For further information
Hilary King, Global PR Manager
Dimension Data plc
Tel : +27 11 575 6728
Cell: +27 82 414 9623
Hilary.king@dimensiondata.com

NTT GROUP ANNOUNCES AVAILABILITY OF ANNUAL GLOBAL THREAT INTELLIGENCE REPORT

2016 Report includes insights on the threat landscape partners including Lockheed Martin, Wapack Labs, Recorded Future and the Center for Internet Security

London, United Kingdom – 19 April 2016 – Dimension Data, the USD 7.5 billion global ICT solutions and services provider, and an NTT Group company, is pleased to announce the release of the annual NTT 2016 Global Threat Intelligence Report (GTIR). NTT Group has expanded its view of the threat landscape to include findings from key partners – Lockheed Martin, Wapack Labs, Recorded Future and the Center for Internet Security – to analyse the attacks, threats and trends from the previous year. The 2016 GTIR is the most comprehensive report to date, drawing information from 24 security operations centres, seven R&D centres, 3.5 trillion logs, 6.2 billion attacks and nearly 8,000 security clients across six continents.

The 2016 GTIR gives security personnel and decision makers the information they need to enable their organisations to disrupt attacks. Practical application of a comprehensive, integrated solution and strategy will not only enable efficiency and effectiveness, but also support the security life cycle of the entire organisation.

To achieve this goal, this year's GTIR identifies controls (based on the Center for Internet Security's Critical Security Controls) that can be effective at each stage of the Lockheed Martin Cyber Kill Chain®. Organisations that have implemented controls at each stage of the Kill Chain have an increased ability to disrupt attacks. The report also includes a breakdown of a case study in a "Practical Application of Security Controls to the Cyber Kill Chain."

Key findings from the report include:

Incident Response and Case Studies

- **Trend data from incident response activities illustrates on average only 23% of organisations are capable of responding effectively to a cyber incident.** 77% have no capability to respond to critical incidents, and often purchase support services after an incident has occurred.
- **Activity related to the Reconnaissance phase of the Lockheed Martin Cyber Kill Chain (CKC) accounted for nearly 89% of all log volume.** These logs accounted for approximately 35% of escalated attack activity, making Reconnaissance the largest single element in the CKC.

- **Spear phishing attacks accounted for approximately 17% of incident response activities supported in 2015**. In many cases, the attacks targeted executives and finance personnel with the intent of tricking them into paying fraudulent invoices.

Geographic and Vertical Market Trends

- **The retail sector experienced the most attacks per client.** Retail was followed by the hospitality, leisure and entertainment sector, then insurance, government and manufacturing. While the finance sector showed the highest *volume* of attacks overall, on a per-client basis, retail clients experienced 2.7 times the number of attacks as finance.
- **NTT Group observed an 18% rise in malware detected for every industry other than education.** NTT clients from the education sector tended to focus less on the more volatile student and guest networks, but malware for almost every other sector increased.

Vulnerabilities, Attacks and Exploitation

- **Nearly 21% of vulnerabilities detected in client networks were more than three years** old. Results included vulnerabilities from as far back as 1999, making them more than 16 years old. This is for vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 4.0 or higher.
- **DoS/DDoS attack volume fell 39% from levels observed in 2014.** Implementation of better mitigation tools, along with fewer attacks, combined for a drop in detections of denial of service (DoS) and distributed denial of service (DDoS) activities. But, extortion based on the victim's paying to avoid or stop DDoS attacks became more prevalent.
- **All of the top 10 vulnerabilities targeted by exploit kits during 2015 are related to Adobe Flash.** In 2013, the top 10 vulnerabilities targeted by exploit kits included one Flash and eight Java vulnerabilities. That has changed as new Java vulnerabilities have dropped steadily since 2013. The number of publicized Flash vulnerabilities jumped by almost 312% over 2014 levels.

This year's GTIR provides actionable intelligence, guidance about what attackers are doing, and comprehensive security controls designed to disrupt attacks. Controls recommended in this report will contribute to an organization's survivability and resiliency in the face of an attack.

To download the full report, please visit: annual NTT 2016 Global Threat Intelligence Report

About Dimension Data

Dimension Data harnesses the transformative power of technology to help organisations achieve great things in the digital era. As a member of the NTT Group, we focus on digital infrastructure, hybrid cloud, workspaces for tomorrow, cybersecurity, and network as the platform. With a turnover of USD 7.5 billion and offices in 58 countries, we deliver services wherever our clients are, at every stage of their technology journey. Accelerate your ambition. Go to dimensiondata.com