UGANDA NATIONAL COMPUTER EMERGENCY RESPONSE TEAM (CERT.UG)

07/09/20

INFORMATION SECURITY VULNERABILITY ALERT

Target: Financial Sector (Including; Banking, Fintech, Microfinance, Investment Firms, Insurance Companies, Mobile Money, Money Transfer, Money Exchange e.t.c)

Risk Rating: **HIGH** - due to the attack techniques used.

Risk Assessment: A North Korean group known as BuggleBoys is targeting financial sectors across the globe using a Remote Access Tool (RAT) malware for exploiting weak network and system defenses. The goal is to plant backdoors in financial institutions networks to steal credentials, capture screen activity and log keystrokes.

Impact: The malware is used as a reconnaissance tool and has the ability to steal credentials for critical systems as well as maintain the attacker's presence on the network through a backdoor. This can potentially allow the attacker to perform multiple attacks on a target institution with a primary objective of stealing enormous amounts of money. The group behind the financial sector targeted attacks in purely financially motivated.

Source reference:

https://us-cert.cisa.gov/ncas/analysis-reports/ar20-239a
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-23b
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-239c

Mitigation: To prevent and/or mitigate the impact of compromise;

- Strengthen e-mail security and undertake periodic user awareness and training on the dangers of email phishing
- Strong network security controls should be implemented and existing ones should be enhanced.
- Endpoint security should be updated continuously. In addition, monitor network hosts for vulnerabilities and insecure protocols/services
- Network segmentation should be adopted to isolate critical network segments.

- Threat detection tools should be implemented to identify and stop cyber-attacks
- Frequently keep operating systems updated and install patches and security updates. For example, you shouldn't be running any version below Windows 10 if you operate a windows environment
- Use the principle of least privileges and restrict access to network resources using authentication and authorization mechanisms

//END

Uganda National Computer Emergency Response Team
Plot 7A, Rotary Avenue (Former Lugogo Bypass)
Twitter: @CERT.UG | Facebook: Cert1.ug
info@cert.ug | www.cert.ug