In the Market for a New Car? Beware Not to Get on the Phishing Bandwagon

Table of Contents

Executive Report

In an earlier post, we looked at how cybersquatters took advantage of the popularity of seven car manufacturers to lure unwitting victims to fake sites. Since then, we were alerted to a phishing campaign this time targeting several German car dealers via age-old but still effective phishing.

What the Public Knows So Far

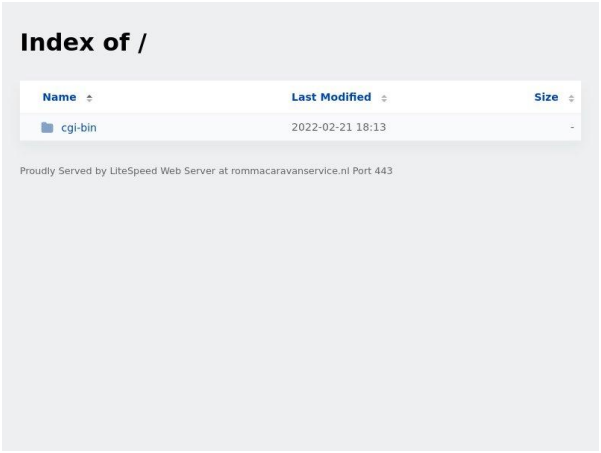
A published report identified 37 domains as indicators of compromise (IoCs) related to this threat. We used these as jump-off points for a more in-depth investigation and found:

- A couple of unredacted registrant email addresses
- More than 1,200 possibly connected domains (some registered using the identified unredacted email addresses while others shared the domain IoCs' IP hosts or contained the same strings)
- Several IP address resolutions of the domain IoCs
- A dozen possibly connected domains dubbed "malicious" by various malware engines

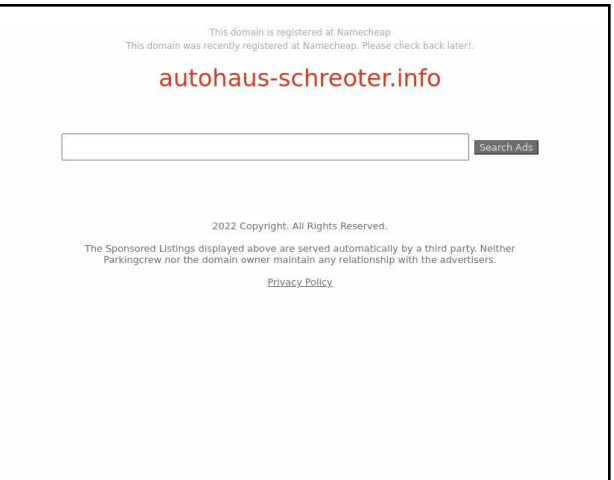
Deep Dive Revelations

We began by subjecting the 37 domain IoCs to a bulk WHOIS lookup and found that none of them seemed to belong to a legitimate carmaker or auto dealership company. Two of them (bornagroup[.]ir and groupschumecher[.]com), however, were registered using what looked to be personal email addresses left unredacted.

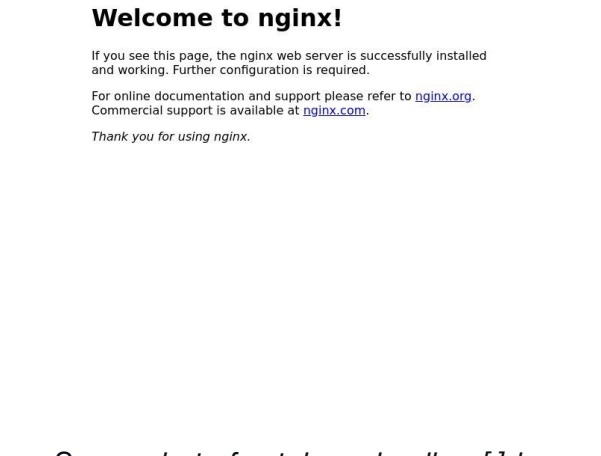
Screenshot lookups showed that many of the domain IoCs resolved to index pages while a few were parked or currently under development. One—auto-falkanhahn[.]de—looked to be still up and running and should be avoided, especially by biking aficionados given the content it hosts.



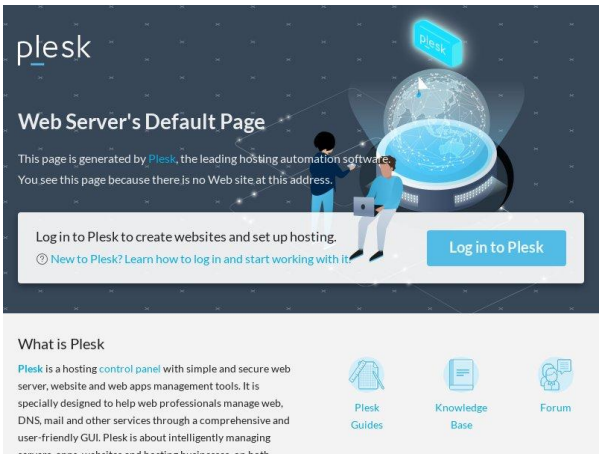
Screenshot of rommacaravanservice[.]nl



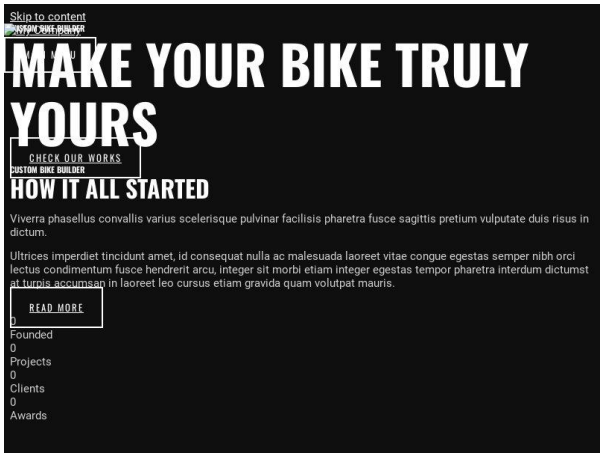
Screenshot of autohaus-schreoter[.]info



Screenshot of autohaus-landharr[.]de



Screenshot of auto-viotel[.]de



Screenshot of auto-falkanhahn[.]de

Using the unredacted registrant email addresses as reverse WHOIS search terms led to the discovery of 10 possibly connected domains.

We also used the domain IoCs as DNS lookup search terms and found 21 active and unique IP resolutions. Utilizing these as reverse IP lookup search terms allowed us to uncover 1,011 more domains.

Interestingly, screenshot lookups for these additional domains showed that 26 hosted the same content as auto-falkanhahn[.]de or were redirects, namely:

- admin-shopify[.]com
- appleId[.]logn-alert[.]com
- inc-ialert[.]com
- Icloud[.]inc-ialert[.]com
- Icloud[.]logn-alert[.]com
- logn-alert[.]com
- mail[.]inc-ialert[.]com
- mail[.]logn-alert[.]com
- maps[.]inc-ialert[.]com
- maps[.]logn-alert[.]com
- post-redelivery[.]co[.]uk
- support[.]inc-ialert[.]com
- support[.]logn-alert[.]com
- themasterdevin[.]us

- www[.]appleld[.]inc-ialert[.]com
- www[.]appleld[.]logn-alert[.]com
- www[.]inc-ialert[.]com
- www[.]lcloud[.]inc-ialert[.]com
- www[.]lcloud[.]logn-alert[.]com
- www[.]logn-alert[.]com
- www[.]maps[.]inc-ialert[.]com
- www[.]maps[.]logn-alert[.]com
- www[.]myfundcheckers[.]com
- www[.]support[.]inc-ialert[.]com
- www[.]support[.]logn-alert[.]com
- www[.]themasterdevin[.]us

Similarities in the hosted content and strings used ("logn-alert," "inc-alert," and "themasterdevin") provide supporting evidence that these domains could be part of the same infrastructure or owned by the same individual or group. Refraining from accessing them may thus be a great idea as well.

Given that the domain IoCs featured common string combinations like "auto + center," "auto + haus," and "auto + house," we obtained other domains via Domains & Subdomains Discovery that could be considered artifacts. We found 206 such domains.

Finally, subjecting the web properties (domains and IP addresses) not yet identified as possibly related to this campaign to a bulk malware check via the Threat Intelligence Platform showed that 12 of them should be blocked on user networks as they have been dubbed "malware hosts" by various engines.

—

Users currently in the market for their next cars but do not want to get their credentials stolen instead should avoid accessing the artifacts (12 domains) deemed unsafe in this post. Refraining from accessing any site with the same content as auto-falkanhahn[.]de is also a good idea. And should you receive an email coming from the email addresses we identified, don't even think of opening them.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Artifacts and IoCs

Unredacted Email Addresses Used to Register Some of the Domain IoCs

- amir*****@yahoo[.]com
- app*****@yahoo[.]com

Domains Registered Using the Domain IoCs' Email Addresses

- turbocell[.]ir
- bornagroup[.]ir
- groupschumecher[.]com
- rbcplc[.]com
- nt-ttb[.]com
- meiar-ratio[.]com
- btg-bleumel[.]com
- al-nahedhfinancebrokers[.]com
- gedikdukom[.]com
- teghleefindustry[.]com

IP Address Resolutions of the Domain IoCs

- 46[.]17[.]98[.]115
- 46[.]17[.]98[.]116
- 162[.]0[.]217[.]151
- 217[.]144[.]104[.]53
- 85[.]214[.]219[.]166
- 85[.]214[.]47[.]68
- 85[.]214[.]25[.]11
- 85[.]214[.]36[.]65
- 192[.]64[.]119[.]46
- 111[.]90[.]140[.]225
- 111[.]90[.]140[.]218
- 111[.]90[.]140[.]220
- 111[.]90[.]140[.]216
- 111[.]90[.]140[.]226
- 111[.]90[.]140[.]224
- 111[.]90[.]140[.]215
- 111[.]90[.]140[.]214
- 111[.]90[.]140[.]217
- 81[.]169[.]185[.]209
- 111[.]90[.]156[.]165
- 162[.]255[.]119[.]90

Domains That Shared Some of the Domain IoCs' IP Hosts

- a-list-jobs[.]com
- a-pennington[.]com
- a-social[.]vip
- a-vollbrecht[.]de
- a00931833[.]xyz
- a10r[.]co
- a1iseasy[.]com
- a1ventures[.]us
- a2zbizz[.]com
- a3plumbing[.]com
- a7dul[.]xyz
- a8236[.]xyz
- aa[.]associates
- aaa-security[.]net
- aaaabb[.]xyz
- aaaproplus[.]com

- aaaventures[.]us
- aacraoedge[.]org
- aaiqb[.]xyz
- aalpirez[.]com
- aaniescollection[.]com
- aaol[.]live
- aaronandhurmedia[.]com
- aaronmarco[.]com
- aaronrosa[.]com
- aaronswoodwork[.]xyz
- aashroff[.]dev
- aau-utah[.]org
- aautohero[.]com[.]de
- aayushsrivastava[.]com
- abadimkr[.]net
- abakah[.]org
- abbbac[.]com
- abbysbailbonds[.]com
- abdisamad[.]net
- abdounmall[.]net
- abdrn[.]co[.]uk
- abdulganiyshehu[.]com
- abejareinajoyeria[.]com
- abeljosefo[.]icu
- abelson-odds-feed[.]com
- abend-labs[.]com
- aberrantla[.]com
- abfabrugcleaning[.]com
- abhishektomar[.]com
- abici[.]xyz
- abigailramos[.]com
- abilityoga[.]com
- abilliondollarcompany[.]com
- abiskoo[.]com
- abizimage[.]com
- ablogeditor[.]com
- ablueprintorganic[.]com
- abngold[.]com
- abnoginsec[.]com
- abnwebstore[.]com
- abookstereotype[.]com
- abortion[.]capital
- aboumalak[.]com
- about-oic[.]com
- abp-teletech[.]eu
- abrahamrosav[.]me
- abrarpalace[.]com
- abraxaspetroleum-engineers[.]com
- abrilamericana2021br[.]xyz
- absinthedirect[.]com
- absolmoney[.]com
- absoluteexihbits[.]com
- absolutefunnels[.]com
- absoluteroyaljelly[.]net
- absurdads[.]com
- abubakrzoubi[.]com
- abucamber[.]com
- abundanceaffirmations[.]com
- abundancecycle[.]org
- abundantcoachingtransformation[.]com
- abundantlivingwoman[.]com
- abushaban[.]com
- abyayalafest[.]com
- abyyss[.]com
- ac3tx[.]com
- acabe[.]science
- acaciasalmundo[.]com
- academyofspiritualmastery[.]net
- acadiaem[.]com
- acadiaengineering[.]org
- acadimo[.]com
- acbusiness[.]news
- accademiaevolutiva[.]net
- accessboatsupply[.]com
- accessia[.]xyz

- accidentalcsuite[.]com
- accidentallysuccessfulentrepreneur[.]com
- acclimate[.]to
- accmove[.]org
- accounting[.]sbs
- accountingforcreatives[.]org
- accountz[.]xyz
- accsunday[.]cc
- accudynplasticinjectionmolding[.]com
- accuraterank[.]com

Domains Containing Similar String Combinations as the Domain IoCs

- fclassicars[.]it
- buyclassiccars[.]au
- classiclacars[.]com
- spclassic-cars[.]com
- laclassicalcars[.]com
- classiccarsprod[.]com
- acesclassiccars[.]com
- ifixclassiccars[.]com
- carusoclassiccars[.]us
- classiccarservice[.]us
- us-classic-cars[.]club
- classicscarscenes[.]ml
- classic-supercars[.]nl
- club55classiccars[.]es
- classic-eventcars[.]de
- classiccarspeakers[.]com
- webuyanyclassiccars[.]ws
- majorcaclassiccars[.]com
- classiccarsales[.]online
- imperialclassiccars[.]com
- jyclassiccarstorage[.]com
- willenclassiccars[.]co[.]uk
- laarhovenclassiccars[.]nl
- guernseyclassiccars[.]com
- classiccarsandcigars[.]com
- jyclassiccarstorage[.]co[.]uk
- gassmann-classic-cars[.]com
- retrochargeclassiccars[.]com
- classiccars-rungreen[.]co[.]uk
- retrochargeclassiccars[.]net
- carsonvalleygolfclassic[.]com
- tanatvalleyclassiccars[.]co[.]uk
- historicclassiccarsbikes[.]com
- mallorcaluxuryclassiccars[.]com
- historicclassiccarsbikes[.]co[.]uk
- autohouse[.]rs
- zerohouse[.]autos
- autosaetyhouse[.]com
- autohousegrand[.]com
- autolyna-house[.]com
- houseautomation[.]app
- autoharneshouse[.]com
- rivertreehouse[.]autos
- calautowarehouse[.]com
- autostartwarehouse[.]com
- 4houseautomacao[.]com[.]br
- franksautohouse[.]com[.]au
- premierautohouse[.]co[.]za
- houseautomatesmarter[.]com
- whitehouse-automation[.]com

Unpublicized Malicious Domains

- turbocell[.]ir
- bornagroup[.]ir
- groupschumecher[.]com
- rbcplc[.]com

- 00069[.]digital
- 14myuser[.]com
- auto-falkanhahn[.]de
- boulevardnew[.]xyz
- europe-news[.]xyz
- topprofitnew[.]xyz
- yasuipotto[.]com
- autohaus-sh[.]com