UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00252

LAPSUS$ GANG MOVES IN ON NVIDIA, SAMSUNG & UBISOFT

DATE ISSUED: 15th March 2022

IMPACT	LOW	[✓ MEDIUM]	HIGH
EASE OF EXPLOIT	[✓ HARD]	MEDIUM	EASY

OVERVIEW

In the last two weeks, known cybercrime gang Lapsus$ once well known for ransomware has hit three major tech giants but instead of infecting their systems with malware, it seems the group is more interested in stealing sensitive company data, announcing their conquests on their telegram channel.

BREAKDOWN

The group appears to have stolen Samsung source code and in a “supply-chain-attack” style move, also stealing from one of their suppliers Qualcomm. The data posted by the group appears to be related the TrustZone environment, responsible for storing especially sensitive data such as biometric information. This is deeply concerning, as if Samsung has lost control of its signing keys, there may be no way to securely update devices. Samsung claimed in a press release that it appeared that no customer or employee data was leaked. This is contrary to the prior attack on NVIDIA where all employee login credential hashes were leaked, as well as the theft of code signing certificates. Attackers are now applying these stolen certificates to malware to make it appear as legitimate. While there have been no leaks of sensitive data relating to the Ubisoft compromise as yet, there was some significant disruption to their services and games.

REMEDIATION STEPS

- These attacks highlight the importance of implementing secure practices around data storage, and highlights that attackers are no longer only looking for confidential information on individuals.
- If you are involved in a data breach, be sure to understand your obligations under the NZ Privacy Act 2020.

REFERENCES & RESOURCES

WCCFTech	https://wccftech.com/samsung-data-compromised-190gb-info-stolen/
Secureworld	https://www.secureworld.io/industry-news/nvidia-source-code-breach
Cloud7	https://cloud7.news/security/lapsus-group-has-hacked-ubisoft-as-well/
Threatpost	https://threatpost.com/samsung-lapsus-ransomware-source-code/178791/
Bleeping Computer	https://www.bleepingcomputer.com/tag/lapsus/