Custom Code for Targeted Attacks

Peter Silva, 2011-14-06

Botnets? Old school. Spam? So yesterday. Phishing? Don't even bother…well, on second thought. Spaghetti hacking like spaghetti marketing, toss it and see what sticks, is giving way to specific development of code (or stealing other code) to breach a particular entity. In the past few weeks, giants like Sony, Google, Citibank, Lockheed and others have fallen victim to serious intrusions. The latest to be added to that list: The IMF – International Monetary Fund. IMF is an international, intergovernmental organization which oversees the global financial system. First created to help stabilize the global economic system, they oversee exchange rates and functions to improve the economies of the member countries, which are primarily the 187 members of the UN.

In this latest intrusion, it has been reported that this might have been the result of 'spear phishing,' getting someone to click a malicious but valid looking link to install malware. The malware however was apparently developed specifically for this attack. There was also a good amount of exploration prior to the attempt – call it spying. So once again, while similar to other breaches where unsuspecting human involvement helped trigger the break, this one seems to be using purpose built malware. As with any of these high-profile attacks, the techniques used to gain unauthorized access are slow to be divulged but insiders have said it was a significant breach with emails and other documents taken in this heist. While a good portion of the recent attacks are digging for personal information, this certainly looks more like government espionage looking for sensitive information pertaining to nations. Without directly pointing, many are fingering groups backed by foreign governments in this latest encroachment.

A year (and longer) ago, most of these types of breaches would be kept under wraps for a while until someone leaked it. There was a hesitation to report it due to the media coverage and public scrutiny. Now that many of these attacks are targeting large international organizations with very sophisticated methods there seems to be a little more openness in exposing the invasion. Hopefully this can lead to more cooperation amongst many different groups/organizations/governments to help defend against these. Exposing the exposure also informs the general public of the potential dangers even though it might not be happening to them directly. If an article, blog or other story helps folks be a little more cautious with whatever they are doing online, even preventing someone from simply clicking an email/social media/IM/txt link, then hopefully less people will fall victim. Since we have Web 2.0 and Infrastructure 2.0, it might be time to adopt Hacking 2.0, except for the fact that Noah Schiffman talks about misuse and all the two-dot-oh-ness, particularly Hacking 2.0 in an article 3 years ago. He mentions, '*Security is a process'* and I certainly agree. Plus I love, '*If the term Hacking 2.0 is adopted, or even suggested, by anyone, their rights to free speech should be revoked*.' So how about Intrusion 2.0?

ps

Resources:

- Inside The Terrifying IMF Hack: Who The Hackers Were And What They Took
- IMF Hacked; No End in Sight to Security Horror Shows
- Join the Club: International Monetary Fund Gets Hacked
- IMF State-Backed Cyber-Attack Follows Hacks of Atomic Lab, G-20
- IMF cyber attack boosts calls for global action
- I.M.F. Reports Cyberattack Led to 'Very Major Breach'
- IMF Network Hit By Sophisticated Cyberattack
- Where Do You Wear Your Malware?
- The Big Attacks are Back…Not That They Ever Stopped
- Technology Can Only Do So Much
- 3 Billion Malware Attacks and Counting
- Unplug Everything!
- And The Hits Keep Coming
- Security Phreak: Web 2.0, Security 2.0 and Hacking 2.0
- F5 Security Solutions

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com