Yui Kee Computing Ltd.

Newsletter

July 2010

Contents

Malware is Not News

<web-link for this article>

Allan Dyer

A journalist contacted me recently. It's a long time since the heady days of LoveLetter, Code Red and Slammer when anti-virus experts were in hot demand, so it was a little excitement on a quiet Sunday afternoon. But what did the journalist want to hear about? "The new Shanghai Expo virus that arrives in an email and destroys computers."

That's a difficult question to answer, because there isn't one. Well, there was a targeted email sent to some journalists in March with a trojan PDF attachment, but that is not new, not a virus, and was not "destroying" computers (or even wiping data and programs). On the other hand, malefactors are sending out spam with malicious attachments using all sorts of news-worthy events as a hook, so maybe there was one that I had not seen, or had reported, yet. The important message is not about this particular, possibly fictional, example, but about the real threat from people using messages like this to infect your computer and use it to silently steal valuable information (your online banking password, perhaps), or use it to launch further attacks as a zombie in a botnet.

The journalist did not seem impressed by my explanation, and I don't think he quoted me. Even the mention of breaking into bank accounts failed to excite, I suppose it didn't match the "Deadly New Disease Spreading" story he had already half-written.

It would be wrong to blame the journalist alone for this, we are all complicit. The public expect their news to be, well, new, and it is so accessible that each story has only a short time to have a lasting effect. Experts know they only have a small window of opportunity to get their message across, so they trim it down to the most important essentials. In the right conditions, an essential point can become common knowledge, but it trains people to expect short, simple answers, which is bad in the long term.

We live in a highly complex, technology-rich world. How can we address the challenge of raising the general level technical understanding?

More Information

Trend Micro - Shanghai Expo Spam Carries Backdoor
Malware attack uses China World Expo guise

Microsoft Renames "Responsible Disclosure"

<web-link for this article>

In a blog post on 22 July, Microsoft unveiled its renaming of how it would like security researchers to handle flaws in its products, saying,

Today, Microsoft is announcing a shift in philosophy on how we approach the topic of vulnerability disclosure, reframing the practice of "Responsible Disclosure" to "Coordinated Vulnerability Disclosure."

The shift is interesting because Microsoft has heavily supported Responsible Disclosure since 2001 when the manager of Microsoft's Security Response Centre, Scott Culp, published an article, "It's Time to End Information Anarchy" advocating refraining from publishing details of vulnerabilities until the vendor concerned had a patch ready for release. The article is currently not locatable on Microsoft's website. In November of 2001, Microsoft was the driving force behind a proposed RFC (Request For Comment, the *de facto* standards of the internet) called "Responsible Vulnerability Disclosure Process", but it did not become a standard.

Yui Kee Chief Consultant Allan Dyer commented, "This can easily be seen as a climbdown by Microsoft. The choice of the term 'responsible' in 2001 was pure spin - those who advocated full disclosure became, by implication, 'irresponsible'. However, the continued efforts of security researchers to find and publish vulnerabilities that Microsoft had failed to find has been acknowledged by the users and now, eventually, Microsoft has decided to stop condemning them by implication."

This is unlikely to end the discussions on the best balance between secrecy and disclosure for vulnerability discoveries.

More Information

Announcing Coordinated Vulnerability Disclosure
Coordinated Vulnerability Disclosure: Bringing Balance to the Force
Microsoft to banish 'responsible' from disclosure debate
How Do We Define Responsible Disclosure?
Internet Draft: Responsible Vulnerability Disclosure Process
Full Disclosure
Responsible disclosure
'Responsible Disclosure' Draft Could Have Legal Muscle
IETF Receives Proposal: Responsible Vulnerability Disclosure Process
Full Disclosure: The Impending RFC

Security Implications of Tab Candy

<web-link for this article>

The Firefox browser developer, Mozilla, has released a test version of their new way to organise browsed pages, called "Tab Candy". The feature allows users to organise browser tabs into related groups in two dimensions, and switch between them easily. However, two proposed features have security implications:

A helper extension can start suggesting other pages related to a group. Who controls that? Could be a very useful propaganda tool (start a group on evolution, it fills up with "intelligent design" pages, or Tienanmen and it fills up with pro-government analyses), or marketing (search for cameras, the "best deals" page you see is the one that gives the biggest kickback to the extension developer), which, inevitably, leads to tab spam (every group you start gets a "buy viagra" page).

Sharing. You can zoom out and see your friends' tab groups. You'll have to be able to control who sees what, but it will be a pain to remember to do it all the time, and how will organisations control what "friends" of their employees see? It's not just in the workplace, your R&D staff might casually browse something related to your top secret project while at home or in a coffee shop. At the moment, that's a risk a spy would have to be lucky to exploit, candy could make it a lot easier and more reliable.

Tab Candy may or may not be a leap forward in browsing convenience, but the security implications should be considered at an early stage.

More Information

[An introduction to Firefox's Tab Candy (video)]
[Mozilla tames Firefox tab monster with Candy]
[Firefox/Projects/TabCandy/FAQ]

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/