

Bryley Tips and Information

December 2010

1. What to expect in Internet Explorer 9

Internet Explorer 9 Beta was released three months ago on September 15, 2010. This faster, more reliable, more secure, easier to use web browser is also sleeker and more sophisticated than its predecessor. While we do not recommend downloading software still in development, we do want to highlight the new features to anticipate in the finalized version of Internet Explorer 9 (IE9) which at present does not have a release date but will be coming in the New Year.

1. **Better Design** – With IE9 the web is brought to the forefront as more websites now fit within a window. IE9 also boasts an optimized user interface. Controls have been both enhanced and simplified (for example the address and search bars have been combined and the Notification Bar is no longer a hassle) while command menus have been streamlined.
2. **Faster Browsing** – By utilizing the graphics processors of PCs IE9 is all around faster than IE8 and can keep up with everything the Internet has to offer (for instance you can watch videos smoothly or zoom in and out quickly with the picture staying crystal clear).
3. **SmartScreen** – This new feature detects malware and phishing websites and blocks them for you automatically, increasing the security of your PC while you browse the web.
4. **Domain Highlighting** – The Domain Highlighting feature displays the true domain name of the page you are viewing, alerting you to fraudulent web sites.
5. **Crashed Page Isolation and Automatic Recovery** – If a web page crashes in IE9, only the one page will stop working and will automatically recover while you continue on with your browsing session.
6. **Pinned Sites** – This new feature allows you to drag and pin a website directly to your taskbar, allowing you direct access to your favorite sites with just a single click of the mouse.
7. **Download Manager** - Keeping an up-to-date and cumulative list of all of the files that you download from the Internet, Download Manager allows you to pause and restart a download, shows you where to locate all downloaded files, and notifies you when a download might be potentially malicious.
8. **Enhanced Tabs** – The Enhanced Tabs feature generates easy movement between multiple open web pages in a single window – each page delineated by a tab. You can even observe two pages simultaneously by dragging a web page outside the open window through the Tear-Off Tabs function and then use the Snap function for side-by-side viewing.

9. **New Tab Page** – This redesigned feature displays all of your most frequented sites, color coded for quick navigation. The Site-Indicator function even displays how often you visit each site.
10. **Add-on Performance Advisor** – The Add-on Performance Advisor audits each add-on you acquire, alerting you if the add-on is slowing down your browser performance. This feature also allows you to disable and remove any add-ons you select.
11. **InPrivate Browsing and Filtering** – InPrivate optimizes browsing privacy. The Browsing feature opens a new window wherein private information such as search history, temporary files, usernames or passwords cannot be traced. The Filtering feature controls what information third party websites can and cannot track about your browsing history.

The new Internet Explorer 9 will indeed revolutionize the web interface. Features such as SmartScreen, Domain Highlighting and Download Manager will increase the security of web browsing while the Enhanced Tabs, New Tab Page and Pinned Sites will make surfing faster than ever. While the upgrade is recommended, you should abstain from downloading the beta version as it is still in development and prone to err. We suggest that you wait for the finalized version to surface before enjoying all of the latest features.

Want to learn more?

Contact Bryley today. Call 888.280.5799 or email Sales@Bryley.com.

2. Recognizing and blocking malicious traffic with IP/DNS Reputation Services from HP

With approximately 5,500 active CnC servers, anywhere from 2,500 to 50,000 new Malware depots discovered daily, 50,000 new Phishing sites discovered monthly, and millions of known compromised devices the world over it is clear that we are facing a network security pandemic.

In order to protect your network, all traffic must be thoroughly inspected for legitimacy. Unfortunately, there is a lot of ambiguous traffic to sift through nowadays as hackers and their procedures become more and more covert.

CnC Servers

Command and control (CnC) servers are utilized by bot herders for remote control of their botnets. CnC servers are very dynamic and therefore extremely hard to pinpoint. Bot herders also use dynamic algorithms to select CnC servers and both DNS and IP addresses for CnC location, making it virtually impossible for firewall ACLs to block. CnC servers create a lot of ambiguous traffic through their covert use of proper channels such as IRC, P2P and HTTP traffic to communicate with their bots (including Twitter and Instant Messenger messages).

Malware Depots

Malware depots are used as “drop sites” for botnets or hosts for malware updates. They are either websites designed to lure you in and infect your computer or legitimate sites that have been compromised. The trouble with such sites is that they are dynamic and therefore hard to pinpoint.

Phishing Sites

Phishing sites attempt to steal personal information such as bank account or social security numbers. As with Malware depot sites, Phishing sites are either purpose-built or are legitimate sites that have been compromised. Again, the use of dynamic IP addresses makes Phishing sites hard to pinpoint.

Compromised Devices

Servers, computers and laptops can become compromised and turned into Malware hosts and zombies. What is more, the compromised status attempts to remain covert until it has furthered its reach within a network.

HP's Solution

This new ambiguous traffic requires deep packet inspection to determine whether or not it is wanted by or harmful to your network. In response to this need, HP conducted a worldwide accumulation of attack information and compromised devices as well as performed its own web traffic crawling and analysis. With the information compiled, HP then created a master database of all of the known CnC servers, Malware depots, Phishing sites, compromised devices and DNS names and IP addresses linked to compromised devices and/or malicious activity. This Reputation Database not only contains the reputations of all IPv4 and IPv6 addresses and DNS names known to cause attacks (a list that is updated every 2 hours by HP partner TippingPoint) but it also scores all other ambiguous traffic with unknown IP addresses and DNS names based on set parameters of what constitutes good from bad traffic reputations based on recent Malware research and analysis. Not only are the new HP Reputation Services effective, but they are also custom tailored to your needs; you may set your own blocking policies based upon reputation scores, country of origin, type of device, and data source.

Want to Learn More?

Contact Bryley today. Call 888.280.5799 or email Sales@Bryley.com.

3. Best Practices for Data Security Optimization

Data is the very pulse of all business and as such an airtight data security strategy is absolutely vital for business functionality and growth. In order to protect your ever growing and changing

data sets we advise that you incorporate a daily, automated and scalable data security routine that includes these 5 best practices:

1. A Ban on All Global Groups

Be aware of folder access control permissions such as “everyone” or “domain users.” Although a global group is seemingly very convenient, it is ill advised as it presents a potential human error security risk because any data placed within that file or folder will inherit the lax access permissions. This is problematic if an employee accidentally places data within these wide-open folders that was meant for specific eyes only or if the employee was unaware of the extreme laxness of the access permissions.

Most users only need access to a small portion of the business data residing on file servers and user access to data that is not necessary for their specific role constitutes a security threat. All global group access should be removed and replaced with ACLs that permit access to only the specific groups within one’s business that have the authority to use such data.

2. Awareness of Unused Data and Accounts

Not all access accounts or data on shared file servers or network attached storage devices are in active use. Not only is the unused information unnecessary but it is harmful as well. Unused access accounts pose a security threat while unused data complicates your shared files and slows down your network.

User accounts for employees that are no longer with your business should be deleted as these unused accounts could be harnessed by those with a working knowledge and access to user directories in an effort to steal data. By deleting or archiving your data to an offline storage you will make the management of the remainder of your data simpler as the data will now be easier to organize and quicker to access.

3. Conserve Access Changes

Now that your user access accounts are all current, valid and secure you should also get into the practice of maintaining a searchable archive of all user access changes. This extra safeguard will assist in forensic analysis should data misuse or loss occur. By searching on a username, filename, date, or any combination thereof you will be equipped to determine who accessed what data when and how.

By adhering to these three simple practices you will vastly improve the accuracy of your data access entitlement and therefore data protection.

4. Announcements, News and Events

- **Service Ticket Raffle Winner**

Every month we hold a raffle with all of the completed service tickets we receive. The prize is a Dunkin' Donuts gift card. Last month's winner was Geary Lashua of United Solutions, Inc. Congratulations Geary.

Client service

If you have questions about, or issues with, our client service or response, please contact Beverley Denio, Client-Service Manager, at 978.562.6077 x201, or Gavin Livingstone, President, at 978.562.6077 x215. (Respective email addresses are BDenio@Bryley.com and GLivingstone@Bryley.com.)

Bryley's Client-Service Portal

Over the past years, Bryley has made significant investments in our business systems and infrastructure to enable real-time communications regarding the timeliness and quality of services we deliver. A result is that client-service requests (with resulting service tickets) may now be added, viewed, or updated through our Client-Service Portal.

This real-time environment is available 24 x 7 at www.Bryley.com by selecting "Client Login" from the upper-right corner of the home-page. Registered users may perform these functions:

- View the current status and details of their service tickets
- Enter new service requests
- Review invoices
- View reports

To use this capability, please contact Beverley at 978.562.6077 x201 to setup a username and password. Training is also available at no charge.

Contact Bryley Systems Inc.

Bryley Systems is a full-service, end-to-end provider of business-technology solutions, fulfilling the information technology needs of organizations throughout New England since 1987. Areas of expertise include:

- Managed Technology
- Computer-network performance and reliability
- Network security
- Unified Communications

Email: Info@Bryley.com

Phone: 978.562.6077

Fax: 978.562.5680

www.Bryley.com

Bryley Systems Inc.
12 Main Street

Hudson, MA 01749-9990

Business Technology Solutions Since 1987

How to Subscribe or Unsubscribe

Bryley Tips and Information is a free e-newsletter sent each month (except July). It provides information and user level tips on computer and telephone-system issues.

You are receiving this e-newsletter because:

- You are a Bryley client
- You have received a quote or proposal from Bryley sales, or
- You have had business contact with Bryley Systems.

Subscribe

If you or a colleague wishes to subscribe to this e-newsletter, please e-mail Newsletter@Bryley.com, visit www.Bryley.com/news_and_events-newsletter.html, or contact Beverley at 978.562.6077 x201 or via BDenio@Bryley.com.

Unsubscribe

Options to unsubscribe from this e-newsletter:

- Please reply to this newsletter with the word "unsubscribe" in the subject header.
- Visit www.Bryley.com/news_and_events-newsletter.html.
- Email Newsletter@Bryley.com.
- Call us at 888.280.5799.

Copyright 2010. Bryley Systems Inc. All Rights Reserved.

THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. The information contained in this document represents the current view of Bryley Systems Inc. on the issues discussed as of the date of publication. Bryley Systems Inc. cannot guarantee the accuracy of any information presented.

INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED 'AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND FREEDOM FROM INFRINGEMENT. The user assumes the entire risk as to the accuracy and the use of this document.