Probing Lorec53 Phishing through the DNS Microscope

Table of Contents

Executive Report

Lorec53, a relatively new APT group according to NSFocus, actively targeted various Eastern European government institutions in 2021. The threat actors used well-crafted phishing campaigns to gather and steal data from their targets. Two years after their heyday, is the threat Lorec53 poses gone? Or has the group left still-active traces in the DNS?

Using the 21 indicators of compromise (IoCs)—19 domains and two IP addresses—NSFocus shared via AlienVault OTX as jump-off points, the WhoisXML API research team sought to find digital bread crumbs the APT group may have left behind in the DNS. Our analysis found:

- 21 domains that were registered using the same email address as two of the IoCs, two of which turned out to be malicious
- 12 unique IP addresses to which the domains identified as IoCs resolved
- 1,818 domains that shared the IoCs' IP hosts
- 168 domains that shared unique strings with some of the IoCs

Locus53 Campaign Tidbits

Locus53 used various lures in their targeted phishing campaigns, including:

- A supposed document confirming the target's agreement to a disease prevention and control-related proposal
- Proof of being chosen as a bitcoin recipient
- Evidence of a fake COVID variant dubbed "COVID-21"
- A supposed update for Adobe Acrobat Reader DC
- A fake Android app

All of the email file attachments above, along with others sent by Lorec53, were laced with malware meant to exfiltrate confidential data.

NSFocus shared the list of IoCs they collated via AlienVault OTX, which we listed in the table below.

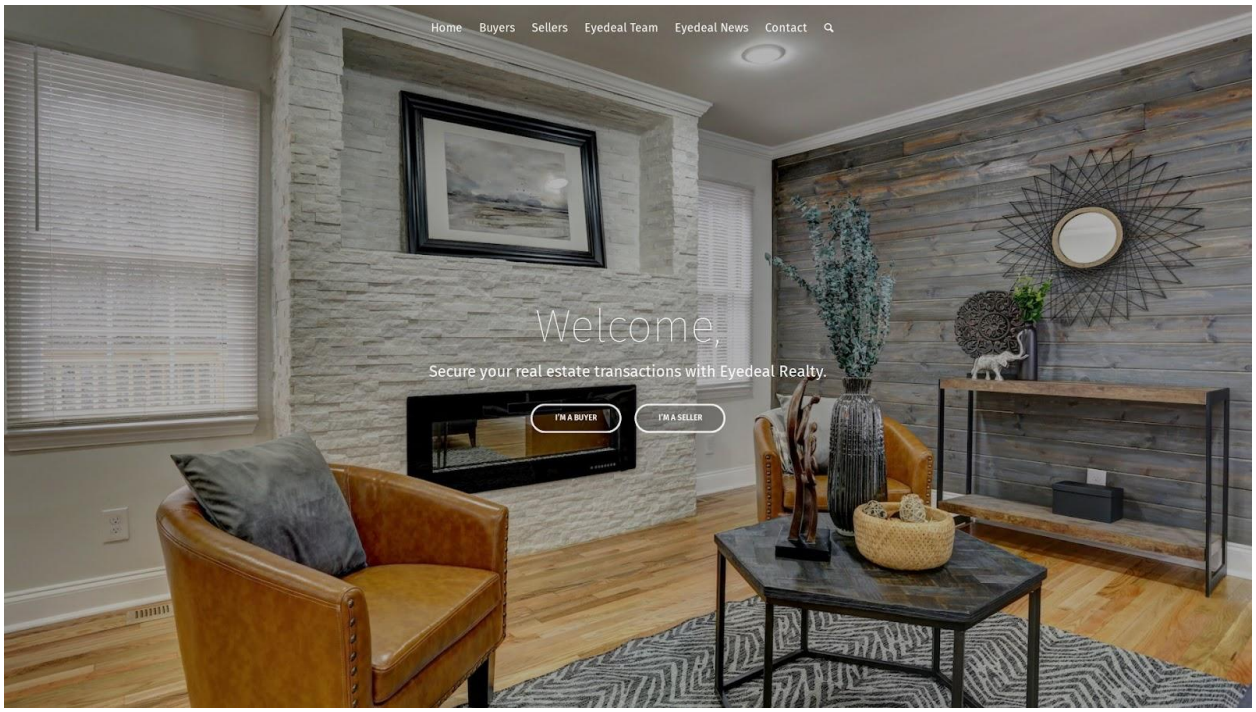
Domains	IP Addresses
• name4050[.]com • name1d[.]site • 2330[.]site • 1833[.]site • 1221[.]site • 1000020[.]xyz • smm2021[.]net • greatgardenplantsblog[.]com • intelpropertyrd[.]com • citylimitshog[.]com • eyedealrealty[.]com • cabiria[.]biz • 33655990[.]cyou • 2215[.]site • 16868138130[.]space • 1681683130[.]website • stun[.]site • eumr[.]site • 3237[.]site	• 45[.]146[.]165[.]91 • 194[.]147[.]142[.]232

Collating Lorec53 Digital Bread Crumbs

We began our investigation by determining which of the domain IoCs remained live via screenshot lookups. Only two of the domain IoCs continued to host live content to this day.

Screenshot of intelpropertyrd[.]com

The other live page—eyedealrealty[.]com—hosts a real estate company site consistent with its name.



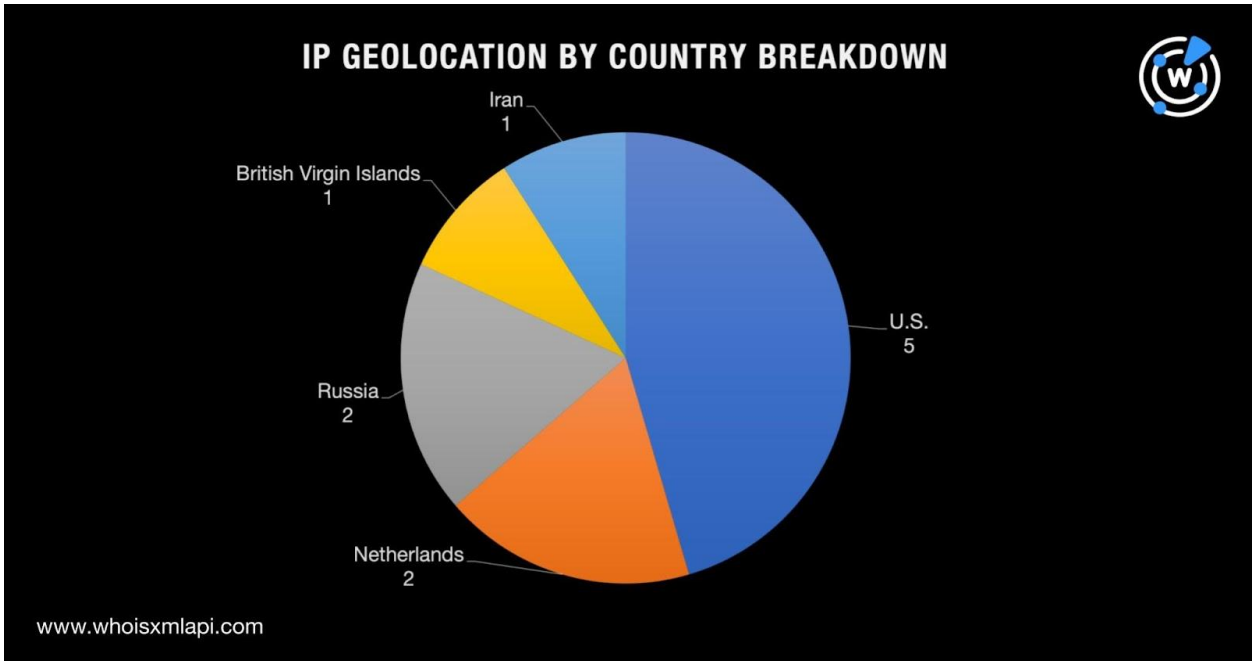
Screenshot of eyedealrealty[.]com

To trace Lorec53's digital footprint, we then sifted through the domain IoCs' WHOIS records. The current WHOIS records of the two domains above also indicated their registrants' personal email addresses.

Reverse WHOIS searches for the email addresses revealed they were historically used to register 21 domains in total, two of which turned out to be malicious. An example would be matosariasrealstate[.]com.

Next, DNS lookups for the domain IoCs showed they resolved to nine unique IP addresses, giving us a total of 11 IP hosts when combined with the two identified as IoCs. Six of these were shared hosts, three were dedicated, and two had no matching DNS records.

The 11 resolving IP addresses were scattered across five countries. The U.S. accounted for five IP hosts, followed by the Netherlands and Russia with two each.



Reverse IP lookups for the 11 IP addresses led to the discovery of 1,818 domains. A huge majority of these sites were parked.

A couple of connected domains also contained at least three well-known brands—CNN, Google, Intel, and Visa. Examples include:

- 0[.]www[.]cnn[.]jobs[.]com--indeed[.]com

- 0078d3ff03b13d29f710d0e6602bcc4a[.]safeframe[.]googlesyndication[.]co
- mail[.]intelpropertyrd[.]com
- 108visa[.}online

These could figure in phishing and other malware-enabled campaigns targeting job seekers, syndication customers, real estate investors, and credit card holders.

Finally, we noticed that some of the domains tagged as IoCs had unique strings listed in the following table. We sought to find how many other domains contained each string but used different top-level domain (TLD) extensions via Domains & Subdomains Discovery.

IoC	String Found in an IoC	Number of Domains Containing the String with a Different TLD Extension
smm2021[.]net	***smm2021.***	4
cabiria[.]biz	***cabiria.***	20
stun[.]site	***stun.***	128
eumr[.]site	***eumr.***	16

While none of them were confirmed to be malware hosts, their close resemblance to the IoCs may warrant close monitoring for signs of suspicious activity.

Conclusion

Based on the continued existence of live sites either identified as Lorec53 IoCs in 2021 and those that may be part of the threat group's infrastructure through email, IP address, or string usage connections, the risks they pose may not be gone. That is especially true for the two malicious domains we identified that were registered using the same email addresses as two of the original IoCs.

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

Sample Domains Registered Using the Same Email Addresses as Two of the IoCs

- gomezduranadministradores[.]com
- myfconsultinggroup[.]com
- intelpropertyrd[.]com
- matosariasrealstate[.]com
- rayzacastillo[.]com
- administradoresgn[.]com
- healthandfitnessmarket[.]com
- myfconsultingroup[.]com
- servihogarrd[.]com
- houseasist[.]com
- condoservicerd[.]com

Sample IP Addresses to Which the Domains Identified as IoCs Resolved

- 204[.]11[.]56[.]48
- 81[.]68[.]250[.]191
- 109[.]234[.]38[.]122
- 35[.]208[.]138[.]97
- 162[.]241[.]192[.]26

Sample Domains That Shared the IoCs' IP Hosts

- a-renewedyou[.]com
- a-thoughtfull-journal[.]com
- aaosajao[.]com
- aaosajao[.]jaimasihki[.]org
- aapc[.]callistowebstudio[.]com
- aarongadams[.]com
- aaronharrisfitness[.]com
- aaronsehmar[.]co[.]uk
- abaitulshop[.]shop
- abbeygoldenberg[.]com
- abc[.]jillfk[.]com
- b2blegprom[.]market
- babybaristabook[.]com
- babyshop[.]mu
- baileylynndphotography[.]com
- balda[.]games
- barlupwine[.]com
- barlupwinery[.]com
- bay-sports-photography[.]com
- bdgblogs[.]com
- bdgblogs[.]org
- cabiria[.]biz
- campro[.]tk
- caps-login[.]top
- carbonstrategic[.]com
- carcancreative[.]com
- cassierajewich[.]com
- catalinainfante[.]cl
- catherine-forsman[.]com
- caymanmarinelab[.]com
- cbcspartners[.]com
- d-watch[.]xyz
- d[.]mushderi[.]xyz
- d0k8y[.]cyou
- daemon-tols[.]com
- daemvsem[.]com
- dallyps[.]site
- danandraos[.]com
- datadrivenec[.]com
- datadudes[.]ai
- datasource[.]cat
- e812[.]space
- eastfiber[.]com
- easydiypowerplan[.]net
- eclecticsmarketplace[.]com
- ecommpromarketing[.]com
- edbinljzqzd[.]terrasnaya-doska-dpk-kukmor[.]ru
- edxo[.]xn--c1akhmbht[.]xn--p1acf
- efoodtrucktrailers[.]com

- elaineparksart[.]com
- eldersburgchiro[.]com
- fa2000ca[.]com
- fadedmidnight[.]org
- fafolifestyle[.]com
- fakrvs[.]bar
- famatplay[.]com
- fatalgame[.]net
- fbngfnhgf[.]top
- fdamaskchina[.]com
- fencecompanysandiegoca[.]com
- fernandezconsultoria[.]com
- g-watch[.]xyz
- gabeconsultores[.]com
- gainesvillehomeservices[.]com
- galactus[.]top
- gallegosfornm[.]com
- gazono-kosilka[.]ru
- ge[.]yuzhige[.]club
- geauxplatinum[.]com
- geolandingpages[.]com
- georgiyevsk[.]ru
- haibianyujia[.]com
- hasosodo[.]com
- hdro[.]changerdota2csgo[.]store
- heatherdurkin[.]com
- helloshift[.]net
- help-youla[.]site
- henrikboes[.]com
- hevoreste[.]store
- hithriving[.]com
- hjfgxxds[.]com
- iaconolegal[.]com
- icelandicoutfitters[.]com
- icmglobalfunding[.]com
- icrqofgvaqb[.]terrasnaya-doska-dpk-novocheboksarsk[.]ru
- iddadvancednutrition[.]com
- iex[.]la
- iiexcellence[.]com
- iippgj[.]bar
- ij19[.]co[.]uk
- ilsisgbvqgc[.]streamgreen[.]ru
- jajhrxflxzf[.]xn----7sbagnvdj0dbnhfo6p[.]xn--p1acf
- jamalandkiran[.]com
- jbvpgj[.]bar
- jeancyrillebado[.]com
- jeff-young[.]net
- jennaforcitycouncil[.]com
- jenniferforaz[.]com
- jessicahortman[.]com
- jewelryforwhsle[.]com
- jfin[.]app

Sample Domains That Contained Strings Also Found Among Some of the IoCs

- smm2021[.]ru
- smm2021[.]com
- smm2021[.]org
- smm2021[.]online
- cabiria[.]shop
- cabiria[.]net
- cabiria[.]rocks
- cabiria[.]co
- cabiria[.]com
- cabiria[.]info
- cabiria[.]org[.]es
- cabiria[.]org
- cabiria[.]today
- cabiria[.]com[.]cn
- cabiria[.]me
- cabiria[.]it
- cabiria[.]cn
- cabiria[.]com[.]br

- cabiria[.]com[.]au
- cabiria[.]mom
- cabiria[.]fr
- cabiria[.]asso[.]fr
- cabiria[.]es
- cabiria[.]eu
- stun[.]lol
- stun[.]ninja
- stun[.]wales
- stun[.]tv
- stun[.]gg
- stun[.]solutions
- stun[.]nl
- stun[.]ga
- stun[.]us
- stun[.]ru
- eumr[.]top
- eumr[.]se
- eumr[.]icu
- eumr[.]ru
- eumr[.]info
- eumr[.]net
- eumr[.]de
- eumr[.]xyz
- eumr[.]win
- eumr[.]ch
- eumr[.]org
- eumr[.]wang
- eumr[.]com
- eumr[.]com[.]cn
- eumr[.]party
- eumr[.]cn