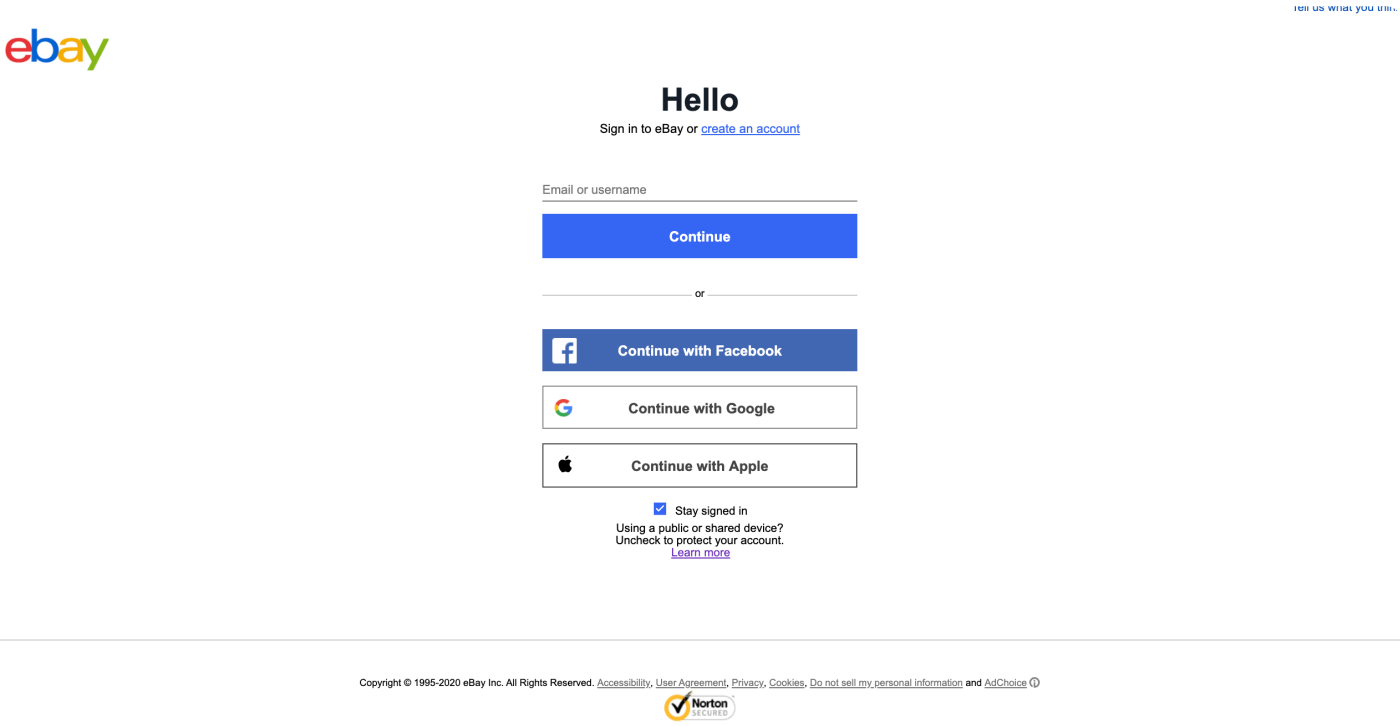
Take a look at http[:]//signin[.]eby[.]de[.]4dyrkjyyvxkxeou[.]arcseam[.]com[.]au, for instance. It is a verified phishing website, according to PhishTank.



Fake eBay page when users click http[:]//signin[.]eby[.]de[.]4dyrkjyyvxkxeou[.]arcseam[.]com[.]au from PhishTank

While “ebay” was misspelled in the URL, the use of the eBay logo and the page’s uncanny resemblance (down to the security service provider details in the footer) to the real eBay login

page could be enough to fool one into thinking they're signing in to the real deal.



Real eBay login page when users click "Sign in" on ebay[.]com

Internal Data: From a Passive DNS Database

Apart from enlisting the help of publicly accessible threat databases, organizations can also benefit from access to a robust passive DNS database. Doing so would help them cover potentially harmful domains and subdomains that have yet to be publicly identified as IoCs.

As was mentioned earlier, we obtained 4,330 subdomains that contained the text string "ebay" which resolved to 6,013 IP addresses from our passive DNS database.

We subjected 10% of the subdomains and their corresponding IP addresses to further scrutiny. We ended up with a reduced sample containing 433 subdomains and 917 IP addresses.

Checking each of the 917 IP addresses on AbuseIPDB allowed us to determine that 122 were suspicious and may require blacklisting.

The table below lists the top 10 IP addresses based on the number of times they were reported on AbuseIPDB, along with the subdomains that pointed to them.

IP Address	Number of Times Reported on AbuseIPDB	Subdomain
208[.]91[.]197[.]27	196	signin[.]ebay[.]it[.]izarbrokers[.]com
199[.]59[.]242[.]153	140	accedi[.]ebay[.]it[.]spamed[.]co
204[.]11[.]56[.]48	110	keepkey[.]ebay[.]detailsfoundhere[.]com autodiscover[.]ebay[.]omega-aluminium[.]com www[.]cryptosteel[.]ebay[.]detailsfoundhere[.]com www[.]keepkey[.]ebay[.]detailsfoundhere[.]com www[.]nanos[.]ebay[.]detailsfoundhere[.]com mail[.]ebay[.]omega-aluminium[.]com www[.]trezor[.]ebay[.]detailsfoundhere[.]com trezor[.]ebay[.]detailsfoundhere[.]com
204[.]11[.]58[.]194	89	signin[.]ebay[.]es[.]jobsclebson[.]com
91[.]195[.]240[.]117	31	signin[.]ebay[.]frisbees[.]com
91[.]195[.]241[.]136	24	suchen[.]ebay[.]co[.]uk[.]de
103[.]224[.]212[.]222	23	magento[.]ebay[.]federalbank[.]co
31[.]184[.]198[.]147	16	kgvrfn[.]ebay[.]de-otp[.]webredirect[.]org

72[.]52[.]10[.]14	15	rover[.]ebay[.]co sid[.]ebay[.]co sellerstandards[.]ebay[.]sg logs-cdn[.]ebay[.]com[.]weareebay[.]com api-rnpci[.]ebay[.]com[.]weareebay[.]com cdnrest[.]stratus[.]phx[.]ebay[.]com[.]weareebay[.]com cdnrest[.]vip[.]slc[.]ebay[.]com[.]weareebay[.]com
205[.]178[.]189[.]129	13	signin[.]ebay[.]it[.]ahqfood[.]com www[.]signin[.]ebay[.]it[.]ahqfood[.]com

While none of the suspicious subdomains seemed to be under eBay's control, as they sported other root domains (not ebay[.]com), they could still pose a threat to the e-commerce company and its reputation. The subdomains in the table above can figure in phishing emails targeting the company's user base.

Expanding corporate blacklists to include IoCs from publicly accessible threat databases and monitoring domains and subdomains through passive DNS data can be important cybersecurity endeavors to support the detection and prevention of possible DNS hijacking attacks.