54bb47h BLOG

ASL Napoli 3 Sud Network Seized

54BB47H TEAM / JANUARY 12, 2022 / DATA LEAK

On 2022-01-07, the computer network of the regional healthcare provider ASL Napoli 3 Sud (https://www.aslnapoli3sud.it, site is down) was successfully hacked.
During the hacking, we stole absolutely all personal data, databases, financial documents and other important data. Subsequently, the virtual machines on 42 HYPER-V servers were encrypted with a military-grade encryption protocol, for a total of about 240 virtual machines based on windows, linux and other operating systems. That is 90% of all their essential infrastructure (See appendix Report).
Some of their systems were protected by the IDS Cortex XDR system (https://www.paloaltonetworks.com/cortex/cortex-xdr).

As far as we know, this provider is a regional company funded by the Italian state. An important aspect of its work is the protection of personal and medical data. As a result, we can say that neither the IT team nor the IDS Cortex XDR coped with the task and were unable to successfully protect the network perimeter and internal resources. The insurance company is in no hurry to eliminate the threat of the

spread of personal data. Now the only thing they are doing is to hide the results of the operation.

In connection with the termination of our activity, the company has 2-3 days to resolve the issue, since later the data will be made public in full, and the
decryption keys will be deleted.

```
==================
DOMAIN CONTROLLERS
==================

       DcNola.aslnapoli5.local       [DS] Site: Nola
   DcSorrento2016.aslnapoli5.local       [DS] Site: Sorrento           +
      DCLeo2016.aslnapoli5.local       [DS] Site: SanLeonardo
       DC2016-2.aslnapoli5.local       [DS] Site: Nome-predefinito-primo-sito  +
  DCBrusciano2016.aslnapoli5.local       [DS] Site: Brusciano       +
    DC-Bosco2016.aslnapoli5.local       [DS] Site: Bosco
       DC2016-1.aslnapoli5.local [PDC]  [DS] Site: Nome-predefinito-primo-sito  +

=========================
VMS AND DEDICATED SERVERS
=========================

Name           Operatingsystem                IPv4Address       Servicess    Cortex
XDR    HYPER-V       VMName
----           ---------------                -----------    ---------    ----------   --------  ------

SRVPACSTORRE    Windows Server 2012 R2 Standard   10.24.157.76     +     +
QUANIDB         Windows Server 2016 Standard      10.24.0.4        +     +
DC2016-1        Windows Server 2016 Standard      10.24.0.41       +     +
SRVDELLLEO3     Windows Server 2016 Datacenter    10.27.2.227      +     +     +
SRVDELLLEO1     Windows Server 2016 Datacenter    10.27.2.225      +     +     +
PERNICEFATTURE  Windows Server 2012 R2 Datacenter 10.24.1.10       +     +
+
SRVDELLBLADE09  Windows Server 2012 R2 Datacenter 10.27.1.183      +     +
+
-------------------------------------------------------------------------------------------------------------
```

SRVDELLBLADE10 Windows Server 2012 R2 Datacenter 10.27.1.184 +
+ (HYPERVDG04)

SERVER3 Windows Server 2012 R2 Standard 10.24.0.250 + +
Andra - RIS

SECTRAWISEDB Windows Server 2012 R2 Standard 10.27.1.61
+ Andra - Wise DB Server

SRVDATAANALYSIS Windows Server 2012 R2 Standard 10.27.1.22
+ CID - Data Analysis

CID-DB Windows Server 2012 R2 Standard 10.24.0.188 + +
CID - DataBase - Esercizio

CLUBRUDELL Windows Server 2012 R2 Datacenter 10.24.190.210 + +
(DELLBRUSCIANO04)

ASL070C31BDC5C1 Windows Server 2003 192.168.0.80 +
Cacom-Sincro

Elaborazioni Jacob

Protocollo Geprow EX4

SRVDELLBLADE08 Windows Server 2016 Datacenter 10.27.1.182 + +
(HYPERVDG03)

CID - LibrettiPediatrici

SRVEMOGASANALIS Windows Server 2016 Datacenter
10.27.1.82 Emogas

Enco CLient x32

Eng - Script Recover

Engi Oliam Web Demone

Gesan - App NOLA DG

Gesan - Consultori CPI

Gesan - Liste di attesa

GPI - AsTer App

SYNCROCOVID19 Windows Server 2016 Standard 10.24.1.241
+ Magaldi - Syncro-Covid19-Smart-Lea

MANADS Windows Server 2003 10.24.1.160 +
Management ADS

TABULARBI Windows Server 2016 Standard 10.27.1.69 +

TabularBI

DELLBRUSCIANO02 Windows Server 2012 R2 Datacenter 10.33.190.202

+ +

DCBRUSCIANO2016 Windows Server 2016 Standard 192.168.0.22 +

+ Dc-Brusciano2016

Jacob CaComm Esercizio

JACOB Windows Web Server 2008 R2 10.24.190.130 +

Jacob CaComm Esercizio

DNS02BRUSCIANO Windows Server 2012 R2 Standard 192.168.0.23 +

+ SrvDNS02Brusciano

Temporanea OLIAMM Vecchio

DELLBRUSCIANO01 Windows Server 2012 R2 Datacenter 10.33.190.201

+ +

REGTUMORISQL Windows Server 2016 Datacenter 192.168.19.33

+ Registro Tumori

DELLBRUSCIANO03 Windows Server 2012 R2 Datacenter 10.33.190.203

+ +

Proxy Brusciano

Proxy Brusciano

SRVDELLBOSCO4 Windows Server 2016 Datacenter 10.27.3.158 + +

Gesan - Bosco2019 Db

SrvLaboBoscoStorico

SRVDELLNOLA3 Windows Server 2016 Datacenter 10.27.191.7 + +

Gesan - CPI Nola

MEDTRONICFS Windows Server 2016 Standard 10.27.191.110

+ MedTronic - Server

SrvDHCPNola

SRVDELLBOSCO1 Windows Server 2016 Datacenter 10.27.3.155

\+ +

Gesan - BoscoDb

SrvDHCPBosco

SRVPACSBOSCO Windows Server 2012 R2 Standard 10.24.156.160 +

\+ SrvPacsBosco

SRVDELLLEO4 Windows Server 2016 Datacenter 10.27.2.228 + +

DCLEO2016 Windows Server 2016 Standard 10.27.2.20 +

Dc-Leo2016

Gesan - App Leo

Gesan - DB Leo

MTFSCMARE Windows Server 2016 Standard 10.27.2.236 +

Medtronic - FileServer

ROCHEANAPAT Windows Server 2016 Standard 10.27.2.25

\+ Roche - AnaPat

SrvSectraSanLeo

SRVDELLBOSCO3 Windows Server 2016 Datacenter 10.27.3.157 + +

DC-BOSCO2016 Windows Server 2016 Standard 10.27.3.30

\+ Dc-Bosco2016

Gesan - BoscoApp

Gesan - CPI Db

SRVDELLBOSCO2 Windows Server 2016 Datacenter 10.27.3.156 + +

Gesan - Bosco2019 App

Gesan - Bosco2019 CPI

Gesan - CPI

SRVDELLBLADE03 Windows Server 2016 Datacenter 10.27.1.177 + +

ADS - RH65 - DSM

ADS - WIN2003STBLADE1

ADS - WIN2003STBLADE1

SrvHL7cid2012 Windows Server 2012 R2 Standard 10.27.1.62 + +
CID - Gateway HL7
SRVDKDIC Windows Server 2016 Standard 10.27.1.117 +
DatevKoinos - Dichiarativi
Enco
Engi - ADT Storico - Server
Fastwef Giuseppe
Gesan DB Centralizzato
GPI - Gef-Mule
SRVGRICODE Windows Server 2016 Standard 10.24.1.128 +
Grifols - GRICODE
SRVNETWORKER9 Windows Server 2016 Standard 10.27.1.88 +
+ NetWorker9
JOSEFLAB Windows Server 2016 Datacenter 10.24.1.170 + +
New Virtual Machine
phpIPAM
RMAN Windows Server 2008 R2 Standard 10.27.1.15 +
RMAN
TECNICOGARE Windows Server 2012 R2 Standard 10.24.0.127 +
+ Servizio Tecnico Gare
SRVDHCP01 Windows Server 2012 R2 Standard 10.24.0.56 +
SrvDHCP01
Test - Zabbix
WIN-TREXOM Windows Server 2012 R2 Standard 10.24.0.237
+ Trexom - Server timbrature
Werfen - James TAO
Werfen - Zabbix
wn06 Vecchio protocollo clinch-flinch
wn06 Vecchio protocollo clinch-flinch

SRVDELLLEO2 Windows Server 2016 Datacenter 10.27.2.226 + +
CheckpointFW
CheckpointFW
Gesan - CPI
Gesan - CPI Db
LaboExGragnano
LaboExGragnano

LaboUrgenze - Storico
SrvDHCPLeo

SRVDELLNOLA2 Windows Server 2016 Datacenter 10.27.191.6 + +
DCNOLA Windows Server 2016 Datacenter 10.24.191.30
+ DC-Nola
Gesan - AppNola
Gesan - CPI DB Nola

SRVDELLNOLA1 Windows Server 2016 Datacenter 10.27.191.5 + +
Gesan - DbNola

SRVDELLBLADE01 Windows Server 2016 Datacenter 10.27.1.175 + +
ADS - CentOS New Paghe
ADS - CentOS New SAN
ADS - Centos Paghe Clone
ADS - Clone SAN
Eng - ADT Storico
Eng - Portale Gare
RECOVERTEST Windows Server 2008 R2 Standard 10.24.1.108
+ Engi - recover TEST
Engi - Screening Db
SRVPERITONEALE Windows Server 2016 Standard 10.27.1.67 +
+ Fresenius - PatientOnLine
SRVGPIGESAL Windows Server 2012 R2 Standard 10.27.1.26 +
+ GPI - Affari legali
SRVMONTRAFRIG Windows Server 2016 Datacenter 10.27.1.153
+ Laboindustria (Monitoraggio Frigoriferi Trasfusionale)
LESIONICUTANEE Windows Server 2012 R2 Standard 10.27.1.36 +
+ LesioniCutanee
SRVMETEDA Windows Server 2012 R2 Standard 10.27.1.37 +
+ Meteda - Cartella diabetologica
Mirko Sperimntazione Xp
Pensioni S7 Ex4
Pensioni S7 Ex4

SRVTALETEAPP Windows Server 2016 Standard 10.27.1.94
+ Talete - Application
Test - Rsyslog
Unlimited - GDI
SRVSENTRY Windows Server 2016 Standard 10.27.1.115 +
Vyaire - Sentry

SRVDELLBLADE04 Windows Server 2016 Datacenter 10.27.1.178 + +
AK-12-Artensys-FarmaQuRa
Cavalcanti Amianto
SRVCASSA2012 Windows Server 2012 R2 Standard 10.24.1.104 +
+ CID - Cassa 2012
CONSOLE-JAVA Windows Server 2012 R2 Datacenter 10.23.0.140
+ Console Java
SRVDSMTS Windows Server 2008 R2 Standard 10.24.0.8 +
DSM
DSM DSM
Engi - ScreeningWeb
Engi - ScreeningWeb
SRVSMTPRELAY Windows Server 2016 Standard 10.24.1.6 +
+ Exchange - SMTP Relay
FASTBEE Windows Server 2016 Datacenter 192.168.1.223
Fastweb - FastB
Gesan - management
Gipel2
Gipel2
GMASconsole
GMASCONSOLE1 Windows Server 2003 10.28.1.245 +
GMASconsole
GPI - PrivacyCentos7
SRVSISTETEST Windows Server 2016 Standard 10.24.0.231 +
+ GPI - Siste test
Protocollo-Clinch-Fling
SRVSANTECMW Windows Server 2016 Standard 10.27.1.66
+ Santec - MW HL7
SERVERTOTTONE Windows Server 2003 10.24.0.115 +
Server Tottone

SRVBCKNW Windows Server 2016 Datacenter 10.24.0.1 +
SrvBckNw18

SRVDELLBLADE05 Windows Server 2016 Datacenter 10.27.1.179 + +
ADSMAN2016 Windows Server 2016 Standard 10.24.1.37 +
ADS - Management2016
SRVCACHE2CUP Windows Server 2012 R2 Standard 10.24.1.222 +
+ CID - Cache2 CUP 2012
SRVCIDPRENOTAZ Windows Server 2012 R2 Standard 10.27.1.28 +
+ CID - prenotazioni online
Cup - Covisian1
Cup-Covisian2
DC2016-2 Windows Server 2016 Standard 10.24.1.79 + +
Dc2016-2
DUO Auth Proxy
Engi - Integrazione Spagic - Werfen
Engi - OliammRegione
Fortiweb-VM-6.1.1-build0398
Fortiweb-VM-6.1.1-build0398
Fortiweb-VM-6.1.1-build0398
Fortiweb-VM-6.1.1-build0398
Gesan - DbAmbulatori - Alpi
GPI - Phebo
GPI - Phebo
SRVARCHIVIO1 Windows Server 2003 10.24.0.44 +
SRVARCHIVIO1
SRVTMGAEM Windows Server 2016 Standard 10.27.1.56 +
TM GAEM - Gestione Elettromedicali
SRVWERFENMULTI1 Windows Server 2012 R2 Standard 10.27.1.53
+ Werfen - Multi W2012

SRVDELLSOR4 Windows Server 2016 Datacenter 10.27.125.169 + +
DCSORRENTO2016 Windows Server 2016 Standard 10.27.125.20 +
+ Dc-Sorrento2016
Gesan - CPI Db Sorrento

Laboratorio Sorrento Storico Diamante

CluNolaDell Windows Server 2016 Datacenter 10.27.191.8 + +

Gesan - DbNola

SRVDELLSOR1 Windows Server 2016 Datacenter 10.27.125.166

+ +

Gesan - SorrentoApp

SRVSCTRASORR Windows Server 2012 R2 Standard 10.24.125.64 +

+ SrvSectraSorrento

SRVDELLSOR3 Windows Server 2016 Datacenter 10.27.125.168 + +

SrvDHCPSorrent

SRVDELLBLADE14 Windows Server 2016 Datacenter 10.27.1.189 + +

ADS - Clone Oracle SAN

ADS - Oracle SAN

Engi - Application Server GopApp

Engi - DB DWH

Engi - DB-TEST

Engi - Eliot 3.0 App1

Engi - Oracle 2020

Engi - WinSap 3.0 App1

Engi - WinSap 3.0 App2

GPI - Centos 7 SISPI

WORKFLOW Windows Server 2012 R2 Datacenter 10.24.0.239 +

+ SrvWorkflowEsercizio

Werfen - Oracle Suse

SRVDELLNOLA4 Windows Server 2016 Datacenter 10.27.191.4 + +

SRVDELLBLADE02 Windows Server 2016 Datacenter 10.27.1.176 + +

ADS - CentOS - GP4

ADS - Centos65x64 - DSM App

SRVCACHE1CUP Windows Server 2012 R2 Standard 10.24.1.220 +

+ CID - Cache1 CUP 2012

RISCONTROWEB Windows Server 2012 R2 Standard 10.27.1.55 +

+ Cid - Riscontro Web

Engi - Spagic64

Engi - Tomcat Screening 01

EngiTest2

SRVFRESENIUS Windows Server 2008 R2 Standard 10.27.1.38

+ Fresenius - TDMS Dialisi

SRVQLIKVIEW Windows Server 2016 Standard 10.27.1.54 + +

GPI - SrvQlikview

SRVRECLAMI Windows Server 2016 Standard 10.27.1.91 +

Modus - Reclami

Mortara - WebScribeCis

Mortara - WebScribeStore

Mortara - WebScribeView

PensioniS7

SrvFarma1

SRVDELLBLADE06 Windows Server 2016 Datacenter 10.27.1.180 + +

Engi - Areas New

Gesan - Consultori DB

Gesan - SIC-DB

Gesan - SIC-WebApp

Gesan - TdG CPI

Gesan - TdG DB

Gipel1

Gipel1

SRVUMACAAPP Windows Server 2016 Standard 10.27.1.149

+ Santec - App UMACA

SRVGOP Windows Server 2012 R2 Datacenter 10.24.1.43 +

+ SrvGopEsercizio

SRVDELLBLADE07 Windows Server 2016 Datacenter 10.27.1.181 + +

SRVCONCORSI Windows Server 2016 Standard 10.27.1.48 +

+ Be20 - Concorsi

CACOMM2012 Windows Server 2012 R2 Datacenter 192.168.43.43

+ CID - Cacomm - 2012

CID - Cacomm - 2012

SRVCATHLAB Windows Server 2016 Standard 10.27.1.74 +

Ebit - Cathlab

Gesan - Scheda Clinica

Gesan - Tdg App

KYOCERANET Windows Server 2016 Standard 10.27.1.10

+ KyoceraNetAdmin

Logonbox

MedigateMGT

MedigateMGT

Regione Sinfonia - Hl7 Bridge

SrvTamponiLAMPTest - PowerBI

SRVDELLBLADE11 Windows Server 2016 Datacenter 10.27.1.186 + +

ADS - CentOS - SAN

ADS - Oracle Jportal

Bim - QuaniDB

Engi - App DWH

Engi - app1-Test - AMC

Engi - Application Server 1 AMC

Engi - Application Server Cobol

Engi - Application Server HR

Engi - Application server LIFERAY Test

Engi - Fatturazione elettronica Apache

Engi - LIFERAY PortaleApp2

Engi - Web server + Application Server 1

Engi - Web server + Application Server 2

EngiTest1

SRVSISTE Windows Server 2016 Standard 10.27.1.80 + +

GPI - Siste

Proxy Centos 7

SERVERPERSONALE Windows Server 2003 10.24.1.203

\+ ServerPersonaleStipendi

SRVGOPCOLLAUDO Windows Server 2012 R2 Datacenter 10.27.1.166

\+ SrvGopCollaudo

Talete - DB

Wsus - 2019

SRVDELLBLADE12 Windows Server 2016 Datacenter 10.27.1.187 + +

Engi - app2-Test - HR

Engi - Application Server 2 AMC

Engi - Application server Privacy Manager

Engi - DB AREAS AMC HR

Engi - LIFERAY PortaleApp1

SRVDELLBLADE13 Windows Server 2016 Datacenter 10.27.1.188 + +

ADS - CentOS New Jsuite

SECTRAAPP Windows Server 2012 R2 Standard 10.27.1.63 +

\+ Andra - App Server

SRVAPPCUP Windows Server 2012 R2 Standard 10.24.0.211

CID - CUP App Server 2012

Engi - Eliot 3.0 App2

Engi - Fatturazione elettronica Tomcat

Gesan - Integrazione Werfen

GPI - AsTer DB

GPI - OracleTestITLAV - SrvFormazione

Mirko Sperimentazione X

WEBSCRIBEELI Windows Server 2012 R2 Standard 10.27.1.145 +

\+ Mortara - WebScribeEli

CONSOLES2I Windows Server 2012 R2 Standard 10.24.1.249 +

S2I Console

SRVUMACADB Windows Server 2016 Standard 10.27.1.148 +

Santec - DB Umaca

SRVWERFENAPP1 Windows Server 2012 R2 Standard 10.27.1.51

\+ Werfen - App1 W2012

SRVWERFENAPP2 Windows Server 2012 R2 Standard 10.27.1.52
+ Werfen - App2 W2012

CAUCluSoz5z Windows Server 2016 Datacenter 10.27.125.167 + +
CluLeoDell Windows Server 2016 Datacenter 10.27.2.229 + +

emcfs01 EMC File Server 10.27.1.21 +

win2003stBlade1 Windows Server 2003 10.24.0.13 +
DELLBSQKP3J Windows Server 2003 10.24.0.48 +
SNBCKNW Windows Server 2008 R2 Enterprise 10.24.1.250 +
SRVPACSVICO Windows Server 2012 R2 Standard 10.24.155.30 +
SECTRACACHELEO Windows Server 2012 R2 Standard 10.24.132.191 +
CluBosco2016 Windows Server 2016 Datacenter 10.27.3.159 +
SRVDELLSOR2 Windows Server 2016 Datacenter 10.27.125.167 +
CluSor2016 Windows Server 2016 Datacenter 10.27.125.165 +
ARCHIVIOGEF Windows Server 2016 Standard 10.27.1.87 +

If there is no serious contact, we send all private data to interested parties and close the site.
It will be possible to find us only through the blog.

We provide demo data package. If no conversation follow we will apply with data in different way. https://anonfiles.com/d4u0p6Bcxa/IT-MED_7z

Leave a Reply

Name *

Email *

Website

Add Comment

Save my name, email, and website in this browser for the next time I comment.

Post Comment