Data-Theft Trojans & The Changing Face of the Web

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Mary Landesman is a senior security researcher with ScanSafe <http://www.scansafe.com>. Today she contributes an interesting analysis of a significant problem: data-theft Trojans and how changing patterns of Web usage are creating new avenues for harm to users.

* * *

In 2004, Russell Beale of the University of Birmingham penned an interesting article discussing the social changes taking place on the Web.<http://www.usabilitynews.com/news/article1610.asp> In his summation, Professor Beale noted, “We have split the Web atom – previously atomic units were Web pages – once you’d got them you could analyze them into text and graphics, but you generally dealt in whole pages. Now our atomic unit is much smaller – we can construct things out of fragments of pages. And this makes a second difference – consumers can look only at what they want.”

Today, consumers are looking at far more than they bargained for. Attackers are leveraging the multi-source aspect of the modern Website, inserting malicious content designed to silently foist malware onto unsuspecting visitors’ computers. And the malware being delivered is not the prank-style virus or worm of the late 1990s: most Web-delivered malware is for data theft, intended to siphon the intellectual property and capital assets of its victims.

Currently, data-theft Trojans have outpaced all other forms of malware delivered through the Web. As of May 2009, Web attacks were growing at a rate of 1% a day and were up 324% compared to May 2008. The rate of encounters with compromised Websites resulting from those attacks also increased, up 509% in May 2009 compared to May 2007. Most concerning, Web encounters with data-theft Trojans were up 4955% in May 2009 compared to May 2007, and up 1424% compared to May 2008.<http://www.scansafe.com/resources/white_papers/request_forms/whitepaper_request_form7>

Some of the key developments in the battle against data-theft Trojans are as follows:

1. **Data-theft Trojans aren’t limited to games.** Though they may carry labels such as WoWstealer, GameThief, and PSW.OnlineGames, the Trojans themselves are serious business. Data-theft Trojans silently siphon off companies’ most precious assets – the intellectual property that includes designs, inventions, specifications, and marketing plans. What may have been years in the making can be stolen in a matter of minutes. Expected returns on research and development costs can be severely diminished – or lost forever – when markets are suddenly flooded with counterfeit lookalikes or unexpected competitors.

2. **Today’s data-theft Trojans are highly configurable.** Many of today’s data-theft Trojans launch intermittent Address Resolution Protocol (ARP) poisoning attacks on compromised networks.<http://www.grc.com/nat/arp.htm> The subsequent man-in-the-middle attack intercepts targeted network traffic – sniffing, tampering with, or redirecting that traffic. The illegally obtained knowledge gleaned from the ARP poisoning can be used to further configure the data-theft Trojan to target specific intellectual property or network assets.
3. **Data-theft Trojans have a means to spread.** Commonly, today’s data-theft Trojans are facilitated by autorun worms. Though many equate the term “autorun” with removable drives only, autorun worms can spread via any discoverable drives, which includes removable, fixed and mapped drives. The autorun worm spreads by dropping a malicious autorun.inf file to the root of the drive, along with a copy of the worm. When the drive is subsequently accessed, the autorun.inf file is executed and loads the referenced copy of the worm and hence the data-theft Trojan is copied onto the new location.

But the problem isn’t just the severity of today’s malware. Criminals have leveraged all facets of the Web. From compromised Websites to poisoned search results, every interaction a user has with any Web-delivered content today carries the risk of being tainted with malware. And many of those users are our colleagues.

The attackers have an additional edge: the Web is so easy to use that consumers need know nothing about its underlying technologies. As an example, search engine optimization (SEO) is a finely honed skill in black-hat circles but it’s a term that is barely known in consumer circles. Yet black-hat SEO techniques present a significant risk to consumers, because successful manipulation results in malicious Websites given high prominence in search engine results and even enables the nefarious hijacking of innocent keywords that drive much of the Web’s advertising.<http://www.scansafe.com/resources/white_papers/request_forms/whitepaper_request_form7>

Social networking sites are also rife with criminal manipulation. <http://www.pcworld.com/businesscenter/article/155589/arm_yourself_against_social_networking_malware.html> This problem is exacerbated by a penchant for accepting any friend request in a bid to win a virtual popularity contest among one’s peers. The result of this promiscuous friending is a network is filled with scam artists and malware distributors intent on harm instead of a network of trustable friends.

In the case of Twitter, criminals don’t even need to be added to have a negative impact. In a recent attack, new accounts were dynamically created and used to repeatedly send malicious links with #trending topic as the draw. Those who subscribed to the abused trending topic were thus exposed to the scam; those who fell for it would have been infected. In recent months, Twitter has begun filtering malicious links out of its messages.<http://mashable.com/2009/08/03/twitter-malicious-links/>

In “Yes, the Web Is Changing Your Brain”,<http://www.internetevolution.com/author.asp?section_id=567&doc_id=173469> Dr. Kim Solez discusses “a new kind of human intelligence particularly suited for the digital age,” noting that it involves “an ability to identify and take advantage of potential connections, to separate information into transformable chunks, and to reassemble these chunks for new purposes.” From a security perspective, this may well be the key for safe use of the Web as well.

Network and security administrators must investigate the uses of the new generation of social-networking and instant-messaging systems on corporate systems so that we can design our appropriate use and security policies with today’s risks in mind. Readers will do well to talk to users personally to learn the extent to which corporate or institutional resources are being exposed to threats spread via the channels discussed above. Organizations will have to add new elements to security-awareness programs to help users avoid this new generation of threats.

* * *
Mary Landesman has a distinguished background in the anti-malware field. She created and contributes regularly to the ScanSafe Security Blog.

M. E. Kabay, PhD, CISSP-ISSMP specializes in security and operations management consulting services. CV online.

Copyright © 2009 Mary Landesman & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.