<table>
<thead>
<tr>
<th>Page</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>02</td>
<td>executive summary</td>
</tr>
<tr>
<td>03</td>
<td>hiding data like a ninja</td>
</tr>
<tr>
<td>05</td>
<td>man in the email-attack</td>
</tr>
<tr>
<td>08</td>
<td>chip-off forensics</td>
</tr>
<tr>
<td>11</td>
<td>byod forensics</td>
</tr>
<tr>
<td>13</td>
<td>android malware investigation</td>
</tr>
<tr>
<td>15</td>
<td>about us</td>
</tr>
</tbody>
</table>
executive summary

Any Organization – big or small, can be target of any Cyber-attack. Password only protection are weak authentications and are too risky. Also, with the adoption of Cloud based IT Infrastructure, Organizations are expected to secure what they don’t own, manage or control. Users want the complete freedom to browse on web, not only when and how but also with the devices of their own choice. Cyber criminals are taking advantage of today’s “any-to-any” world where individuals are using any device. The threats targets are across domains without discriminating by Industry, Businesses, size or Country. Cyber criminals are constantly evolving new techniques to bypass security. “Forensic Bulletin” is special CCFIS monthly Series Bulletin based on advancements and upcoming trends in digital forensics as per research work done by CCFIS Team, who is constantly watching vigilantly all new advanced techniques and cyberspace threats.

As per recent survey by one of reputed Research Center, 50% of Organizations had experienced at least one occurrence of economic crime in last 1 year. Instances of such frauds losing billions of dollars. Those, who commit frauds have become craftier and are launching more complex plan. However, only few of the Organizations are responding to growing threats by tightening up their controls and investing in fraud detection and prevention as per professionals/expert opinion.

The “any-to any” evolution already involves billions of internet connected devices and is expected to grow many folds in next few years.
hiding data like a ninja

A cyber-espionage case study

We all have some data either related to our business or personal that we don’t want to share with anyone. These data may be your trade secrets, financial documents, patent files or whatever that matters to your business and hence your life. To achieve this, we use different encryption software, folder locks and what not but due to increase in responsible disclosures we have came to know that no matter what you do, your data is not secure at all. Encrypting data isn’t a good option, as the most trusted encryption utility 'truecrypt' announced that 'WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues'. Now most of us are not left with any options to rely upon for security of our data. Data theft can not be curbed completely but it can be minimized.

First of all torn out the label pasted on your HDD that tells about its specification like size, RPM, brand, model no etc. Now create the size of HDD to 250 GB with just one partition having OS installed on it. To understand it more, let us explain the basic structure of internals of an HDD.
As shown in the pictograph, inside a HDD there are two platters and two heads to perform read/write functions on them, data exists on both the platters.

Now behold the genius of the plan: What if you stores the confidential data on the second platter and disables its head and configures HDD such it only works with one head and reads data off only one platter?

**This method is effective as its known to very few of us.** The head count of the HDD will show Two (2) heads in total but the engaged head count will show only one (1) head in total.

Now store your confidential data on that hidden drive. Later on when you want to access it back, reconfiguring the HDD, enable the disengaged head of the Hard Disk and you will get your hidden partition. For better security, you can encrypt this drive too. So now you can make a 500 GB HDD into 250 GB HDD with 250 GB as your hidden ninja storage.

Note : - For technical specifications, drop a mail at info@ccfis.net.
In last one year CCFIS has been asked to give expert advisory in cases related to email spoofing from various LEAs and private companies. This particular email scam can be called as ‘Man-in-the-E-mail’ attack. Following are two most prominent email scams using ‘Man-in-the-E-mail’ attack technique:

The modus operandi of this particular email scam victimizing businesses nationwide starts with compromising the email accounts of businesses, studying the email correspondence of active business deals which involves a substantial amount of money transfer. The perpetrator then identifies the target company’s e-mail domain and creates a similar domain by altering one or two letter in the email address. To an unsuspecting eye it is easily deceptive and passes as the original email address. The perpetrator then starts acting as a relay point between both the parties passing on either party’s email message to the other. Thus gaining control over the communication, editing & forwarding the content of email messages to his benefit. In other cases, the perpetrator identifies when the company executives are travelling from the information gathered from social media sites like Facebook/twitter or compromised the executive’s e-mail account.
When the executives are out-of-town, the subject sends an e-mail to an individual in the company who is authorized for wire transfers and bill payments. The e-mail usually appears to come from the company’s CFO requesting the wire-transfers on behalf of the CEO. To make the request appear legitimate, the e-mail contains a fraudulent e-mail chain started by the CEO requesting the transfer. The email consistently asks for money to quickly be wired to a specified account and usually states that the wire transfer should be coded to “Misc. Expense-executive” or “Admin-Expense.” The success of these email spoofing scams largely depends on the awareness of the employee. A normal employee fails to identify the differences between a spoofed email and a genuine email. Lack of cyber security training is must for small and medium enterprises of our country to prevent such loses in the future.

CCFIS advises that while reporting similar incidents to the authorities, victim organizations should maintain the e-mails with the original extended headers and any attachments such as .PDF files that provide directions for the money transfers as these can proved to be crucial evidences.
As digital forensic professionals we are accustomed to face challenges. How do we obtain a full forensic image from embedded flash memory chips if physical extraction is not supported, what if the device is itself physically broken & damaged beyond repair? In such cases we perform chip-off forensic analysis, defined as the extraction and analysis of data stored on flash memory chips.

Few chip-off scenarios we encountered at CCFIS:

A phone broken in two pieces – with its connecting ports damaged there is no way to access the data or image the data stored inside. We need to take of the chip and perform recovery procedures on it.

Pen drive shot by an AK 47 bullet – The pen drive was broken and the connecting port was melted by the heat of the bullet. A chip-off analysis is now required to access the data inside.

Also, the chip-off process makes it possible for water damaged devices and items lacking connection ports to be acquired or analyzed. A chip-off requires a different setup than a normal computer forensics lab has. An ideal chip-off workbench has electrical rework equipment and chip programmers.
The rework equipment is used to remove, clean, and prepare memory chips prior to data acquisition. The chip programmers are used to actually interface with the memory chip and download the stored data to a raw image file.

The ultimate goal of a chip-off project is to capture and analyze the raw data saved on a target device's flash memory chip on the printed circuit board (PCB). In order to accomplish this, **A typical chip-off project progresses through three distinct phases - Assessment, Acquisition and Analysis.**

**The Assessment Phase** - The assessment phase involves researching the target device to make sure it is a good chip-off candidate and to confirm no other full-physical memory extraction possibilities exists then only preparing it for the extraction.

**The Acquisition Phase** - The acquisition phase involves the actual chip removal and capture of data. This is when the rubber meets the road and actual chip-off happens. This is accomplished by disordering the chip from PCB, utmost care is to be taken.

**The Analysis Phase** – The analysis phase involves the recovery and interpretation of the acquired data. Once the raw data has been extracted, analysis can begin. The data examination is often the most challenging aspect of a chip off project. In addition to vast differences in device operating systems, file systems, and data storage structures, the examiner must understand and account for the low-level characteristics of flash memory.
The process can be daunting and may require development of custom programs or scripts for a particular device. In addition to vast differences in device operating systems, file systems, and data storage structures, the examiner must understand and account for the low-level characteristics of flash memory. The process can be daunting and may require development of custom programs or scripts for a particular device.

The common issues & problems faced by the examiner is to identify the target memory chip and virtually built the controller of the chip. In these cases, the examiner will need to communicate with the various programmer manufacturers and request support be added for the new chip model. The removal process does carry some risk of damage to the memory chip and loss of data when the chips are exposed to high-temperature profiles which are required to melt lead-free solder.

The chip-off process is definitely an advanced technique and can be utilized in majority of devices as flash memory is utilized in all sorts of other devices.

Certainly, the vast majority of chip-off projects we work involve mobile phones, but nearly any device that contains embedded permanent storage capabilities can be extracted these include tablet, GPS units, voice recorders, printers/ scanners, music players, cameras, video game consoles, vehicles, industrial machines, medical testing equipment, network devices and security systems.
byod forensics

Extracting a full bit-stream image from devices containing embedded flash memory

The concept of BYOD is not new, the oldest example of BYOD would be carrying personal USB thumb drives to work. Since then technology grew so did the BYOD trend, statistics indicate that the medium by which most people access the internet wirelessly is using a portable device like a smartphone or a tablet.

As mobile devices continues to evolve and expand their availability, utility and versatility increases. Corporations and law firms face increasing pressure from employees and consultants to permit the use of personal devices on the organization's network. With BYOD policies implemented employees shows improved productivity, ease of mobility, and a more satisfying end-user experience.

But this trend of BYOD, poses serious challenges and risks for organization's data and its network security. There is the significant risk that permitting such connectivity might introduce viruses, malware and other forms of trouble into the organization's file servers, email systems and mission critical infrastructure. Second, there is the increased likelihood of data breaches, theft of proprietary information and trade secrets, and loss of intellectual property.
Just a month ago we came to know about serious data theft in a company who lost a million rupee tender by a thin margin. Company officials were baffled on how could their rival company come so near to their bid. They suspected someone from their company leaked those confidential bidding documents. Later on it was revealed that one of their employee used her iPod to copy those documents by accessing the USB port of the computer system on the name of charging it.

In a similar case, an IT company had to face serious repercussions after its software code was stolen. On investigation it was established an android smartphone opened in USB Mass Storage Mode was used to copy the source code.

So how can organizations reach a compromise between appropriate and adequate security while implementing an effective BYOD policies which fulfils the technology wants and needs of their internal client base?

Through proper planning, appropriate policy, and periodic review and assessment, organizations can successfully permit employees' use of personal devices, without sacrificing information security.
As smart phones are increasing, so does the mobile malware

In fast few years we have seen that companies hire competitor’s employees to perform better. Now competitors hack into each other’s email accounts, servers to get data relevant to their business. Now a days competitor are now targeting mobile devices which are now equally powerful as desktop pc holding more confidential data. Sophistication of mobile hacking has increased to such a level that the victim never realizes that he was ever comprised.

Our internal research shows that these types of attacks has increased exponentially and mostly in IT industry. We everyday hear about incidence of e-mail security breach and email stealing of a top level official of an IT Company due to which confidential files, client details, their account numbers and financial information are compromised. When these incidence happens, most of us are in suspicion that email server or the personal/official computer might have been compromised by a malware. But we rarely notice that we also accesses emails through our Android based smart phone. Most of android malware are detected by security software but targeted malware are always dormant and smart enough to perform their tasks without leaving any suspicion.
It can be analyzed by acquiring dumps of physical, logical and memory of the smartphone. From the physically acquired dumps of the mobile phone, every application executable file can be extracted along with metadata like installation date and time.

The extracted android executable (.apk) can be then installed and executed in android emulator (a virtual phone that runs on computer) for further analysis. Out of all installed applications, you may find some application behaving suspiciously. Further analysis can be done of these suspicious executable (.apk) like reverse engineered to know the permissions given to the application, source code of the application and associated JAR files (java executable). For in-depth analysis one can also connect mobile phone in a sandboxed environment and capture all data packets for several hours to analyze its behavior.

If your device is compromised that very soon you will get IPs to which your device is communicating. Close all applications and run only selected suspicious applications, you will see a lot of data packets are exchanged between your device and detected IP.

If you run a business then there are possibilities that the IP can be of your competitor.

The internet is full of these types of malicious android apps that can compromise your android device in minutes using 0-day exploits.
Center for Cyber Forensics and Information Security (CCFIS) is a Research Organization incubated at Amity Innovation Incubator which is a Technology Incubator supported by NSTEDB, Ministry of Science & Technology (Government of India).

Cyber Security Employee Development Program

- Comprehensive cyber security training customized according to your industry and employees.
- Research shows that human is the weakest link of security chain of any Organization
- The training is offered by Security & Forensics Experts and it is perfect blend of practical and theoretical aspects of cyber-attacks.

REQUEST DEMO

Are you safe from cyber attacks from your rivals?

- Protection from sophisticated targeted attacks
- Get business intelligence information about attackers
- Analyze what specific IT infrastructure or company department are targeted
- Blocks around 65 to 70% of targeted attacks in your network.

- Detailed information about attack & attacker, motive and actual targets.
- Complete ‘Monthly’ analysis report with region, malware analysis, IPs, business intelligence report.
- List of targeted vulnerable IT assets with recommendations to secure
- Security advisory & complementary services

Noida Office HQ : 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

Gwalior Office: Amity University Madhya Pradesh, Maharajpura (Opposite Airport), Gwalior

Jaipur Office: Amity University Rajasthan, 14, Gopalwadi, Ajmer Road, Jaipur, Rajasthan

Manesar Office: Amity University Haryana, Panchgaon, Manesar, Gurgaon, Haryana

Disclaimer—This report was prepared as an account of work done by CCRS research and analysis wing. Neither the CCRS, 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.

© Center for Cyber Forensics & Information Security