DNSの顕微鏡でLorec53のフィッシングを精査

目次

要旨

NSFocusの言葉を借りればまだ比較的新しいAPTグループである「Lorec53」は、2021年に東欧諸国の政府機関を狙ったフィッシングキャンペーンを活発に行い、標的からデータを収集、窃取しました。その全盛期から2年が経過した現在、Lorec53がもたらす脅威はなくなったのでしょうか？それともDNSにまだ活動の痕跡を残しているのでしょうか？

WhoisXML APIの研究チームがこのほど、AlienVault OTXを介してNSFocusが公開した21個のセキュリティ侵害インジケーター（IoC）（19個のドメイン名と2個のIPアドレス）を出発点として、Lorec53がDNSに残した可能性のある痕跡を調査しました。その結果、以下を発見しました。

- 2つのIoCと同じメールアドレスを使って登録された21個のドメイン名。そのうち2つは悪意あるドメイン名と確認
- IoCとして特定されたドメイン名が名前解決した12個のユニークなIPアドレス
- IoCのIPホストを共用していた1,818個のドメイン名
- 一部のIoCと同じ固有の文字列を含んだ168個のドメイン名

Lorec53がキャンペーンで使うルアー

Lorec53は、標的型フィッシングキャンペーンにおいて以下を含むに様々なルアーを使っていました。

- 疾病予防・管理に関する提案に標的が同意したことを確認する文書と思われるもの
- ビットコインの受取人に選ばれた証明
- 「COVID-21」という偽のCOVID亜種の証拠
- Adobe Acrobat Reader DCの更新情報と思われるもの
- 偽のAndroidアプリ

これらはLorec53が送信したメールの添付ファイルで、すべてに機密データを流出させるマルウェアが混入していました。

NSFocusは、照合したIoCのリストをAlienVault OTXを介して公開しました（以下）。

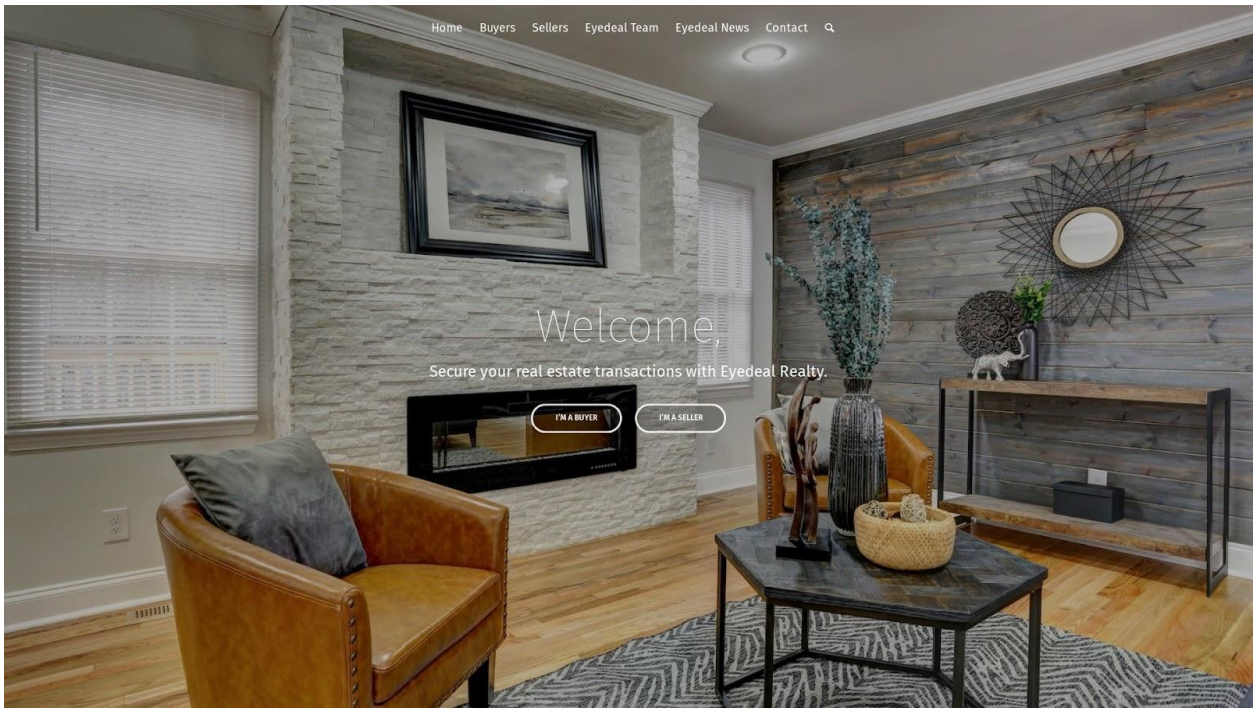
ドメイン名	IPアドレス
• name4050[.]com • name1d[.]site • 2330[.]site • 1833[.]site • 1221[.]site • 1000020[.]xyz • smm2021[.]net • greatgardenplantsblog[.]com • intelpropertyrd[.]com • citylimitshog[.]com • eyedealrealty[.]com • cabiria[.]biz • 33655990[.]cyou • 2215[.]site • 16868138130[.]space • 1681683130[.]website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

Lorec53の痕跡を照合

当社ではまず、IoCと特定されたドメイン名のうちどれが今も有効かを確認するため、screenshot lookupを使って検索しました。その結果、現在もコンテンツをホストし続けているドメイン名は2個だけであることがわかりました。そのうち一つ、*intelpropertyrd[.]com*がホストしているサイトのスクリーンショットは以下の通りです。

*intelpropertyrd[.]com*のスクリーンショット

もう一つのドメイン名eyedealrealty[.]comは、その文字列が表現している通り、不動産会社のサイトをホストしています。



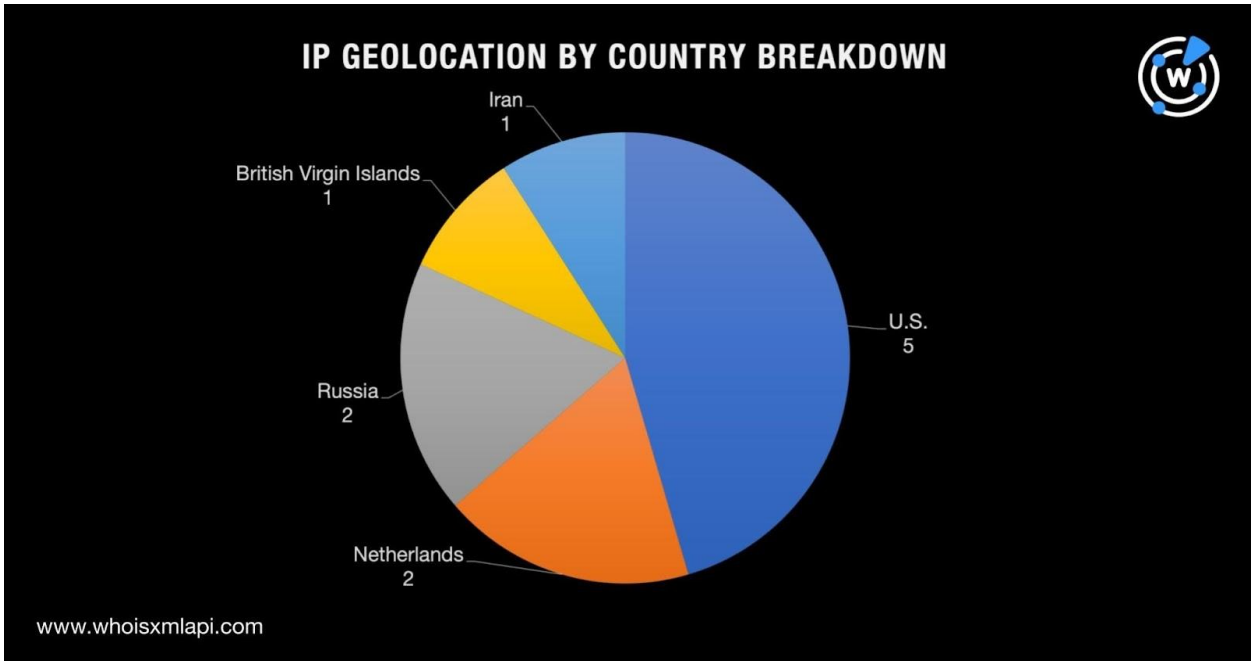
*eyedealrealty[.]com*のスクリーンショット

次に、Lorec53のデジタルフットプリントを追跡するため、ドメインIoCのWHOISレコードを調べました。そして、上記2ドメインの現在のWHOISレコードに、登録者の個人的なメールアドレスも記載されていることを確認しました。

それらのメールアドレスをReverse WHOIS searchesで検索したところ、それらが過去に21個のドメイン名の登録に使われたことが判明しました。そのうち2つは悪意あるドメイン名でした。その例として、matosariasrealstate[.]comが挙げられます。

さらに、ドメインIoCをDNS lookupsにかけた結果、9つのIPアドレスに名前解決されました。これをIoCとして特定済みの2つのIPアドレスと合わせると、合計11個のホストが判明したことになります。このうち6つは共用、3つは専用のホストでした。また、2つは合致するDNSレコードがありませんでした。

11個のIPアドレスは、地理的には5カ国に分散していました。最も多かったのは5つが所在していた米国で、次いでオランダとロシアが多く、それぞれ2つずつありました。



また、11個のIPアドレスをReverse IP lookupsで検索したところ、1,818個のドメイン名が見つかりました。それらの大部分はパークドメインでした。

いくつかの関連ドメイン名には、3つを超える有名ブランドの名前（CNN、Google、Intel、Visa）が含まれていました。以下はその例です。

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

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

これらは、求職者、独立系放送番組の視聴者、不動産投資家またはクレジットカード保有者を標的としたフィッシングや、その他のマルウェアを使用したキャンペーンに登場した可能性があります。

最後に、IoCとされたドメイン名の中に、下表に示すような固有の文字列を含んだものがあることに着目しました。そして、Domains & Subdomains Discoveryで、そうした文字列を含み、かつ複数の異なるトップレベルドメイン（TLD）の下に登録されているドメイン名がどれだけあるか調べました。

IoC	IoCに見られた固有の文字列	固有の文字列を含み、かつ異なるTLDの下に登録されているドメイン名の数
smm2021[.]net	***smm2021.***	4
cabiria[.]biz	***cabiria.***	20
stun[.]site	***stun.***	128
eumr[.]site	***eumr.***	16

いずれもマルウェアのホストであることは確認できませんでしたが、IoCと酷似していることから、不審な活動の兆候がないか注意深く監視する必要があります。

結論

2021年にLorec53のIoCとして特定されたサイト、そして共通のメールアドレス、IPアドレス、または文字列の使用からLorec53のインフラの一部になっていることが疑われるサイトのいくつかは、今も存在し続けています。したがって、Lorec53のリスクはなくなったわけではないようです。特に今回当社が特定した2つの悪意あるドメイン名は、元のIoCのうち2つと同じメールアドレスを使用して登録されたもので、危険だと考えられます。

同様の調査をご希望のお客様、または本調査のデーター式をご希望のお客様は、こちらまでお気軽にお問い合わせください。

付録：アーティファクトとIoCの例

2つのIoCと同じメールアドレスを使って登録されたドメイン名の例

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

IoCとして特定されたドメイン名が名前解決したIPアドレスの例

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

IoCのIPホストを共用していたドメイン名の例

- 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

IoCの一部に含まれていた文字列を含むドメイン名の例

- 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