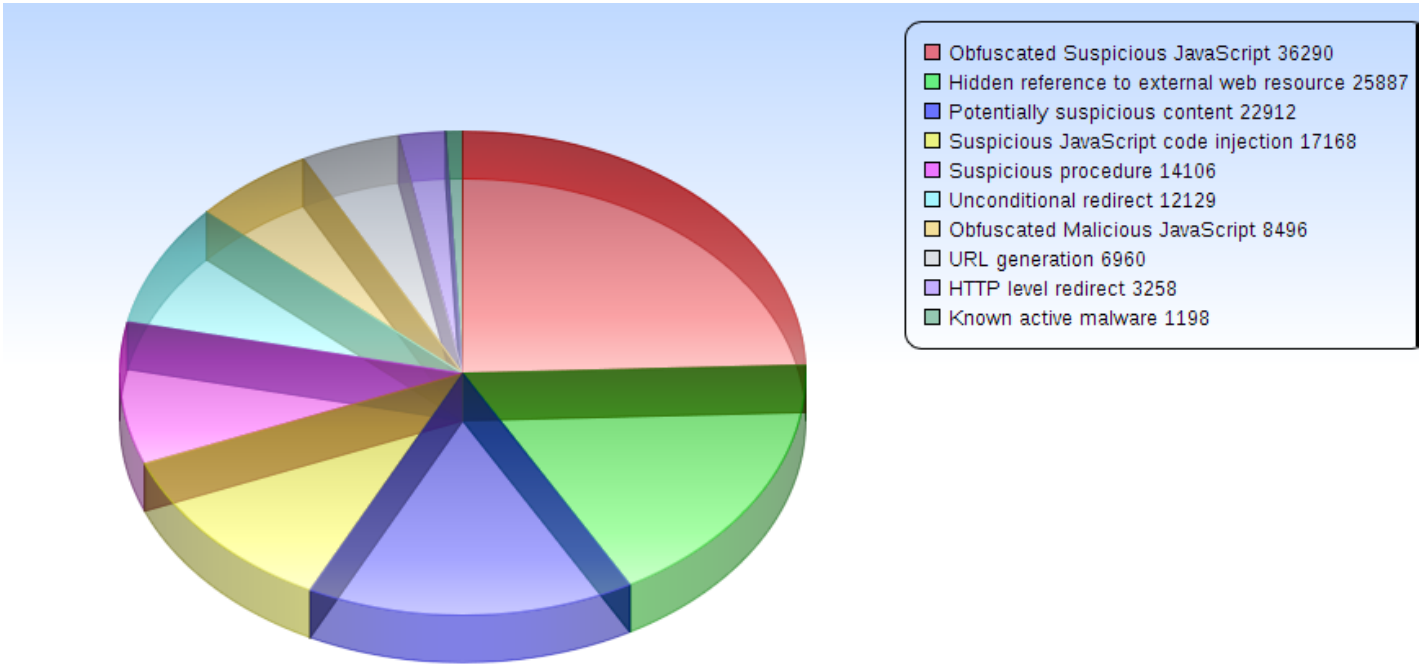
The Top 10 Threats

Statistics from Online Website Malware Scanner by Quttera

This report was compiled from May 2014 malware statistics as detected on scanned websites.



Obfuscated Suspicious JavaScript

Encoded JavaScript code commonly used to hide suspicious behavior was detected in 36290 web pages.
In majority of cases, the decoded script was either injecting malicious JavaScript code from compromised servers using <script> tag (<script src="url-to-malicious-script-file-on-remote-server"></script>) or such scripts generates and injects hidden iframes (<iframe src="link-to-infected-or-black-seo-page" style="display:none;"> </iframe>) leading to suspicious HTML pages.

Hidden reference to external web resource

Infected web pages count is 25887. The reason was a compromised server having its all or part of HTML pages served infected by threat that injects hidden iframes leading to malicious or "black-hat" SEO HTML pages. In case of static HTML pages, such infection was done by injection and execution of malicious script that iterates over all HTML pages and infects them one by one. In case of PHP-based CMS platforms like WordPress or Joomla, such infection is often more complex and maybe hidden into (a) callback function that is invoked upon generation of every page or inside (b) PHP code that is automatically added to header and/or footer of the infected CMS.

Contact Us

https://helpdesk.quttera.com/
Quttera.com

References

http://quttera.com/website-scanner-statistics-last-month

QUTTERA
Web Security Advantage

The Top 10 Threats

Statistics from Online Website Malware Scanner by Quttera

Potentially suspicious content

Such infection was detected on 22912 pages having the diversity of potential threat. Quttera heuristic engines (investigation layers) detected JavaScript code performing suspicious actions that could not be automatically treated as malicious and require human investigation for further decision. Like JavaScript packers for example that were already detected along with known malware.

Suspicious JavaScript code injection

In 17168 web pages there was JavaScript code attempting to perform various suspicious actions. Prevalent case of which was suspicious <script> tag loading JavaScript libraries from not trusted and or suspicious servers.

Suspicious procedure

Procedures that are commonly used in suspicious activity were found in 14106 web pages. JavaScript provides multiple procedures and functions that widely used to hide malicious activity on loaded web pages.
For example ‘eval’, ‘unescape’, ‘String.fromCharCode’, ‘String.replace’ and others used to hide malicious activities like ‘JavaScript code injection’, ‘iframe injection’, execution of ‘drive by download’ attack and etc. No active malware detected at the time of the scan.

Unconditional redirect

12129 web pages were trying to redirect visitors’ browsers to external web resource(s) without visitors’ intervention - HTML (<meta http-equiv="refresh" content="0; url=http://example.com/" />) or
JavaScript levels (<script> window.location.href = new_url; </script>). From the experience, such redirects are result of injected malicious HTML/JavaScript code into compromised HTML/JavaScript/PHP files.

Obfuscated Malicious JavaScript

In 8496 web pages the obfuscated JavaScript was similar or identical to those used in hiding the malware. From further investigation, such websites were serving active malware. In some cases, they were already blacklisted by one or more authorities. Prevalent threats: Trojans and AdWare.

URL generation

6960 web pages contained URLs that were generated during execution. This technique is widely used by malware distributors to hide malicious URLs from pattern based detection mechanisms like application firewalls and IDS systems. The concept is based on separation of the malicious URL to serveral parts into the source JavaScript code and URL generation upon code execution.
For example following JavaScript code will redirect user to infected malicious page

```
<scirpt>
 var malicious_url = "ht" + "tp:" + "//this" + ".is." + "mali" + "cio" + "us" + "." + "url" + "/?qu" + "ery" + "par" + "ams"
 window.location.href = malicious_url;
</script>
```

Contact Us

https://helpdesk.quttera.com/
Quttera.com

References

http://quttera.com/website-scanner-statistics-last-month

HTTP level redirect

Suspicious redirect to external web resources at HTTP level was identified in 3258 web pages. These pages were hosted by compromised websites which root .htaccess file included redirection to suspicious third party server that further redirected visitors to another server or just served ads or pharms.

Known active malware

Known malicious content was detected in 1198 web pages during this report time frame. The malware landscape was comprised of: Trojans, Adware, Viruses, Vulnerability Exploits and others.