Threat Analysis Report based on

# Captured Cyber Attack on simulated Healthcare sector

CyberPeace
Foundation

# DISCLAIMER

This report is purely based on technical findings made by the research team during an analysis of the data captured on the simulated Healthcare based network. It does not intend to malign or in any way target any country, actor or person. All the information provided in this report has been extracted during the analysis.

## Introduction

Cyber attacks on healthcare facilities have been rising in recent years, and the pandemic has only worsened matters. With hospitals and other healthcare facilities struggling to keep up with the demand for care, they have become an easy target for cybercriminals. While this may seem like a small amount, it can be devastating for a hospital that is already stretched thin.

## Preface

Threat intelligence is a technique of gathering information about the threats and threat actors that helps to mitigate harmful events in Cyberspace which Includes Indicators of Compromise such as IP addresses, injected Malware samples, Hashes etc. and can be used to indulge in identification of threat actors and their behavioral techniques of attack. A credible intelligence on real time threats empower Organisations or a Country to build Cybersecurity policies.

**e-Kawach** is an initiative of CyberPeace Foundation (CPF) to implement a comprehensive public network and threat intelligence sensors across the country in order to capture internet traffic and analyse the real time Cyber attacks that a location or an organisation faces. The Objective is to build credible intelligence in the domain of Cybersecurity.

The Research Wing of CyberPeace Foundation and Autobot Infosec Private Limited along with the Academic Partners under CyberPeace Center of Excellence (CCoE) have deployed the Threat Intelligence sensor network based on the simulation of Healthcare network to gather commendable intelligence on state and non-state actors.

## Objective of the Work

The objective for this research is to examine the different types of signatures that can be used as exhibitors of compromise on the simulated Healthcare network by collecting information which can mitigate the future attacks on real networks. By deploying the simulated network we can collect data on patterns of attack, the different types of attack vector for the different protocols and the recent trends of malicious activity.

**Data Collection :** January 2022 - November 2022

CyberPeace
Foundation

## Attack Statistics

During the time period the deployed sensor captured a total number of **18,51,607** attack events from a total number of **41181** Unique IP addresses globally.

## Mostly Attacked destination protocols

| | |
|---|---|
| SMB | (1644476) |
| MSSQL | (91131) |
| FTP | (83497) |
| MYSQL | (4919) |

## Unique Payloads Captured

**1629**

## Payload Type

GenericRXFL-OG!FFC995DC8C4B, BehavesLike.Win32.Generic.th, Trojan.Agent.CZTF, Gen:NN.ZedlaF.34796.@x5@aC0WZ7ei, TR/AD.DPulsarShellcode.gohtr

| | |
|---|---|
| **Unique Username used for brute forcing** | **27** |
| **Unique Password used  for brute forcing** | **2494** |

Total number of attacks

18,51,607

Unique IP Addresses

41,181

Mostly Attacked destination protocols

| | | | |
|---|---|---|---|
| SMB | (1644476) | FTP | (83497) |
| MSSQL | (91131) | MYSQL | (4919) |

Unique Payloads Captured

1,629

Unique Username used for brute forcing

27

Unique Password used for brute forcing

2,494

## Attacker Countries -- Top 10

Most of the traffic came from **Vietnam** followed by **Pakistan, India, China** etc.

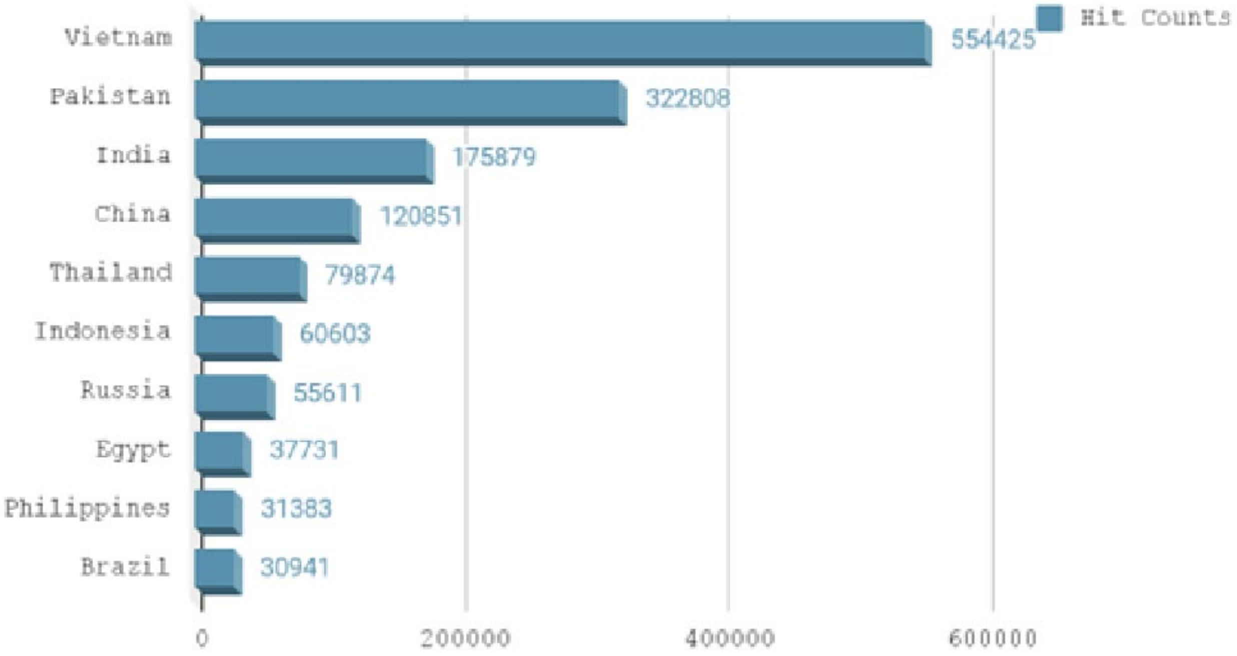


Figure : Top 10 Countries with Hit Counts

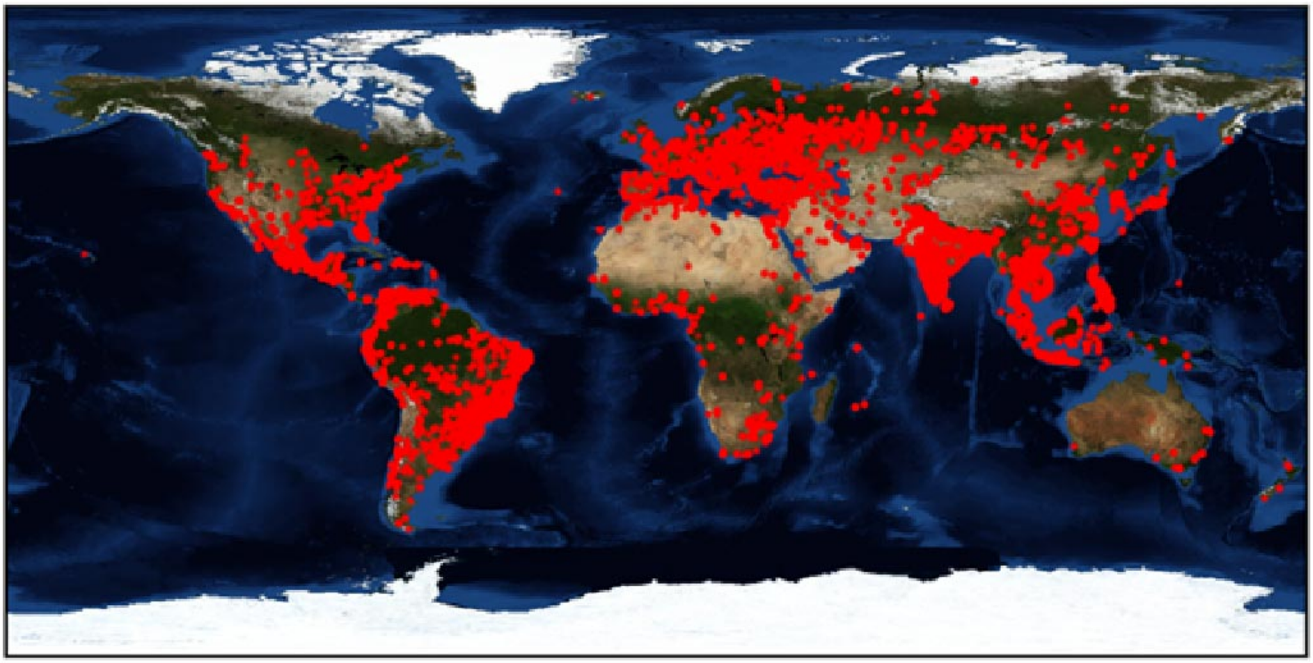


Figure : Map view of the attacker's IP locations

## Attacker IP addresses -- Top 10

Table shows the top 10 unique IP addresses across the globe with the hit counts.

| IP Address | Hit Count |
|---|---|
| 101.53.6.141 | 253090 |
| 101.53.17.77 | 81509 |
| 223.244.83.165 | 39362 |
| 101.53.249.33 | 29842 |
| 101.53.17.2 | 26228 |
| 101.53.236.95 | 24933 |
| 101.53.226.52 | 21774 |
| 201.216.239.205 | 16564 |
| 113.160.198.88 | 15889 |
| 101.53.236.136 | 15652 |

Table: Top 10 Attacker IP Addresses with hit count and percentage

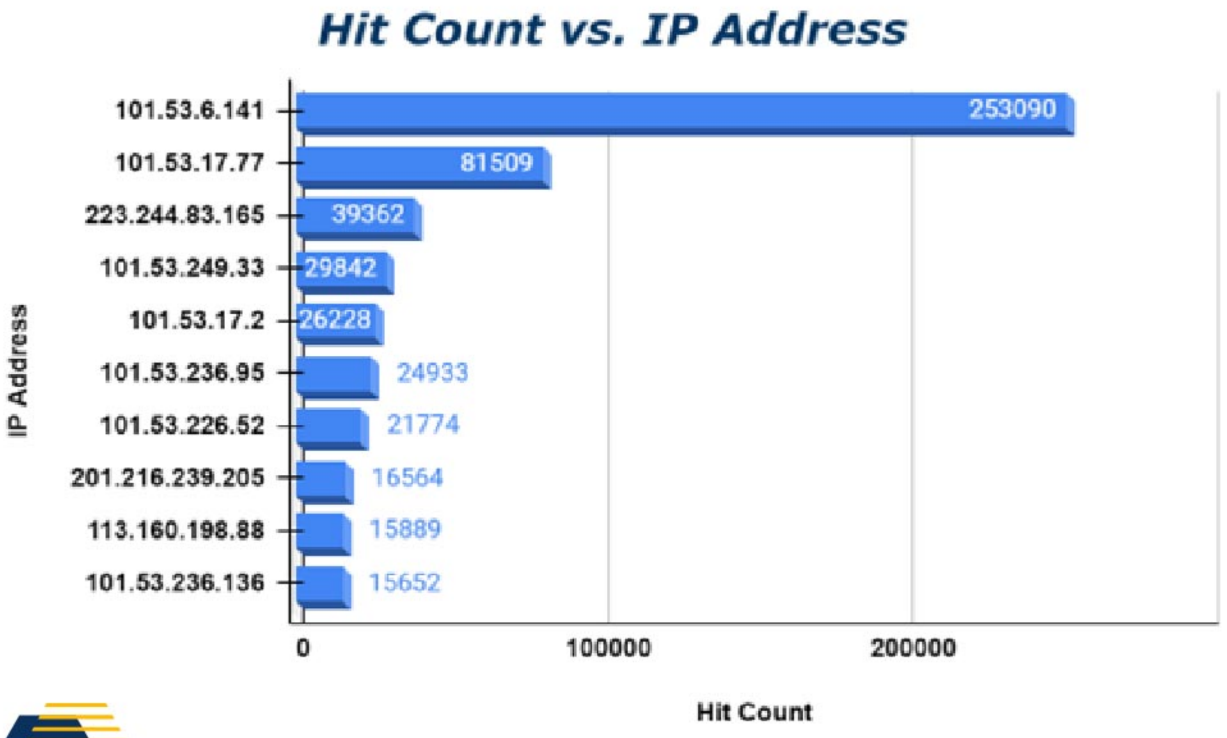


Figure : Top 10 Unique IP with Hit Count

## IP GeoLocation

Note: Geo Location data might differ after generating the report due to Load balancing technologies.

| IP Address | 101.53.6.141 Hit Counts: 2,53,090 |
|---|---|
| **ISP** | Netnam Corporation |
| **Organization** | Netnam Corporation |
| **ASN** | 24176 |
| **Country** | Viet Nam |
| **State/Region** | Ho Chi Minh |
| **City** | Ho Chi Minh City |

## IP is Blacklisted / Flagged as Malicious or Suspicious by

- ✗ Rbl.rbldns.ru
- ✗ SORBS Spamhost
- ✗ SPFBL.net RBL

**Abuse Tag :** Port Scan, Brute-Force

| IP Address | 101.53.17.77 Hit Counts: 81,509 |
|---|---|
| **ISP** | Netnam Corporation |
| **Organization** | Netnam Corporation |
| **ASN** | 24173 |
| **Country** | Viet Nam |
| **State/Region** | Khanh Hoa |
| **City** | Nha Trang |

## IP is Blacklisted / Flagged as Malicious or Suspicious by

- ✗ Abusix Mail Intelligence Combined IP blacklist
- ✗ Abusix Mail Intelligence Policy list
- ✗ Barracuda Reputation Block List
- ✗ Barracuda Reputation Block List (for SpamAssassin)
- ✗ JustSpam.org

- ✗ Polspam BL-H3
- ✗ Rbl.rbldns.ru
- ✗ RFC-Clueless (RFC$^2$) abuse RBL
- ✗ RFC-Clueless (RFC$^2$) Metalist RBL
- ✗ RFC-Clueless (RFC$^2$) postmaster RBL
- ✗ SORBS Spamhost (any time)
- ✗ SPFBL.net RBL
- ✗ UCEPROTECT Level 3
- ✗ V4BL/DDNSBL

**Abuse Tag :** Port Scan

| IP Address | 223.244.83.165 | Hit Counts: 39362 |
|---|---|---|
| **ISP** | ChinaNet Anhui Province Network | |
| **Organization** | ChinaNet Anhui Province Network | |
| **ASN** | 4134 | |
| **Country** | China | |
| **State/Region** | Anhui | |
| **City** | Chuzhou | |

## IP is Blacklisted / Flagged as Malicious or Suspicious by

- ✗ Abusix Mail Intelligence Combined IP blacklist
- ✗ Abusix Mail Intelligence Policy list
- ✗ nsZones.com Dyn
- ✗ nsZones.com SBL+Dyn
- ✗ SORBS Aggregate zone
- ✗ SORBS Aggregate zone (safe)
- ✗ SORBS Dynamic IP Addresses
- ✗ Spamhaus PBL Policy Block List
- ✗ Spamhaus ZEN Combined Block List
- ✗ SPFBL.net RBL

**Abuse Tag :** Port Scan

| IP Address | 101.53.249.33 Hit Counts: 29,842 |
|---|---|
| ISP | Cyber Internet Services Pakistan |
| Organization | Cyber Internet Services Pakistan |
| ASN | 9541 |
| Country | Pakistan |
| State/Region | Sindh |
| City | Karachi |

## IP is Blacklisted / Flagged as Malicious or Suspicious by

- ✗ Abusix Mail Intelligence Combined IP blacklist
- ✗ Abusix Mail Intelligence Policy list
- ✗ nsZones.com Dyn
- ✗ nsZones.com SBL+Dyn
- ✗ JustSpam.org
- ✗ Mailspike Blacklist
- ✗ Mailspike Zero-hour Data
- ✗ rbl.rbldns.ru
- ✗ Spamhaus PBL Policy Block List
- ✗ Spamhaus ZEN Combined Block List
- ✗ SPFBL.net RBL
- ✗ V4BL-FREE/DDNSBL-FREE
- ✗ V4BL/DDNSBL

**Abuse Tag :** Port Scan, Hacking, Brute-Force, Exploited Host

| IP Address | 101.53.17.2 Hit Counts: 26,228 |
|---|---|
| ISP | Netnam Corporation |
| Organization | Netnam Corporation |
| ASN | 24173 |
| Country | Viet Nam |
| State/Region | Khanh Hoa |
| City | Nha Trang |

## IP is Blacklisted / Flagged as Malicious or Suspicious by

- ✗ Abusix Mail Intelligence Combined IP blacklist
- ✗ Abusix Mail Intelligence Policy list
- ✗ Barracuda Reputation Block List
- ✗ Barracuda Reputation Block List (for SpamAssassin)
- ✗ Polspam BL-H3
- ✗ rbl.rbldns.ru
- ✗ RFC-Clueless (RFC$^2$) abuse RBL
- ✗ RFC-Clueless (RFC$^2$) Metalist RBL
- ✗ RFC-Clueless (RFC$^2$) postmaster RBL
- ✗ SORBS Spamhost (any time)
- ✗ SpamRATS! All
- ✗ SpamRATS! Dyna
- ✗ SPFBL.net RBL
- ✗ SPFBL.net RBL
- ✗ UCEPROTECT Level 3
- ✗ V4BL-FREE/DDNSBL-FREE
- ✗ V4BL/DDNSBL

**Abuse Tag :** Port Scan, Hacking, Brute-Force, Exploited Host

| IP Address | 101.53.236.95 | Hit Counts: 24,933 |
|---|---|---|
| **ISP** | Cyber Internet Services Pakistan | |
| **Organization** | Cyber Internet Services Pakistan | |
| **ASN** | 9541 | |
| **Country** | Pakistan | |
| **State/Region** | Sindh | |
| **City** | Larkana | |

## IP is Blacklisted / Flagged as Malicious or Suspicious by

- ✗ Abusix Mail Intelligence Combined IP blacklist
- ✗ Abusix Mail Intelligence Policy list
- ✗ nsZones.com Dyn
- ✗ nsZones.com SBL+Dyn
- ✗ rbl.rbldns.ru

- ✗ Spamhaus PBL Policy Block List
- ✗ Spamhaus ZEN Combined Block List
- ✗ SPFBL.net RBL

**Abuse Tag :** Port Scan, Hacking, Brute-Force, Exploited Host

| IP Address | 101.53.226.52 | Hit Counts: 21,774 |
|---|---|---|
| ISP | Cyber Internet Services Pakistan | |
| Organization | Cyber Internet Services Pakistan | |
| ASN | 9541 | |
| Country | Pakistan | |
| State/Region | Sindh | |
| City | Karachi | |

## IP is Blacklisted / Flagged as Malicious or Suspicious by

- ✗ Abusix Mail Intelligence Combined IP blacklist
- ✗ Abusix Mail Intelligence Policy list
- ✗ nsZones.com Dyn
- ✗ nsZones.com SBL+Dyn
- ✗ rbl.rbldns.ru
- ✗ Spamhaus PBL Policy Block List
- ✗ Spamhaus ZEN Combined Block List
- ✗ SPFBL.net RBL

**Abuse Tag :** Port Scan, Hacking

| IP Address | 201.216.239.205 | Hit Counts: 16,564 |
|---|---|---|
| ISP | NSS S.A. | |
| Organization | NSS S.A. | |
| ASN | 16814 | |
| Country | Argentina | |
| State/Region | Santa Fe | |
| City | Rosario | |

## IP is Blacklisted / Flagged as Malicious or Suspicious by

- ✗ Barracuda Reputation Block List
- ✗ Barracuda Reputation Block List (for SpamAssassin)
- ✗ Hostkarma blacklist
- ✗ rbl.rbldns.ru
- ✗ RFC-Clueless (RFC$^2$) abuse RBL
- ✗ RFC-Clueless (RFC$^2$) Metalist RBL
- ✗ RFC-Clueless (RFC$^2$) postmaster RBL
- ✗ Hostkarma

**Abuse Tag :** Port Scan, Hacking, Brute-Force, Exploited Host

| IP Address | 113.160.198.88 Hit Counts: 15,889 |
|---|---|
| **ISP** | Vietnam Posts and Telecommunications Group |
| **Organization** | Vietnam Posts and Telecommunications Group |
| **ASN** | 45899 |
| **Country** | Viet Nam |
| **State/Region** | Ha Nam |
| **City** | Phu Ly |

## IP is Blacklisted / Flagged as Malicious or Suspicious by

- ✗ Abusix Mail Intelligence Combined IP blacklist
- ✗ Abusix Mail Intelligence Policy list
- ✗ nsZones.com Dyn
- ✗ nsZones.com SBL+Dyn
- ✗ rbl.rbldns.ru
- ✗ DRBL gremlin.ru (vote node)
- ✗ DRBL gremlin.ru (work node)
- ✗ s5h.net RBL
- ✗ Spam Grouper Net block list
- ✗ Spamhaus PBL Policy Block List
- ✗ Spamhaus ZEN Combined Block List
- ✗ SpamRATS! All
- ✗ SpamRATS! Dyna
- ✗ SpamRATS! Spam
- ✗ SPFBL.net RBL

- ✗ V4BL-FREE/DDNSBL-FREE
- ✗ V4BL/DDNSBL
- ✗ Scrollout F1 Reputation Domain

**Abuse Tag :** Port Scan, Hacking, Brute-Force, Exploited Host

| IP Address | 101.53.236.136 | Hit Counts: 15,652 |
|---|---|---|
| **ISP** | Cyber Internet Services Pakistan | |
| **Organization** | Cyber Internet Services Pakistan | |
| **ASN** | 9541 | |
| **Country** | Pakistan | |
| **State/Region** | Sindh | |
| **City** | Larkana | |

### IP is Blacklisted / Flagged as Malicious or Suspicious by

- ✗ Abusix Mail Intelligence Combined IP blacklist
- ✗ Abusix Mail Intelligence Policy list
- ✗ nsZones.com Dyn
- ✗ nsZones.com SBL+Dyn
- ✗ rbl.rbldns.ru
- ✗ Spamhaus PBL Policy Block List
- ✗ Spamhaus ZEN Combined Block List
- ✗ SPFBL.net RBL

**Abuse Tag :** Port Scan, Hacking, Brute-Force

## Destination Ports

The statistics show the top most attacked destination protocols. Attackers tried to exploit **SMB, MSSQL, FTP** and **MYSQL**.

| Protocols | Hit Count |
|---|---|
| SMB | 1644476 |
| MSSQL | 91131 |
| FTP | 83497 |
| MYSQL | 4919 |

Table: Destination protocols with hit counts

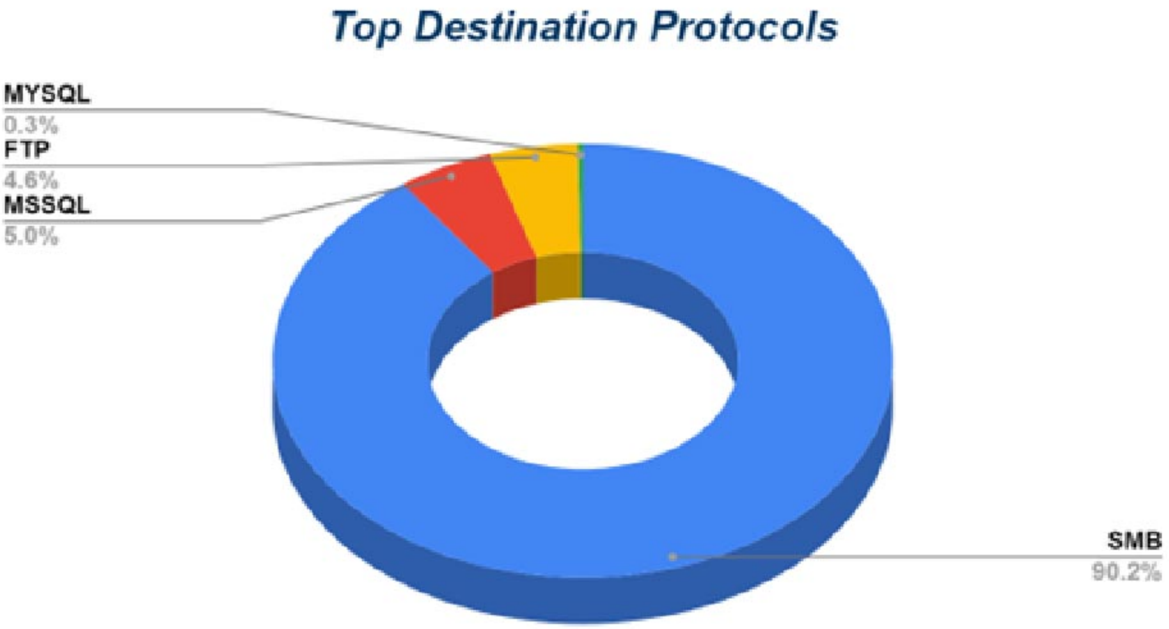


Table: Destination protocols with hit counts

This implies, the vulnerable internet-facing systems, vulnerable SMB and Database services enabled, and old Windows server Platforms were mostly attacked.

The Server Message Block (SMB) protocol is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network. The SMB protocol can be used on top of its TCP/IP protocol or other network protocols.
(https://learn.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview)

Apart from this, we also noticed, massive exploit requests were received for the Remote Desktop Protocols (RDP).

Analysis of data has drawn the attention that attackers also tried to exploit **DICOM/MYSQL/MSSQL** protocols to access the sensitive patients data like medical images, diagnostic databases etc. DICOM is standard protocol used in most medical and healthcare facilities for the management and transmission of medical images and related data.
Some common FTP commands were also captured - "USER", "PASS", "PWD", "CWD", "PASV", "STOR", "PASV", "STOR", "PASV", "STOR", "PASV", "STOR", "PASV", "STOR", "PASV", "STOR", "TYPE”.

## Brute force attack

We also noticed a massive brute force, dictionary attacks were performed against the protocols FTP, MYSQL and MSSQL using common credentials like ‘root’, ‘ftp’, ‘admin’, ‘web’, ‘web!’, ‘qwerty’, ‘password1’, ‘sql2005’, ‘passw0rd’, ‘administrator’ etc.

A trend has also been noticed that attackers are nowadays using long passwords, not usually mentioned in the English dictionary, for example ‘**4yqbm4,m` ~!@~#$%^&*(),.;**’ and ‘**!@#$%^&***’.

## FTP Username

| | Username | Count |
|---|---|---|
| FTP Username | anonymous | 516 |
| | admin | 430 |
| | root | 428 |
| | data | 427 |
| | www-data | 426 |
| | ftp | 426 |
| | administrator | 426 |
| | www | 425 |
| | Admin | 425 |
| | wwwroot | 424 |
| | web | 424 |
| | test | 424 |
| | user123 | 423 |
| | user | 423 |
| | db | 423 |

Table: Top 15 FTP Username

## FTP Password

| | Password | Count |
|---|---|---|
| FTP Password | anonymous | 115 |
| | root | 114 |
| | admin | 114 |
| | admin123 | 112 |
| | test | 111 |
| | woaini | 105 |
| | tomcat | 105 |
| | r00t | 105 |
| | qwerty123456 | 105 |
| | qwerty | 105 |
| | qwa123 | 105 |
| | qazxswedc`123 | 105 |
| | qazxswedc | 105 |
| | password1 | 105 |
| | password | 105 |

Table: Top 15 FTP Password

## MSSQL Username

** Note: [null] means blank

| MSSQL Username | Username | Count |
|---|---|---|
| | sa | 48471 |
| | administrator | 865 |
| | [null] | 39 |
| | useraccess | 5 |
| | odin | 1 |

Table: Top 5 MSSQL Username

## MSSQL Password

** Note: [null] means blank

| MSSQL Password | Password | Count |
|---|---|---|
| | [null] | 1617 |
| | 1qaz2wsx | 151 |
| | password | 133 |
| | 12345678 | 131 |
| | abc123 | 117 |
| | saadmin | 110 |
| | 123456 | 104 |
| | 123 | 99 |
| | 123456789 | 91 |
| | 1234 | 91 |

Table: Top 10 MSSQL Password

## MYSQL Username

** Note: [null] means blank

| | Username | Count |
|---|---|---|
| MYSQL Username | root | 2138 |
| | mysqld | 31 |
| | admin | 25 |
| | [null] | 6 |
| | bob | 4 |

Table: Top 5 MYSQL Username

During the time span attackers tried only blank passwords [null] to exploit the MYSQL protocol.

## Injected Payloads

A total number of 1629 unique payloads have been identified that were injected to the environment.

Some of them are --

| File Hash | Detection Name | No. of engines detected | Virustotal Link |
|---|---|---|---|
| bafed7492141845dd14abbed42dc695be678a1b2cea79f48e8cda285914991ce | GenericRXFL-OG!FFC995DC8C4B | 60 | https://www.virustotal.com/gui/file/bafed7492141845dd14abbed42dc695be678a1b2cea79f48e8cda285914991ce/details |
| cced6bfb1951559cd72e1028d4d56a4d3e7cb7c96770b32016c410d20ccf18d9 | BehavesLike.Win32.Generic.th | 57 | https://www.virustotal.com/gui/file/cced6bfb1951559cd72e1028d4d56a4d3e7cb7c96770b32016c410d20ccf18d9 |
| 399275dd7c6e009e2cefa398c25f08c046c51bc51563503d808cf2aade40d883 | Trojan.Agent.CZTF | 60 | https://www.virustotal.com/gui/file/399275dd7c6e009e2cefa398c25f08c046c51bc51563503d808cf2aade40d883 |
| 860b79fe4a3ca0edc98e8aef1060930324de020626046654a988d7d6acb8f801 | Gen:NN.ZedlaF.34796.@x5@aC0WZ7ei | 61 | https://www.virustotal.com/gui/file/860b79fe4a3ca0edc98e8aef1060930324de020626046654a988d7d6acb8f801 |
| d35188af422653e693ba2be6acaf8b02229e00e4ea5cb55c3f81688383fb482c | TR/AD.DPulsarShellcode.gohtr | 65 | https://www.virustotal.com/gui/file/d35188af422653e693ba2be6acaf8b02229e00e4ea5cb55c3f81688383fb482c |
| 8be754ece09a85ebb1879e636f0f854b3145ce79bc146d3cdee286698d49aedb | Ransom_WCRY.SMALYM | 63 | https://www.virustotal.com/gui/file/8be754ece09a85ebb1879e636f0f854b3145ce79bc146d3cdee286698d49aedb |
| a182a7cd093411e487c43a46659a854b7ca950f23771f9a47313897a79c27121 | Trojan.Encoder.11432 | 58 | https://www.virustotal.com/gui/file/a182a7cd093411e487c43a46659a854b7ca950f23771f9a47313897a79c27121 |
| 012b957bbd7d5b9e4ef323e4174df3c69f3c88b7be4f907084606e97285b90e7 | Gen:NN.ZedlaF.34646.@x5@aC0WZ7ei | 65 | https://www.virustotal.com/gui/file/012b957bbd7d5b9e4ef323e4174df3c69f3c88b7be4f907084606e97285b90e7 |
| 74a44fff67a973f63667687fac01afc5f12449ed2b450f7b4d510986340121ca | ML/PE-A + Mal/Wanna-A | 61 | https://www.virustotal.com/gui/file/74a44fff67a973f63667687fac01afc5f12449ed2b450f7b4d510986340121ca |
| 8fdc6d1ef80ce9003d2e8f505445694f541f264ae4fd694e935422cbc484b362 | Ransom-WannaCry!48FBFC03E81F | 61 | https://www.virustotal.com/gui/file/8fdc6d1ef80ce9003d2e8f505445694f541f264ae4fd694e935422cbc484b362 |

Table: Downloaded payloads

## Sample Malicious Payload Analysis

**MD5 :** ff988bc6e0c576f2989208af77c315ac

**SHA-1 :** ca2bcd87c163dac33ec3541d9e7408a6b4e085ca

**SHA-256 :** cced6bfb1951559cd72e1028d4d56a4d3e7cb7c96770b32016c410d20ccf18d9

**Vhash :** 156056151d1565cz805&z1

**Authentihash :** 3d8a953ef628cd36987b8fe11557982266d6067d19908c496d4bea20c2ad737f

**Imphash :** 2e5708ae5fed0403e8117c645fb23e5b

**Rich PE header hash :** 4949dadf1b06f4f569906fda4710f8e4

**SSDEEP :** 98304:ED9PoBhz1aRxcSUDk36SAEdhvxWa9P593R8yAVp2HP:ED9Pe1Cxcxk3ZAEUadzR8yc4H

**TLSH :** T1B3363398662CA1FCF0440EF40473895AB7B73C6967FB5E1F8BC086660D53B5BABD0A41

**File type :** Win32 DLL

**Magic :** PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit

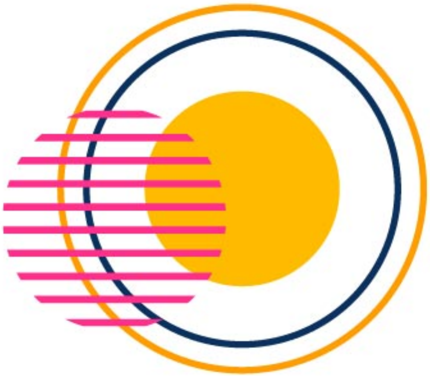
**TrID :** Win32 Executable MS Visual C++ (generic) (37.8%) Microsoft Visual C++ compiled executable (generic) (20%) Win64 Executable (generic) (12.7%) Win16 NE executable (generic) (8.5%) Win32 Dynamic Link Library (generic) (7.9%)

**File size :** 5.02 MB (5267459 bytes)

**PEiD packer :** Microsoft Visual C++ v6.0 DLL

**Portable Executable Info:**

**Compiler Products**



[ C ] VS98 (6.0) build 8168 count=4
[---] Unmarked objects count=15
id: 93, version: 4035 count=3
[C++] VS98 (6.0) build 8168 count=1
[RES] VS98 (6.0) cvtres build 1720 count=1
[LNK] VS98 (6.0) imp/exp build 8168 count=3

**Header**

Target Machine : Intel 386 or later processors and compatible processors
Compilation Timestamp : 2017-05-11 12:21:37 UTC
Entry Point : 4585
Contained Sections : 5

## Sections

| Name | Virtual Address | Virtual Size | Raw Size | Entropy | MD5 | Chi2 |
|---|---|---|---|---|---|---|
| .text | 4096 | 652 | 4096 | 1.44 | 8de9a2cb31e4c74bd008b871d14bfafc | 769060 |
| .rdata | 8192 | 472 | 4096 | 0.73 | 3dd394f95ab218593f2bc8eb65184db4 | 906659.63 |
| .data | 12288 | 340 | 4096 | 0.09 | fe5022c5b5d015ad38b2b77fc437a5cb | 1030197.13 |
| .rsrc | 16384 | 5242976 | 5246976 | 6.41 | 89ff7bf7c8d7537438f6c02f6c8bbaaa | 126396976 |
| .reloc | 5263360 | 684 | 4096 | 0 | 620f0b67a91f7f74151bc5be745b7110 | 1044480 |

## Imports

| KERNEL32.dll | MSVCRT.dll |
|---|---|
| CreateProcessA<br>SizeofResource<br>LoadResource<br>LockResource<br>WriteFile<br>CloseHandle<br>CreateFileA<br>FindResourceA | _adjust_fdiv<br>_initterm<br>malloc<br>free<br>sprintf |

**Exports :** PlayGame

## Overlay

| | |
|---|---|
| offset | 5267456 |
| chi2 | 765 |
| filetype | ASCII text |
| md5 | 693e9af84d3dfcc71e640e005bdc5e2e |
| size | 3 |

### HTTP Traffic

| Endpoint | Request | URL | Data |
|---|---|---|---|
| 104.16.173.80:80 | GET | www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com/ | GET / HTTP/1.1 Host: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com Cache-Control: no-cache |

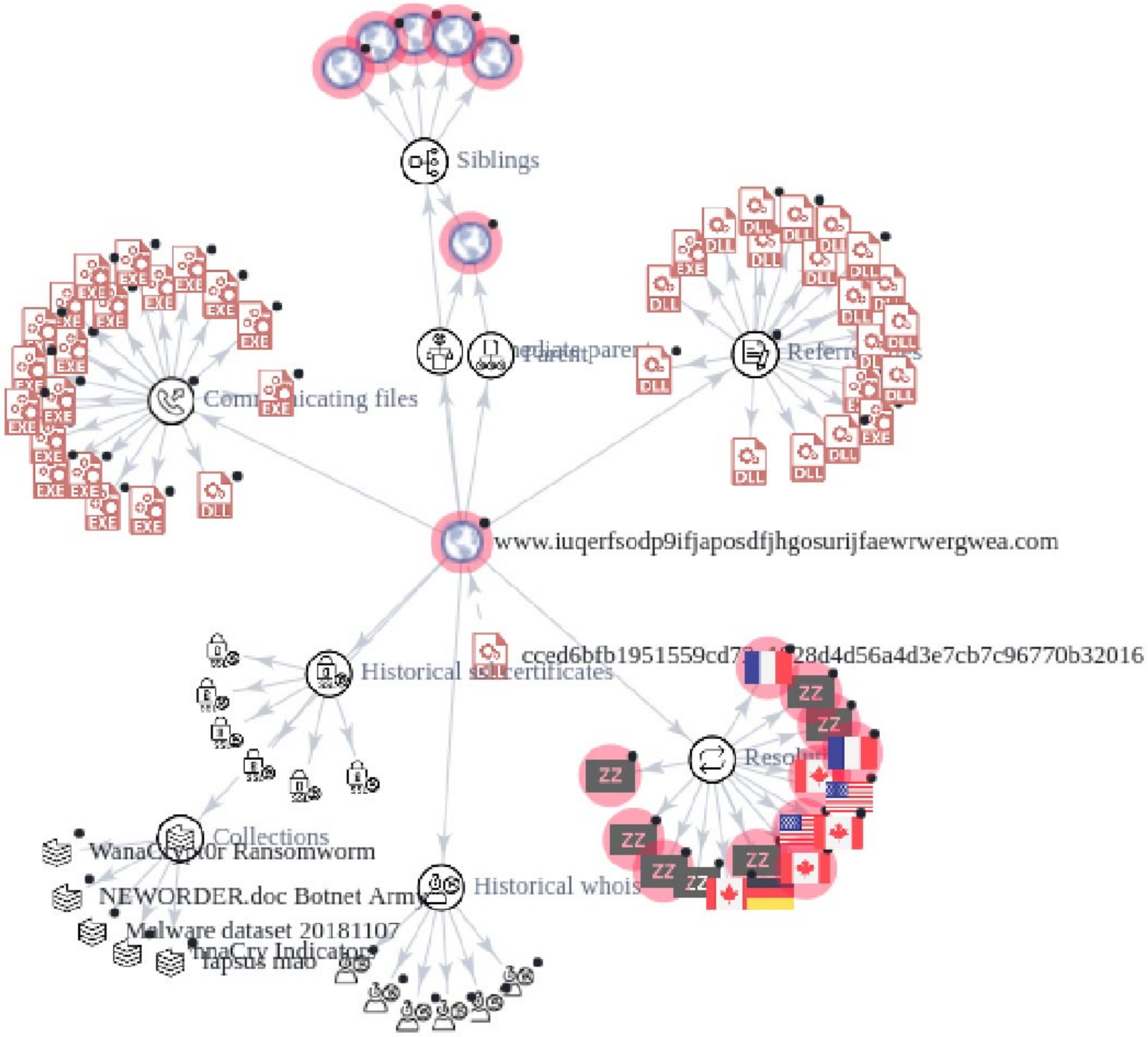
| Domain Name | iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com |
|---|---|
| **Website Title** | **Sinkholed by Kryptos Logic** |
| **HTTP Status Code** | **200 [ Active ]** |
| **IP Address** | **104.16.173.80, 104.17.244.81** |
| **ISP** | Cloudflare |
| **ASN** | 13335 |
| **Country** | United States 🇺🇸 |
| **Sate/Region** | California |
| **City** | San Francisco |

**Domain Name: iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com**
**Registry Domain ID:** 2123519849_DOMAIN_COM-VRSN
**Registrar WHOIS Server:** whois.cloudflare.com
**Registrar URL:** https://www.cloudflare.com
**Registrar:** Cloudflare, Inc.
**Registrar IANA ID:** 1910

**Updated Date:** 2021-02-05T09:06:31Z
**Creation Date:** 2017-05-12T15:08:04Z
**Registry Expiry Date:** 2024-05-12T15:08:04Z

**Registrant Country:** US

**Name Server:** bruce.ns.cloudflare.com
**Name Server:** sara.ns.cloudflare.com



**Ref: Virustotal**

**By analysis of the graph it is clear that the domain is associated with other malicious payload and activities.**

**Registry Keys Set**

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\BITS\StateIndex

HKLM\SYSTEM\ControlSet001\Control\BackupRestore\FilesNotToBackup\BITS_BAK

HKLM\SYSTEM\ControlSet001\Control\BackupRestore\FilesNotToBackup\BITS_LOG

HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#SW#{eeab7790-c514-11d1-b42b-0

```
0805fc1270e}#asyncmac#{ad498944-762f-11d0-8dcb-00c04fc3358c}\#{78032B7E-4968-42D3-9F37-287EA86C0AAA}\Control\Linked

HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#SW#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-8dcb-00c04fc3358c}\#{78032B7E-4968-42D3-9F37-287EA86C0AAA}\SymbolicLink

HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#SW#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-8dcb-00c04fc3358c}\Control\ReferenceCount

HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#SW#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-8dcb-00c04fc3358c}\DeviceInstance

HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#SW#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-82e6-71a87abac361}\#\Control\Linked

HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#SW#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-82e6-71a87abac361}\#\SymbolicLink

HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#SW#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-82e6-71a87abac361}\Control\ReferenceCount

HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#SW#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-82e6-71a87abac361}\DeviceInstance

HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}\{B5DA8633-954C-4495-AE46-0BB5B5FB1CDC}\Connection\PnpInstanceID

HKLM\SYSTEM\ControlSet001\Control\Nsi\{eb004a03-9b1a-11d4-9123-0050047759bc}\22\(Default)

HKLM\SYSTEM\ControlSet001\Control\N-
```

si\{eb004a03-9b1a-11d4-9123-0050047759bc}\24\ffffffffffffffffffffffffffffff00

HKLM\SYSTEM\ControlSet001\Control\Nsi\{eb004a03-9b1a-11d4-9123-0050047759bc}\24\ffffffffffffffffffffffffffffff01

HKLM\SYSTEM\ControlSet001\Control\Nsi\{eb004a03-9b1a-11d4-9123-0050047759bc}\24\ffffffffffffffffffffffffffffff02

HKLM\SYSTEM\ControlSet001\Control\Nsi\{eb004a03-9b1a-11d4-9123-0050047759bc}\24\ffffffffffffffffffffffffffffff03

HKLM\SYSTEM\ControlSet001\Control\TimeZoneInformation\ActiveTimeBias

HKLM\SYSTEM\ControlSet001\Services\BITS\Performance\PerfMMFileName

HKLM\Software\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading

HKLM\Software\Microsoft\WBEM\CIMOM\List of event-active namespaces

HKLM\Software\Microsoft\WBEM\WDM\%windir%\system32\advapi32.dll[MofResourceName]

HKLM\Software\Microsoft\WBEM\WDM\IDE\DiskAMDX_HARDDISK____________________________2.5+____\5&2770a7af&0&0.0.0_0-{05901221-D566-11d1-B2F0-00A0C9062910}

HKU\S-1-5-21-575823232-3065301323-1442773979-1000_CLASSES\Local Settings\MuiCache\17b\52C64B7E\LanguageList

\\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Time Zones\Greenland Standard Time\TZI

\\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Time Zones\Iran Standard Time\TZI

\\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Time Zones\Middle East Standard Time\TZI

\\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Time Zones\Paraguay Standard Time\TZI

### Associated Crypto Address

| ADDRESS | MD5 |
|---|---|
| 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn | ff988bc6e0c576f2989208af77c315ac |
| 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw | ff988bc6e0c576f2989208af77c315ac |
| 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb 94 | ff988bc6e0c576f2989208af77c315ac |
| 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn | c2c066dfd2a09a9d4f5af0637c9d23d5 |

## CyberPeace Advisory

- Do not expose critical services unnecessarily to the internet.
- Add the IOCs mentioned in the report to the blacklist of your firewall solution in order to block inbound connections appearing from the respective IP addresses and to prevent the Cyberattacks involving the same attack patterns.
- Network firewalls should always be patched with the latest security updates.
- Isolate the critical network from the public network.
- Periodically perform technical audits of Healthcare Infrastructure Devices, networks and any other end-points directly or indirectly connected to it, to identify security concerns.
- Run CyberAwareness Drive by Cyber Experts at regular intervals for the team.
- Develop an R&D lab to enhance CyberSecurity skills among the employees.
- **Maintain strong Password Policy :**
  - Use a strong password for all devices and online accounts.
  - Passwords should be at least 8-13 characters long.
  - Passwords should contain at least one upper case [A-Z], numeric character [0-9], and a special character [!@%&....].
  - Where possible it is recommended to use key based authentication along with passwords.

- Do not use the same password for all your online accounts. All the passwords should be different for different versions.

- Try avoiding a password that consists of dictionary words.

- **Stay away from Phishing links :** Phishing is an attempt of social engineering techniques to inject malware or obtain sensitive information such as usernames, passwords, and credit card information by spreading fake links and pretending to be acting as a trustworthy entity. Please do not click on such links before verifying the authenticity of the same.

## Conclusion

Cyber criminals are taking advantage of the fact that healthcare organizations are under immense strain and are more likely to pay a ransom to get their systems up and running again. Organisations should ensure their systems are secured by reducing unnecessary data, improving the patch level of software, backup and restore procedures and auditing systems to build awareness of any threats.

## Reference:

https://www.virustotal.com/
https://otx.alienvault.com/

## Issued by

Research Wing, CyberPeace Foundation.
Research Wing, Autobot Infosec Private Ltd.

CyberPeace
Foundation

CyberPeace
Foundation

www.cyberpeace.org | secretariat@cyberpeace.net

/cyberpeacefoundation /cyberpeacengo /cyberpeacefoundation