The Code Zer0 Magazine

Let the Hacking Begin...

Companies face huge loses due to data theft, you are at a risk. No one is secure. You might get owned!

Corporates, Is your data safe?

Let's see what our experts have to say!

Presented By: Cyber Wizards

April 2014, Issue 3

Contents

Cover Story

In this issue, we have two main cover stories, BYOD and risks that asset management companies face because of insecure storage of data and because of the company's incorrect and incompetent security policies. We also discuss JSI, LightBeam at a basic level so that Corporates can understand what to ask their Security Officials for.

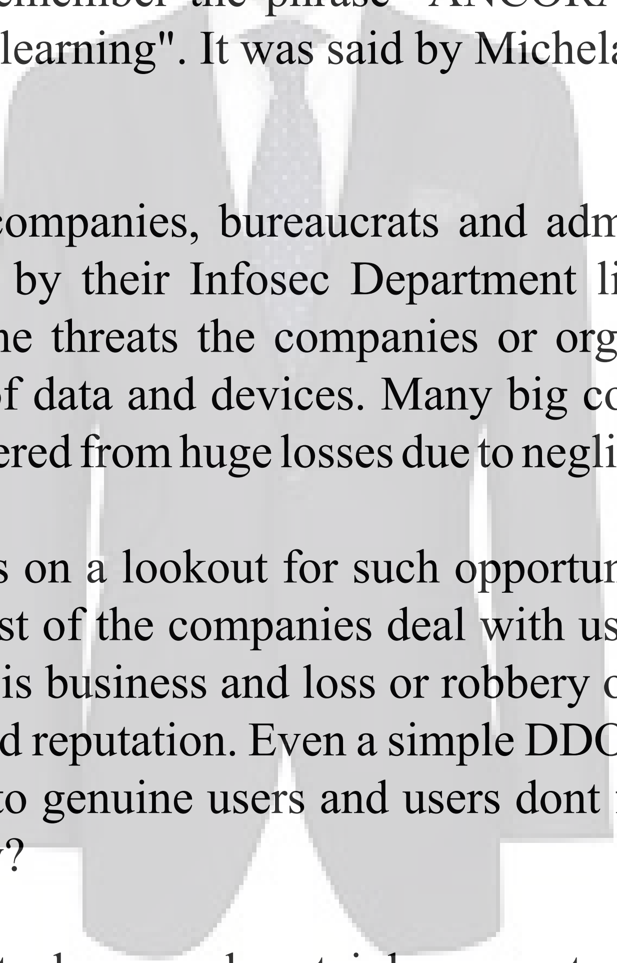
Deep Web

Two established security researchers share their experience of their first encounter with Deep Web. They explain in details what Deep Web is, what are the 8 levels of deep web and what does the deep web consists of.It is an interesting article which is enriched in knowledge for all of us, and helps us to understand the underground market and threat to companies in a better way.

From The Editor's Desk

Hello Dear Readers,

Welcome to the third issue of Code Zer0. This edition revolves around "Corporate Security" and other interesting topics related to "Hacking and Cyberspace".We highly encourage all the corporates to read this issue of magazine. Always remember the phrase "ANCORA IMPARO", which stands for "I am still learning". It was said by Michelangelo, at the age of 87 years.



People working in companies, bureaucrats and administrators take the security policies set by their Infosec Department lightly because they do not understand the threats the companies or organisations face due to insecure storage of data and devices. Many big companies like Sony, Barclays, AT&T suffered from huge losses due to negligence of IT security.

Blackhats are always on a lookout for such opportunities. Why are they interested? Well, most of the companies deal with user data daily, right? For companies, data is business and loss or robbery of this data will lead to loss of business and reputation. Even a simple DDOS attack will render the services useless to genuine users and users dont forgive you for loss of their time, do they?

It is never too late to learn and certainly never too late to secure the confidential and private data of your company. This time we will talk about issues related to security for companies, such as BYOD (Bringing your own Devices), the security threats that corporates can face due to this culture and how can the companies, on adopting suitable security policies can safeguard themselves without causing dissent among their employees. Then we will analyse if the companies are managing their assets in a suitable way.

Along with these topics, we will learn how to recognise third party interaction on the web, what really the deep web is (and about the dark and mysterious secrets that it holds) and then we have a look at the Security and the Privacy model of the Firefox OS and we will reason, why it is advisable for corporates to make a switch to FxOS phones. No issue is complete without discussing the dangers our websites face, so we have a short article on JavaScript Injection and its Cheat Codes.

We hope that you enjoy the articles, learn from them and implement the security solutions advised by our experts to safeguard your company and the precious data it holds. Until next time,

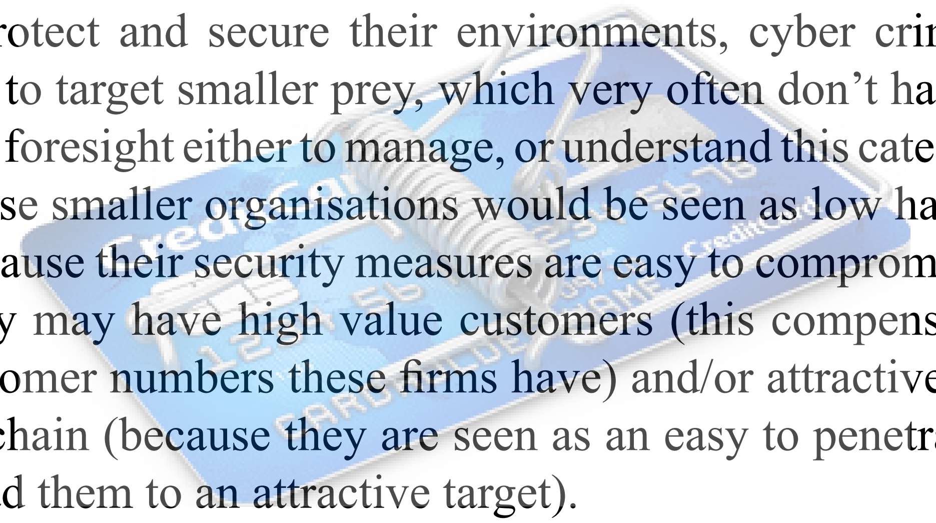
STAY HUNGRY, STAY FOOLISH

With Warm Regards,
Tanay Pant
Editor-In-Chief

DO ASSET MANAGEMENT COMPANIES KNOW THEIR ASSETS?...

Because of the substantial value they hold, financial services organisations have always been a prime target for cyber criminals. We have seen many data breaches and targeted attacks against networks, applications, websites and, most importantly, data and information. In recent years, organised crime has shown increasing sophistication. This has meant that in addition to the more traditional hacks used to ultimately perpetrate fraud; we have seen a surge in attacks targeted at disrupting business operations in order to extract ransom.

Consequently, as large financial services institutions have increased their efforts to protect and secure their environments, cyber criminals have been forced to target smaller prey, which very often don’t have the time, resources or foresight either to manage, or understand this category of risk. Some of these smaller organisations would be seen as low hanging fruits not only because their security measures are easy to compromise, but also because they may have high value customers (this compensates for the smaller customer numbers these firms have) and/or attractive partners in their value chain (because they are seen as an easy to penetrate gateway that may lead them to an attractive target).



As has been evidenced many times, small and medium businesses often believe they are too small to attract the notice of cyber criminals. Asset management firms, including hedge funds, alternative investment, wealth management and other boutique firms fall into that category.

Investment firms have struggled with information security because they have historically focused on business continuity planning, often leaving information security at best as an afterthought and at worst when reacting to a data breach. Cultural differences may have played a part in this disconnect, where the inherent risk-taking culture of these businesses has clashed with the traditionally risk- averse approach of information security departments. Because of the media exposure of cyber-attacks over the last few years and the increasing focus on risk management, company boards and investors are now fortunately paying more attention. The steady move of the information security community to greater understanding of risk management is also playing a role in this shift.

I personally believe that organisations cannot truly assess their information risk if they haven't clearly determined what their assets are. Asset management firms have a wealth of criminally attractive information assets, including:

- proprietary trading algorithms and other patented technologies
- client data
- trading/ market data
- partnerships

Whilst asset management companies may be subject to the type of fraudulent activities other market sectors experience (e.g. payment fraud, phishing, ID Theft, etc.), organised criminals can specifically target this sector in many ways, such as blackmailing clients, selling illegally obtained information on the black market, or placing fraudulent trading orders. In addition, fraudsters may also use these organisations as a springboard to infiltrate partner businesses, rendering them unwitting parties to the crime cycle because of weak security practices.

Conversely, these organisations should look diligently at their supply chain, lest the reverse happen due to partner/ supplier potentially weak security practices – again here, due diligence is key.

With this in mind, more investors, trading partners and regulatory bodies are asking the hedge funds, alternative investment and other financial markets firms to provide proof of strong security programs and data privacy, covering their entire value chain.

Apparently, most investment management companies do not yet exhibit best in class (or even sector peer group average) data protection and information security practices. The realisation needs to come that they potentially face not only financially motivated cyber criminals, but also politically and socially motivated attackers (e.g. through system downtime, hijacking of public accounts or even defacement of websites). I am sure we're all familiar with the Associated Press twitter account hijack which led to a spectacular, if short-lived, crash of the Dow Jones.

In addition, with the increasing convergence and cooperation between cybercrime and cyber espionage (and the Symantec Internet Security Threat Report 2013 revealed a 42% increase in cyber espionage, leading to IP Theft), these organisations are also potentially facing a double jeopardy.

This can lead to potential fines and penalties related to standards such as the Payment Card Industry Data Security Standards (PCI DSS) and other compliance, client data and privacy regulations. On this last point, the EU data privacy regulations will affect all organisations already using or contemplating the use of cloud services which, with their very obvious benefits, must nevertheless be assessed within a clear risk management framework.

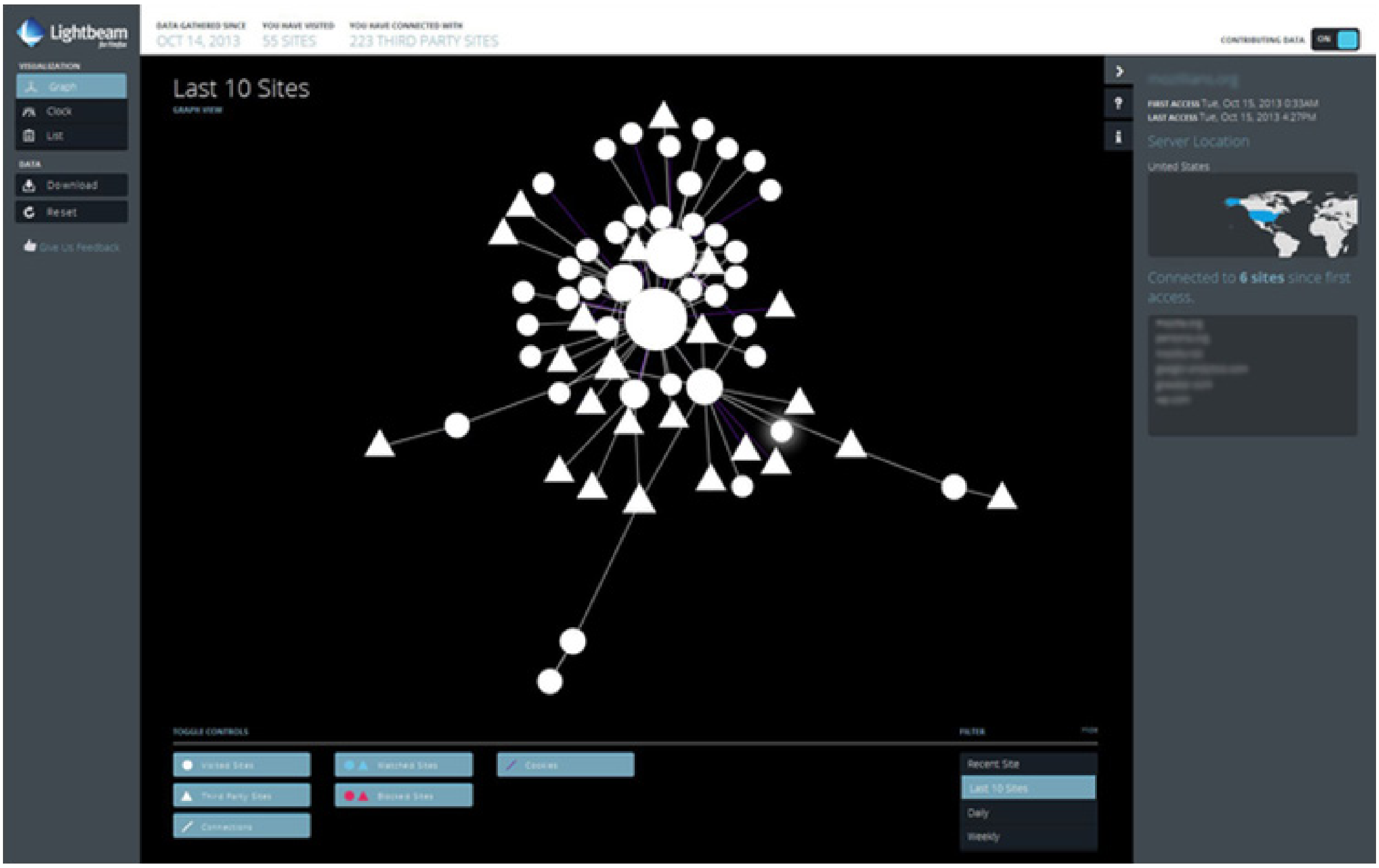
Finally, aside from the obvious financial damage, attacks leading to security breaches will damage a firm's reputation and expose it to losses due to system downtime, potential lawsuits and stolen intellectual property as well as impacting the trust their customers place in them. This therefore must be viewed as organisational change, taking into account not only the technologies, but also the processes and people dimensions. Some might think that their insurance covers them, think again...

Raising awareness is a good start.
(http://about.me/neirajones)

This article was written by Miss. Neira Jones. She strives to demystify risk, information security and payments and is regularly invited to advise organisations and address global audiences on these topics.

Light Beam for Firefox (Shows First and Third Party Interactions on the Web)

Well, here's another great Add-on to our favourite Open-Source web browser, Firefox. This was released quite some time ago, but I feel that our corporate friends, should be aware of it. Lightbeam is a Firefox add-on that enables you to see the first and third party sites you interact with on the Web. Using interactive visualizations, Lightbeam shows you the relationships between these third parties and the sites you visit.



DATA GATHERED SINCE OCT 14, 2013

YOU HAVE VISITED 55 SITES

YOU HAVE CONNECTED WITH 223 THIRD PARTY SITES

CONTRIBUTING DATA ON

Last 10 Sites

GRAPH VIEW

FIRST ACCESS Tue, Oct 15, 2013 0:33AM

LAST ACCESS Tue, Oct 15, 2013 4:27PM

Server Location

United States

Connected to **6 sites** since first access.

Using interactive visualizations, Lightbeam enables you to see the first and third party sites you interact with on the Web. As you browse, Lightbeam reveals the full depth of the Web today, including parts that are not transparent to the average user. Using three distinct interactive graphic representations — Graph, Clock and List — Lightbeam enables you to examine individual third parties over time and space, identify where they connect to your online activity and provides ways for you to engage with this unique view of the Web.

How Lightbeam Works ::

When you activate Lightbeam and visit a website, sometimes called the first party, the add-on creates a real time visualization of all the third parties that are active on that page. The default visualization is called the Graph view. As you then browse to a second site, the add-on highlights the third parties that are also active there and shows which third parties have seen you at both sites. The visualization grows with every site you visit and every request made from your browser. In addition to the Graph view, you can also see your data in a Clock view to examine connections over a 24-hour period or in a List view to drill down into individual sites.

How You Can Use Lightbeam to Help Us Illuminate the Inner Workings of the Web ::

As a part of Lightbeam, we're creating a big-picture view of how tracking works on the Internet, and how third-party sites are connected to multiple other sites. You may contribute your data to our crowdsourced directory by simply turning on the share switch within the add-on. To disable crowdsourcing, you can turn it off at any time. You can view your local data stored within Lightbeam at any time, or save your data by clicking the "Save" button under the data section on the left side of the add-on.

How is my information stored? ::

As a default, all info generated and used for Lightbeam’s visualizations and features are only stored locally on your computer. You can save a copy of your connection history at any time, which is also where you can see the specific data collected by the add-on. You may also reset Lightbeam to erase your locally stored connection history, disable it to stop data collection or uninstall it to instantly remove all locally stored data related to Lightbeam.

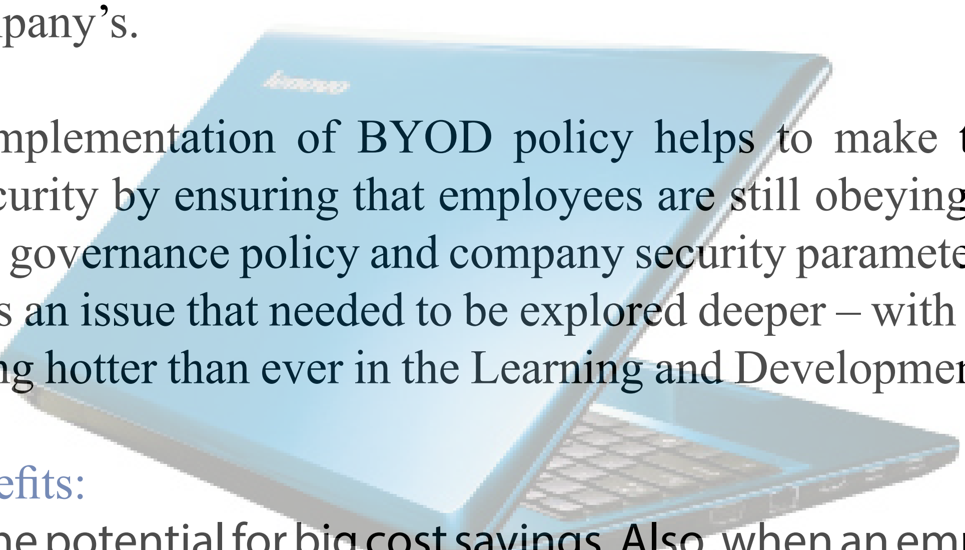
You can download the plugin from:

https://addons.mozilla.org/en-US/firefox/addon/lightbeam/

BYOD: Bring Your Own Device, Is it safe?

According to webopedia: In the consumerization of IT, BYOD, or bring your own device, is a phrase that has become widely adopted to refer to employees who bring their own computing devices to the workplace for use and connectivity on the secure corporate network.

Here employees bring in personally owned mobile devices such as smartphones and tablets and allow them to access privileged business data such as databases and email on their own device. It also allows them to remotely access this information from locations outside the office. The important thing when it comes to BYOD is that the device is their own, not the company's.



A proper implementation of BYOD policy helps to make transparent network security by ensuring that employees are still obeying according to company governance policy and company security parameters. We feel that this was an issue that needed to be explored deeper – with the BYOD debate raging hotter than ever in the Learning and Development Industry.

BYOD benefits:

BYOD has the potential for big cost savings. Also, when an employee can work from and use a device of his own choosing, it's more enjoyable than being forced to use a corporate-issued device. That means happier and more productive users. Another advantage of BYOD is that it supports a mobile and cloud-focused IT strategy.

However, Viruses and Spyware can cause untold damage to your business. So before setting BYOD up, research the security options available and see if they will cover what you need. If they don't, it is probably not worth taking the risk .

What BYOD policy includes?

BYOD policy comprises of the security requirements for each personal device, which is used by an employee in the organization. It includes password configuration of device, prohibition of unknown software installation, data encryption, limiting activities like social sites engagement, email usage, carry out official data outside workplace, periodic IT audit to ensure the compliance of such policy.

Why is BYOD Policy a Must?

As more products and services become accessible via mobile platform; security aspect becomes difficult for both organization and employee. If organization does not adopt a policy for personal device, then the official data that the employee carries in their Smartphone remains vulnerable.

For example, when you are in cafe using unprotected WI-FI network, you might not be aware about the hacker who is monitoring your device, and can read all official data exists in your device. It is true that BYOD brings flexibility and accessibility, but also brings security risks that help cyber attacker to swipe confidential data without your awareness.

Dangers of BYOD:

Along with benefits, there are several disadvantages with BYOD concept.

1. Data security is a main concern in BYOD. Employees can put an organization at risk, if an organization is not following strict policy for personal use of the device.
2. When an employee leaves the company, retrieving of official data and information is worrisome because these data is quit important for organization. In this case, a written signed BYOD policy should be implemented helps to get back confidential data from an employee.
3. All employees do not regular update their device with the latest hardware and software updates thus their devices become weak against updated patches. Even many of them do not install antivirus in their Smartphone, which is a serious concern, and could welcome malware attack.

4. Employees should lock their device. If the device is not protected with password or biometric security, then an unknown person can easily access personal data of the device.

The Security Solutions:

1. Securing mobile devices

Security risk expansion happens both on the basis of a more diverse device portfolio, and as a function of the number of devices. End users often have more than one device and would like to connect multiple devices to the organization's infrastructure, which increases the net number of devices that must be secured.

When it comes to mobile devices, well-developed programs should be based on an understanding of different user types and a clearly defined set of user segments. Risks relating to securing mobile devices are categorized into five basic concerns:

- Lost and stolen devices
- Physical access
- The role of end user device ownership
- Always on with increased data access
- Lack of awareness

2. Addressing app risk

Apps have largely driven the smartphone revolution and have made it as significant and as far-reaching as it is today. While apps demonstrate utility that is seemingly bound only by developer imagination, it also increases the risk of using BYOD devices in a corporate environment.

As the organization enables employees to bring their own, the need for using the same devices to access work-related data inevitably presents itself. This presents mainly two security risks:

- Malicious apps (malware): the increase in the number of apps on the device increases the likelihood that some may contain malicious code or security holes

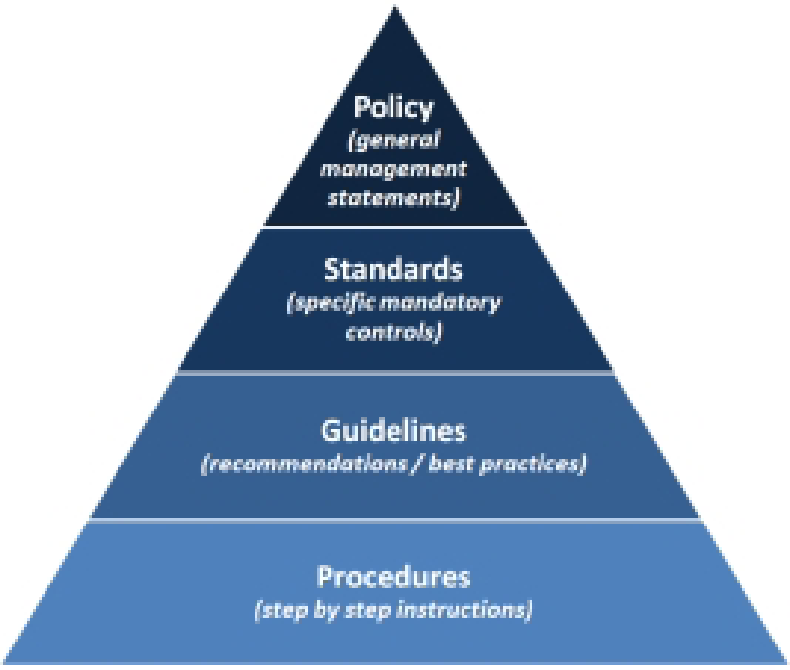
- App vulnerabilities: apps developed or deployed by the organization to enable access to corporate data may contain security weaknesses

Allowing your employees, contractors, and guest workers to use mobile devices on your network is not without challenges.

- New demands will be placed on your network bandwidth as the number of devices increase.
- Web site filtering, spam filtering, data leak protection and application control technologies will become even more important as information is transferred to and from each user's individual device.
- Wi-Fi technology will need to be tightly integrated into your security infrastructure.
- Networks will need to be segmented so that guest devices are not allowed on your production network.
- Authentication and encryption techniques may need to be extended to mobile devices.
- 'Per-user' licensing of your network security infrastructure will need to be reevaluated as the number of devices on your network explodes.

Security Solutions offered by companies:

1.Centrify for Samsung KNOX
2. Airwatch.
3. Cisco BYOD Smart Solution
4. Citrix BYOD Solutions
5. ForeScout


Policy
(general management statements)
Standards
(specific mandatory controls)
Guidelines
(recommendations / best practices)
Procedures
(step by step instructions)

JavaScript Injections And Their Cheatcodes

Summary:

JavaScript injection is a little technique that allows you to alter a sites contents without actually leaving the site. This can be very useful when say; you need to spoof the server by editing some form options. Examples will be explained throughout.

Using JavaScript, a user can modify the current cookie settings. This can be performed with some basic JavaScript commands. To view the current contents of your current cookies, use the following JavaScript command. Put this in your browser's URL bar.

```
javascript:alert(document.cookie);
```

I. Injection Basics:

JavaScript injections are run from the URL bar of the page you are visiting. To use them, you must first completely empty the URL from the URL bar. That means no http:// or whatever.

JavaScript is run from the URL bar by using the javascript: protocol.\ but if you are a JavaScript guru, you can expand on this using plain old JavaScript.

The two commands covered in this tutorial are the alert(); and void(); commands. These are pretty much all you will need in most situations. For your first JavaScript, you will make a simple window appear, first go to any website and then type the following into your URL bar:

Code:

```
javascript:alert('Hello, World');
```

You should get a little dialog box that says "Hello, World". This will be altered later to have more practical uses. You can also have more than one command run at the same time:

Code:

```
javascript:alert('Hello'); alert('World');
```

This would pop up a box that said 'Hello' and than another that says 'World'.

2. Cookie Editing

First off, check to see if the site you are visiting has set any cookies by using this script:

Code:

```
javascript:alert(document.cookie);
```

This will pop up any information stored in the sites cookies. To edit any information, we make use of the void(); command.

Code:

```
javascript:void(document.cookie="Field = myValue");
```

This command can either alter existing information or create entirely new values. Replace "Field" with either an existing field found using the alert(document.cookie); command, or insert your very own value. Then replace "myValue" with whatever you want the field to be.

For example:

Code:

```
javascript:void(document.cookie="Authorized=yes");
```

Would either make the field "authorized" or edit it to say "yes"... now whether or not this does anything of value depends on the site you are injecting it on.

3. Form Editing

Sometimes, to edit values sent to a given website through a form, you can simply download that HTML and edit it slightly to allow you to submit what you want. However, sometimes the website checks to see if you actually submitted it from the website you were supposed to. To get around this, we can just edit the form straight from JavaScript.

Note: The changes are only temporary, so it's not use trying to deface a site through JavaScript injection like this.

Every form on a given webpage (unless named otherwise) is stored in the forms[x] array. where "x" is the number, in order from top to bottom, of all the forms in a page. Note that the forms start at 0, so the first form on the page would actually be 0, and the second would be 1 and so on.

Lets take this example:

Code:

```
<form action="http://www.website.com/submit.php" method="post">
<input type="hidden" name="to" value="admin@website.com">
```

Note: Since this is the first form on the page, it is forms[0]

Say this form was used to email, say vital server information to the admin of the website. You can't just download the script and edit it because the submit.php page looks for a referrer. You can check to see what value a certain form element has by using this script.

Code:

```
javascript:alert(document.forms[0].to.value)
```

This is similar to the alert(document.cookie); discussed previously. In this case, It would pop up an alert that says "admin@website.com"

So here's how to Inject your email into it. You can use pretty much the same technique as the cookies editing shown earlier:

Code:

```
javascript:void(document.forms[0].to.value="xyz@xyz.com")
```

This would change the email of the form to be "xyz@xyz.com". Then you could use the alert(); script shown above to check your work. Or you can couple both of these commands on one line.

Other codes:

```
javascript:alert("XSS By Priyanshu");

javascript:alert(0);

javascript:alert(document.forms[0].to.value="something")

document.body.contentEditable='true';document.designMode='on';void0
```

To move things around on the webpage

So, this is how the website of your company can get hacked/defaced. There are a lot of vulnerabilities that could be there in your website, which are mostly due to errors in programming or unsanitized input fields.

Always ask your programmers to follow security guidelines while programming web applications, so that XSS, SQLI and other attacks can be checked.

This article was written by Mr. Priyanshu Sahay, founder of HackersOnlineClub and iGadgetware. He is a tech geek and a certified cyber security expert. He is working om cyber security research.

The Dark and Mysterious Deep Web

In March 2013, a member of our community hackerDesk sent an email regarding a domain name with onion extension, we thought let's check it out and we opened that domain in a browser which gave the message "Server not found".

We then checked with Google to find relevant information about it. We searched throughout Google and finally came to know, the importance of onion domain.

In lots of article we found the word "Deep Web", our curiosity was heightened about the topic and we started to research on it. Now our aim is to share some insights and our practical experience which had so far.

Let's take a look on the full story about "Deep Web".
According to Wikipedia, "The Deep Web (also called the Deepnet, Invisible Web, or Hidden Web) is a World Wide Web content that is not a part of the Surface Web".

So what is Surface web? The surface web is the usual web, in which we surf in our day to day life. The sites for which we search on Google, Videos on YouTube, they all are the part of surface web.

But the sites, to which we don't have direct access, are part of the Deep Web. So what does that mean? Maybe most of you heard about the Tor network and I am sure many of you might have used Tor.

Firstly we would like to throw some light on "what Tor basically is"?
Tor is a web browser which works on a network of proxies. To access Deep Web sites is by using Tor or simply by using different proxy methods.

There is a rough estimate that Deep web contains 7,500 terabytes of information, compared to the 19 terabytes of the surface web. So that's a really huge source of information which we generally don't know about. So this is the web or internet which is beyond reach of Google and some other search engines.

Now the question is, what's exactly is on Deep Web?
Drug markets, services like hitmen, Heavy Jailbait etc.

Basically Deep web is a threatening zone. While surfing the Web, you are really just floating at the surface level. Dive in and you would see that there is a sea with a very deep bottomt -- an unfathomable space, which most of us would have never seen. That includes everything from boring statistics to human body parts for sale (illegally).

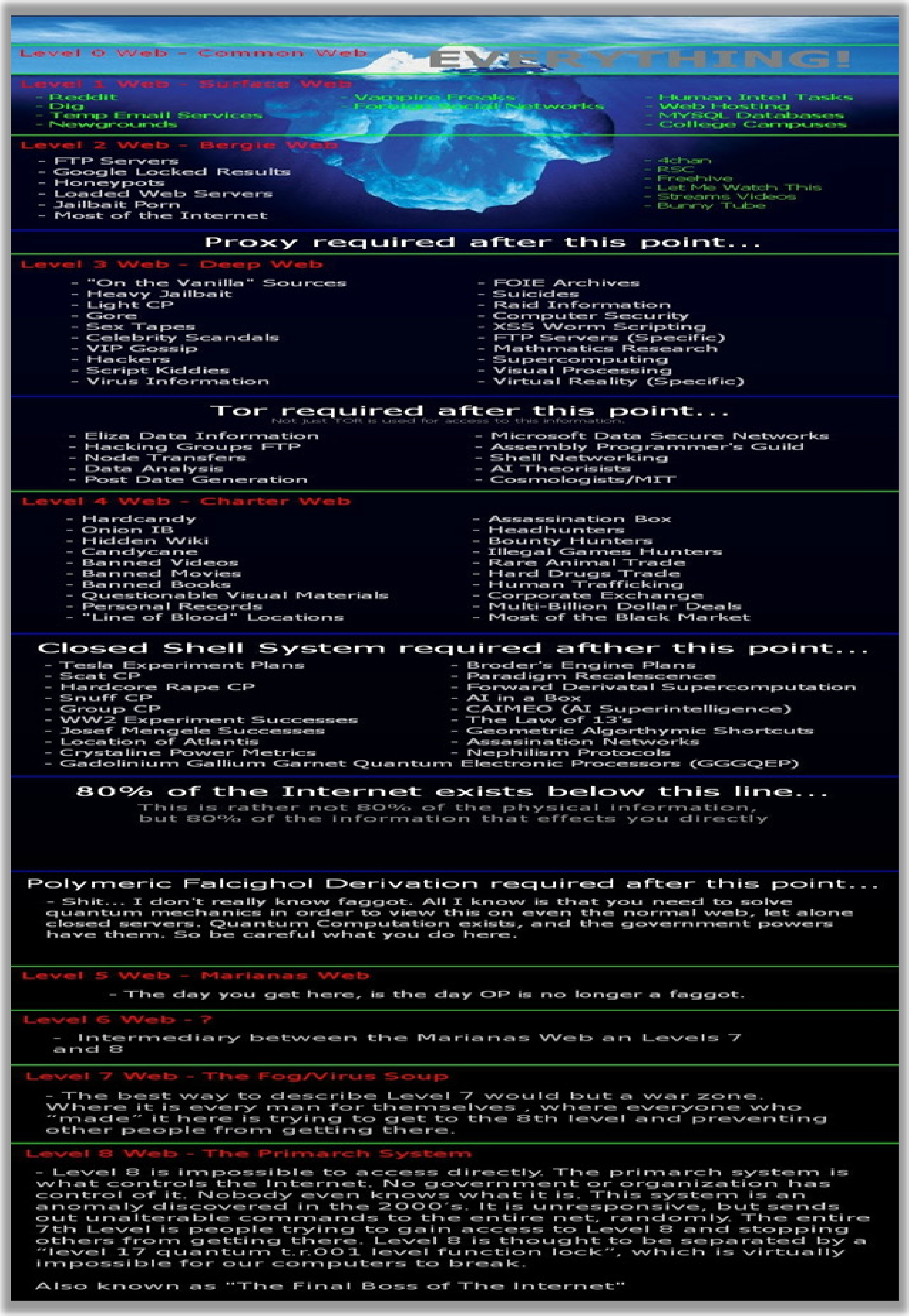
The immense majority of the Deep Web holds pages with valuable information. A report in 2001 -- the best till date -- estimates 54% of onion sites are actual databases, among the worlds largest are of U.S.National Oceanic and Atmospheric Administration (NASA), the Patent and Trademark Office and the Securities and Exchange Commission's EDGAR search system -- all of which are public.

The next batch has pages kept private by companies that charge a fee to access them, such as government documents on LexisNexis and Westlaw or the academic journals on Elsevier. Another 13% of pages lie hidden because they're usually found on an Intranet.

These internal networks -- say, at corporations or universities -- have access to message boards, personnel files or industrial control panels that can flip a light switch or shut down a complete power plant.

There is another story about Deep Web that Deep has 8 layers. Depicted in this picture below:

Please zoom to view the image properly :)



Level 0 Web - Common Web

EVERYTHING!

Level 1 Web - Surface Web

- Reddit
- Dig
- Temp Email Services
- Newgrounds
- Vampire Freaks
- Foreign Social Networks
- Human Intel Tasks
- Web Hosting
- MYSQL Databases
- College Campuses

Level 2 Web - Bergie Web

- FTP Servers
- Google Locked Results
- Honeypots
- Loaded Web Servers
- Jailbait Porn
- Most of the Internet
- 4chan
- RSC
- Freehive
- Let Me Watch This
- Streams Videos
- Bunny Tube

Proxy required after this point...

Level 3 Web - Deep Web

- "On the Vanilla" Sources
- Heavy Jailbait
- Light CP
- Gore
- Sex Tapes
- Celebrity Scandals
- VIP Gossip
- Hackers
- Script Kiddies
- Virus Information
- FOIE Archives
- Suicides
- Raid Information
- Computer Security
- XSS Worm Scripting
- FTP Servers (Specific)
- Mathmatics Research
- Supercomputing
- Visual Processing
- Virtual Reality (Specific)

Tor required after this point...

Not just TOR is used for access to this information.

- Eliza Data Information
- Hacking Groups FTP
- Node Transfers
- Data Analysis
- Post Date Generation
- Microsoft Data Secure Networks
- Assembly Programmer's Guild
- Shell Networking
- AI Theorisists
- Cosmologists/MIT

Level 4 Web - Charter Web

- Hardcandy
- Onion IB
- Hidden Wiki
- Candycane
- Banned Videos
- Banned Movies
- Banned Books
- Questionable Visual Materials
- Personal Records
- "Line of Blood" Locations
- Assassination Box
- Headhunters
- Bounty Hunters
- Illegal Games Hunters
- Rare Animal Trade
- Hard Drugs Trade
- Human Trafficking
- Corporate Exchange
- Multi-Billion Dollar Deals
- Most of the Black Market

Closed Shell System required afther this point...

- Tesla Experiment Plans
- Scat CP
- Hardcore Rape CP
- Snuff CP
- Group CP
- WW2 Experiment Successes
- Josef Mengele Successes
- Location of Atlantis
- Crystaline Power Metrics
- Gadolinium Gallium Garnet Quantum Electronic Processors (GGGQEP)
- Broder's Engine Plans
- Paradigm Recalescence
- Forward Derivatal Supercomputation
- AI in a Box
- CAIMEO (AI Superintelligence)
- The Law of 13's
- Geometric Algorthymic Shortcuts
- Assasination Networks
- Nephilism Protocols

80% of the Internet exists below this line...

This is rather not 80% of the physical information, but 80% of the information that effects you directly

Polymeric Falcighol Derivation required after this point...

- Shit... I don't really know faggot. All I know is that you need to solve quantum mechanics in order to view this on even the normal web, let alone closed servers. Quantum Computation exists, and the government powers have them. So be careful what you do here.

Level 5 Web - Marianas Web

- The day you get here, is the day OP is no longer a faggot.

Level 6 Web - ?

- Intermediary between the Marianas Web an Levels 7 and 8

Level 7 Web - The Fog/Virus Soup

- The best way to describe Level 7 would but a war zone. Where it is every man for themselves , where everyone who "made" it here is trying to get to the 8th level and preventing other people from getting there.

Level 8 Web - The Primarch System

- Level 8 is impossible to access directly. The primarch system is what controls the Internet. No government or organization has control of it. Nobody even knows what it is. This system is an anomaly discovered in the 2000's. It is unresponsive, but sends out unalterable commands to the entire net, randomly. The entire 7th Level is people trying to gain access to Level 8 and stopping others from getting there. Level 8 is thought to be separated by a "level 17 quantum t.r.001 level function lock", which is virtually impossible for our computers to break.

Also known as "The Final Boss of The Internet"

By observing the above figure, you may say using Tor we usually search for 2nd level on deep web, but what about other levels?

So, let's go around and grab insights for other levels. The whole story began with 4chan when someone posted the above picture on 4chan.

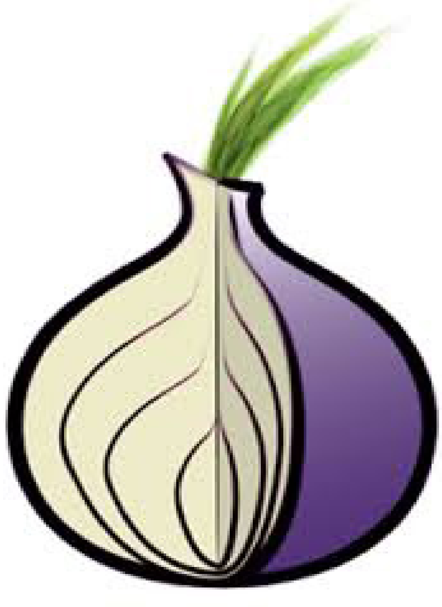
Now the question is, are these levels "real"? If you go all around through what is Close Shell System ,it does sound like 2-3 PC's connected over Local Area Network (LAN). So, searching for this level is a waste of time, you won't find anything, eh? As we know that ICANN's main 7 servers control the internet, from that we had a prediction that 8th level of Deep Web is accessible to someone who really has control to all those servers.

Go move on to DEEP WEB:-

Use tor browser and search for Hidden Wiki. Hidden Wiki contain links for other Deep Web sites.

Hidden Wiki Address: - https://kpvz7ki2v5agwt35.onion.to

Recent Report says that NSA monitors Tor network. So be safe, be proud, the world is yours :)



Gurjant Singh Sadhra and Mayank Kapoor are Independent Security Researchers. They discovered some major security issues in high profile companys like Facebook,Yahoo,Twitter,Ebay etc. They are speakers at Null Chapter's. Gurjant Singh Sadhra is also a speaker at OWASP.

The Security and Privacy Model of Firefox OS

This article talks about why the people working in the companies and all those who want to keep their data safe should consider making the switch to mobiles having Firefox OS.

Here we will discuss the privacy and security model of the Firefox OS, demonstrating its strengths and sound security infrastructure. None of us wants our private data to be monitored, or our contacts to go into the hands of the wrong people. So, we present before you some great features of FxOS which will convince you that THIS is the smart solution!

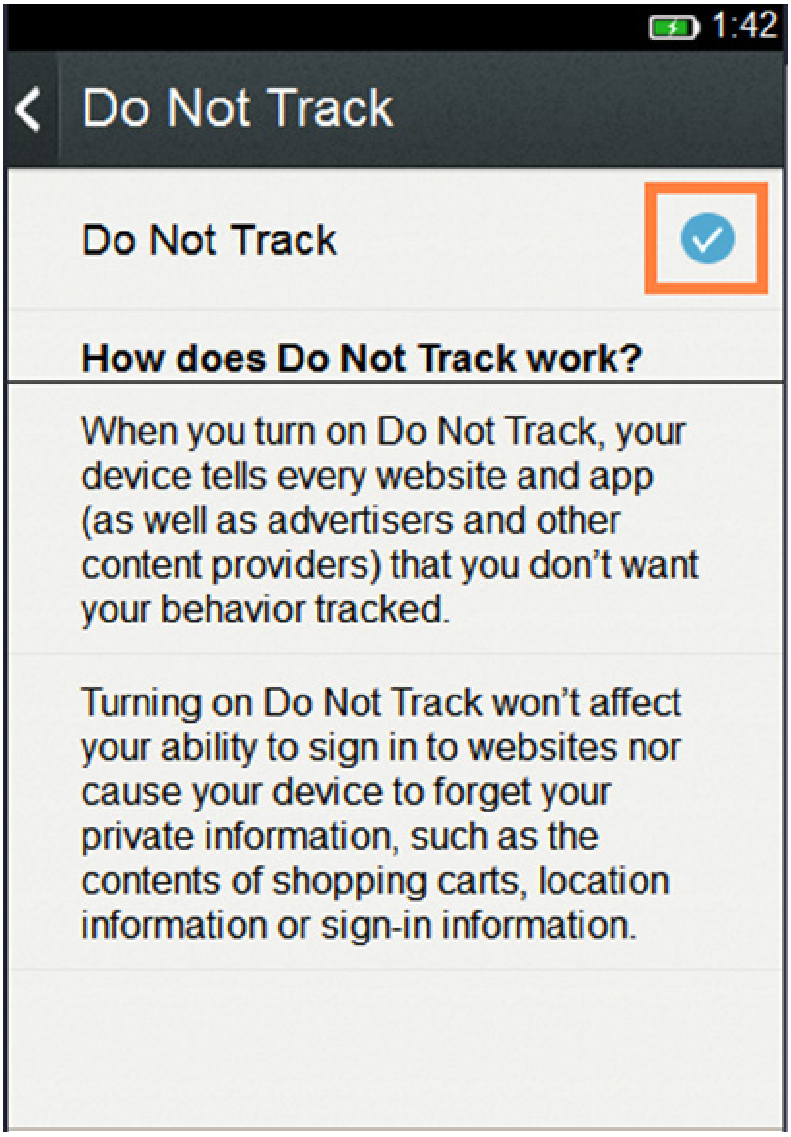
How does the Do Not Track feature work?

When you turn on the Do Not Track feature, Firefox tells every website you visit (as well as their advertisers and other content providers) that you don't want your browsing behavior tracked. Honoring this setting is voluntary — individual websites are not required to respect it. Websites that do honor this setting should automatically stop tracking your behavior without any further action from you.

Turning on Do Not Track will not affect your ability to log in to websites nor cause Firefox to forget your private information — such as the contents of shopping carts, location information or login information.

The Security Model of Firefox OS

The Firefox OS platform uses a multi-layered security model that is designed to mitigate exploitation risks at every level. Front-line countermeasures are combined with a defense-in-depth strategy that provides comprehensive protection against threats. Gecko is the gatekeeper that enforces security policies designed to protect the mobile device from misuse.



Do Not Track

Do Not Track ☑

How does Do Not Track work?

When you turn on Do Not Track, your device tells every website and app (as well as advertisers and other content providers) that you don't want your behavior tracked.

Turning on Do Not Track won't affect your ability to sign in to websites nor cause your device to forget your private information, such as the contents of shopping carts, location information or sign-in information.

Subsequent upgrades and patches to the Firefox OS platform are deployed using a secure Mozilla process that ensures the ongoing integrity of the system image on the mobile phone. The update is created by a known, trusted source — usually the device OEM — that is responsible for assembling, building, testing, and digitally signing the update package.

An application's trust level determines, in part, its ability to access mobile phone functionality.

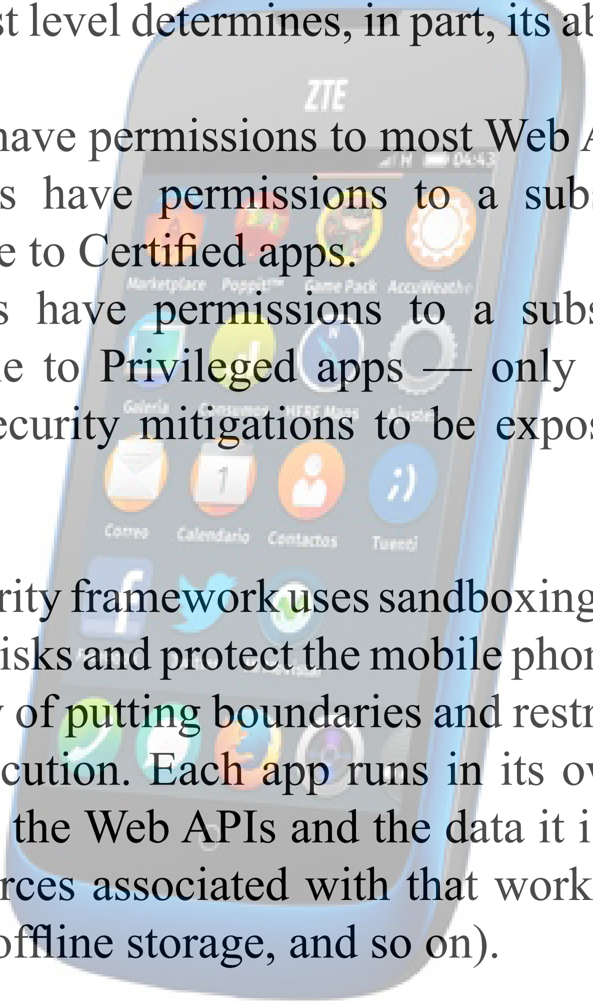
- Certified apps have permissions to most Web API operations.
- Privileged apps have permissions to a subset of the Web API operations accessible to Certified apps.
- Untrusted apps have permissions to a subset of the Web API

The Security Model of Firefox OS

The Firefox OS platform uses a multi-layered security model that is designed

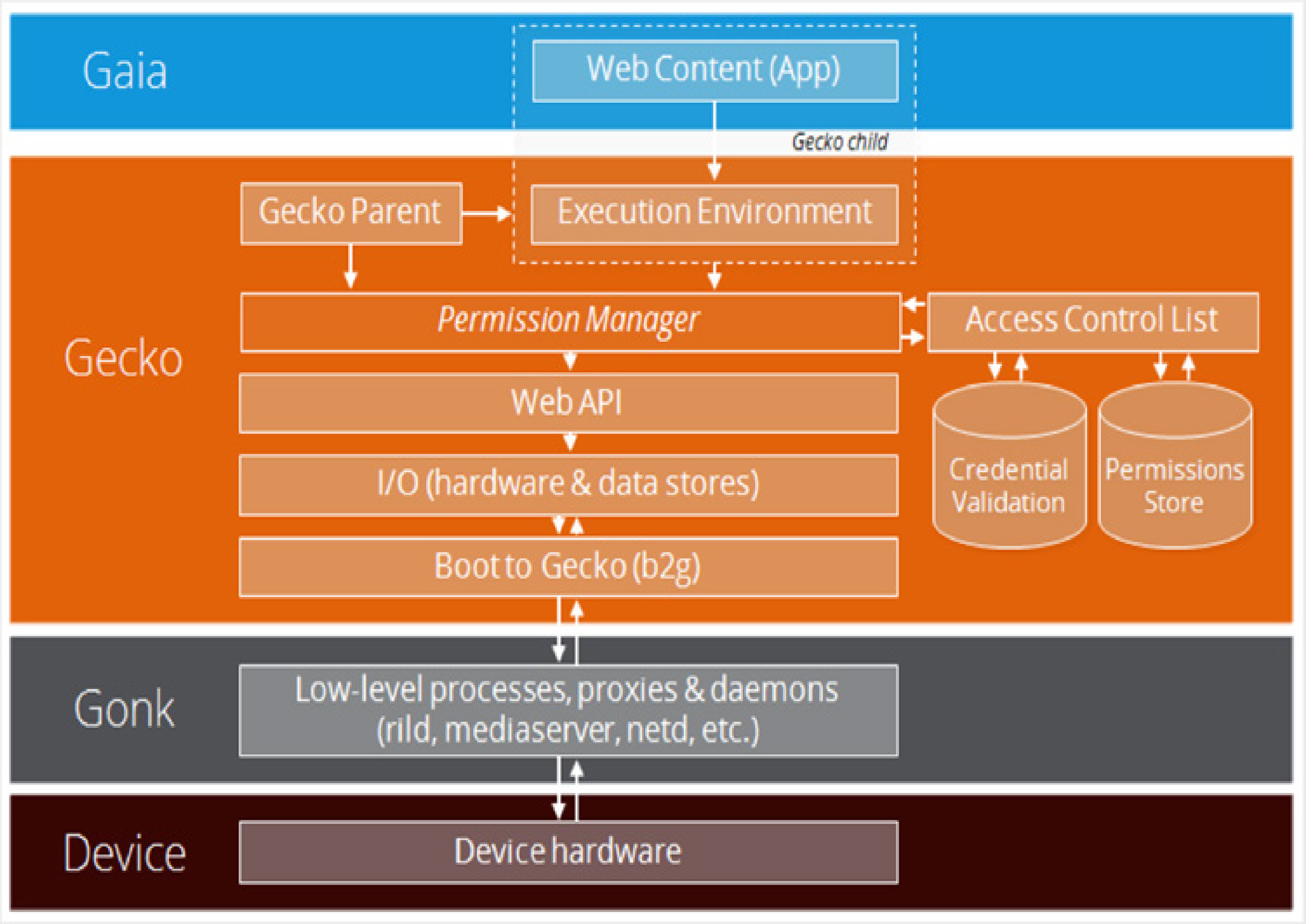
to mitigate exploitation risks at every level. Front-line countermeasures are combined with a defense-in-depth strategy that provides comprehensive protection against threats. Gecko is the gatekeeper that enforces security policies designed to protect the mobile device from misuse.
Subsequent upgrades and patches to the Firefox OS platform are deployed using a secure Mozilla process that ensures the ongoing integrity of the system image on the mobile phone. The update is created by a known, trusted source — usually the device OEM — that is responsible for assembling, building, testing, and digitally signing the update package.
An application's trust level determines, in part, its ability to access mobile phone functionality.

- Certified apps have permissions to most Web API operations.
- Privileged apps have permissions to a subset of the Web API operations accessible to Certified apps.
- Untrusted apps have permissions to a subset of the Web API operations accessible to Privileged apps — only those Web APIs that contain sufficient security mitigations to be exposed to untrusted web content.



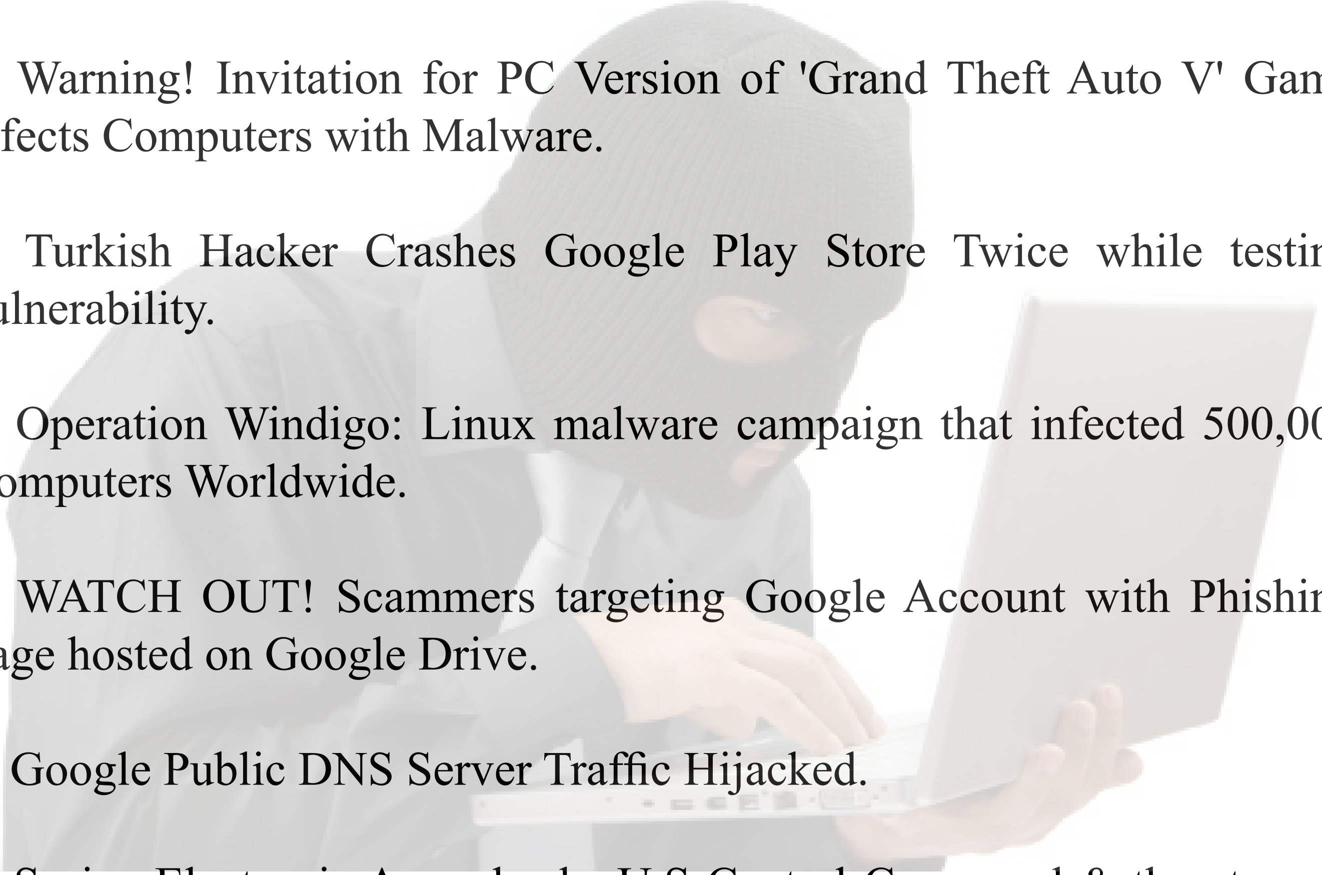
The Firefox OS security framework uses sandboxing as a defense-in-depth strategy to mitigate risks and protect the mobile phone, platform, and data. Sandboxing is a way of putting boundaries and restrictions around an app during run-time execution. Each app runs in its own worker space and it has access only to the Web APIs and the data it is permitted to access, as well as the resources associated with that worker space (IndexedDB databases, cookies, offline storage, and so on).

B2G (Gecko) runs in a highly-privileged system process that has access to hardware features in the mobile phone. At runtime, each app runs inside an execution environment that is a child process of the B2G system process. Each child process has a restricted set of OS privileges — for example, a child process cannot directly read or write arbitrary files on the file system. Privileged access is provided through Web APIs, which are mediated by the parent B2G process.



Apart from all this, the FxOS has features like Serialised Data Storage and a more efficient and secure data destruction mechanism. The Gecko engine is a very efficient technology which makes the OS to run smoothly. The FxOS marketplace is being developed zealously by the developers. Huge array of popular apps like Facebook, Twitter and Cut The Rope have already been ported to FxOS. I would advise all the readers, to try FxOS and get a taste of freedom, security and privacy!

Latest Tech Crunches



1. Microsoft sells your Information to FBI; Syrian Electronic Army leaks Invoices.

2. Linux Worm targets Internet-enabled Home appliances to Mine Cryptocurrencies.

3. Back off, NSA! Gmail now Encrypts every single Email.

4. Warning! Invitation for PC Version of 'Grand Theft Auto V' Game infects Computers with Malware.

5. Turkish Hacker Crashes Google Play Store Twice while testing vulnerability.

6. Operation Windigo: Linux malware campaign that infected 500,000 Computers Worldwide.

7. WATCH OUT! Scammers targeting Google Account with Phishing Page hosted on Google Drive.

8. Google Public DNS Server Traffic Hijacked.

9. Syrian Electronic Army hacks U.S Central Command & threatens to leak Secret Documents.

10. Twitter enables StartTLS for Secure Emails to prevent Snooping.

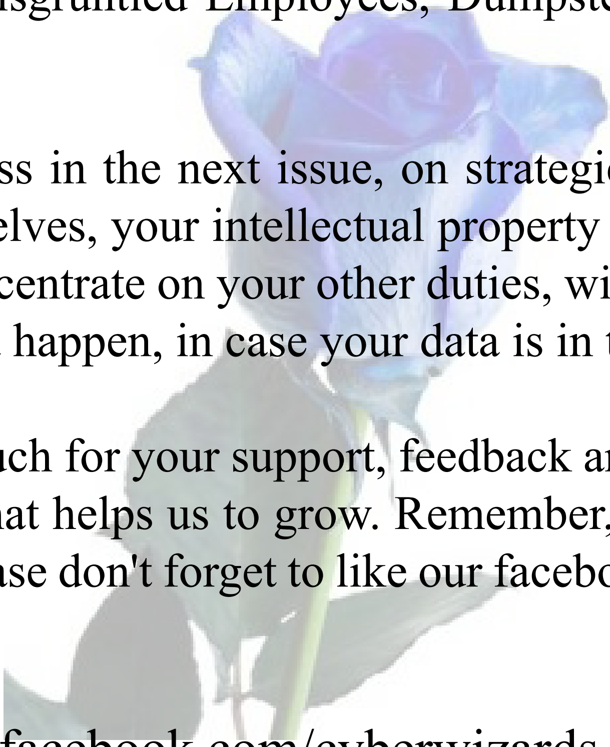
11. BEWARE of new Facebook Malware Claims, 'Malaysia Plane MH370 Has Been Spotted'.

Credits: The Hacker News (www.thehackernews.com)

An Epilogue

Thank you for being with us yet again. We hope that you would have enjoyed our magazine! Stay tuned with us for the next issue, which contains more interesting articles.

In the next issue, we will be diving deeper into "Corporate Security" and the "Cyber Culture". We will be discussing OWASP Open Source Testing Methodology, Cyber Law, the risks companies face from within like Insider Trading, Disgruntled Employees, Dumpster Diving and Social-Engineering.



We will also discuss in the next issue, on strategies that you can adopt to safeguard yourselves, your intellectual property and your data, so that you can amply concentrate on your other duties, without having to worry about all that could happen, in case your data is in the wrong hands!

Thank you very much for your support, feedback and response. It is your support and love that helps us to grow. Remember, it is never too late to learn. And yes, please don't forget to like our facebook page, we really do need more likes ;)

www.facebook.com/cyberwizards.codezero

That's all folks. Keep learning, keep practicing and have a safe and secure hunting session.

With Warm Regards,
The Code Zer0 Magazine Crew
(www.cyberwizards.org)