Informational Alert

Alert No: AIA170302 **Date: 02-Mar-17 11:17 AM**

SWIFT Application Access & Cloudfare Vulnerability & Dridex Banking Trojan

SWIFT Application Access	● SWIFT is being used by various global and Sri Lankan financial institutes for its financial services. ● While not being a direct vulnerability, we have information on an incident where a general user has requested access to one of Financial Institute SWIFT network and the request has been transferred to the Institute administrator. ● Even though the request has been declined and there is no direct vulnerability in the approval process, It is best to make proper attention to emails sent out by SWIFT network and before proceeding, every request should be properly verified. ● Inform all SWIFT administrators to make necessary attention to the SWIFT.com alerts and approval requests before proceeding.
Cloudfare Vulnerability	● Cloudfare is a major DOS mitigation service which sits in front of your website/application and manages traffic. ● A major vulnerability has been found (named cloudbleed) in the cloudfare service where your SSL encrypted data is being cached with cloudfare and search engines like google / Bing ● While the vulnerability has already been patched, previously leaked data such as session keys, passwords, cookies can still be available in loose. ● Members are advised to inform the IT staff or the hosting providers on the incident and take necessary actions. ● Only sites hosted behind www.cloudflare.com are affected. (Please note your Hosting provider may have host your site behind this service) ● For technical information needed on the matter, please contact FINCSIRT.
Dridex Banking Trojan	● The infamous banking Trojan Dridex has been armed with the newest technique of windows attacks called "AtomBombing" ● **AtomBombing** is a newer type of attack, which can be used in all version of Microsoft windows including windows 10. ● With the help of these new capabilities, Dridex is targeting banking information on user PCs. ● It is recommended to be on alert at proper patches and virus guard definitions in the coming days.
Additional Information	● https://bugs.chromium.org/p/project-zero/issues/detail?id=1139 ● https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/ ● http://www.darkreading.com/attacks-breaches/new-version-of-dridex-banking-trojan-uses-atombombing-to-infect-systems/d/d-id/1328299
Disclaimer	The information provided herein is on "as is" basis, without warranty of any kind.

Financial Sector Computer Security Incident Response Team, Sri Lanka
Hotline: + 94 112039777
Report incident to incident@fincsirt.lk