Network Packet Capturing and Incidence Response Planning to Avoid Ransomware

(Packet Capturing, Ransomware)

Mrs. Varanasi Usha Bala[#1], Akhil Karrothu[*2], B.Sanat Kumar[#3]

[#] *Assistant Professor, Department of Computer Science and Engineering,*
Anil Neerukonda Institute of Technology and Sciences,Visakhapatnam,
Andhra Pradesh, India.

Abstract

Nowadays ransomware has become the alarming situation over the internet which attacks the user's system over the internet and demands ransom to get back to the original working state of the user's system. Our main idea is to avoid ransomware by capturing and analyzing the packet which is sent through the mail server and then block that packet so as to avoid the ransomware attack. The packet which is captured is tested for a malware and then blocked. We also propose an incident plan to avoid the ransomware attack. This method of avoiding ransomware attack might increase the organizations' performance thereby increasing the business continuity.

Keywords:

Cyber Attack, Packet Capturing, Network Packet Analysis, Ransomware, Ransom, business continuity, malware, Incidence Response Plan, Ransomware Incidence Response Life Cycle(RIRLC).

I. INTRODUCTION

Computer security is the process of protecting the computer systems from unauthorized access. This can be done either by preventing or avoiding the unauthorized access to the computer system.

Security over the network can be defined as policies and procedures used to provide safety to the computer systems over the internet and to provide the goals of security which are confidentiality, integrity and availability. This can also be termed as Network security. The components of network security include the data, hardware, software and firmware. This can also be referred to as Cyber security.

If the security of the systems and the network is compromised then there will be a huge loss to the electronic assets of the organization or an individual. The databases, mail servers, the expert systems etc. can be compromised. In this paper we suggest techniques to detect, capture, analyze, and then plan for avoiding the ransomware attacks.

II. RANSOMWARE

Ransomware is the latest form of cyber-attack where the hacker attacks the user's system and locks it for a demand of ransom over the network. This is a type of online crime where the users are badly affected. Unless and until the users pay the ransom their systems will not be unlocked for accessing. This ransomware attacks usually originate through malicious emails. Once the user tries to access the email which is sent by the attacker then the user's system will be automatically attacked and locked for ransom thereby displaying intimidating messages or horrifying links. This email might redirect the user to click on to a link for making the payment and this link might be malicious and may contain more infectious malware which will be active only for a given period of time or else the user might lose the data forever.

The protection of electronic assets is to be given the highest priority in all the organizations by improving the basic controls of the network security and information security. There are two categories of ransomware. They are crypto-based ransomware and locking. In crypto-based ransomware all the user's data or files will be encrypted and demands ransom for decrypting the original data or files. In locking based ransomware the user will not be able to use his/her machine only but full system is locked without being used. These attacks can be termed as vulnerabilities that compromise the user's network.

Once the user's system is prone to ransomware attack then the malware that affected the user's system will make sure that there is significantly less network traffic so as to make sure user's system is compromised.

Our main motto is to mitigate the risk of the ransomware attacks. In this paper we suggest techniques and plans to avoid ransomware attacks through phishing mails. One best way is to capture the network traffic on the user's system and try following the Ransomware Incidence Response Life Cycle (RIRLC).

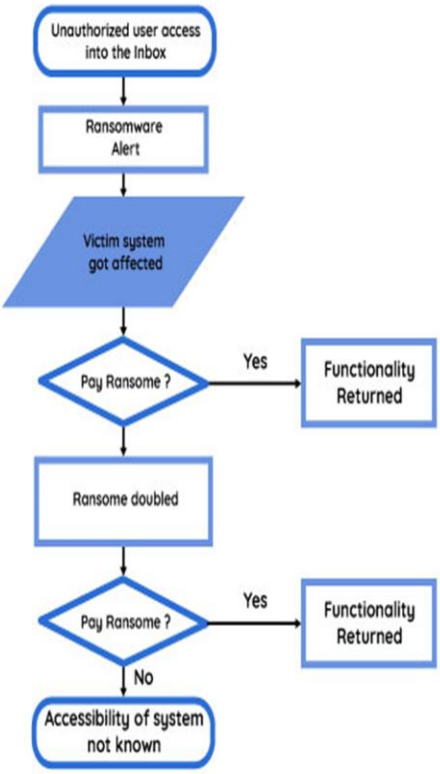


Fig 1: The Ransomware Process

The process of preventing, avoiding and mitigating cyber-attacks can be referred to as Incident Response. This Incident Response is a systematic approach that avoids security breaches by:

- Identifying Vulnerabilities;
- Strengthening network security parameters; and
- Safeguarding access to sensitive data.

The Ransomware Incident Response Life Cycle (RIRLC) is the method we suggest to avoid the ransomware attacks. It can be executed in seven stages.

A) RIRLC Life Cycle Stages:

1. *Preparation:*

this is the first phase for all the organizations to be prepared for any incident or attack that is going to occur. This phase indicates the trigger of an incident or a ransomware attack, response and recovery techniques used and suggested, training the employees to handle the attacks, modifications in the existing policies and procedures etc.,

2. *Identification:*

the most crucial phase is the identification phase where the identification of the actual incident, in this case identification of the ransomware attacks. This phase is used to analyze the symptoms of the attack. The network traffic will be monitored if it is regular or looks for any deviations. Root Cause Analysis can be used to identify the occurrence of the Ransomware incident. When the user's system is compromised for ransom then the user should know whom to contact for reporting anomalies. There may be different vectors that fall under this category of identification of the incident such as :

a. Emails
b. Macros
c. Attachments
d. Temporary folders
e. Patch management and updating
f. Antivirus protection
g. Disabling Flash
h. Disabling Windows Scripting Host

i. Root Cause Analysis: it is one of the ways to identify the potential cases how ransomware attacks a system. The cause of ransomware into an organization may be thru an unsolicited email attachment or web browser vulnerabilities.

3. *Containment:*

once the ransomware infected system is identified we need to contain it at the beginning of the incident response itself. This can be done by the following steps:

a. Disconnect the system from the network;
b. Shutdown the network and the system, then report to the authorities;
c. Continue the system to be on the network and monitor the network traffic;
d. Identifying the operational status of the affected system.

4. **Investigation:**

this is the step that involves systematic review of what actually happened to the affected system or network. The detailed study of the logs, storage and memory are to be considered.

5. *Eradication:*

this is the phase that involves the removal of the Ransomware from the user's system. The systems that have been identified and infected with ransomware should be rebuilt from the scratch. There are two steps to be followed during eradication phase. They are:

a. *Clean-up:*

If the Root Cause Analysis reports that ransomware is caused due to an email then the organization should eradicate or exclude all the messages from that mail source and isolate the system which is working with that email. If the Root Cause Analysis reports that ransomware is caused due to a web browser those sites should be either blocked or uninstalled from being accessed. Passwords also should be changed on a regular basis.

b. *Notification*:

it includes the notifying authorities to whom the incident occurrence is to be reported.

6. *Recovery*:

once the root cause for the ransomware attack has been identified and contained the immediate step is the recovery phase. This is the step that restores the system or the organization to normalcy. There are two steps for recovery process.

a. Service Restoration:

this implies restoring the affected files from the backups or the data warehouse available.

b. System/ Network Validation:

once the system restoration is done the system should be tested for validating the necessary constraints of security i.e. confidentiality, integrity and availability.

7. Follow-up:

this can also be referred to as post-incidence activity that includes the lessons learnt and the security controls used during the incident response. This documentation helps to mitigate future ransomware attacks.

INCIDENT MANAGEMENT ACTIVITIES:

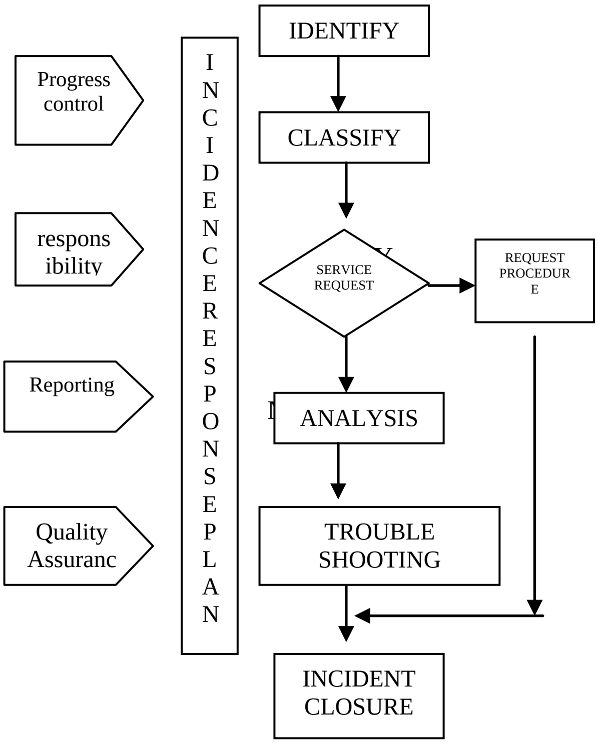


Fig 2: Incident Response Plan

III. PACKET CAPTURING AND PENETRATION TESTING

Packet capturing is the process of capturing the packets over the network and analyse it. It can also be called as packet analysing. Packet capturing is the technique used by the network administrators and network security professionals to troubleshoot the network problems. It can also be called as packet sniffing.

Penetration testing is a process of testing a computer system or a network for any malicious activity. It can also be referred to as Pen testing. It is done to test the system's efficiency over the network. It is a process of testing for vulnerabilities within the systems or the networks etc. Some of the famous penetration testing tools are listed below:

- Wireshark
- Metasploit
- AirCrack
- Kali Linux
- TCP Dump
- Sqlmap
- Nmap etc.

IV. METHODOLOGY

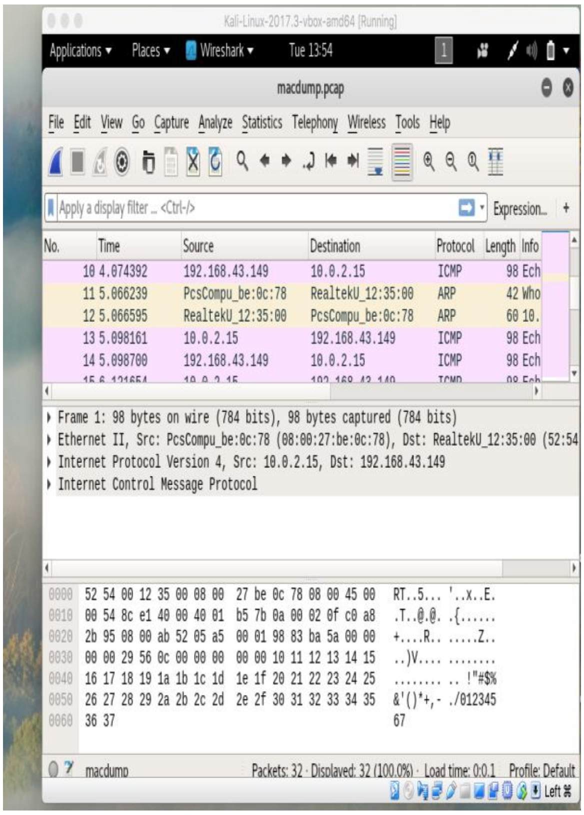
A. *Packet Capturing*

a. Wireshark:

Wireshark is a packet analyser and is used for network troubleshooting. It provides the smallest details of network protocols, encryption types, decryption types, packet information etc. Earlier it is known an Ethereal. It supports more than 1200 protocols with a wide range of filters. This is a graphical user interface to capture the packets. This Wireshark provides many options for the network engineers to perform network traffic auditing.

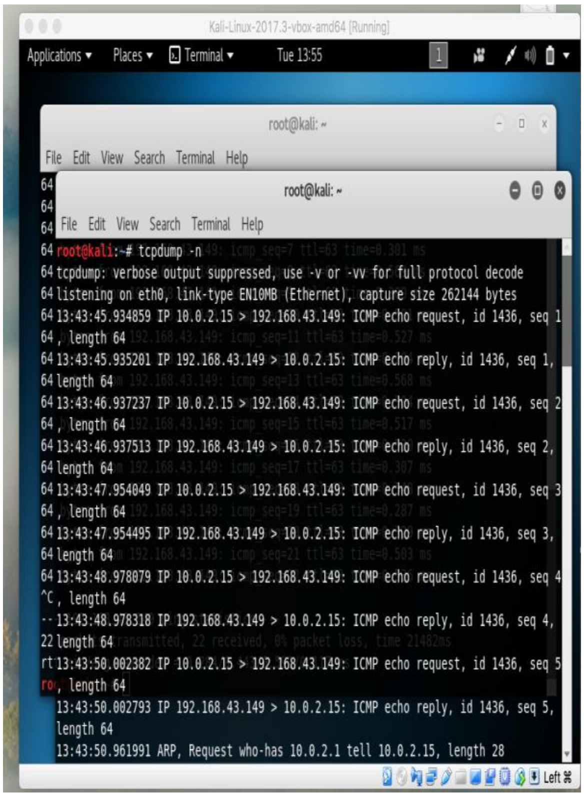
***b. TCP Dump*:**

it is also a packet analyser that dumps the traffic onto the network. TCP Dump can be used to print the headers or the contents of the packets on a network. It also monitors the network activities. It is a command line interface packet sniffer. It allows the user to display different types of packets received over the network. TCP Dump uses libcap or wincap to capture the data.


Kali-Linux-2017.3-vbox-amd64 [Running]
Applications ▾ Places ▾ Wireshark ▾ Tue 13:54
macdump.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression... +
macdump
Left ⌘

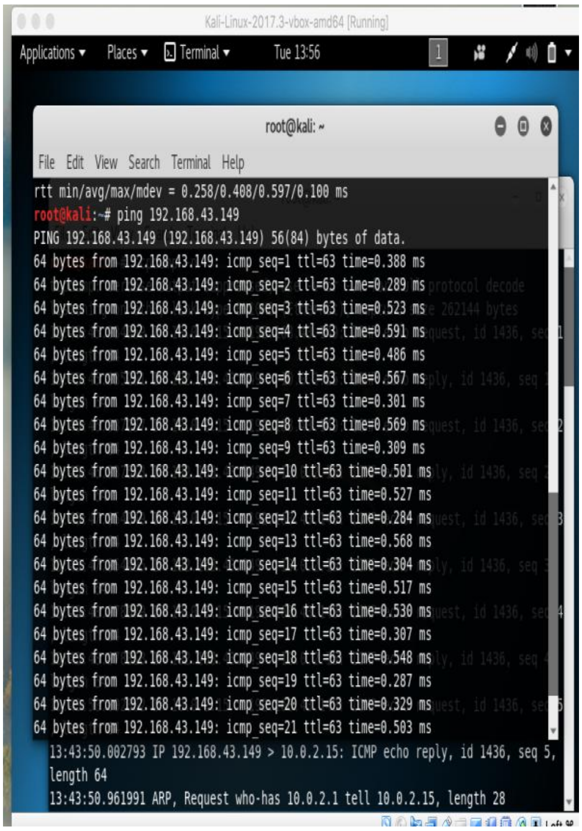
```
No.   Time        Source              Destination         Protocol  Length Info
   10 4.074392    192.168.43.149      10.0.2.15           ICMP          98 Ech
   11 5.066239    PcsCompu_be:0c:78   RealtekU_12:35:00   ARP           42 Who
   12 5.066595    RealtekU_12:35:00   PcsCompu_be:0c:78   ARP           60 10.
   13 5.098161    10.0.2.15           192.168.43.149      ICMP          98 Ech
   14 5.098700    192.168.43.149      10.0.2.15           ICMP          98 Ech

▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▸ Ethernet II, Src: PcsCompu_be:0c:78 (08:00:27:be:0c:78), Dst: RealtekU_12:35:00 (52:54
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.43.149
▸ Internet Control Message Protocol

0000  52 54 00 12 35 00 08 00  27 be 0c 78 08 00 45 00   RT..5... '..x..E.
0010  00 54 8c e1 40 00 40 01  b5 7b 0a 00 02 0f c0 a8   .T..@.@. .{......
0020  2b 95 08 00 ab 52 05 a5  00 01 98 83 ba 5a 00 00   +....R.. .....Z..
0030  00 00 29 56 0c 00 00 00  00 00 10 11 12 13 14 15   ..)V.... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67

Packets: 32 · Displayed: 32 (100.0%) · Load time: 0:0.1   Profile: Default
```

Fig 3: MAC Dump with pcap


Kali-Linux-2017.3-vbox-amd64 [Running]
Applications ▾ Places ▾ Terminal ▾ Tue 13:55
root@kali: ~
File Edit View Search Terminal Help
Left ⌘

```
root@kali:~# tcpdump -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:43:45.934859 IP 10.0.2.15 > 192.168.43.149: ICMP echo request, id 1436, seq 1
, length 64
13:43:45.935201 IP 192.168.43.149 > 10.0.2.15: ICMP echo reply, id 1436, seq 1,
length 64
13:43:46.937237 IP 10.0.2.15 > 192.168.43.149: ICMP echo request, id 1436, seq 2
, length 64
13:43:46.937513 IP 192.168.43.149 > 10.0.2.15: ICMP echo reply, id 1436, seq 2,
length 64
13:43:47.954049 IP 10.0.2.15 > 192.168.43.149: ICMP echo request, id 1436, seq 3
, length 64
13:43:47.954495 IP 192.168.43.149 > 10.0.2.15: ICMP echo reply, id 1436, seq 3,
length 64
13:43:48.978079 IP 10.0.2.15 > 192.168.43.149: ICMP echo request, id 1436, seq 4
^C, length 64
13:43:48.978318 IP 192.168.43.149 > 10.0.2.15: ICMP echo reply, id 1436, seq 4,
length 64
13:43:50.002382 IP 10.0.2.15 > 192.168.43.149: ICMP echo request, id 1436, seq 5
, length 64
13:43:50.002793 IP 192.168.43.149 > 10.0.2.15: ICMP echo reply, id 1436, seq 5,
length 64
13:43:50.961991 ARP, Request who-has 10.0.2.1 tell 10.0.2.15, length 28
```

Fig 4: TCP Dump screenshot


Kali-Linux-2017.3-vbox-amd64 [Running]
Applications ▾ Places ▾ Terminal ▾ Tue 13:56
root@kali: ~
File Edit View Search Terminal Help

```
rtt min/avg/max/mdev = 0.258/0.408/0.597/0.100 ms
root@kali:~# ping 192.168.43.149
PING 192.168.43.149 (192.168.43.149) 56(84) bytes of data.
64 bytes from 192.168.43.149: icmp_seq=1 ttl=63 time=0.388 ms
64 bytes from 192.168.43.149: icmp_seq=2 ttl=63 time=0.289 ms
64 bytes from 192.168.43.149: icmp_seq=3 ttl=63 time=0.523 ms
64 bytes from 192.168.43.149: icmp_seq=4 ttl=63 time=0.591 ms
64 bytes from 192.168.43.149: icmp_seq=5 ttl=63 time=0.486 ms
64 bytes from 192.168.43.149: icmp_seq=6 ttl=63 time=0.567 ms
64 bytes from 192.168.43.149: icmp_seq=7 ttl=63 time=0.301 ms
64 bytes from 192.168.43.149: icmp_seq=8 ttl=63 time=0.569 ms
64 bytes from 192.168.43.149: icmp_seq=9 ttl=63 time=0.309 ms
64 bytes from 192.168.43.149: icmp_seq=10 ttl=63 time=0.501 ms
64 bytes from 192.168.43.149: icmp_seq=11 ttl=63 time=0.527 ms
64 bytes from 192.168.43.149: icmp_seq=12 ttl=63 time=0.284 ms
64 bytes from 192.168.43.149: icmp_seq=13 ttl=63 time=0.568 ms
64 bytes from 192.168.43.149: icmp_seq=14 ttl=63 time=0.304 ms
64 bytes from 192.168.43.149: icmp_seq=15 ttl=63 time=0.517 ms
64 bytes from 192.168.43.149: icmp_seq=16 ttl=63 time=0.530 ms
64 bytes from 192.168.43.149: icmp_seq=17 ttl=63 time=0.307 ms
64 bytes from 192.168.43.149: icmp_seq=18 ttl=63 time=0.548 ms
64 bytes from 192.168.43.149: icmp_seq=19 ttl=63 time=0.287 ms
64 bytes from 192.168.43.149: icmp_seq=20 ttl=63 time=0.329 ms
64 bytes from 192.168.43.149: icmp_seq=21 ttl=63 time=0.503 ms
13:43:50.002793 IP 192.168.43.149 > 10.0.2.15: ICMP echo reply, id 1436, seq 5,
length 64
13:43:50.961991 ARP, Request who-has 10.0.2.1 tell 10.0.2.15, length 28
```

Fig 5: Pinging of Captured IP Screenshot

B. *Techniques for preventing Ransomware Attack*

- Regular backup of the entire data is very important to prevent ransomware;
- Disable Macros;
- Personalizing the anti-spam settings;
- Updating the OS regularly;
- Updating the browsers and Adobe Flash Player in a timely manner;
- Regularly updating the anti-virus and other system files;
- Conducting Security awareness campaigns inside and outside the organization;
- Revision of the security procedures and policies on a regular basis;
- Conducting pen testing regularly;
- Disabling Windows Script Host;
- Disable remote services and file sharing;
- Usage of strong passwords to avoid hacking thru brute-force techniques;
- Turn on Windows Firewall settings on and if necessary opt for the advance settings;
- Blocking of famous malicious IP addresses.

V. CONCLUSION AND FUTURE WORK

Packet capturing tools such as Wireshark and TCP Dump are very helpful in analysing, detecting and monitoring network traffic for malicious activities such as ransomware. Penetration testing plays a vital role in assessing the network traffic so as to protect the confidential data and information assets. This paper mainly focuses on malicious ransomware activities and the Ransomware Incidence Response Plan to avoid ransomware. This work can be further extended by deploying the Incidence Response Plan.

ACKNOWLEDGMENTS

We would like to thank the staff and management of ANITS Engineering College for encouraging and supporting throughout our academics. Our special thanks to our mentors for giving us this opportunity.

REFERENCES

[1] Gammons, B. (2016). 5 Things to know about the Rise of Ransomware among Healthcare Providers Retrieved from https://blog.barkly.com/rise-of-ransomware-healthcare-stats.

[2] Kim Boatman, “Beware the Rise of Ransomware”,http://in.norton.com/yoursecurityresource/detail.jsp?aid=rise_in_ransomware

[3] Zetter, K. (2016, March 30). Why Hospitals are the Perfect Targets for Ransomware. Retrieved from https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

[4] Carrier, B. “File System Forensic Analysis”, Addison-Wesley Professional, (2005).

[5] Krebs, B. (2016, March 22). Hospital Declares ‘Internal State of Emergency’ After Ransomware Infection. Retrieved from http://krebsonsecurity.com/2016/03/hospital-declares-internet-state-ofemergency-after-ransomware-infection/

[6] CISCO,Inc. Ransomware on Steroids: Cryptowall2.0.http://blogs.cisco.com/security/talos/cryptowall-2.

[7] Narayanan A, Shmatikov V. De-anonymizing social networks, in: Proceedings of the 30th IEEE Symposium on Security and Privacy (S&P 2009), IEEE Computer Society, 2009, pp. 173–87. Perito D, Castelluccia C, Kaafar MA, Manils P. How unique and traceable are usernames? In: Privacy Enhancing Technologies. Springer; 2011. p. 1–17.

[8] Ali, Murthy, R., & Kohun, F.(2016). Recovering from the nightmare ransomware-How savvy users get hit with viruses and malware: A personal case study: Issues in Information Systems, 17(4),58-69.

[9] Zeng, Kazemian, Varghese,and Nick “Automatic Test Packet Generation”,VOL. 22, NO. 2, APRIL, 2014.

[10] Knowles W, Baron A, McGarr T. The simulated security assessment ecosystem: does penetration testing need standardisation? CompSec 2016;62:296–316. Kontaxis G, Polakis I, Ioannidis S, Markatos EP. Detecting social network profile cloning,in: Pervasive Computing and Communications Workshops(PERCOM Workshops),2011 IEEE International Conference on, IEEE, 2011, pp. 295–300.

[11] Dewan P, Kashyap A, Kumaraguru P. Analyzing social and stylometric features to identify spear phishing emails. In: APWG Symposium on Electronic Crime Research (eCrime), Institute of Electrical and Electronics Engineers. 2014.

[12] p.1–13. doi:10.1109/ecrime.2014.6963160.

[13] Krebs on Security, “Inside a Reveton RansomwareOperation”http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

[14] Bowen, B. M., Hershkop, S., Keromytis, A. D., Stolfo, S. J. “Baiting inside attackers using decoy documents”, Springer, (2009).

[15] Kharraz, W. Robertson, D. Balzarotti, L. Bilge, E. Kirda, “Cutting the gordian knot: A look under the hood of ransomware attacks”,12th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2015), July 9-10, 2015, Milan, Italy.

[16] Green B, Prince D, Busby J, Hutchison D. The impact of social engineering on industrial control system security, in: Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy, ACM, 2015, pp. 23–9. Huber M, Kowalski S, Nohlberg M, Tjoa S. Towards automating social engineering using social networking sites, in: International Conference on

[17] Computational Science and Engineering, 2009 (CSE‘09), Vol. 3, IEEE, 2009, pp. 117–24.

[18] K.Cabaj, P.Gawkowski, K.Grochowski, D. Osojca, “Network activity analysis of CryptoWall ransomware”, Przeglad Elektrotechniczny, vol. 91,

[19] nr11,2015,ss.201-204,URL:http://pe.org.pl/articles/2015/11/48.pdf.

[20] Zhang H, Yao DD, Ramakrishnan N, Zhang Z. Causality reasoning about network events for detecting stealthy malware activities. Comp Sec 2016;58:180–98

[21] Bharadwaj, A.,Avasthi, V.,Sastry, H.,& subrahmanyam, G.V.B.(2016). Ransomware digital extortion: A rising new age threat. Indian Journal of Science and Technology, 9,14.

[22] Azad Ali, Ransomware: A research and a personal case of Dealing with this nasty malware (IISIT.org), Volume 14, 2017.

[23] Ransomware Response Guide, IBM Incidence Response Services, May 2016.