Severity

High

Analysis Summary

DPRK-nexus is a threat actor group that compromises its victims by sending spear-phishing emails containing Korean-based malicious documents with different lures. The lures utilized in their recent efforts are quite diverse. These lures varied from the impersonation of the Korea Internet Information Center (KRNIC) to the impersonation of numerous South Korean Internet Security companies or Cryptocurrency companies. This effort appears to have a broad goal of stealing data from South Korean individuals. The victims of the majority of the infections were users who had an email address registered on naver dot com, a South Korean web platform that offers free email boxes, news, and search engine capabilities.

Impact

- Information Theft
- Exposure of Sensitive Data

Indicators of Compromise

Filename

- 유사수신고소장-1[.]docx 202203_BTC_ETH추가계정정보[.]docx

MD5

- 277de31debc234414aa16252b1ae5106
- ce00749c908de017010055a83ac0654f
- 5144a35d9f120339b8374177714e199e
- bb9ee3a6504fbf6a5486af04dbbb5da5
- 2677f9871cb340750e582cb677d40e81
- d47f7fcbe46369c70147a214c8189f8a
- 9775ef6514916977d73e39a6b09029bc
- a2aca7b66f678b85fc7b4015af21c5ee
- 1a536709554860fcc2c147374556205d

SHA-256

- ab01143169a142b246441b778b7865532ec88fd37e19f690efd00ee5302f0683
- f265a04e08a79ea6a4eeacd8294b3af2e1a08ae131018dd1ca195ae900437767
- 6ed3447bb9fcb5abfe78a628ebcd1a0987c75b18eac5673a3a90a4bbe745b527
- 96754f46e1ce19a337c3a4368e63ad1135405b383f3d3bd77beefe20926cf89d
- a7c17e5fa55bcc60d4cff64dd37d0a1f0cc93f4f44b3cebd5633ca5af413e5cc
- dfb4270fb6dc92fdfd9903b4b12bf67897e86a626925f76e4336af60c14683be
- a7976205ce8a0e1859df40eb6479fe90cd479644862cdcc8ad99082be0f1d5a1
- d2b32b233489eb120c50d7f862e2d20b89c8bb89e595086f85728e69668533e0
- ae7275988753fffb29bdb254babdf46773daf935b2721006fe66a1747af3d1d4

SHA-1

- 6eaca4e57c78af7fccd5799593cc0b770a984040
- d12a92c4b41349ca76d0a44c2fd50cb1fd0b1f35
- ca0051815ceae216e467e25d7a6189e3b9a114cf
- b0f2fb3744c84634b30620910943e7d3dfe8d99c
- c5ae757463b2015ef2d472fa26aec0f6aac1fa3f

- 22fdd547cca436f15d48b15cf988f5785ba49fd8
- e6c1379789291c24b7bb52ad402f1358af283c96
- 33e3019cb515586b031e513c1305287193973dd9
- bb3a0dc01309162971ad6a11c5cb159fe93fedee

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.
- Always be suspicious about emails sent by unknown senders.
- Never click on the links/attachments sent by unknown senders