IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005024

Malware Incident Prevention and Handling

Shubham Choudhari[1], Aditya Gupta[2], Rajeshwari Gundla[3]

Student, School of Engineering, Ajeenkya D Y Patil University, Pune, India[1]

Student, School of Engineering, Ajeenkya D Y Patil University, Pune, India[2]

Assistant Professor, School of Engineering, Ajeenkya D Y Patil University, Pune, India[3]

ABSTRACT: Malware, also known as malicious code, is software that is hidden inside another programme with the aim of causing data loss, running disruptive or intrusive programmes, or jeopardising the protection, integrity, or availability of the victim's data, applications, or operating system. Malware is the most prevalent external threat to most hosts, causing widespread damage and destruction as well as substantial recovery efforts within most organisations. This guide will show you how to make your company's malware incident response procedures better. It also includes concrete suggestions for strengthening an organization's current crisis management capabilities. It also includes detailed recommendations for enhancing an organization's current incident response capabilities so that it can better manage malware incidents, particularly those that are widespread.

KEYWORDS: Malware, Virus, Worms, Incident Prevention and Incident Handling

I. INTRODUCTION

Malware, known also as malicious code, is a programme secretly installed on a computer, to jeopardise the safety, integrity, or availability of the victim's data, programmes or the operating system, or to annoy or otherwise interrupt the victim. The most major external threat to most networks has been malware, causing considerable damage and devastation and requiring substantial recovery efforts in most organisations.Businesses also worry about spyware malware invading the privacy of a user. While the privacy-invading malware has been around for some time, spyware infiltrated several systems recently, which monitor personal activities and commit financial fraud, is much more common. Organisation, which are often associated with malware, are at risk of a range of non-malware threats. Phishing is one of these commonly used means of using misleading computer-based methods to make people share sensitive data. Another common type of virus hoaxes are fake notices of new threats to malware.

II. LITERATURE SURVEY

Christodorescu et al., 2005[1] recommends that the prevention of malware by a company be enhanced. It also includes detailed recommendations to enhance the capability of an organisation to respond to incidents more effectively, particularly in cases of malware commonly encountered. The guidelines cover viruses, worms, trojans, mobile code, mixed attacks, cookies and intruders for spyware monitorings, such as backdoors and rootkits. The guidelines encompass a range of methods of delivery, including networks and removable media.

Malicious code is described by McGraw and Morrisett (2000) as "any code added, modified, or removed from a software system in order to deliberately cause harm or subvert the system's intended purpose." Malware developers can create applications that appear normal but are designed specifically to obtain approved access to a target's smartphone and steal personal information to sell for profit or conduct other harmful activities. These applications can seriously compromise a user's privacy, steal personal data, spy on the user, and commit other malicious activities.

[3] According to Wikipedia, malware is “a generic concept that covers viruses, Trojans, spywares, and other intrusive code” (Vasudevan and Yerraballi, 2006). Malware targeting Android phones has risen by 76% in the last few months, posing a threat to Android security, and malware targeting other platforms is also on the rise. In addition to ransomware, personal spyware and greywater are the other two major forms of threats to mobile devices. Without the victim's awareness, spyware gathers data such as the victim's location, MS messages, and call history. While spyware cannot be categorised as illegal since it does not send information to the application's author, installing personal spyware on a mobile phone without the permission of the device's owner could be considered unethical.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005024

III. MALWARE INCIDENT PREVENTION

This section includes recommendations for preventing malware attacks inside a business. The most critical aspects of prevention are regulation, identification, risk reduction, hazard mitigation, and protective architecture. As a foundation for implementing preventive controls, ensure that policies discuss malware security. To reduce the number of accidents caused by human error, it is critical to develop and sustain general malware awareness programmes for all users, as well as specialised malware awareness training for IT staff explicitly engaged in malware prevention–related operations [3,4].

Policy

The following are some of the most common malware mitigation policy considerations:

- requiring the scanning of external media for malware before it can be used
- requiring the scanning of email file attachments before they are opened
- Limiting or preventing the use of unnecessary software, such as user applications that are often used to transmit malware, by prohibiting the sending or receiving of certain types of files via email
- limiting the use of portable media (e.g., flash drives) on hosts that are at high risk of contamination, such as public kiosks.
- listing the high-level specifications for configuring and maintaining preventive software (e.g., antivirus software, content filtering software) for each type of host (e.g., email server, web server, laptop, smart phone) and application (e.g., email client, web browser), and specifying which types of preventive software (e.g., antivirus software, content filtering software) are available for each type of host (e.g., email client, web browser)
- limiting or banning the usage of company-issued and personal-owned mobile devices on company networks and for telework/remote access [8].

Awareness

A successful awareness programme outlines the correct rules of behaviour for IT hosts and expertise in an organisation. As a result, consumer advice on malware incident prevention should be included in awareness campaigns, which could help reduce the frequency and severity of malware incidents [8]. The following are some examples of such practises:

- not opening suspicious emails or attachments, clicking on hyperlinks, etc. from unknown or identified senders, or visiting websites with malicious material
- not clicking on suspicious pop-up windows in web browsers
- not opening files with file extensions that are likely to be associated with malware (e.g.,.bat,.com,.exe,.pif,.vbs) (e.g., antivirus software, content filtering software, reputation software, personal firewall)
- not using administrator-level accounts for day-to-day host operations - not installing or running applications from untrustworthy sources.

Organizations should educate their users on the social engineering tactics that are used to trick users into sharing information as part of their awareness activities [8]. The following are some suggestions for preventing phishing and other types of social engineering:

- Instead, call or visit the person's or organization's official phone number or website. Do not use the email's contact information, and do not open any attachments or click on any hyperlinks in the email.
- Do not respond to emails or unsolicited popup windows with passwords, PINs, or other access codes. Such details can only be entered into a valid website or application.
- Even if the email comes from a known source, do not open suspicious email file attachments. If you receive an unwanted attachment, contact the sender to confirm that it is genuine (preferably using a means other than email, such as phone).
- Do not respond to any unsolicited or suspicious emails. (Asking to get an email address deleted from a hostile party's mailing list confirms the email address's presence and active usage, which may lead to further attack attempts)

Vulnerability Mitigation

Malware often attacks hosts by exploiting bugs in operating systems, services, and software. As a consequence, patching vulnerabilities is essential for preventing malware attacks, particularly when malware is released shortly after a replacement vulnerability is revealed, or even before a vulnerability is publicly acknowledged.[2, 6].

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005024

Organizations can follow sound host hardening principles when it comes to security configurations. Other host hardening steps, such as the following, should be implemented to further minimise the likelihood of malware incidents:

Disabling or removing unnecessary services (especially network services), which can be used by malware to spread.

- removing unsecured file shares, which are a popular way for malware to spread.
- deleting or modifying default usernames and passwords for operating systems and applications that malware might use to gain unauthorised access to hosts
- Disabling automatic execution of binaries and scripts on Windows hosts, including Auto Run
- modifying the default file associations for file types that are often used by malware but not by users (e.g.,.pif,.vbs) so that these files are not automatically run when users try to open them.

The ability to rapidly change software configuration settings, including temporary remediation steps, is also very useful in quickly remediating vulnerabilities. A configuration change, for example, may temporarily disable a compromised service while its provider prepares and deploys a patch to permanently fix the flaw. If the patch is usable and installed, the company can reverse the configuration update to reactivate the not vulnerable service. In the event of a malware attack, organisations should think about how configuration settings could be changed and identify and manage appropriate protocols ahead of time [2].

Threat Mitigation

Organizations may use threat monitoring to detect and prevent malware before it has a chance to damage their intended goals. Even if a host's vulnerabilities have been mitigated to a large degree, threat mitigation is still necessary to avoid malware that does not exploit vulnerabilities, such as social engineering attacks that trick users into running malicious files [7].

Antivirus Software

The most widely used technical control for malware threat reduction is antivirus software. Antivirus software comes in a variety of flavours, but they all provide similar security through the features mentioned below [4]:

- Examining important host components including start-up files and boot records.
- Monitoring host activities in real time to look for suspicious behaviour
- Observing how popular applications like email clients, web browsers, and instant messaging apps behave.
- Looking for suspected malware in files.
- Recognizing common malware types as well as attacker resources.
- Disinfecting and quarantining files, which refers to removing malware from inside a file and storing malware-infected files in isolation for possible disinfection or review.

Intrusion Prevention Systems

Network-based intrusion prevention systems (IPS) sniff packets and analyse network traffic in order to identify and prevent malicious behaviour. Network-based IPS devices are often deployed inline, which means the system acts as a network firewall. It receives packets, analyses them, and then enables the transfer of relevant packets. Because of the network-based IPS architecture, certain attacks can be detected on networks before they reach their intended targets [7]. To detect potentially malicious activity, most network-based IPS products combine attack signatures with network and system protocol analysis, which means they compare network activity for frequently attacked applications to expected behaviour.

Firewalls

A network firewall is a system that is installed between networks to control which types of traffic are allowed to move from one to the other. A host-based firewall is software that runs on a single host and controls incoming and outgoing network traffic for that host alone. Both types of firewalls can help protect against malware attacks. Organizations should set up their firewalls with deny by default rulesets, which means that all incoming traffic that isn't explicitly allowed is denied [7].

Content Filtering/Inspection

Stopping email-based malware threats requires the use of content inspection and filtering technologies. Spam filtering tools can be used by businesses to reduce the amount of spam that reaches users. Since spam is frequently used to distribute malware, especially phishing attacks, reducing spam should result in a decrease in spam-triggered malware incidents. Organizations should also suggest configuring their email servers and clients to block attachments with malicious file extensions (e.g.,.pif,. vbs) and questionable file extension combinations[5].

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005024

Application Whitelisting
Application whitelisting systems, also known as application management programmes, are used to determine which applications are permitted to run on a particular host. There are two modes of operation for most programme whitelisting technologies: audit and compliance. In enforcement mode, the technology usually prevents the execution of any applications not on the whitelist. In audit mode, the technology records all non-whitelisted applications running on the host but does little to stop them [10].

Defensive Architecture
Malware incidents can occur regardless of how thorough vulnerability and threat mitigation efforts are. This section outlines four complementary approaches that organisations should consider using to change the protective architecture of a host's software and reduce the effect of incidents: BIOS protection, sandboxing, window separation, and virtualization-based segregation [9].

BIOS Protection
Because of the BIOS's special and privileged location within the PC architecture, malicious software modifying the BIOS firmware poses a significant danger. A malicious BIOS alteration could be part of a complex, coordinated attack on an enterprise, resulting in either a permanent denial of service (if the BIOS is corrupted) or a long-term malware presence (if the BIOS is implanted with malware) [11].

Sandboxing
Sandboxing is a security paradigm in which applications are run in a managed environment that limits the operations that they can perform and isolates them from other applications operating on the same host. In a sandbox security model, only permitted "secure" operations are allowed to be conducted inside the sandbox; the sandbox prevents applications from performing any other operations. To keep the sandbox's applications apart from the host's other applications, the sandbox limits access to device resources including memory and the file system [3].

Browser Separation
On a single host, multiple browser brands (such as Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, Google Chrome, and Opera) can be enabled. Accessing malicious Web pages, such as malicious plug-ins installed inside a browser, is one of the most popular ways for hosts to be targeted. Users should use one brand of browser for business applications and another brand for all other website access to reduce the effect of such attacks [5].

Malware incident response
The incident response process has four main stages, according to NIST SP 800-61, Computer Security Incident Handling Guide: planning, identification and review, containment/eradication/recovery, and post-incident operation. This segment of the guide expands on the ideas presented in SP 800-61 by offering additional information on how to deal with malware [3].

Preparation
Organizations should take precautions to ensure that they are capable of successfully reacting to malware incidents [10].

Building and maintaining malware-related skills
Malware incident responders should have a firm grasp on how each major type of malware infects and spreads. Also, incident handlers should be familiar with the organization's malware detection tool frameworks and configurations so that they can properly analyse supporting data and identify threat characteristics [1].

Facilitating communication and coordination
Bad communication and teamwork is one of the most common issues encountered when dealing with malware incidents. Because of their limited view or perception of the situation, anyone involved in an incident, including users, may unwittingly trigger additional problems. An organisation should appoint a few individuals or a small team to be responsible for coordinating the organization's responses to malware incidents ahead of time to enhance communication and planning [6].

Acquiring tools and resources
Organizations should also make sure they have the right equipment (hardware and software) and services in place to help with malware incident response [1].

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005024

Detection and analysis

To reduce the number of infected hosts and the amount of harm sustained by the company, organisations should aim to identify and verify malware incidents as quickly as possible. Since malware may take several forms and be spread in a variety of ways, there are numerous potential indicators of a malware incident, as well as numerous places within an organisation where they can be recorded or detected [5].

Identifying malware incident characteristics

Since no indicator is 100% accurate—even antivirus software can misclassify benign behaviour as malicious—incident handlers must investigate any suspected malware incident and confirm the malware is to blame. Validation may be unnecessary in some situations, such as a major, organization-wide outbreak, since the essence of the incident is apparent. Antivirus vendors are likely to have a significant amount of data on it, such as the following:

- Malware classification (e.g., virus, worm, Trojan horse)
- Vulnerabilities that are abused - Attacked services, ports, protocols, and so on (e.g., software flaws, misconfigurations, social engineering)
- Filenames, sizes, content, and other metadata that are malicious (e.g., email subjects, web URLs)
- How the malware affects the compromised host, including the names and locations of affected files, altered configuration settings, mounted backdoor ports, and so on.
- Which versions of operating systems, computers, applications, and so on, could be affected.
- How malware spreads and how to tackle its containment
- How to get rid of the malware on the host [7, 8].

Identifying infected hosts

Every malware incident includes identifying hosts that have been infected with malware. Infected hosts may be detected and treated with the necessary containment, eradication, and recovery steps. Unfortunately, the complex nature of computation makes finding all infected hosts difficult [4].

Forensic Identification

The method of detecting contaminated hosts by searching for signs of recent infections is known as forensic identification. The data may be very recent (only a few minutes old) or very old (hours or days old); the older the knowledge is, the less reliable it is likely to be [6].

DNS Server Logs

Infected hosts often leave records in DNS server logs attempting to obtain the IP address of an external malicious site with which they are attempting to communicate.

Other Application Server Logs

Email and HTTP, which are commonly used as malware transmission mechanisms, may store information in their logs that indicates which hosts were infected [2].

Network Forensic Tools

Software that captures and records packets, such as network forensic analysis tools and packet sniffers, may contain a wealth of knowledge about malware operation [8].

Network Device Logs

Network monitoring software, as well as firewalls, routers, and other filtering devices that record link behaviour, can be useful in detecting network connection activity associated with specific malware [3].

Active Identification

To determine which hosts are currently infected, active identification methods are used. Some active methods may be used to conduct containment and eradication steps for the host immediately after detecting an infection, such as running a disinfection utility, deploying patches or antivirus updates, or transferring the host to a VLAN for infected hosts [4]. Active identification can be accomplished in a variety of ways, including the ones mentioned below:

Security Automation

Security automation technologies, especially those used for continuous monitoring (e.g., network access control technologies), may be used to look for signs of a current infection, such as a specific configuration setting or a system

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005024

file with a specific size that suggests an infection.

Custom Network-Based IPS or IDS Signature
Writing a custom IPS or IDS signature that detects infected hosts is a powerful technique. Some businesses have dedicated IPS or IDS sensors with powerful signature-writing capabilities for detecting malware infections.

Packet Sniffers and Protocol Analysers
Configuring packet sniffers and protocol analyzers to only search for network traffic that matches the characteristics of a specific malware threat will help distinguish infected hosts [7].

Manual Identification
Another choice for identifying infected hosts is to do so manually. This method is the most time-consuming of the three. It can only be used in situations where automated solutions aren't possible, such as when networks are completely overburdened by infection-related traffic through spoofed emails [3].

Identification Recommendations
The most accurate results come from active procedures, but they aren't always the quickest way to diagnose infections. Since hosts that have been disconnected or switched off will not be identified, scanning every host in an organisation will take a long time. If the forensic data is recent, it can be a good source of easily accessible information, but it is not always complete. While manual methods are rarely feasible for enterprise-wide detection, they are an important part of the process when other methods fail [2].

Prioritizing incident response
Since some types of malware, such as worms, spread rapidly and can have a significant effect in minutes or hours, they often require a high-priority response. Other types of malware, such as Trojan horses, appear to impact a single host; in such cases, the response should be based on the value of the host's data and services. Organizations should develop a set of guidelines for determining the acceptable level of response in different malware-related scenarios.

Malware analysis
By forensically analysing malware behaviour, incident handlers may learn more about it. On an infected host, forensic methods are preferable because they can inspect the host while the malware is still running. Tracking malware during execution, on the other hand, can be a much faster and easier way to analyse it. Such active methods should be used on malware test systems rather than manufacturing costs to mitigate the possible harm incurred by enabling the malware to execute [7].

Containment
Malware containment has two main components: keeping the malware from spreading and preventing further damage to hosts. Almost any malware incident necessitates containment measures. It is critical for an organisation to determine the containment strategies to use first, early in the response, when dealing with an incident [11].

Containment techniques are classified into four categories: depending on user interaction, automating identification, temporarily stopping services, and blocking certain forms of network access [8].

Containment through user participation
User involvement used to be an important part of containment efforts, particularly during large-scale incidents in unmanaged environments. Users were given instructions about how to spot infections and what to do if a host was infected, such as calling the support desk, disconnecting the host from the network, or turning it off. Malware eradication instructions may include things like upgrading antivirus signatures and running a host scan, as well as receiving and running a specialised malware eradication utility [3].

Containment through automated detection
Many malware incidents can be managed through the use of automated technologies for preventing and detecting infections. These technologies include antivirus software, content filtering, and intrusion prevention software. Antivirus software on hosts can detect and remove viruses, so it's often used as a prevention method to help with containment [5].Other than antivirus apps, below are some examples of automatic detection methods:

- Content Filtering

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005024

- Network-Based IPS Software
- Executable Blacklisting

Containment through disabling services

For certain malware events, more severe and potentially destructive containment steps are needed. These occurrences require heavy use of a specific facility. A loss of resources, such as shutting down a service used by malware, blocking a specific service at the network perimeter, or disabling parts of a service, may be used to rapidly and efficiently contain such an event [8].

Containment through disabling connectivity

By temporarily limiting network access, incidents may be easily contained. Handlers should recommend blocking all connections to the external host if compromised hosts attempt to connect to it in order to download rootkits (by IP address or domain name, as appropriate). Similarly, if infected hosts inside the organisation attempt to spread malware, the organisation will block network traffic from the infected hosts' IP addresses to keep the situation under control until the infected hosts are located and disinfected [3].

Containment recommendation

Containment can be achieved in a number of ways, including those mentioned in the four categories above (users, automated detection, loss of services). Since no single malware containment category or approach is appropriate or successful in every situation, incident handlers should combine containment methods that are likely to be effective in containing the current incident while limiting host damage and mitigating the impact of containment methods on other hosts. Shutting down all network access, for example, could be a safe way to prevent malware from spreading, but it also allows infections on hosts to continue damaging files and disrupting many critical business functions. [8].

Eradication

While the primary aim of eradication is to eradicate malware from compromised hosts, it usually entails a lot more. If an infection was effective due to a host vulnerability or other security flaw, such as an unsecured file share, eradication involves the removal or mitigation of that vulnerability, which can prevent the host from being reinjected or compromised by a variant of the original threat [3].

Instead of conducting traditional eradication actions, organisations can restore any host that has any of the following incident characteristics:

- Administrative access to the host was obtained by one or more attackers.
- Anyone may gain unauthorised administrator-level access to the host through a backdoor, an insecure share generated by a worm, or other means.
- A Trojan horse, backdoor, rootkit, intruder software, or other means replaced system files.
- After the malware has been removed by antivirus software or other programmes or techniques, the host becomes vulnerable or ceases to function properly. This means that the malware hasn't been fully removed or that it has corrupted important device or programme files or settings.
- There is uncertainty regarding the existence and scope of the infection, as well as any unauthorised access obtained as a result of it.

If a malware incident lacks all of these characteristics, removing the malware from the host rather than restoring the host is usually appropriate [6].

Recovery

The restoration of compromised hosts' functionality and data, as well as the elimination of temporary containment steps, are the two most important aspects of malware recovery. Most malware events that cause only minor host harm do not necessitate additional actions to restore hosts [3].

Organizations should carefully analyse worst-case scenarios, such as a new malware attack requiring the reconstruction of a significant percentage of the organization's workstations, and decide how the hosts will be recovered in these situations. This should include deciding who will perform the recovery activities, calculating how many hours of labour will be required and how much time will pass on the calendar, and prioritising the recovery efforts [8].

Future of Malware

Today, all of this specialisation and business interaction is troublesome enough, but what lies ahead? One source of concern is the automation of malware variant production. Attackers could churn out thousands of functionally distinct samples every day using machine learning techniques similar to those used by defenders to detect and dissect malware. These variants may each differ in function and nature, overwhelming defenders, and no longer had the subtle

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15680/IJIRSET.2021.1005024

adjustments intended to fool intrusion detection and prevention systems. Groups can rent or sell these automated assembly lines to the highest bidder, with competition driving innovation in new capabilities and features[2].

IV. CONCLUSION

Finally, malware markets are a way of describing governments', companies', criminals', and individuals' global relationships. On the internet, attackers and defenders battle for vulnerability awareness and advantage. Understanding these markets will help to emphasise the importance of high-profile arrests and convictions while also highlighting how difficult it is to shut them down entirely[4].

REFERENCES

[1] Christodorescu, Mihai, et al. "Semantics-aware malware detection." 2005 IEEE Symposium on Security and Privacy (S&P'05). IEEE, 2005.
[2] McGraw, Gary, and Greg Morrisett. "Attacking malicious code: A report to the infosec research council." IEEE software 17.5 (2000): 33-41.
[3]Vasudevan, Amit, and Ramesh Yerraballi. "Spike: engineering malware analysis tools using unobtrusive binary-instrumentation." Proceedings of the 29th Australasian Computer Science Conference-Volume 48. 2006.
[4] Aycock, John. Computer viruses and malware. Vol. 22. Springer Science & Business Media, 2006.
[5] Arief, Budi, and Denis Besnard. "Technical and human issues in computer-based systems security." School of Computing Science Technical Report Series (2003).
[6] Fred, Cohen. "Computer viruses." Proceedings of the 7th DoD/NBS Computer Security Conference 1984. 1986.
[7] Moser, Andreas, Christopher Kruegel, and Engin Kirda. "Limits of static analysis for malware detection." Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007). IEEE, 2007.
[8] Skoudis, Ed., and Lenny. Zeltser. Malware : Fighting Malicious Code. Upper Saddle River, NJ: Prentice Hall PTR, 2004. Print. Prentice Hall Ser. in Computer Networking and Distributed Systems.
[9] Anderson, Hyrum S., et al. "Evading machine learning malware detection." Black Hat (2017).
[10] Arp, Daniel, et al. "Drebin: Effective and explainable detection of android malware in your pocket." Ndss. Vol. 14. 2014.
[11] Azmoodeh, Amin, Ali Dehghantanha, and Kim-Kwang Raymond Choo. "Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning." IEEE transactions on sustainable computing 4.1 (2018): 88-95.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details