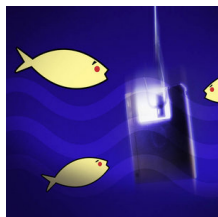


12 July 2008

By: George Craciun, Security News Editor



Sysda is the latest Trojan discovered by FaceTime Security Labs
Silicon Republic

[FaceTime Warns about Latest Sysda Phishing Threat](#)

The most recently discovered phish

According to Chris Mannon, senior threat researcher with FaceTime Security Labs, the latest phishing security threat has been identified as Sysda. Although at this point only Chinese users should be worried about it, FaceTime expects it to jump over to the US, and other parts of the world, in the near future. Sysda is a Trojan that attempts to steal the passwords used by people when logging into various Chinese web pages. Chris Mannon comments on the FaceTime spyware [blog](#): "This is not really a threat to most businesses in the US, but judging from the malware trend coming from China and spreading to the rest of the world, I'd say its only a matter of time before we start seeing the same method of theft. The name of this new threat has been named [sic] Sysda. All it really needs is to hook into iexplore.exe to steal your user credentials." After infecting a user's machine, the Trojan simply goes dormant until certain user actions trigger it, such as browsing through a certain web page. Usually, these are pages that require you to insert your username and password. Sysda grabs this information and posts it on a remote site to which the hacker has access to. "Whether this is simply a new way to phish for information, or something more sinister along the lines of fraud is still unclear at this point. I'll let you know what I found out," says Chris Mannon, whose job with FaceTime Security Labs is to keep track of malware and virus trends, investigate the most recent scam and hijack attempts, as well as to become familiar with the latest methods employed by hackers and attackers. FaceTime Security Labs specializes in providing security solutions meant to protect applications such as instant messaging programs, Skype, web conference programs, and P2P file sharing. All of these software programs are known as greynet applications.