A GUIDE TO REPORTED ENCRYPTION PRACTICES AND CUSTOM CIPHER DEVELOPMENT ATTRIBUTED TO NORTH KOREA

Purpose: Provide an open-source, high-level overview of what reputable research has reported about encryption practices attributed to the Democratic People's Republic of Korea (DPRK), including the use of standard algorithms, patterns in custom or modified cryptography within malware, and considerations around how nation-states may approach “custom cipher suites.” This is an analytical summary for policy, OSINT, and security research audiences and avoids operational instructions.

EXECUTIVE SUMMARY

- DPRK-attributed actors generally rely on widely available, industry-standard cryptographic primitives (e.g., AES, RSA, SHA-2) and public implementations (e.g., OpenSSL), similar to other nation-state operators.
- In offensive operations (malware/implants), researchers frequently observe bespoke protocol wrappers, XOR-based obfuscation, and modified or simplified crypto routines rather than truly novel, peer-reviewed cryptographic primitives.
- Public-facing DPRK infrastructure and services observed on the open internet commonly negotiate mainstream TLS cipher suites; the isolated domestic network (Kwangmyong) is poorly documented, with limited reliable technical detail.
- When DPRK-linked toolchains appear to “invent” crypto, they typically create custom application-layer protocols or misuse standard crypto, introducing detectable artifacts defenders can leverage.
- Open-source reports from vendors and research groups (e.g., Kaspersky, ESET, Google TAG, Mandiant, Recorded Future, UN Panel of Experts) underpin most public knowledge; granular details vary by campaign and are often incomplete.

BACKGROUND: WHAT “CIPHER SUITES” MEAN IN PRACTICE

In modern security, a cipher suite often refers to a negotiated set of algorithms and parameters used by a protocol like TLS (key exchange, bulk cipher, MAC/AEAD, PRF). Outside TLS, the term is used informally to describe any bundle of cryptographic choices in a system or custom protocol (e.g., key exchange + symmetric encryption + integrity). Nation-state operators rarely design *new primitives*; instead, they select from existing algorithms and may craft custom wire protocols or misuse implementations to meet operational constraints.

REPORTED USE OF STANDARD CRYPTOGRAPHY

- **Public Websites and Services:** When DPRK-linked domains or infrastructure appear on the public internet, passive observations typically show standard TLS stacks using common cipher suites of the era (e.g., ECDHE_RSA with AES-GCM). Specifics shift over time as servers, libraries, and configs are updated.
- **Red Star OS:** Community analyses of certain versions of Red Star OS (the DPRK Linux derivative) have documented conventional cryptographic libraries bundled with the OS and additional watermarking/monitoring features. The cryptography used for system integrity and file watermarking appears standard in primitives but customized in policy and application. Data points are version- and build-specific and not fully comprehensive.
- **Domestic Intranet (Kwangmyong):** Very limited technical detail is publicly confirmed. Most accounts focus on network isolation rather than cryptographic innovation. Assertions about unique national cipher suites for domestic services lack strong open-source corroboration.

CUSTOM OR MODIFIED CRYPTO IN OFFENSIVE OPERATIONS

In malware and C2 frameworks attributed to DPRK-linked groups, analysts frequently note:

- **Obfuscation Layers:** Simple XOR, rolling XOR, or substitution to conceal strings, configs, and network beacons before applying standard cryptography (or in lieu of it).
- **Non-Standard Protocol Wrappers:** Custom framing and message structures that may mimic HTTP/TLS or use covert channels in expected traffic. Sometimes these include hardcoded keys or simplistic key schedules.
- **Standard Primitives, Custom Integration:** AES (CBC/CTR/GCM), RSA, and SHA-2 are commonly found, often with non-ideal choices (e.g., static IVs, ECB/CBC without integrity, homegrown padding) that create signatures for detection.
- **Implementation Bugs:** Reuse of keys, predictable PRNGs, improper padding, or lack of authenticated encryption—issues seen across many threat actors, not uniquely DPRK.

REPRESENTATIVE CAMPAIGNS AND REPORTED CRYPTO TRAITS

Actor/Campaign (attribution as reported)	Crypto/Protocol Traits Noted in OSINT	Analyst Takeaway
Lazarus Group (umbrella term)	Use of AES/RSA in payload protection and C2; custom network protocols; string/config obfuscation; occasional misuse of modes or padding.	Relies on standard primitives with custom wrappers; implementation quirks can aid detection.
Andariel / Bluenoroff / BeagleBoyz	Banking and financial-intrusion malware often include encrypted configs, packed loaders; observed AES/RC4/XOR blends.	Operational focus drives pragmatic crypto—data hiding and C2 secrecy over cryptographic novelty.
WannaCry lineage (attribution widely discussed)	Hybrid cryptography typical of ransomware families (RSA+AES), with post-exploitation tooling.	No novel primitive; leverage common ransomware crypto patterns.

HOW NATION-STATES TYPICALLY “DEVELOP” CIPHER SUITES

- **Selection over Invention:** Agencies commonly select vetted primitives (AES, ChaCha20, Curve25519, SHA-2/3) and compose them with operational constraints (performance, portability, stealth).
- **Library Reuse:** OpenSSL, mbedTLS, BoringSSL, libsodium, or platform crypto APIs are typical bases, sometimes *statically linked* and stripped for OPSEC.
- **Customization Points:** Unique message framing, key derivation tweaks, custom handshakes, and domain fronting/CDN mimicry rather than designing new ciphers from scratch.
- **Testing and OPSEC:** Closed internal testing, key management practices, and fallback behavior to survive degraded environments; not publicly documented.
- **Risk Tradeoffs:** Customization can introduce bugs that undermine security and create distinctive fingerprints for defenders.

WHY “HOMEGROWN” CRYPTO APPEARS

- **Stealth and Anti-Analysis:** Evade signature-based detection and frustrate quick static analysis.
- **Supply Constraints:** Use portable, dependency-minimal code that functions in restricted environments.
- **Attribution Management:** Novel protocol designs can complicate rapid clustering by defenders, at least initially.

DEFENDER-FOCUSED SIGNALS (NON-OPERATIONAL)

- **Protocol Oddities:** Traffic that superficially resembles TLS/HTTP but fails strict parsing; unusual cipher suite negotiation patterns; fixed client hellos; or deterministic, non-random fields.
- **Crypto Misuse Indicators:** Repeated IVs/nonces, hardcoded keys, ECB/CBC without integrity, or rolling XOR stages prior to decryption.

- **Artifact Reuse:** Consistent KDF mistakes, padding bugs, or string obfuscation routines reappearing across families.
- **Build/Toolchain Clues:** Static OpenSSL symbols, partial mbedTLS artifacts, or recognizable PRNG usage.

LIMITATIONS AND UNCERTAINTIES

- Open-source visibility is partial and campaign-specific; details can change rapidly.
- Attribution is probabilistic and based on multiple lines of evidence; cryptographic traits alone are insufficient for attribution.
- Claims about fully novel, national cipher suites for domestic networks lack strong, public, technical corroboration.

ETHICAL AND LEGAL CONSIDERATIONS

- This guide avoids providing operational instructions, code, or step-by-step designs for cryptosystems.
- Researchers should comply with applicable laws, sanctions, and institutional review requirements when handling DPRK-related data.
- Use vetted, responsible-disclosure practices when encountering active malicious infrastructure.

KEY TAKEAWAYS

- DPRK-linked operations appear to prioritize practical, accessible cryptography and protocol customization over cryptographic invention.
- Misconfigurations and custom wrappers often create defender-detectable artifacts.
- Robust conclusions require correlation across malware analysis, infrastructure, timelines, and independent sources.

SELECTED OPEN-SOURCE REPORTING REFERENCES (NON-EXHAUSTIVE)

- Vendor and research reports from Kaspersky, ESET, Mandiant/Google Mandiant, CrowdStrike, Recorded Future, Trellix, and Google TAG.
- UN Panel of Experts reports on DPRK cyber operations and sanctions evasion (methodological context, high level).
- Academic and conference papers analyzing DPRK-attributed malware families and toolchains.

APPENDIX: GLOSSARY

- **Cipher Suite:** A defined combination of algorithms for key exchange, encryption, and message authentication within a protocol such as TLS.
- **Primitive:** A fundamental algorithm (e.g., block cipher, hash function) used to build higher-level protocols.
- **Obfuscation:** Techniques that hide intent or data structure without providing cryptographic security.
- **Authenticated Encryption (AEAD):** Encryption that simultaneously assures confidentiality and integrity (e.g., AES-GCM, ChaCha20-Poly1305).

David Keith Jr "mrdj" ✓