SkidSec Hacker Group Announces Plans to Spread North Korean Propaganda Through Hacked Printers in South Korea

medium.com/@criminalip/skidsec-hacker-group-announces-plans-to-spread-north-korean-propaganda-through-hacked-printers-in-fdd314178dc4

Criminal IP December 3, 2023

On November 29, SkidSec hacker group announced its intentions on Telegram to attack exposed printers in South Korea to spread North Korean propaganda. North Korean propaganda refers to leaflets and other materials designed to promote North Korean ideas and criticize the South. **According to the sudden announcement of the attack, it appears that the scheme is to attack all vulnerable printers in South Korea this upcoming weekend, printing and spreading North Korean propaganda.**

Example of a North Korean propaganda posterSource: on Vox

How SkidSec Hacker Group Plans to Attack Printers in South Korea to Spread North Korean Propaganda

The attack method announced on Telegram is to use the network and system security intelligence gathering service ‘Censys’ to locate and connect to exposed Internet Printing Protocol (IPP) HP printers in South Korea and print North Korean propaganda posters.

How to Hack Printers in South Korea to Spread North Korean Propaganda

1. Connect to Censys.
2. In the search bar, paste ((services.software.product=JetDirect) and services.service_name=IPP) and location.country='South Korea'.
3. Use the open IPP (Internet Printing Protocol) to print North Korean propaganda posters.

Searching on "Censys" with their disclosed methods reveals thousands of printers in South Korea connected to the internet. However, it is expected to be difficult to attack printers that require authentication. Printers without an authentication process are more susceptible to falling victim to unwillingly printing North Korean propaganda posters.

The hacker group even said it would pay out Monero cryptocurrency to the person who attacked and printed the most North Korean propaganda posters over the weekend. South Korean companies and government institutions must act quickly to prevent North Korean propaganda posters from being unexpectedly printed this upcoming weekend.

Find Printers in South Korea Exposed on the Internet, Targeted by SkidSec Hacker Group

In Criminal IP Asset Search, you can enter a query that resembles the attack methods of SkidSec hacker group to find exposed printers in South Korea.

> Search Query: HP port: 631 country: KR

Searching for exposed printers in South Korea targeted by SkidSec hacker group in Criminal IP Asset Search

Search results show more than 2,000 exposed printers vulnerable as attack targets.

To further identify the attack targets, you can check the AS Name statistics of the servers with exposed printers.

AS Name statistics of exposed printer servers searched in Criminal IP Element Analysis

Checking the same query on Element Analysis provides AS Name statistics, showing that South Korean telecommunications company KT (Korea Telecom) has the most exposed devices. This is due to households and corporate institutions in South Korea conventionally using KT IP addresses.

However, upon closer examination of the AS Name statistics, it reveals the inclusion of universities and businesses.

How to Prevent Vulnerabilities in Exposed Printers

Initially, the SkidSec hacker group's announcement of printing North Korean propaganda posters may seem not very threatening, let alone menacing. However, exposed printer devices are also prone to leaking other important information in internal systems and servers. Therefore, organizations operating such exposed printers should quickly inspect their attack surface and take measures to prevent the printers from further exposure.

Removing threats of an exposed attack surface is fairly simple. This can be done by closing open ports or modifying weak authentication settings to block external access.

This report is based on data from Criminal IP, a Cyber Threat Intelligence search engine.

Create a to access the search results cited in the report and search for more extensive threat Intelligence.

Source: Criminal IP (https://www.criminalip.io)