ヘルスケア関連のIoCをもとにEHRのなりすましを検知

目次

要旨

新型コロナウイルス感染症の広まりにより、医療業界はここ数年大変な目に遭っています。しかし、これによって脅威アクターの攻撃が止むことはなく、複数の医療機関がランサムウェア、データ漏洩、その他のサイバー攻撃の標的にされました。

しかし、早期発見・早期対応により、こうした脅威から医療施設やシステムを保護することは可能です。Armisは「Internet of Medical Things (IoMT) Playbook」の中で、でセキュリティ侵害インジケーター（IoC）の特定をその重要なプロセスとして詳述しています。

WhoisXML APIの研究者は、上記のプレイブックで紹介されていたFBIの速報からデータを収集し、IoCを調査することにしました。特に、民間・公的医療機関を標的としたCubaランサムウェアに関連するIoCのリストを分析、拡充しました。

また、フィッシング攻撃の手段となるサイバースクワッティングドメインを検出するため、Forbesに掲載された電子健康記録（EHR）ソフトウェアの上位企業がDNSにどのように登録されているかを調査しました。その結果、次のことがわかりました。

- 米国のFBIとサイバーセキュリティ・インフラセキュリティ庁（CISA）が共同発表した「サイバーセキュリティ勧告（CSA）」およびAlienVaultのOTXに掲載されたIPアドレスとドメイン名からなる、90を超えるCubaランサムウェアのIoC。
- IoCと同じIPアドレス、ネームサーバー、登録者情報を共有している1,700超のアーティファクトまたは関連ドメイン名。
- これらのアーティファクトの9%は、すでに悪意があることが確認済みのもの。
- EHRソフト開発のトップ企業の名称を含む1,700超のサイバースクワッティングドメイン。そのうち正規の企業に所属していることが公に証明できたのはわずか10個。

CubaランサムウェアのIoC：収集、文脈付け、そしてリスト拡張

Cubaランサムウェアの実行者は、医療を含む重要セクターに属する100超の事業体を攻撃しています。CISAは、サイバー犯罪者が1億4,500万米ドルを要求し、6,000万米ドルの身代金を受け取ったと報告しました。

Cubaランサムウェアに関連したDNSの脅威情報を収集するため、CISAとAlienVaultによって脅威IoCとされた76個のIPアドレスと20個のドメイン名を抽出しました。次にIPアドレスをreverse IP lookupsで検索し、26個の関連プロパティを見つけました。

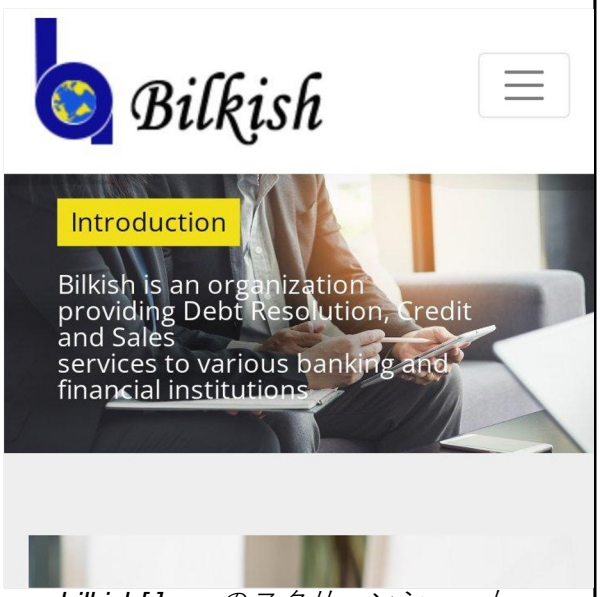
さらに、IoCとされたドメイン名のWHOIS上の繋がりを調べました。当該ドメイン名の現在のWHOISレコードはほとんどが非公開になっていたため、WHOIS History Lookupを使って調べました。その結果、ほぼ全てのドメイン名が2017年後半までWHOISレコードを公開していたことがわかりました。それ以前は、多くが正確な登録者の詳細情報を公開していました。また、ほとんどのIoCは同じネームサーバーを使用していました。

下の表は、 IoCのWHOISレコードに多く見られた情報の例と、それぞれのデータを共有していたドメイン名の数を示しています。

過去のWHOIS情報	そのWHOIS情報を共有していたIoCの数
Name servers: ***.cnmsn.com | ***.msn.com	7
Name servers: ***.xtremeweb.de | ***.xtremeweb.de	7
Registrant name: ***** Ziedonis Registrant email: *****.ziedonis@mail.lv	3
Registrant name: ***** Kazuewsky Registrant email: *****kazuewsky@gazeta.pl	4

この文脈情報をもとにreverse WHOIS searchesで調べたところ、関連しているドメイン名を1,731個発見しました。それらのドメイン名は、ある時点においてIoCと同じネームサーバー、登録者名、メールアドレスを使っていたことがわかりました。

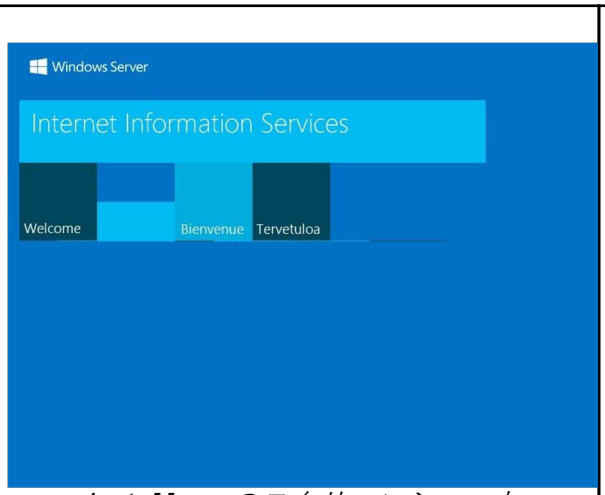
そして、IPアドレスの名前解決とWHOISのデータにより、CubaランサムウェアのIoCに関連した1,757個のドメイン名を特定しました。それらのうち約9.4%は悪意があるドメイン名としてフラグが立てられていました。また、悪意あるドメイン名の一部は、以下のように有効なウェブサイトをホストしていました。



bilkish[.]comのスクリーンショット

lucas[.]atのスクリーンショット

悪意ありと報告されていない一部のドメイン名を使った不審なコンテンツも見つけました。例えば、anigota[.]comはWindowsにそっくりなウェブサイトをホストしており、jussionsharepoint[.]comは、Microsoftの公式アプリを模倣した複数のアプリケーションを提供しているように見えました。それらのウェブサイトのスクリーンショットを以下に示します。



anigota[.]comのスクリーンショット

jussionsharepoint[.]comのスクリーンショット

この種のコンテンツは非常に重要な情報を私たちに提供してくれます。というのは、アプリケーションのトロイの木馬版をホストすることで知られているRomComの脅威アクターと、Cubaランサムウェアが結びついている可能性があるとCISAが警告したためです。

フィッシング手段になり得るEHRソフトウェアベンダーのなりすまし

Cubaランサムウェアなどの脅威アクターが標的のシステムに最初にアクセスする方法の一つに、フィッシングがあります。サイバースクワッティングドメインは、よく使われるフィッシングの手段です。

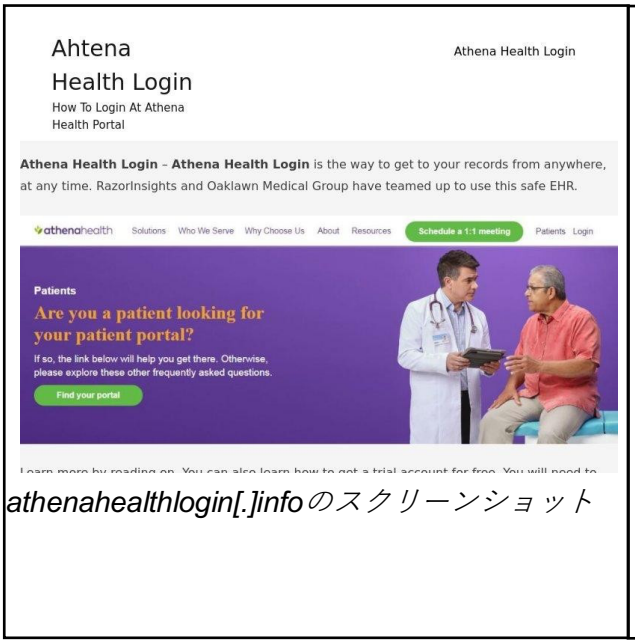
医療業界では、EHRソフトウェアベンダーのなりすまし、すなわち脅威アクターがEHRソフトウェアベンダーのドメイン名を真似たドメイン名を登録する、といった攻撃が考えられます。当社のDomains & Subdomains Discoveryを使用して、そのようなドメイン名を1,743個発見しました。

これらのドメイン名は、AdvancedMD EHR、AthenaHealth、DrChrono、eClinicalWorks、Kareo Clinical、Netsmart myUnity、NextGen、Practice Fusionなど、Forbesが挙げた上位のEHRソフトウェアプロバイダーを詐称しています。下の表は、各企業の下で確認されたサイバースクワッティングドメインの数と、使用された検索文字列を示したものです。

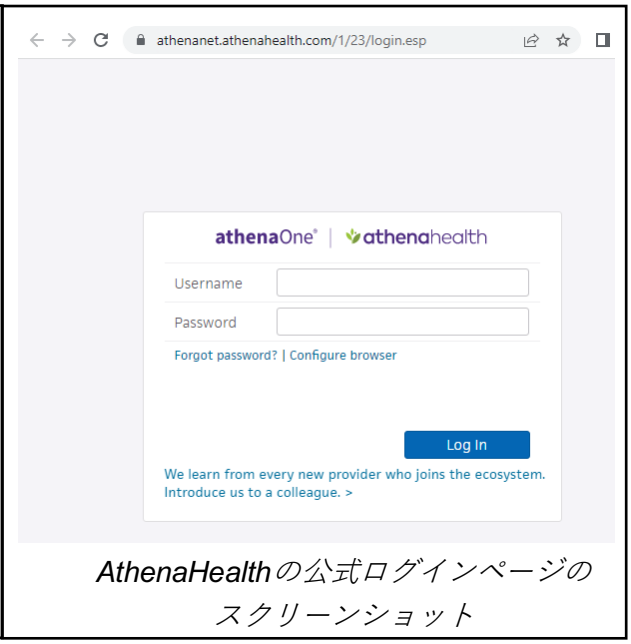
EHRソフトウェアプロバイダー	正規のドメイン名	使用された検索文字列	確認されたサイバークワッティングドメインの数
AdvancedMD EHR	advancedmd[.]com	***advancedmd***	119
AthenaHealth	athenahealth[.]com	***athenahealth***	313
DrChrono	drchrono[.]com	***drchrono***	73
eClinicalWorks	eclinicalworks[.]com	***eclinicalworks***	138
Kareo Clinical	kareo[.]com	***kareo* (excluding *kareoke*)**	713
Netsmart myUnity	ntst[.]com	***ntst* + *unity***	61
NextGen	nextgen[.]com	***nextgen* + *health***	204
Practice Fusion	practicefusion[.]com	***practicefusion***	122

WHOISの登録者情報からEHRソフトウェアベンダーに帰属していることが確認できたのは、それらのドメイン名のうち10個にとどまっています。また、2つはすでに悪意があるドメイン名として報告されていました。

また、複数のサイバースクワッティングドメインが不審なコンテンツをホストしていました。例えば、athenahealthlogin[.]infoは、AthenaHealthのブランドカラーとログイン要素を真似たページをホストしていました。しかし、正規のAthenaHealthのログインページはサブドメインでホストされており、デザインも異なるものでした。以下は、2つのサイトを比較したものです。



*athenahealthlogin[.]info*のスクリーンショット



*AthenaHealth*の公式ログインページのスクリーンショット

—

IoCの特定は、サイバー攻撃の検知および防止に有用です。しかし、IoCとしてタグ付けされたIPアドレスとドメイン名のほとんどは、脅威アクターが散発的に使用し得るより大きなインフラの一部にすぎません。そうしたプロパティにIPアドレスの名前解決とドメイン名所有者の文脈情報を加えることで、悪意あるインフラストラクチャをより網羅的に把握できます。

同様の調査をご希望のお客様、またはこの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

Cubaランサムウェアの IoCの例

- 193[.]23[.]244[.]244
- 94[.]103[.]9[.]79
- 192[.]137[.]101[.]46
- 92[.]222[.]172[.]39
- 92[.]222[.]172[.]172
- 10[.]13[.]102[.]1
- 10[.]13[.]102[.]58
- 10[.]133[.]78[.]41
- 10[.]14[.]100[.]20
- 103[.]114[.]163[.]197
- aaa[.]stage[.]16549040[.]dns[.]alleivic e[.]com
- witorophron[.]com
- vu42i55fqimjx6koo7oqh3zzvy2xghq e7ot4h2ftcv2pimbauupjyqyd[.]onion
- tycahatit[.]ru
- torsketronand[.]ru
- toftoflethens[.]com

- tinheranter[.]com
- thehentoftbet[.]ru
- tandugolastsp[.]com
- reninparwil[.]com

CubaランサムウェアのIoCとIPアドレスおよびWHOISデータが共通しているアーティファクトの例

- a[.]tk8001[.]tk
- 149-255-35-131[.]static[.]hvvc[.]us
- 23-227-198-246[.]static[.]hvvc[.]us
- boswars[.]com
- boswars[.]org
- csail[.]seul[.]org
- dfvpn2[.]com
- down1[.]fala8001[.]tk
- durin[.]csail[.]mit[.]edu
- freehaven[.]net
- gravyblicus[.]com
- mixminion[.]net
- moria[.]seul[.]org
- ns1[.]certlogins[.]com
- ns1[.]gravyblicus[.]com
- ns2[.]certlogins[.]com
- ns2[.]cypherpunks[.]ca
- ns2[.]paip[.]net
- quishbyleby2[.]com
- rookbolin[.]net
- seul[.]org
- tk8001[.]tk
- vds2364993[.]my-ihor[.]ru
- worldforge[.]org
- wrens[.]seul[.]org
- yachtdreaming[.]com
- jomet[.]fi
- tambest[.]com
- tambest[.]fi
- autohaus-maeke[.]de
- huster[.]de
- autohaus-tolzin[.]de
- pg-boerde[.]de
- evergreencar[.]de
- autos-weber[.]de
- boschservice-maeke[.]de
- ntpwr[.]de
- eileen[.]fr
- t80[.]org
- lemper[.]biz
- lemper-shop[.]de
- lemper-mode[.]de
- autohaus-georg-maulhardt[.]de
- autohaus-seydel[.]de
- koch-falkenberg[.]de
- fama-greussen[.]de
- maeke-autohaus[.]de
- b-hs[.]de
- teggra[.]com[.]mx
- teggra[.]mx
- ausdermitte-binz[.]de
- fdgb-apartments[.]de
- appartementservice-ruegen[.]de
- france-irlande[.]com
- blackbeltit[.]fi
- wakkao[.]com
- peterson[.]nu
- shkatulka[.]de
- lasimitta[.]fi
- autohaus-maulhardt[.]de
- ah-seidel-wildenfels[.]de
- foamit[.]fi
- salonace[.]fi
- xtremeweb[.]de
- kaltenbach-edv[.]biz
- glitzeria[.]biz
- feeniksbasket[.]fi
- sheldon4vt[.]org

- cityinn-magdeburg[.]de
- kultanenworks[.]fi
- dog[.]bg
- viikinkisauna[.]fi
- lucas[.]at
- protocol9[.]net
- anigota[.]hr
- pinkmoon[.]hr
- sheldon4vt[.]com
- saveewsd[.]org
- hfly[.]com[.]br
- shelden4vt[.]org
- mnmanufacturing[.]biz
- wauzzz[.]ch
- cyberalex[.]org
- nespor[.]uk
- weavers[.]com[.]br
- octopus-ice[.]de
- shelden4vt[.]com
- cuddly[.]monster
- jph[.]icu
- jontyhewlett[.]co[.]uk
- east-md[.]de
- matli[.]net
- thalers[.]at
- shelden[.]org
- tidey[.]co[.]uk
- larisch-dachdesign[.]at
- jh-elektrohandel[.]de
- sely[.]org
- stallcenter[.]com
- okkonen[.]net

2023年3月8日時点で確認された悪意あるアーティファクトの例

- 149-255-35-131[.]static[.]hvvc[.]us
- 23-227-198-246[.]static[.]hvvc[.]us
- lucas[.]at
- detoxninelife[.]ru
- stealsgrowlite[.]ru
- bilkish[.]com
- wronhatsotons[.]ru
- monsterfoxlite[.]ru
- many-date[.]ru
- ketteoneand[.]ru
- wihisheckfa[.]ru
- vathankezas[.]ru
- wogudahert[.]ru
- suphersun[.]ru
- tersintertug[.]ru
- downdintwiltit[.]ru
- littbutlolet[.]ru
- johngasebed[.]ru
- kedhisandheg[.]ru
- dinthisorca[.]ru
- rinressofhedt[.]ru
- siandrerep[.]ru
- toldkedrinheck[.]ru
- tedahopa[.]ru
- henmefagu[.]ru
- hapterhertbe[.]ru
- lonemoning[.]ru
- dleftronanow[.]ru
- lacdileftre[.]ru
- wendortales[.]ru
- shineworlds[.]ru
- woattorstal[.]ru
- wittonshedspar[.]ru
- tersefehow[.]ru
- xablopefgr[.]ru
- superdatew[.]ru
- rechedtthaten[.]ru
- ratlighletdidn[.]ru
- solohaly[.]ru
- rithatteevent[.]ru
- retforhapta[.]ru
- weksrubaz[.]ru
- reftesitor[.]ru
- superdates[.]ru

- sedsoceheg[.]ru
- superdatel[.]ru
- redsofrefsa[.]ru
- rongaboty[.]ru
- justiddirom[.]ru
- andrinredin[.]ru

EHRのトップベンダーを標的にしたサイバースクワッティングドメインの例

- advancedmd[.]ca
- advancedmd[.]io
- advancedmd[.]cm
- advancedmd[.]me
- advancedmd[.]us
- advancedmd[.]gr
- advancedmd[.]co
- advancedmd[.]au
- advancedmd[.]de
- advancedmd[.]cn
- advancedmd[.]eu
- advancedmd[.]dev
- advancedmd[.]vip
- athenahealth[.]in
- athenahealth[.]ws
- athenahealth[.]ru
- athenahealth[.]uk
- athenahealth[.]nl
- athenahealth[.]la
- athenahealth[.]hu
- athenahealth[.]us
- athenahealth[.]eu
- athenahealth[.]cn
- athenahealth[.]co
- athenahealth[.]io
- athenahealth[.]ph
- drchrono[.]de
- drchrono[.]tk
- drchrono[.]cn
- drchrono[.]in
- drchrono[.]nl
- drchrono[.]cm
- drchrono[.]ai
- drchrono[.]ru
- drchrono[.]io
- drchrono[.]us
- drchrono[.]ca
- drchrono[.]co
- drchrono[.]ph
- eclinicalworks[.]ae
- eclinicalworks[.]at
- eclinicalworks[.]uk
- eclinicalworks[.]de
- eclinicalworks[.]ga
- eclinicalworks[.]in
- eclinicalworks[.]fr
- eclinicalworks[.]co
- eclinicalworks[.]eu
- eclinicalworks[.]cc
- eclinicalworks[.]cn
- eclinicalworks[.]us
- eclinicalworks[.]cm
- kareo[.]eu
- kareo[.]ml
- kareo[.]ru
- kareo[.]uk
- kareo[.]pl
- kareo[.]fr
- kareo[.]ca
- kareo[.]it
- kareo[.]cf
- kareo[.]ga
- kareo[.]cm
- kareo[.]in
- kareo[.]fi
- entstcommunity[.]ws

- entstcommunity[.]org
- cantstop[.]community
- unityentstudio[.]com
- unitypointstore[.]com
- unityentstudios[.]com
- cantstopcommunity[.]com
- unitypointstorage[.]com
- unitypointstlukes[.]org
- communityeventstv[.]com
- unitypointstlukes[.]com
- frontstreet[.]community
- clientstocommunity[.]com
- nextgen[.]health
- nextgenhealth[.]de
- nextgenrx[.]health
- nextgenhealth[.]co
- nextgenhealth[.]us
- nextgenhealth[.]ga
- nextgenhealth[.]in
- healthnextgen[.]in
- nextgenhealth[.]com
- nextgenhealth[.]org
- nextgenhealth[.]net
- healthnextgen[.]com
- healthynextgen[.]com
- practicefusion[.]ph
- practicefusion[.]my
- practicefusion[.]ws
- practicefusion[.]xn--node
- practicefusion[.]uk
- practicefusion[.]nl
- practicefusion[.]sg
- practicefusion[.]xn--fiqz9s
- practicefusion[.]xn--fiqs8s
- practicefusion[.]xn--kprw13d
- practicefusion[.]xn--mxtq1m
- practicefusion[.]cm
- practicefusion[.]jp