Cyber Outlook

A Different View of Info Security

January 2016 - Vol. 2 No. 1

Dear Cyber Outlook Reader,

I just made a mistake writing the date on a check, so it must be a new year, and time for a new series in Cyber Outlook.

"Drive-by" is a very negative word. First, there were "drive-by" shootings. Then, new media personalities described their old media competitors as the "drive-by" media. Now, cyber security has to deal with "drive-by" downloads.

One of the most frustrating things about drive-by downloads is that users can be trained in safe computing, follow all their training, and still be afflicted by drive-by downloads, through no fault of their own.

So, we are beginning a series which will cover research approaches to defeating drive-by downloads. As always, we will do our best to make the material practical and interesting, without requiring lots of prior background. And, of course, we continue our popular "Ask the Expert" column, and our cyber-security word puzzle.

We always welcome comments. You can contact us through the links at the end of the newsletter.

Regards,
Adam Enosh
VP, Marketing

Defending Against Drive-by Downloads, Part 1

Have you ever visited a popular news website and waited a long time for advertisements to load into your browser? Have you ever visited a popular real estate website and found that

your computer had suddenly become unresponsive? Have you ever been in the middle of a browsing session and suddenly seen an unfamiliar URL and a new page displayed, urging you to download a new browser version? In each of these cases, there may have been a drive-by download attempting to install itself on your system.

The term “drive-by download” refers to how your browser can become a tool used to infect your computer. This can happen in two ways. First, if you visit a website which is compromised, it will automatically download malicious code on your system. What is scarier is that you can be the subject of a drive-by download even if you did nothing dangerous. If you visit a website, and that website is supported by ads, then those ads are delivered to your browser by an ad syndicator. If the ad syndicator’s site is compromised, your system will be attacked, even though you did nothing unwise, and the website you visited is not itself compromised. The only defense a user has in this situation is to keep accept all software updates for your system, since drive-by downloads typically exploit defects in out-of-date software.

A drive-by download works as follows:

- Malicious code is placed on a web page.
- The web page content is downloaded to the user’s browser, either by user command or indirection.
- A vulnerability in the browser or a browser plug-in is exploited by the malicious code.
- The malicious code is executed.

This series of articles will analyze the benefits and drawbacks of various research platforms for defending against drive-by downloads. It will also suggest ways that these ideas can be incorporated into production environments.

We reviewed 14 refereed research papers promoting technical methods for defeating drive-by downloads. There are several ways to categorize defenses against drive-by downloads.

1. **What indicators do they look for to distinguish safe web pages from malignant ones?**

The papers we reviewed used a dozen different indicators that a web page was dangerous. These included the following:

- Javascript string constants, language constructs, and internal representation,
- Browser environment changes, module communications, and file download events,
- Specific HTML tags and DOM change methods used in drive-by downloads
- URL chains, and lists of URLS of malware distribution networks.

2. **What algorithms do they use for matching the indicators in suspect pages with those found in known drive-by-download pages?**

The papers we reviewed used 8 different approaches to matching indicators. These included the following:

- Support Vector Machines (machine learning),
- Cosine and Jaqard similarity,

- Pearson correlation,
- Regular expressions and deterministic finite automata,
- Custom written rules.

3. Do the approaches execute offline, in pseudo real-time, or in true real-time?

We find this approach provides the most insight into the benefits and drawbacks of the various approaches.

Offline solutions analyze potential threats by crawling web pages or analyzing network traffic, completely independently of a user working with a web browser. One benefit of an offline solution is that it can employ all the server and network resources you wish. Another benefit is that it can be proactive, searching out potential attack sites before users even become aware of them. However, one drawback of offline approaches is that they don't have the entirety of the HTML and Javascript that will be processed by the browser. Thus, they can't find certain types of problems. In addition, they need a suspect list or guidance on where to look for problems.

Pseudo real-time solutions run in a server infrastructure or web proxy. They analyze web pages as they are requested and the requests are serviced. They don't forward malicious pages to the clients who request them. There are two benefits of pseudo real-time approaches. First, the cost of performing the protection analysis can be amortized over multiple requests for a web page, since it is performed once on a server or proxy. Second, the analysis is not performed on the client, which means that there will be no incremental processing time requirement on the client. The drawback of the pseudo real-time approach is that it doesn't have all the HTML and Javascript that will be processed by the browser. Thus, it can't find certain types of problems.

A true real-time approach analyzes each page as it arrives at the client that requested it. Static methods can analyze the parts of the web page as they arrive, and dynamic methods can evaluate the final page and associated scripts as they are interpreted by the browser. The benefit of the pure real-time approach is that the analysis can work on the final version of the HTML and Javascript that will be processed by the browser. The drawback of this approach is that all of the resources expended for the analysis must be on the client. If an analysis method takes too much time, either it will reduce the user's productivity, or it will have to be abandoned.

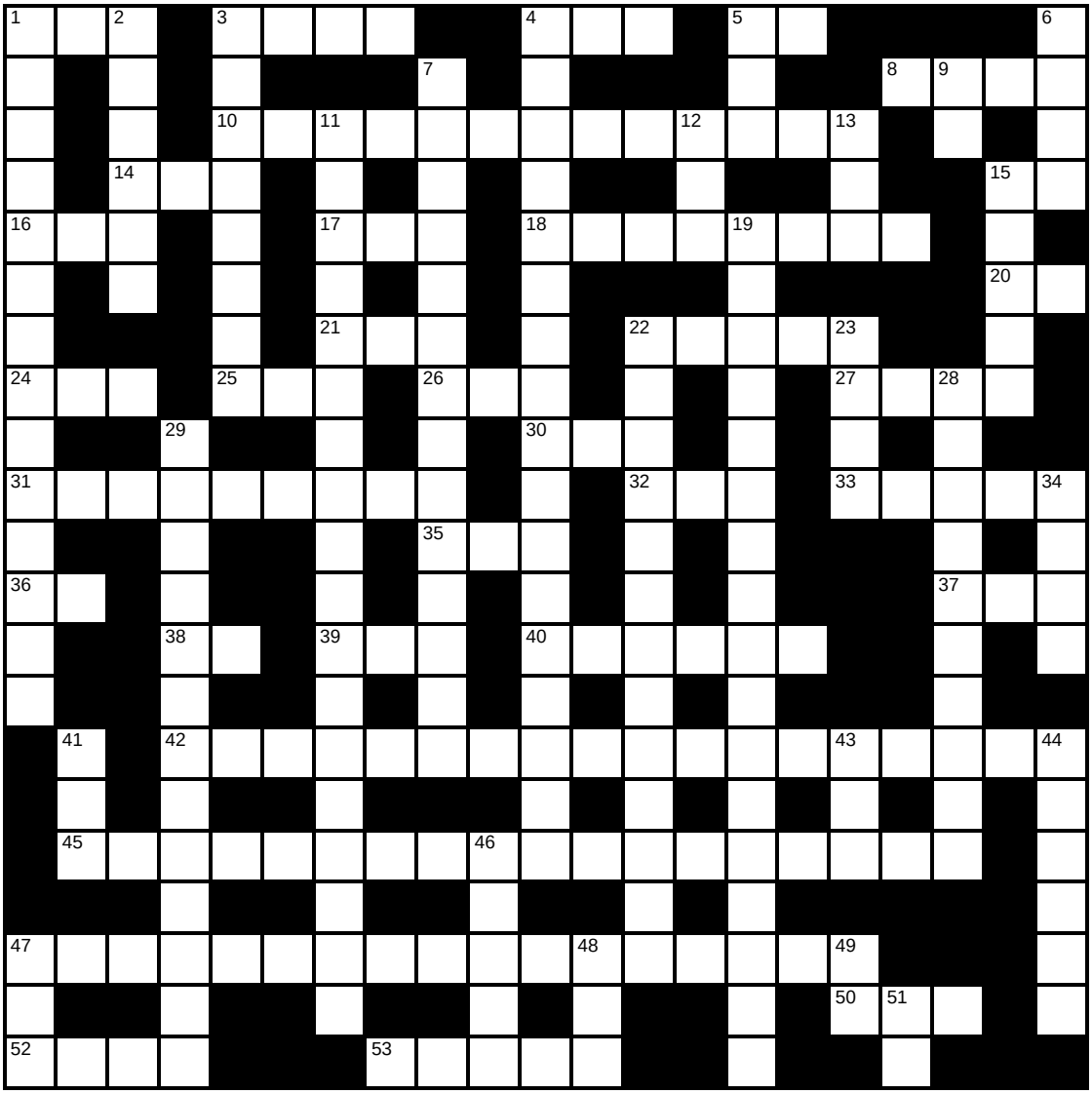
You can find the references to the papers reviewed for this article in the Resources section of our website.

In Our Next Issue

Defending Against Drive-by Downloads, Part 2: Offline Solutions
Crossword Puzzle

CISSP Word Puzzle

All of the terms in this puzzle are from topics covered by the CISSP exam.
Solutions to previous puzzles can be found on our website at
www.cybersecfirm.com/newsletter/



Across

1 TCP counter (3)

3 Microsoft answer to CORBA (4)

4 transmits files in clear (3)

5 identifying flaws in information environment (2)

8 digital signature guarantees integrity (4)

10 pointers to files (8,5)

14 assessment of adverse events (3)

15 values used to strengthen encryption (2)

16 component of Kerberos authentication (3)

17 network operation approach (3)

18 executive advocate (8)

20 configuration management (2)

21 single event potential loss (3)

22 distributed computing standard (5)

24 network layer protocol of IPX/SPX (3)

25 noise generated by appliances (3)

26 requirements soliciting bids (3)

27 high speed token passing technology (4)

30 evaluation subject (3)

31 reducing risk with additional controls (9)

32 terminated certificates (3)

33 long-term increase in electrical power (5)

35 total cost over lifetime (3)

36 real-time text-based chat (2)

37 management actions for survival (3)

38 preparation efforts for disaster (2)

39 international organization (3)

40 intelligent hub (6)

42 attack by modifying input values within URL string (9,9)

45 protecting organizational activities (10,8)

47 objects subject to seizure during a search must fall under this (5,4,8)

50 biometric type II error (3)

52 tests IP address accessible (4)

53 DoD accreditation standard (5)

Down

1 first step of accessing a system (14)

2 open source Unix (6)

3 adverse event of organizational magnitude (8)

4 failed government attempt to create cryptosystem back door (4,13)

5 virtual cluster number (3)

6 video security system (4)

7 technique for preventing exploitation (14)

9 family of hash algorithms (2)

11 highest bit value in a byte (4,11,3)

12 vulnerability assessment process (3)

13 one-time authentication (3)

15 networking storage standard (5)

19 performing many calculations simultaneously (8,9)

22 review disaster recovery checklists (9,4)

23 federal fingerprint identification system (4)

28 database transactions are resilient (10)

29 disk mirroring with duplicate controllers (4,9)

34 extension of Wiretap Act (4)

41 executive responsible for security (3)

43 electrical noise (3)

44 wire connected to the earth (6)

46 IDS on host monitoring network (5)

47 uses IDEA to encrypt Email (3)

48 smart card for U.S. government personnel (3)

49 percentage loss from an attack (2)

51 Microsoft directory service (2)

Taking Care of Business

Contact the editor of this newsletter

Change your subscription email address

Unsubscribe from this mailing list