의료/보건 분야를 노리는 랜섬웨어 조직

 미 법무부는 지난 19일 북한 랜섬웨어 조직으로부터 약 50만 달러를 압수 및 몰수했다고 발표하였다. 미 법원에 따르면 2021년 5월 북한 해커가 마우이 랜섬웨어 변종을 사용하여 캔자스 지역 의료 센터의 파일과 서버를 암호화했다고 한다. 일주일 넘게 암호화된 서버의 접근할 수 없었던 캔자스 병원은 컴퓨터와 장비를 다시 사용하기 위해 약 10만 달러의 비트코인을 지불하였다. 캔자스 의료 센터는 이를 FBI에 알렸고, 중국에 기반을 둔 돈세탁자들을 추적할 수 있었다.

그 결과 2022년 4월 FBI는 캔자스 의료 센터 사고로 인해 압수한 가상화폐 계정 중 하나에서 약 12만 달러의 비트코인이 지불되는 것을 확인하였고, 조사한 결과 콜로라도의 의료기관이 같은 랜섬웨어 변종을 사용하는 조직에 의해 침해당한 후 몸값을 지불한 것으로 확인되었다. 2022년 5월 FBI는 캔자스와 콜로라도 의료기관으로부터 돈을 받은 두 개의 가상화폐 계정을 압수하고 갈취한 돈을 피해자들에게 돌려주기 위한 절차를 시작하였다.

1. 마우이 랜섬웨어

```
Usage: maui [-ptx] [PATH]
Options:
-p dir: Set Log Directory (Default: Current Directory)
-t n:       Set Thread Count (Default: 1)
-x:         Self Melt (Default: No)
```

<그림> 마우이 랜섬웨어 사용법

마우이 랜섬웨어는 인수를 받아 실행하는 수동 실행방법을 제공한다. 이런 방식은 자동으로 실행하는 다른 랜섬웨어와 차이를 보이고 있다.

1) 하드코딩된 RSA 공개키

```
000BEDF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000BEE00  30 81 9F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01  0.Ÿ0...*†H†÷....
000BEE10  05 00 03 81 8D 00 30 81 89 02 81 81 00 B9 08 93  ......0.‰....¹.“
000BEE20  47 B1 44 4E 7C AA 26 27 6D 01 DD 0A B8 2D 91 B0  G±DN|ª&'m.Ý.¸-‘°
000BEE30  E9 80 04 E2 2A 45 16 3C 55 5A 5D FF 67 61 74 FD  é€.â*E.<UZ]ÿgatý
000BEE40  DC 86 97 8A FA 81 BF 73 3C E1 7D 38 D5 40 C6 15  Ü†—Šú.¿s<á}8Õ@Æ.
000BEE50  63 F3 A5 E1 EA A1 CF 3C AB 43 BB EF ED 7C 56 9E  có¥áê¡Ï<«C»ïí|Vž
000BEE60  99 92 3B 46 09 59 84 3E 9A E5 A8 E4 5E 8C A0 1F  ™’;F.Y„>šå¨ä^Œ .
000BEE70  5C 64 6E 68 20 9D 7D 74 8D 7E 59 E0 AC 4B 61 8F  \dnh .}t.~Yà¬Ka.
000BEE80  8C 7D A1 41 E5 ED 54 27 15 12 E7 FD B3 07 56 A6  Œ}¡AåíT'..çý³.V¦
000BEE90  90 31 D0 5A 81 FC 1A 80 2B B6 BA CC 95 02 03 01  .1ÐZ.ü.€+¶ºÌ•...
000BEEA0  00 01 4B 42 55 50 01 00 00 00 A2 00 00 00        ..KBUP....¢...
```

<그림> 마우이 랜섬웨어에 저장된 RSA 공개키

마우이 랜섬웨어를 실행하면 파일의 맨 끝에서 12byte를 로드해서 처음 4byte가 PUBK 값을 포함하는지, 그 다음 2byte에 키 버전을 나타내는 숫자 1을 포함하는지 확인한다. 이 두가지 검사를 통과한 후 PUBK 앞에 있는 162byte 공개키를 로드한다.

구분	Hex value
RSA 공개키	3081 ~ 0001
공개키 식별 값	4B42 5550

KEY 버전	0100

2) 런타임 키

이후 마우이 랜섬웨어는 RSA_generate_key() 함수를 통해 새로운 RSA 키 페어를 생성한다. 새롭게 생성된 개인키는 하드코딩된 공개키로 암호화하고, maui.evd 파일에 쓴다. 새롭게 생성된 공개키는 ₩₩.₩PhysicalDrive0 정보를 사용하여 생성된 16byte XOR키를 사용하여 인코딩하고 maui.key 파일에 쓴다.

파일명	설명
maui.evd	런타임 생성 RSA 개인키로 하드코딩된 공개키에 의해 암호화되어 있음
maui.key	런타임 생성 RSA 공개키로 하드드라이브 정보에 기반해 생성된 XOR키에 의해 인코딩되어 있음
maui.log	실행시 콘솔에 표시되는 내용을 기록한 파일

3) 파일 암호화

파일별로 생성된 32byte 키를 사용하여 CBC모드로 AES 암호화를 수행한다. 32byte 키는 하드코딩된 dogd 문자열과 RAND_bytes() 함수에서 생성된 28byte로 이루어져 있다. 마우이에 의해 암호화된 각 파일들은 커스텀된 헤더가 포함되어 있기 때문에 랜섬웨어 중복실행시 감염여부를 확인할 수 있다. 커스텀된 헤더에는 원래 파일의 실제 경로와 런타임 RSA공개키로 암호화된 AES키가 포함된다.

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  54 50 52 43 01 00 00 00 6D 00 61 00 75 00 69 00  TPRC....m.a.u.i.
00000010  5C 00 61 00 63 00 63 00 6F 00 75 00 6E 00 74 00  \.a.c.c.o.u.n.t.
00000020  2E 00 74 00 78 00 74 00 00 00 0B 00 00 00 00 00  ..t.x.t.........
00000030  00 00 05 B9 FC 30 3D 6E F1 EB 52 0B FD A5 0F 49  ...¹ü0=nñëR.ý¥.I
00000040  F8 EA C2 C0 0E 31 20 59 5E 16 7E 69 3B 84 1C FF  øêÂÀ.1 Y^.~i;„.ÿ
00000050  DE C8 0B 6F 54 BB 2F 24 70 D3 BF B7 81 E2 E4 AB  ÞÈ.oT»/$pÓ¿·.âä«
00000060  9D FF 5D E4 3C 38 37 3A 51 92 0F 00 46 23 AD AA  .ÿ]ä<87:Q’..F#.ª
00000070  4A 00 4A 43 DD 9D A3 82 7E AB 26 2D 2F D0 5D 69  J.JCÝ.£‚~«&-/Ð]i
00000080  E4 F3 27 5D 85 9B 34 89 58 68 7F B0 30 89 52 A6  äó']…›4‰Xh.°0‰R¦
00000090  A3 AD C6 70 C4 A4 94 B5 B1 87 AF B6 8D 2A 03 98  £.ÆpÄ¤”µ±‡¯¶.*.˜
000000A0  77 32 8A 33 98 05 A1 89 D5 99 04 88 9C 66 B8 96  w2Š3˜.¡‰Õ™.ˆœf¸–
000000B0  7B 0B 48 25 22 31 88 96 26 4D A5 78 95 39 A2 95  {.H%"1ˆ–&M¥x•9¢•
000000C0  68 13 D9 CA C2 15 8E BD F4 42 69 3F 54 DC 07 99  h.ÙÊÂ.Ž½ôBi?TÜ.™
000000D0  8E 2B 3E C7 27 59 A4 A3 36 6F 7F C3 A7 66 5D 1C  Ž+>Ç'Y¤£6o.Ã§f].
000000E0  23 CE 1F 6D D7 A6 73 2B 25 CB 6E C4 10 F3 3D 15  #Î.m×¦s+%ËnÄ.ó=.
000000F0  C6 04                                            Æ.
```

<그림> 마우이 랜섬웨어에 의해 암호화된 파일의 헤더

마우이 랜섬웨어에 감염된 파일들의 커스텀 헤더는 다음과 같이 이루어져 있다.

구분	Hex value
커스텀 헤더	5450 5243
정적 값	0100 0000
파일의 원래 경로	6D00 ~
암호화된 AES 키	05B9 ~ 7B0B
암호화된 파일	4825 ~ C604

대부분의 랜섬웨어처럼 대칭 알고리즘인 AES를 사용하여 파일을 암호화하고 AES키는 비대칭 알고리즘인 RSA로 암호화하는 로직을 가지고 있다.

2. 국내 의료/보건 분야 보안현황

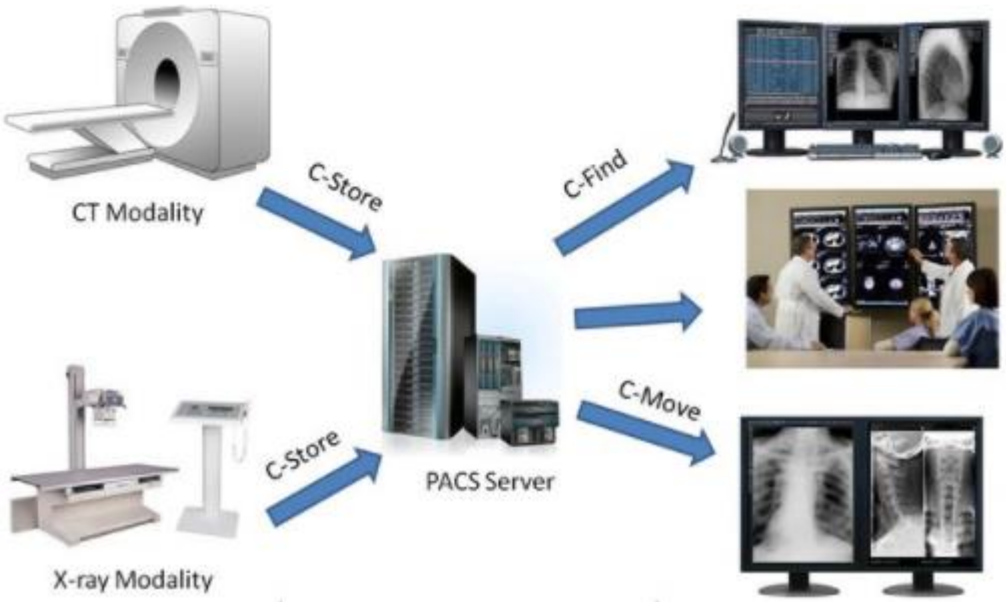
경기일보 | 2021.09.02.

국내 빅5 대형**병원** 2곳 이어 안산 **병원**도 **랜섬웨어** 추정 해킹 공격받아

국내 빅5 대형**병원**인 서울대**병원**과 가톨릭대 서울성모**병원**이 해킹 공격을 받아 경찰이 수사에 나선 가운데... 한 **병원**에서도 **랜섬웨어**로 추정되는 해킹 공격으로 전산장애가 발생한 사실이 뒤늦게 확인됐다. 2일 안산시...

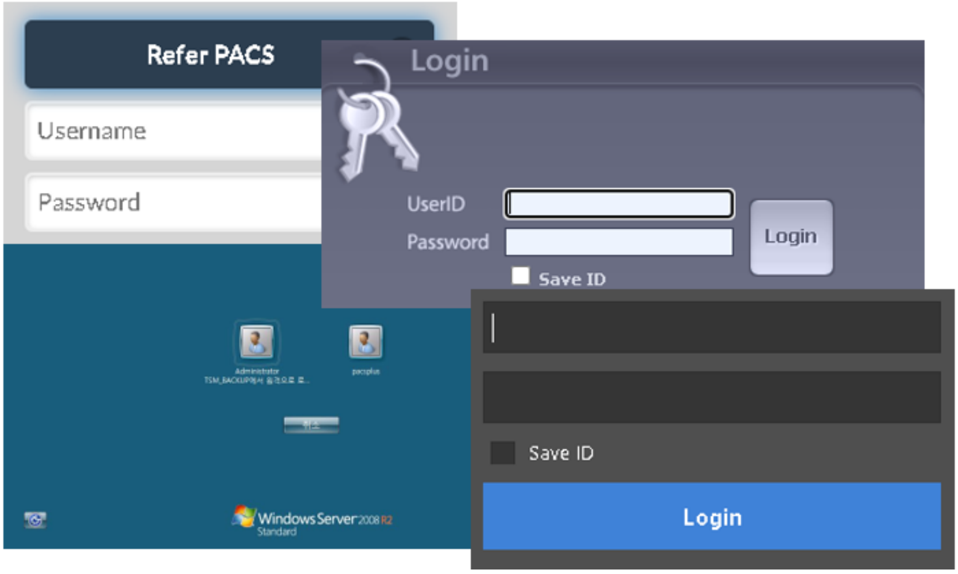
<그림> 의료분야 보안 뉴스

국내 의료분야 침해 사례는 뉴스를 살펴보면 꾸준히 이어져 오고 있음을 알 수 있다. 국내의 의료 보안 현황이 궁금해졌다. 다양한 의료장비 중에서 주로 사용하는 의료영상 저장, 전송 시스템(PACS)과 방사선 치료 장비(nuclear medicine)에 대해서 검색 해 보았다.



<그림> 의료영상 저장, 전송 시스템 (자료화면)

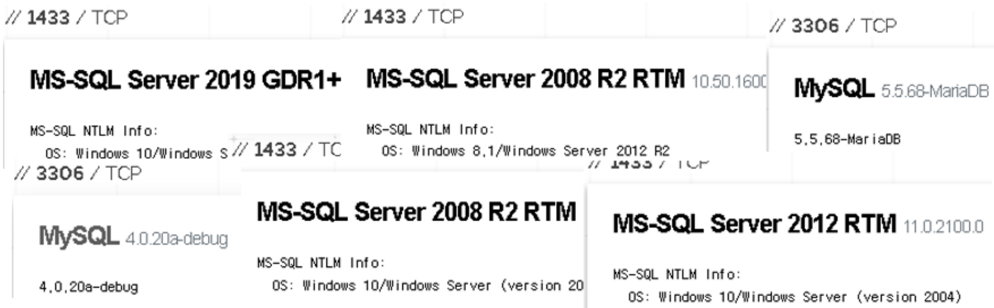
이해를 돕기 위해 PACS는 그림과 같이 CT, X-ray에서 수집한 영상, 이미지를 저장하고, 자료를 검색하거나 뷰어 등으로 확인할 수 있는 시스템으로 중요한 의료정보를 저장하고 있다.



<그림> 국내 의료영상 저장, 전송 시스템 인증 화면 노출

인텔리전스 검색결과, 다양한 PACS 시스템들이 확인되었다. 웹 사이트 접근을 허용하거나 서버 원격을 오픈 해 놓은 경우도 있었다. 원격 오픈 서버의 경우 BlueKeep 취약점에 노출된 것으로 확인되었다. 웹 사이트의 경우 XSS, SQLi, Path traversal, Local file inclusion, CSRF, XXE 등의 다양한 공격 방법이 존재하며, 자동화된 공격 도구들 또한 너무나 많기 때문에 언제든 공격대상이 될 수 있다.

방사선 치료 장비의 경우 PACS 시스템 보다 검색결과가 적었지만 동일하게 원격 데스크톱, NAS 저장 서버 등이 검색되었다.



<그림> 국내 의료 서버 데이터베이스 포트 오픈

조사 과정 중 흥미로웠던 점은 데이터베이스 포트를 오픈 해 놓거나 정보가 저장된 NAS 서버를 오픈해 놓은 경우가 종종 발견되었다는 것이다. 업무상 오픈 해 놓은 것으로 추측되나 공격의 위험에 노출된 환경을 보여주고 있다.

검색범위를 동네병의원(치과 등), 특정 장비 or 분과로 확대하면 더 많은 결과가 도출됨을 확인할 수 있었다.

3. 대응방안

디지털 전환으로 의료, 보건분야 역시 사이버 공격이 끊임없이 이루어지고 있다. 이에 대응하기 위해 국내 의료분야의 경우 의료ISAC에서 보안관련 서비스를 제공하고 있다. 랜섬웨어 대응, 의료 침해사고 사례 등 의료기관

에서 조치해야 할 항목을 매뉴얼 및 자료로 제공하고 있으니 참고하도록 하자.

의료ISAC 자료실: https://www.hisac.or.kr 방문 > 자료실

참고자료

https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors

https://stairwell.com/wp-content/uploads/2022/07/Stairwell-Threat-Report-Maui-Ransomware.pdf