Beyond Healthcare IoCs: Threat Expansion and EHR Impersonation Detection

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts and IoCs

Executive Report

The healthcare industry has had a rough couple of years since the COVID-19 pandemic started. But this didn't stop threat actors from attacking the sector, with several healthcare organizations targeted by ransomware, data breach, and other cyber attacks.

Early detection and response can help protect medical facilities and systems, starting with identifying indicators of compromise (IoCs)—a critical process detailed by Armis in their Internet of Medical Things (IoMT) Playbook.

Inspired by this, WhoisXML API researchers decided to investigate the IoCs by gleaning data from one of the Federal Bureau of Investigation (FBI) flash reports identified in the playbook. In particular, we analyzed and expanded the list of IoCs related to Cuba ransomware, which targeted private and public healthcare organizations, among many others.

We also investigated how the top electronic health record (EHR) software companies listed by Forbes were represented in the DNS to detect cybersquatting domains that could serve as vehicles for phishing attacks. Among our key findings are:

- 90+ Cuba ransomware IoCs comprising IP addresses and domain names published by the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) in their joint Cybersecurity Advisory (CSA) and on AlienVault OTX
- 1,700+ artifacts or connected domains that share the IoCs' IP hosts and name server and registrant details
- 9% of these artifacts were already flagged as malicious
- 1,700+ cybersquatting domains containing the names of the top EHR software providers, only 10 of which could be publicly attributed to legitimate companies

Cuba Ransomware IoCs: Collection, Contextualization, and Expansion

Cuba ransomware actors have attacked more than a hundred entities in critical sectors, including healthcare. CISA reported that the cybercriminals demanded US$145 million and received US$60 million in ransom payments.

To gather targeted DNS threat intelligence relevant to Cuba ransomware, we collected 76 IP addresses and 20 domains tagged as threat IoCs by CISA and AlienVault. We then subjected the IP addresses to reverse IP lookups and found 26 related properties.

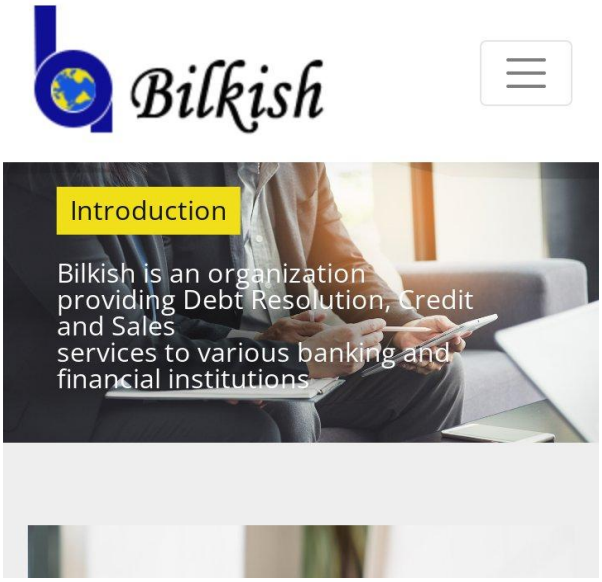
Next, we sought to obtain the WHOIS associations of the domains identified as IoCs. Since most of their current WHOIS records were redacted, we turned to WHOIS History Lookup and found that almost all had public WHOIS records until late 2017. Before that, many of them shared the exact registrant details. Most of the IoCs also used the same name servers.

The table below shows some of the recurring WHOIS record details among the IoCs and the number of domains sharing them.

Historical WHOIS Details	Number of IoCs Sharing the Record Details
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

Armed with this contextual information, we performed reverse WHOIS searches that yielded 1,731 connected domains. These properties shared the IoCs' name server, registrant name, and email address at one point in their registration.

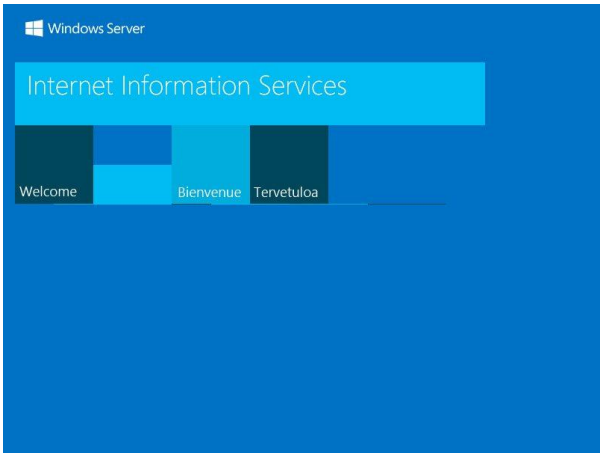
We found 1,757 artifacts connected to the Cuba ransomware IoCs via IP resolution and WHOIS record details. About 9.4% of these artifacts were flagged as malicious. A couple of these malicious domains actively hosted live websites as shown below.



Screenshot of bilkish[.]com

Screenshot of lucas[.]at

We also detected suspicious content hosted on some of the artifacts that haven't been reported as malicious. For instance, anigota[.]com hosted a Windows look-alike website, while jussionsharepoint[.]com appeared to offer several applications possibly imitating official Microsoft apps. The website screenshots are shown below.



Screenshot of anigota[.]com

Screenshot of jussionsharepoint[.]com

These types of content can provide essential details since CISA warned that Cuba ransomware might have ties with the RomCom threat actors who are known to host Trojanized versions of legitimate applications.

EHR Software Vendor Impersonation: Possible Phishing Attack Vehicles

One of the ways the Cuba ransomware or other threat actors for that matter gain initial access to target systems is through phishing. Cybersquatting domains are common phishing vehicles.

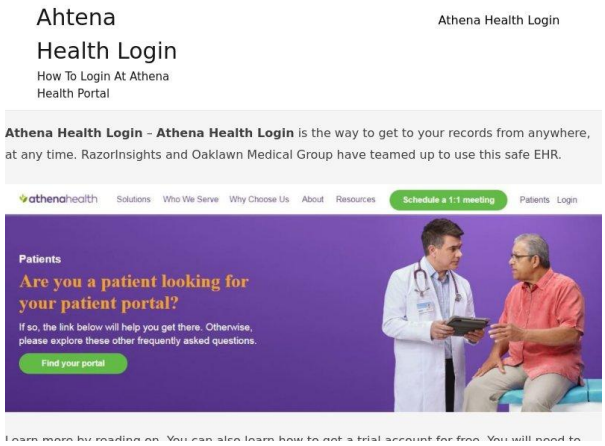
For the healthcare industry, the possible attacks include EHR software provider impersonation, where threat actors register domains that imitate the EHR software vendor's domain. We found 1,743 such domains using Domains & Subdomains Discovery.

These domains spoofed the top EHR software providers named by Forbes, including AdvancedMD EHR, AthenaHealth, DrChrono, eClinicalWorks, Kareo Clinical, Netsmart myUnity, NextGen, and Practice Fusion. The table below shows the number of cybersquatting domains found under each company and the search string used.

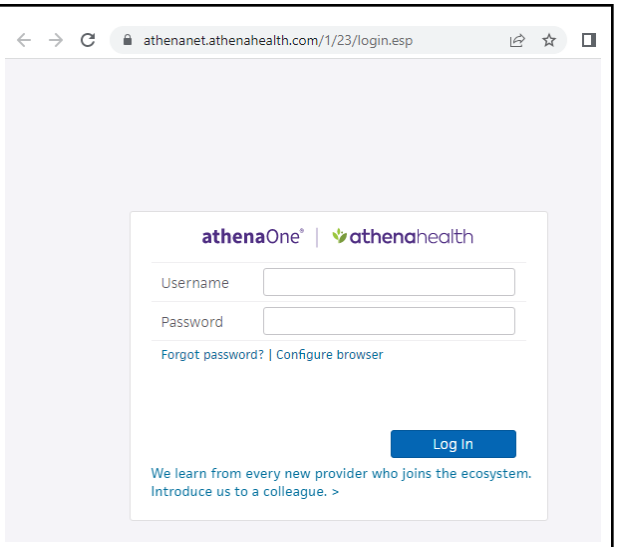
EHR Software Provider	Official Domain	Search String Used	Number of Cybersquatting Domains Found
AdvancedMD EHR	advancedmd[.]com	***advancedmd***	119
AthenaHealth	athenahealth[.]com	***athenahealth***	313
DrChrono	drchrono[.]com	***drchrono***	73
eClinicalWorks	eclinicalworks[.]com	***eclinicalworks***	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

Only 10 of these cybersquatting domains could be publicly attributed to the imitated EHR software vendor based on their WHOIS registrant details. Furthermore, two cybersquatting domains were already reported as malicious.

Several cybersquatting domains actively hosted questionable content. For example, athenahealthlogin[.]info featured AthenaHealth's brand colors and login elements. However, the legitimate AthenaHealth login page was hosted on a subdomain and had a different design. Below is a side-by-side comparison of the two sites.



Screenshot of athenahealthlogin[.]info



Screenshot of the official login page of AthenaHealth

—

Identifying IoCs can help security teams and solutions detect and prevent cyber attacks. However, most IP addresses and domains tagged as IoCs are part of a larger infrastructure that threat actors may use sporadically. Providing IP resolution and ownership context to these properties can help map out malicious infrastructures, enabling security teams and solutions to have a broader view of the threat.

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 Cuba Ransomware IoCs

- 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[.]alleivice[.]com
- witorophron[.]com
- vu42i55fqimjx6koo7oqh3zzvy2xghqe7ot4h2ftcv2pimbauupjyqyd[.]onion
- tycahatit[.]ru
- torsketronand[.]ru
- toftoflethens[.]com

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

Sample Artifacts Sharing Cuba Ransomware IoCs' IP Host and WHOIS Details

- 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

Sample Malicious Artifacts as of 8 March 2023

- 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

Sample Cybersquatting Domains Targeting the Top EHR Software Vendors

- 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