

HEALTHCARE | STILL RANSOMED

Since early 2022, leading security industry experts have made broad estimations that ‘ransomware is on the decline’, but did they properly contextualize their data and findings? Given destabilization from the Russia-Ukraine conflict and tightening U.S. and EU law enforcement activities, ‘ransomware is on the decline’ proponents underestimate their adversaries’ motivations, resiliency, and abilities to support persistent criminal operations.

This is daunting to diagnose at-scale across industries and verticals; however, industry specific observations offer evidence that the ransomware threats are still very real in the Healthcare sector.

Industry specific observations offer evidence that the ransomware threats are still very real in the Healthcare sector.

1. U.S. Healthcare targets continue to see heavy threat actor targeting in 2022

ACTOR	2022 PUBLISHED VICTIM	ACTOR	PUBLISHED VICTIM
4C3	EAST TENNESSEE CHILDREN HOSPITAL	HIVE	RAVECO MEDICAL
ALPHV	FAST PACE HEALTH	HIVE	SUPERNUS PHARMACEUTICAL
ALPHV	ALLIANT PHYSICAL THERAPY	HIVE	MAS & CORONIS HEALTH
AVOS LOCKER	AVAMERE HEALTH	HIVE	GREENWAY HEALTH
AVOS LOCKER	CHRISTUS HEALTH	HIVE	DISKRITER
AVOS LOCKER	JACKSONVILLE SPINE CENTER	HIVE	FIRST CHOICE COMMUNITY HEALTHCARE
AVOS LOCKER	MCKENZIE HEALTH SYSTEM	KARAKURT	CENTURY DENTAL ASSOCIATES
BIANLIAN	ALEGRIA FAMILY SERVICES	KARAKURT	SHIELDS HEALTHCARE
BIANLIAN	COMMUNITY DENTAL PARTNERS	KARAKURT	METHODIST MCKINNEY HOSPITAL
BLACKBYTE	GATEWAY REHAB	KARAKURT	METHODIST CRAIG RANCH CENTER
BLACKBYTE	LAMOILE HEALTH	LOCKBIT	FAMILY CLINIC
BLOODY	PRIMARY CARE OF LONG ISLAND	LOCKBIT	VAL VERDE REGIONAL
BLOODY	ONCALLPRACTICE[.]COM	LOCKBIT	TAGUE FAMILY PRACTICE
BLOODY	BRIGHTER DENTAL CENTER	LOCKBIT	DESTINATION HOPE
CONTI	SPINE DIAGNOSTIC & PAIN TREATMENT	LOCKBIT	QUALITY MEDICAL
CONTI	CYTOMETRY SPECIALISTS INC. D/B/A CSI LABORATORIES	LOCKBIT	COASTLMEDPS
DAIXIN	FITZGIBBON HOSPITAL	LOCKBIT	CHRISTIANA SPINE CENTER
DATALEAKBLOG	ALLWELL BEHAVIORAL HEALTH	LORENZ	WOLFE EYE CLINIC
DATALEAKBLOG	CARILLON ASSISTED LIVING	ONYX/VOSP	ADVANTAGE DIRECT
DON#T ...:LEAKS::	MONARCH NC	ONYX/VOSP	WAYNE FAMILY PRACTICE
HIVE	NCG MEDICAL	RANSOMHOUSE	SUMMIT CARE
HIVE	PARTNERSHIP HEALTHPLAN	SNATCH	ATLANTIC DIALYSIS
HIVE	BATON ROUGE GENERAL	SNATCH	CAREFIRST
HIVE	SERV BEHAVIORAL HEALTH SYSTEM	SNATCH	ALTRUS MEDICAL
HIVE	LAVAN & NEIDENBERG	SUNCRYPT	OKLAHOMA CITY INDIAN CLINIC (OKCIC)
HIVE	GOODMAN CAMPBELL SPINE	VICE SOCIETY	FAMILY MEDICINE CENTER
HIVE	FAMILY CHRISTIAN HEALTH CENTER	VICE SOCIETY	BSA HOSPICE OF THE SOUTHWEST

Figure 1. Current published victims as of Sep 2, 2022

2. What's 'not reported', and 'unmasked actors' obscure the true actual size of the problem

[Bishop Eye Center \(mass.gov\)](#)

[Carolina Behavioral Health Alliance \(Wake Forest University and Baptist Medical Center\)](#)

[FPS Medical Center](#)

[Kevin Wolf, DPM d/b/a Goldsboro Podiatry](#)

[Memorial Hospital of Carbon County](#)

[Molecular Pathology Laboratory Network](#)

[OmniCell \(mass.gov\)](#)

[OneTouchPoint \(oag.ca\)](#)

[Onyx Technology](#)

[Orthopedic Associates of Hawaii, All Access Ortho and Specialty Suites d/b/a Minimally Invasive Surgery of Hawaii](#)

[Practice Resources, LLC](#)


[Professional Finance Company](#)

[Wheeling Health Right](#)

[Yuma Regional Medical Center](#)

3. European and International Healthcare is also 'on fire' in 2022

- a. Supply chain attack via Advanced software by unknown actors crippled U.K.'s NHS '111' emergency services and risks [millions of U.K. patients' Carenotes Electronic Patient Record \(EPR\)](#)



advanced MyWorkplace Products IT Services Solutions Resources Company Q 🌐 | Existing Customers

Adastra Security Incident Updates

Status Update - 19th Aug 2022

Recovery Update

For **NHS 111 customers using Adastra** we have now completed our internal security assurance activity and will be sharing evidence with NHS and NCSC for review. Once the evidence provides a high confidence level this will be communicated through via the NHS England EPRR incident management team and customers will be able to reconnect in line with the process set out by NHS England. Monday next week we will be moving forward with the phased process of bringing these organisations back online. The order in which providers reconnect to Adastra is being set by the NHS England EPRR Incident Management Team, which has communicated its process to all relevant users. For our Adastra OOH Customers, we will be working to share a more detailed recovery plan next week.

Forensic Investigation

Our forensic investigation is progressing in line with our timeline and plan. We are now building a much clearer picture of the incident's root-cause and will soon be in a position to confirm and share Indicators of Compromise (IOCs) with customers on request. In parallel, our third-party experts are well advanced in their investigation into any potential data impact as a result of the incident. We will update customers as appropriate and comply with any applicable notification obligations.

We recognise that this has been a challenging time for our customers, and we appreciate your patience and understanding as we work to recover from this attack. We continue to prioritise the safety and security in all of our decision making and are approaching this restoration process with diligence and rigour.

Figure 2. Advanced incident notifications (oneadvanced.com)

b. Late 2021 set the stage, evident via [Hive published chats with Spanish victim, of Center D'Odontologia Integrada Miret-Puig](#)



Hive

Centre D'Odontologia Integrada Miret-Puig
Disclosed

Centre D'Odontologia Integrada Miret-Puig

We are a dental clinic established in Mollerussa that has professionals with extensive experience, always at the technical forefront, which is why we are able to offer the latest treatments when it comes to solving any oral health problem. Our diagnostic tools include modern and minimally invasive methods such as a digital radiology system and a CT scanner, which allows us to perform three-dimensional images, essential in complicated cases of surgery and implantology. This equipment, together with our fish modeling system, allows the realization of implants in just one day. Our goal: to offer a personalized and close treatme

- **Website**[clinicadentalmollerussa.com](#)
- **Tax Number**B25706813
- **Revenue**\$10M
- **Employees**200

Uploaded Files

- [ACVAC.doc](#) 42.5 Kb
- [ASEMB.xls](#) 10.8 Kb
- [3BzJEKBytXurIIcAvNOVxNJZCU1fv18EIpY83BitDRBn_key.jkfn](#) 3.6 Mb

Figure 3. Hive blog

c. International healthcare-related extortion and ransomware victims abound in 2022

[ProvinciaHospital Center Sud Francilien \(LockBit, \\$10M\)](#)

[Benlaux group \(unk, \\$2M ransom\)](#)

[I Health Authority of Messina \(LockBit, .5M\)](#)

[Fatebenefratelli Sacco Territorial Social Healthcare](#)

[Companies \(Vice Society\)](#)

[Hospital Centro de Andalucia \(unk\)](#)

[Argentinian Health Services \(LockBit\)](#)

[Obra Social Seguros \(Vice Society\)](#)

[Local Health Authority 3 Naples South \(54bb47h\)](#)

[Health Protection Agency Insubria \(BlackByte\)](#)

[SaludTotal EPS-S \(Vice Society\)](#)

[Clinica Integral de Emergencias Laura Daniela \(Snatch\)](#)

[Local Health Authority of City of Turin \(unk\)](#)

[GHT Coeur Grand Est. Hospitals \(Vice Society\)](#)

[Hospital San José, Las Palmas De Gran Canaria \(LockBit\)](#)

[Magnachem \(BianLian\)](#)

[Galencia Pharmaceutical Laboratories \(LockBit\)](#)



Figure 4: Vice Society ransom note

d. Italian hospitals have seen prolific ransomware impact thus far in 2022

ACTOR	2022 ITALIAN HOSPITAL VICTIMS	ACTOR	2022 ITALIAN HOSPITAL VICTIMS
54BB47H	PRESIDIO OSPEDALIERO NOLA	LOCKBIT	PRESIDIO OSPEDALIERO SANT'AGATA – MILITELLO
54BB47H	STABILIMENTO DI POLLENA TROCCHIA	LOCKBIT	PRESIDIO OSPEDALIERO SAN SALVATORE – MISTRETTA
54BB47H	STABILIMENTO DI GRAGNANO	VICE SOCIETY	OSPEDALE LUIGI SACCO - POLO UNIVERSITARIO - MILANO
54BB47H	PRESIDIO OSPEDALIERO SANTA MARIA DELLA MISERICORDIA	VICE SOCIETY	OSPEDALE DEI BAMBINI VITTORE BUZZI - MILANO
54BB47H	PRESIDIO OSPEDALIERO VICO EQUENSE	VICE SOCIETY	OSPEDALE FATEBENEFRAPELLI E OFTALMICO - MILANO
54BB47H	PRESIDIO OSPEDALIERO MARESCA – TORRE DEL GRECO	VICE SOCIETY	OSPEDALE MACEDONIO MELLONI – MILANO
54BB47H	PRESIDIO OSPEDALIERO BOSCONTRECASE	UNK	OSPEDALE OFTALMICO – TORINO
54BB47H	PRESIDIO OSPEDALIERO CASTELLAMMARE DI STABIA	UNK	OSPEDALE GIOVANNI BOSCO – TORINO
LOCKBIT	PRESIDIO OSPEDALIERO SAN VINCENZO - TAORMINA	UNK	OSPEDALE MARIA VITTORIA – TORINO
LOCKBIT	PRESIDIO OSPEDALIERO GIUSEPPE FOGLIANI – MILAZZO	UNK	PRESIDIO OSPEDALIERO MARTINI – TORINO
LOCKBIT	PRESIDIO OSPEDALIERO LIPARI	UNK	DISTRETTO NORD-OVEST - TORINO
LOCKBIT	PRESIDIO OSPEDALIERO CUTRONI ZODDA – BARCELLONA	UNK	ISTRETTO NORD-EST - TORINO
LOCKBIT	PRESIDIO OSPEDALIERO IGNAZIO ROMEO - PATTI	UNK	DISTRETTO SUD-OVEST - TORINO

Figure 5. Impacted Italian Hospitals

4. Reporting from U.S. Health and Human Services (HHS) publicly expose impact of ongoing threats

- a. [August 29, 2022 - Evil Corp Threat Profile - PDF*](#)
- b. [August 24, 2022 - Karakurt Threat Profile Analyst Note - PDF*](#)
- c. [HHS Breach Tool](#)

Breach Report Results							
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Methodist McKinney Hospital	TX	Healthcare Provider	110244	08/26/2022	Hacking/IT Incident	Network Server
	Methodist Craig Ranch Surgical Center	TX	Healthcare Provider	15157	08/26/2022	Hacking/IT Incident	Network Server
	First Street Family Health	CO	Healthcare Provider	7310	08/26/2022	Hacking/IT Incident	Network Server
	One Medical, Inc.	TX	Healthcare Provider	1009	08/25/2022	Theft	Paper/Films
	US Able Mutual Insurance Company d/b/a Arkansas Blue Cross and Blue Shield	AR	Health Plan	8871	08/25/2022	Hacking/IT Incident	Network Server
	Health Advantage	AR	Health Plan	1642	08/25/2022	Hacking/IT Incident	Network Server
	EmergeOrtho	NC	Healthcare Provider	68661	08/25/2022	Hacking/IT Incident	Network Server
	General Health System	LA	Healthcare Provider	501	08/25/2022	Hacking/IT Incident	Network Server
	Warner Norcross and Judd, LLP	MI	Business Associate	255160	08/24/2022	Hacking/IT Incident	Network Server
	Henderson & Walton Women's Center, P.C.	AL	Healthcare Provider	34306	08/23/2022	Hacking/IT Incident	Email
	Prowers County Hospital District	CO	Healthcare Provider	1205	08/22/2022	Hacking/IT Incident	Network Server
	Cerebral Medical Group, P.A.	CA	Healthcare Provider	6110	08/19/2022	Unauthorized Access/Disclosure	Paper/Films
	Celanese Medical Plan	TX	Health Plan	704	08/19/2022	Unauthorized Access/Disclosure	Email
	Medical Mutual of Ohio	OH	Health Plan	1377	08/17/2022	Hacking/IT Incident	Network Server
	San Diego American Indian Health Center	CA	Healthcare Provider	27367	08/15/2022	Hacking/IT Incident	Network Server
	Novant Health Inc. on behalf of Novant Health ACE & as contractor for NMG Services Inc.	NC	Business Associate	1362296	08/14/2022	Unauthorized Access/Disclosure	Electronic Medical Record
	OMNI Healthcare, INC	FL	Healthcare Provider	1000	08/14/2022	Unauthorized Access/Disclosure	Electronic Medical Record
	Priti Patel Physician PC	NY	Healthcare Provider	6877	08/14/2022	Hacking/IT Incident	Network Server
	Overlake Medical Center & Clinics	WA	Healthcare Provider	557	08/12/2022	Hacking/IT Incident	Network Server
	Common Ground Healthcare Cooperative	WI	Health Plan	133714	08/12/2022	Hacking/IT Incident	Network Server
	Valley Baptist Medical Center – Harlingen	TX	Healthcare Provider	11137	08/12/2022	Hacking/IT Incident	Network Server
	Valley Baptist Medical Center - Brownsville	TX	Healthcare Provider	7496	08/12/2022	Hacking/IT Incident	Network Server
	Onyx Technology LLC	MD	Business Associate	96814	08/12/2022	Hacking/IT Incident	Network Server
	Conifer Revenue Cycle Solutions, LLC	TX	Business Associate	134948	08/12/2022	Hacking/IT Incident	Email

Figure 6. Aug 2022 breach notifications

5. [Conti](#) assets have either landed with previous affiliates (karakurt) or sparked new ransomware gangs ([blackbasta](#), blackbyte, quantum), and “Medical targets pay very well”

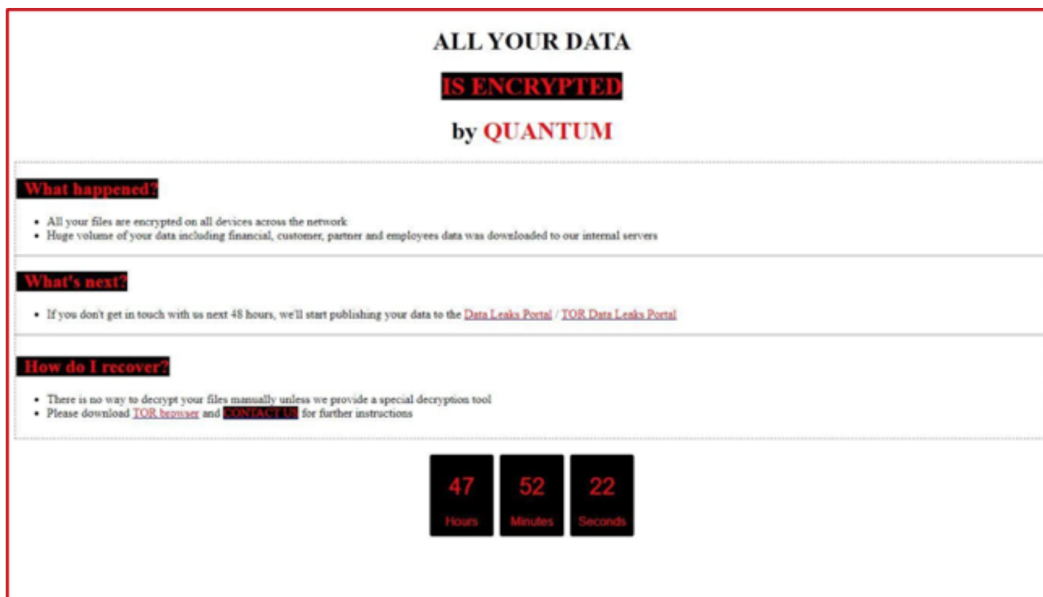


Figure 7. Quantum ransomware notification

6. BONUS - new cyber extortion groups targeting healthcare continue to emerge
- ['Bl00dy' ransomware group](#) hits New York (U.S.) medical practices and openly recruits
 - ['Agenda' ransomware group](#) targets overseas medical sector
 - [Daixin hits Missouri's Fitzgibbon Hospital](#)
 - [North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare](#)
 - Monarch NC, mental health services hit by new ransomware group 'DON#T__::LEAKS::'
 - [LionKebab threat actors looking to ransomware Chinese infrastructure?](#)
 - Extortion and ransom won't go out of style while soft lucrative targets persist

Industry 'experts' and other proponents of '**ransomware is on the decline**' take note; Healthcare Industry specific observations offer evidence that the ransomware threats are still very real.

ABOUT US

Red Sense, LLC is a veteran-owned small business (VOSB), that monitors and tracks significant events and forces within the Security space in order to provide our customers with deep insight into the myriad of new technologies, threat actors, software vulnerabilities and exploits, and sometimes suspect vendor sales pitches. RedSense offers vendor-agnostic and objective counsel to help address the evolving Security and Intelligence spaces.