Security Bulletin

April 2014 | Volume - 1

CENTER FOR
CYBER FORENSICS AND
INFORMATION SECURITY

Index

introduction

CENTER FOR
CYBER FORENSICS AND
INFORMATION SECURITY

We at Amity Innovation Incubator have established a research lab "Center for Cyber Forensics and Information Security". CCFIS (www.ccfis.net) is founded on the core belief that cyber security is a growing concern worldwide because of information technology in personal life and in business, hence it is necessary to secure and protect our country and national technology infrastructure to safeguard future of our country and hence citizens.

CCFIS is a research organization and part of Amity Education Group, which is India leading Education Group having 1,00,000 Students, 5 Universities and many India and Global Campuses. We intend to create Research collaboration forum so that Internet community can fight together against Cyber Crimes. We have started a "National Cyber Alert System" based on our CCFIS sensors installed in different location across the globe. Currently we have the largest network of intelligent CCFIS Sensors across the India and soon planning to have it across the world.

executive summary

A tiny malicious binary code may be the biggest threat of our personal to professional life. There is rapid boom of malicious signed binary codes day by day and year over year. Some of these binary combinations may be potentially unwanted programs and not truly malicious, however, the misuse of legitimate code signing authentication erodes user trust. Many times, it is difficult to distinguish good authentications from malicious authentications. Our research will help the world to identify the trustworthiness of binary. CCFIS Research Labs also assigns the level of trust.

Our lead research is focused on malware attack to our nation's most critical area. CCFIS Advanced Research Threat Report (ARTR) provides a high level overview of computer network attacks discovered by Center for Cyber Forensic and information Security for quarter, January 2014 to March 2014. This report is based on the detailed research on various parameters of captured latest malicious code and thus giving "Alert" trends in Cyber Security.

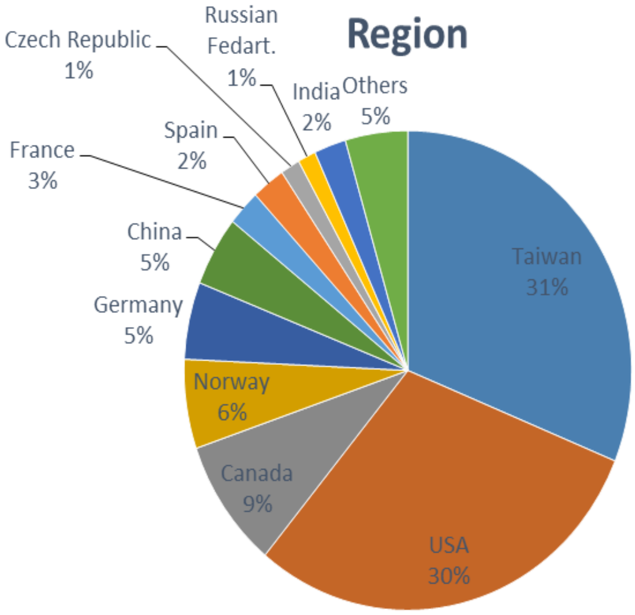
The entire report is completely based on data collected by CCFIS sensors installed at different locations in India and across the globe.

region wise analysis

Based on CCFIS research data, the top most used county's IPs who were involved in malicious activities and for APTs in recent time are -

Country Name	Percentage
Taiwan	31.10%
USA	29.80%
Canada	08.70%
Norway	06.00%
Germany	05.20%
China	04.70%
France	02.60%
India	2.30%
Spain	02.40%
Czech Republic	01.40%
Russian Federation	01.30%
Others	04.50%

According to our analysis based on captured data, the top three country's IPs used for malicious activities are Taiwan, U.S and Canada.

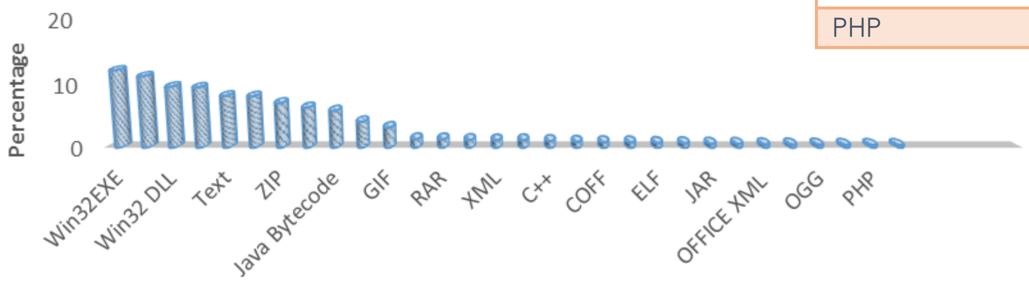


5

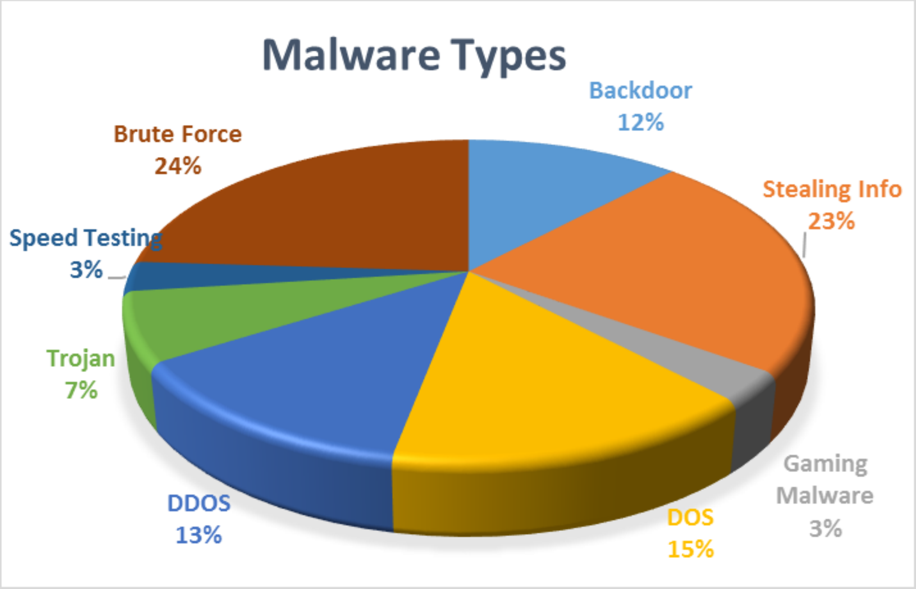
file extension of malware

Malware is one of the highest level weapon used to attack any industry or country. Malware writers use packing technology to bypass automated threat scanners and advanced firewalls. Every time attacker uses new exploit or malware to get the security clearance. The extension of the malware tells for what platforms it has been designed, and the most Interesting fact is that most of the malwares are cross platform and can infect system after understanding its platform and version automatically. According to CCFIS Research Labs, the following extensions were used for suspicious activity.

File Types	Percent
Win32EXE	12.13
JPEG	11.20
Win32 DLL	09.56
HTML	09.45
Text	08.13
PNG	08.05
ZIP	07.01
Android	06.30
Java Bytecode	05.80
PDF	04.07
GIF	03.16
DOS EXE	01.33
RAR	01.31
GZIP	01.20
XML	01.16
C	01.16
C++	01.04
FLASH	00.91
COFF	00.85
MP3	00.83
ELF	00.73
MS Word	00.69
JAR	00.61
MS Excel	00.59
OFFICE XML	00.52
WINDOWS INSTALLER	00.49
OGG	00.48
BMP	00.43
PHP	00.41



malware types

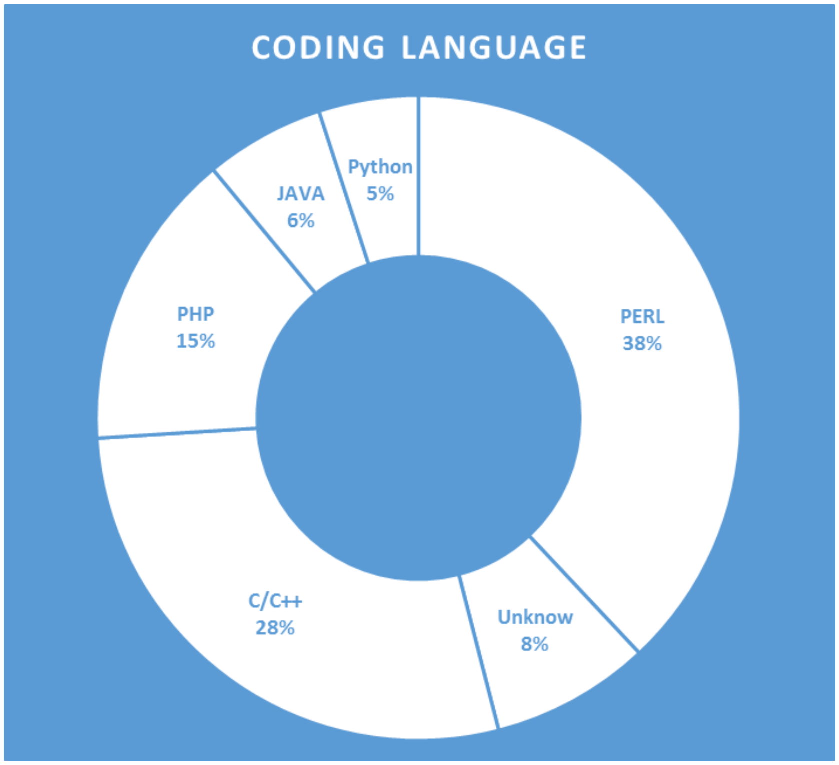


We did analysis of captured malware and detected that most of malwares were targeted malwares. We decoded every malware and analyzed it's behavior and categorized accordingly. We have detected various types of malware ranging from brute force based to information stealing malware.

Brute forced based malwares downloads entire dictionary in infected system and keep trying multiple combinations to find the perfect match of username and passwords. Backdoor malwares create a backdoor in compromise machine and later on provide a route for further pivoting based attacks.

We also analyzed a very smart malware designed specially for stealing information from infected system; these malwares do not perform any suspicious activity and hence, remains undetected by most security software. DDoS based malware make their victims a part of their botnet and perform DDoS attacks using these compromised machines as bots. Few malwares bind themselves in system drives and loads before the operating system boots. Few of the malwares are so sophisticated and packed that it remains dormant in systems and perform their tasks silently.

coding language



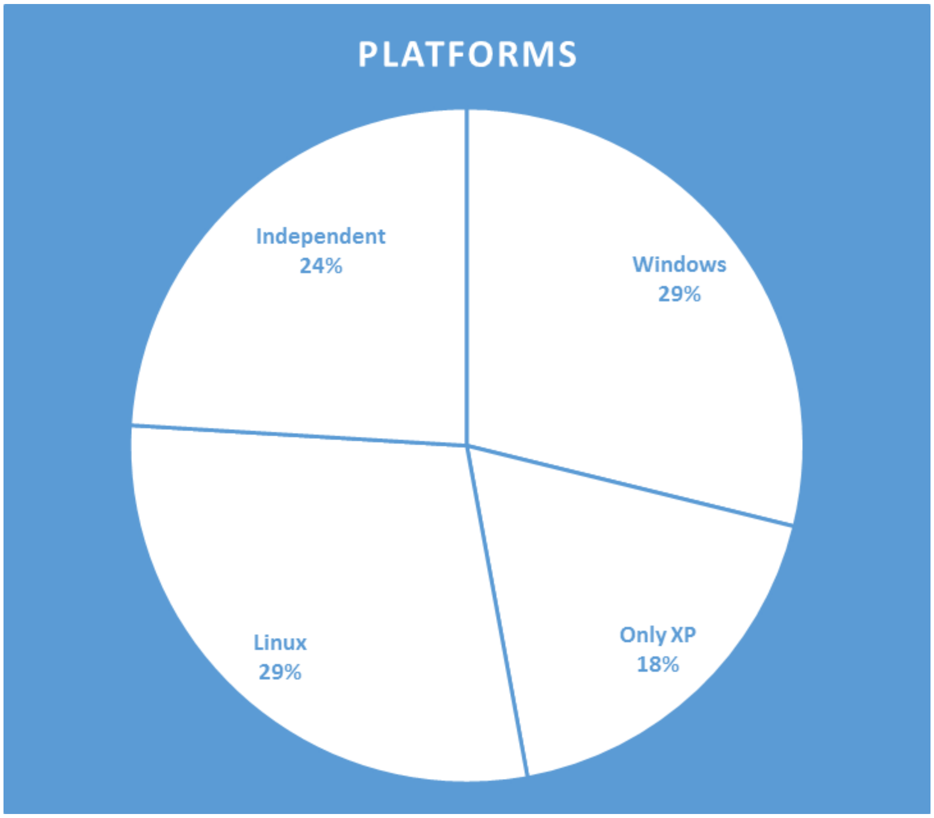
Most of the malwares were highly packed but CCFIS Research Team was able to decode most them in our advance malware analysis lab. We analyzed the code and tried to understand its working, behaviors and intent.

So far, CCFIS research team has concluded that most of the malwares are written in pearl language due to its simplicity, high functionality and full community support. Security professionals' uses python for various purposes, one of them are for writing Proof of Concepts but malware coders take advantage of rich libraries of Python and code state-of-art malwares. Pearl is in the lead role but the base of most of the languages C/C++ also is in race. It is still one of the most favorite attacker's choices.

Also few of malwares were so packed that even our advance research lab were not able to decode the malwares and our belief is that these malware remain undetected by most anti-virus companies. We declared these files as malwares, based on their behavior.

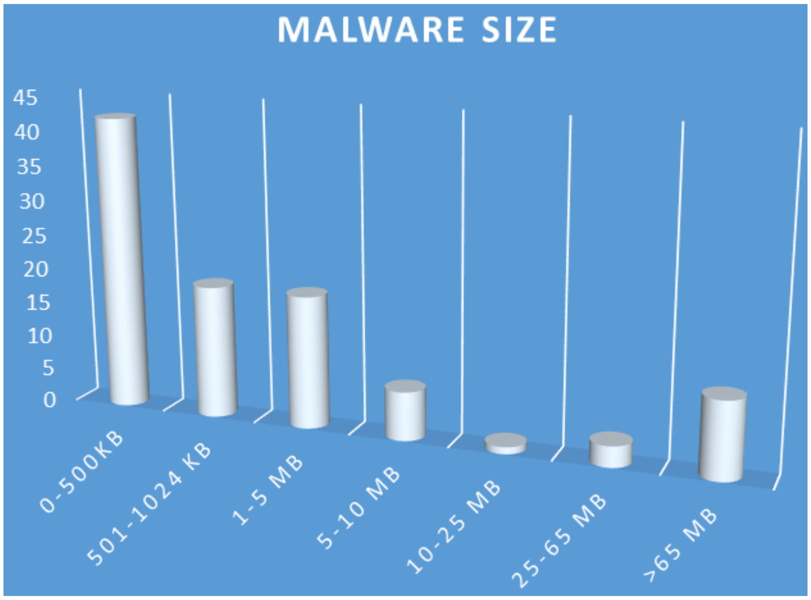
executable platform

Final aim of any attacker is to execute its malware into operating system to get desired access. According to CCFIS Research Labs, we found that most of the malwares were written for Windows platform and majority was for Windows XP systems as Windows is still most preferable Operating System and Windows machines are used in various critical sectors.



We also found that attackers are focusing more on creating cross platform malwares. These cross platform malware detects operating system and its version automatically and infect accordingly ranging from Windows to Android.

malware size



The malicious binaries have no fixed size in the Security World. According to CCFIS Research Lab Report, which is based on malwares captured by our sensors, most of the malwares were very small in size. Malware coders pack the malicious code again and again and try their best to keep the file as short as possible. Some of malwares were coded only to get access into the system and after getting the access of system they start downloading other part of malware to intrude further into network using pivoting. These malware are more intelligent than your general security software.

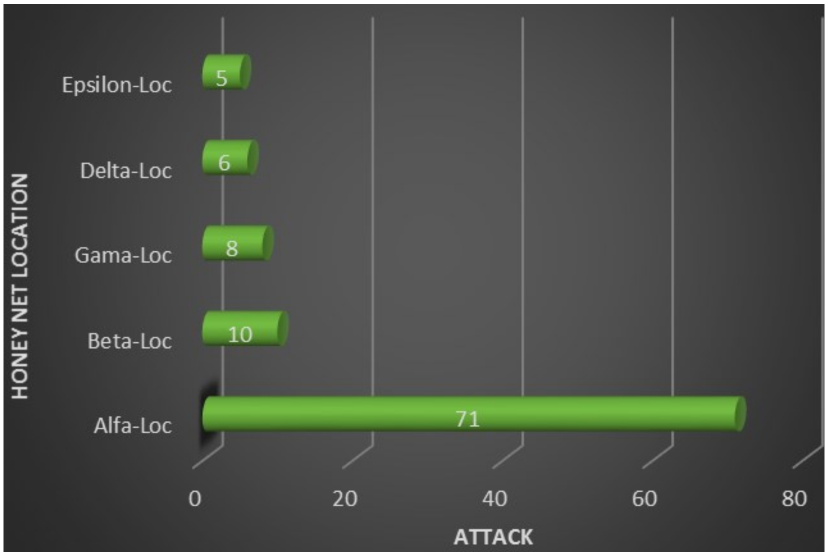
The trend shows that files greater than 65MB are mostly the speed tester files which are used to check the uploading and downloading speed. Below 65 MB to 5 MB files are mostly used for brute force attack as they contain a large username's and password's dictionary. Below 5 MB are either .rar, .tar, or .jpeg extension files used for compromising machines and adding them to botnet. Also small malwares were Trojans, backdoors, adware, bitcoin miners, etc.

Most of the malwares written in Python or Perl are used to be of less size because these scripts acts as a OS backdoor, allowing remote hackers to secretly send commands, uploading code to the computer, stealing files and running commands without the user's knowledge. These functionality can be easily achieved using Perl or Python due to rich libraries and huge community support.

The speed tester files are mostly the corrupted files of older service packs of windows used by an attacker to test the server speed or to degrade OS version to try already available exploits.

region – based on CCFIS sensors

Based on the CCFIS sensors installed on different locations in India, we captured a huge number of malwares. Below graph shows the area which allure attackers.



The analysis shows that Alfa-Loc is at the first place and one of the reasons for choosing the Alfa-Loc by an attacker can be the rapidly growing industries and trade in Alfa-Loc. Most of the DoS and Brute force based malwares were uploaded in this location.

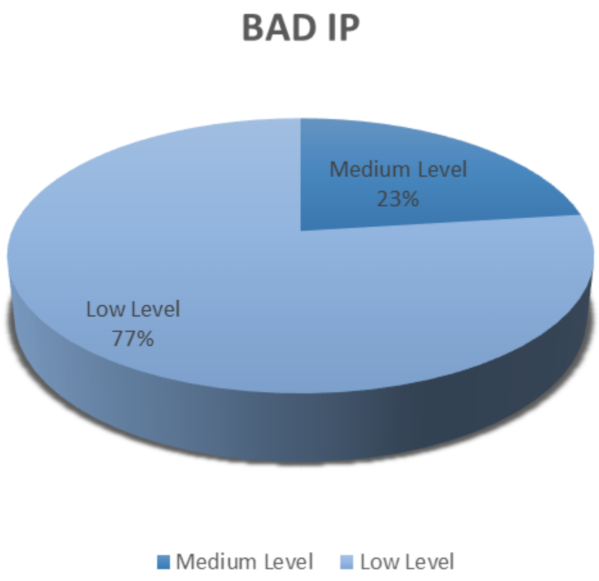
We found various types of malware at Alfa-Loc sensor. The attacker tried to compromise the server by sending the files which could downgrade the server version and make prone to known attacks. All the activities logs and input commands were recorded by CCFIS sensors and a proper analysis were performed. It has been observed that attackers are more interested to attack the location in which could either get benefit financially or steal some information relevant to attacker.

Beta-Loc has recorded the malware files less than 30 MB and the case is similar with Delta-Loc and Epsilon-Loc.

At Gamma-Loc, speed tester files are used to either get the bandwidth of the server or to compromise the server by installing older service packs.

**Alfa, Beta, Gamma, Delta & Epsilon are not the real locations but the code names of CCFIS Sensors.*

list of bad ips



CCFIS has divided the suspicious IP’s into four domains. Each domain represents the severity level. We have defined our levels based on the IP’s found during the analysis. Most of the IP’s are found in malware having behavior quite similar to the categories like backdoors, Brute force attackers, Dos or DDoS.

Compiled from CCFIS’s data, the graph below shows the bad IP’s in the widest range of targeted computer network operations.

Low level: 65.54.89.146, 65.55.95.11, 65.54.89.224, 54.228.232.89, 178.19.99.72, 89.39.89.40, 212.193.243.188, 89.187.135.150, 209.59.194.20, 176.74.176.178, 63.251.38.197, 66.254.108.157, 93.119.25.20, 208.146.35.5, 186.202.153.36

Medium Level: 207.46.120.187(2), 23.67.1.48(2)

High Level: NA

Critical Level: NA

Thus, from the data it indicates that an attacker has always tried to attack from different IP. In that case it is the possibility that we always see the Low level and Medium level percentage quite higher than other levels.

Most of the IP’s after being used are not active now. This means that an IP once used is only active for a short period of time. By the time a network administrator block that malicious IP, it might be left by an attacker. Similar is the case with their subdomains and domains. The domain names once used are not available now. In fact, the domain names found are also available on some of the domain name registration sites, which mean they are not being officially used.

bad domain

Based on the IP addresses found, the analysis is done and list of some domains have been found. These domain names are the one which were used by attacker to attack their targets. Some domain names are still active while some of them are down. Just like IP address, domain name also keeps on changing. It also contains some blacklisted domain names. Our belief is that these IPs or domain names are made live when attackers intent to attack.

Low Level:

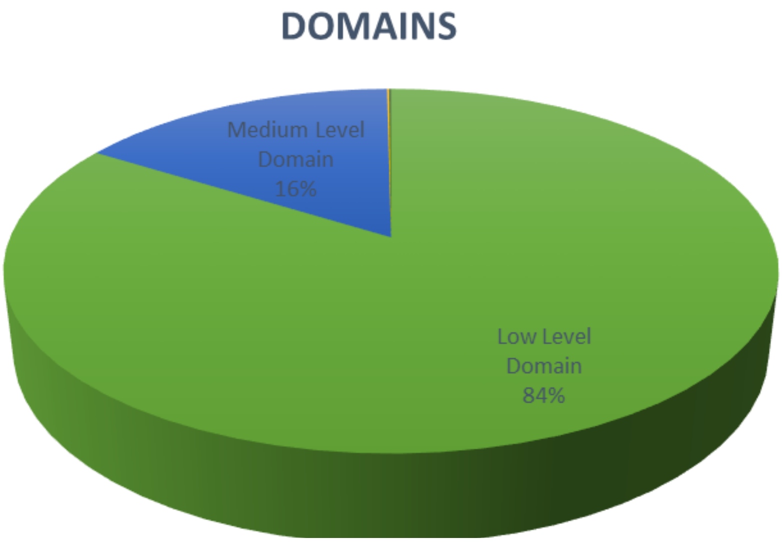
- MundiGames.com
- bc2server.ru
- www.laleagane.ro
- EnjoyGame.ru
- Espana Romania.es
- Herniserver.cz
- Cs.GenerationCs.Net
- Best.FullCs.Com
- FullBK.Best.Com
- DarkZM.SKZ.Com
- Zombie.BestRedDevil.Com
- Hellzone.MasterServer.Com [Zombie Plague]
- WristHaX.com
- MorTaLGaMes.com.br

Medium Level:

- adsyndication.msn.com-2
- cx.msn.com-2
- images.adsyndication.msn.com-2

High Level: NA

Critical Level: NA



about us

CENTER FOR
CYBER FORENSICS AND
INFORMATION SECURITY

Center for Cyber Forensics and Information Security (CCFIS) is founded on the core belief that Cyber security is a growing concern worldwide because of huge involvement of information technology in our personal life as well as business world. Hence, it is necessary to secure and protect daily life of the people, with national infrastructure based on cyber technology to safe the future. We are a team of Security Professionals from across the globe who are involved in creating awareness in the field of Cyber Security and also- to reduce the increasing Cyber-Crimes.

The CCFIS team is working as a research team to help build a proactive and resilient Cyber Defense System and provide solutions to Government & Private Agencies in a guided manner while keeping a watch on malicious attempts for hacking websites and IT infrastructure belonging to the Central or State Government, Private organization's and PSUs.

Our Core Research team had been constantly trying to solve the social problem by creating awareness in the field of Cyber and Digital Information Security to protect kids, students, youths, individuals, and organizations etc. from the unseen criminals of the digital world. The goal is to make India a Cyber-Secure nation in respect of cyber security.

CCFIS is a pure-play Research InfoSec organization, specializing in delivering high quality services through expert with a core focus on Professional Penetration Testing, Vulnerability Assessment, Web Application Security, Cyber Crime Investigation, Computer Forensics Investigation and Malware analysis.

contact us

CENTER FOR
CYBER FORENSICS AND
INFORMATION SECURITY

Noida Office

Amity Innovation Incubator, Block E-3,1st Floor, Amity University,
Sector-125 Noida, UP-201301, India
Email Id: info@ccfis.net
Phone no: +91-120-4659156

Lucknow Office

3rd Floor, AB - 6 Block, Amity University
Malhaur, Lucknow, UP - 226028, India

Disclaimer

This report was prepared as an account of work done by CCFIS. Neither the CCFIS, nor any of their employees, nor any of their contractors, subcontractors or their employees, partners or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use of this report or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights.