INFORMATION SYSTEMS SECURITY ASSESSMENT

OF

North Korean People's Army
N. Korea, Secret Location

PREPARED BY:
William Peterson

Traken Analytics, LLC
Tempe AZ, USA 85224

Executive Summary

For this assessment, the North Koreans People's Army has employed Traken Analytics, LLC to complete an assessment of the security stance of the organization. Traken Analytics is a company concentrated around information security and the protection of assets. The North Korean People's Army is an organization under the rein of the Supreme Leader Kim Junk-Un. The Supreme Leader has employed Traken Analytics, LLC to perform an assessment to be completed within the guidelines of the NSA's IEM & IAM Methodologies. This assessment and finding will be thoroughly documented and reported in the following pages. At the end of the report you will find all the findings and recommendations to improve the overall security of the North Korean People's Army.

Table of Contents

THE INFORMATION CONTAINED IN THIS REPORT WAS DERIVED FROM PROPRIETARY DATA PROVIDED BY THE NORTH KOREAN PEOPLES ARMY ASSESSED BY TRAKEN ANALYTICS, LLC

1. Introduction

For this assessment, the North Koreans People's Army has employed Traken Analytics, LLC to complete an assessment of the security stance of the organization. Traken Analytics is a company concentrated around information security and the protection of assets. The North Korean People's Army is an organization under the rein of the Supreme Leader Kim Junk-Un. The Supreme Leader has employed Traken Analytics, LLC to perform an assessment to be completed within the guidelines of the NSA's IEM & IAM Methodologies. This assessment and finding will be thoroughly documented and reported in the following pages. At the end of the report you will find all the findings and recommendations to improve the overall security of the North Korean People's Army.

This assessment was performed on location in a secret location in North Korea and was performed with the guidance of the Supreme Leader and the methodologies of the IAM and IEM of the United States NSA. The assessment was performed to help North Korea secretly spy on the rest of the world without being hacked themselves. The Supreme Leader is adamant about being the most secure and locked down country in the world without any regard of others.

We would like to notice The Supreme Leader Kim Junk-Un and General Lee U for their superb preparation for the arrival of our team and outstanding accommodations for our stay in North Korea. We have never been treated to such a nice concreate floor and perfect viewing of the assassinations square before. It was a great pleasure to hear their works throughout the night and into the early morning.

1.1 Important Points-Of-Contact

Daniel Sanchez, 480-555-1234, d.sanchez.dsjobs.com
Lee U, 77+655-555-6661, Commanding_Officer@nkorarmy.com
Will Peterson, 480-555-4509, wilpete1@uat.edu

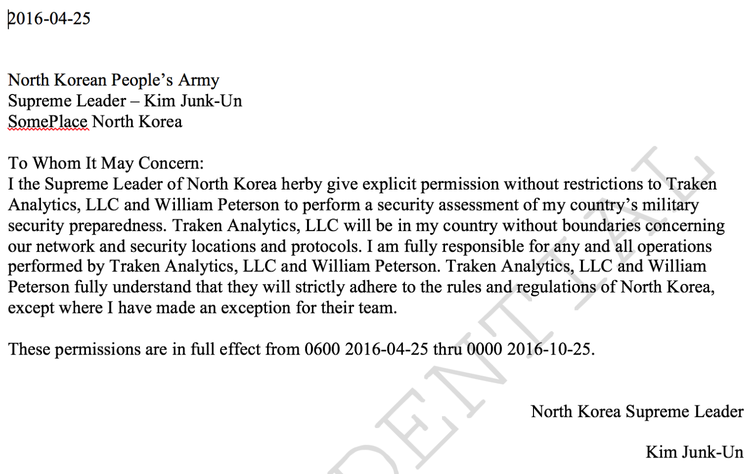
1.2 Coordination Agreement

Traken Analytics, LLC will be conducting a complete security assessment of the North Korean People's Army at the request of the Supreme Leader of North Korea. NKPA has agreed to supply DS Inc. with any and all changes in documentation during or after the beginning of the assessment.

1.3 Rules of Engagement

1- All systems used to perform this assessment will become property of the North Korean People's Army at the conclusion of the assessment. This is built into the initial quote and protocols for the protection of the data. This will protect both involved parties from the possibility of leaked data.
2- Interviews will be conducted at the interviewee's section in the role of their position.
3- Kali 2.0 and all associated tools will be the only authorized operating system used during this assessment.
4- For any questions please refer to the P.O.C. in section 1.

1.4 Letter of Authorization



2016-04-25

North Korean People's Army
Supreme Leader – Kim Junk-Un
SomePlace North Korea

To Whom It May Concern:
I the Supreme Leader of North Korea herby give explicit permission without restrictions to Traken Analytics, LLC and William Peterson to perform a security assessment of my country's military security preparedness. Traken Analytics, LLC will be in my country without boundaries concerning our network and security locations and protocols. I am fully responsible for any and all operations performed by Traken Analytics, LLC and William Peterson. Traken Analytics, LLC and William Peterson fully understand that they will strictly adhere to the rules and regulations of North Korea, except where I have made an exception for their team.

These permissions are in full effect from 0600 2016-04-25 thru 0000 2016-10-25.

North Korea Supreme Leader

Kim Junk-Un

Figure 1 Letter of Authorization

2. Methodology Overview

Daniel Sanchez incorporated will be conducting an Information Security Evaluation of the North Korean People's Army (NKPA), using the NSA IAM and IEM Methodology. Traken Analytics, LLC. will be using a fresh Kali 2.0 images on clean Mac Book Pro laptops for all testing. All tools that come as standard equipment on the Kali distribution has the potential to use during the assessment. NKPA has requested the highest level of recommendation settings. Traken Analytics, LLC. will locate and close within critical information based on the Assessment Plan Criticality table.

3. System Description

The system that we will be accessing is the infrastructure for the North Korean People's Army and it contains all data from low level emails to TOP-SECRET base locations.

3.1. Mission Statement:

To hide and protect critical secret information based on vulnerable procedures, processes, software and training deficiencies. The end goal to conduct discrete clandestine missions around the world without the fear of being caught, up to and including be hacked by other countries.

3.2. Critical Information Types:

The NKPA has several types of data that is considered secret. All this information should be considered 'In Scope" for this assessment. Sensitive data (Level-4)– This would be any information or data to include secret files, locations of secret servers, passwords, etc.
Sensitive Sites (Level-3) – This would include hidden military bases and equipment. This would also include any Nuclear information, location and capabilities.
General Data (Level-2) – This is any data that could be an asset to a nation other than North Korea. This would be spy info, locations, and identities.
Lastly, Sensitive and secret photos and videos (Unknown Level)- This would include pictures to prove military capabilities and or nuclear capabilities, training facilities and most importantly unaltered photos or videos of Kim Jung-un relieving himself, urinating, or defecating. Basically pictures or videos of Mr. Jung-un pooping! I'm talking, we will even take baby poop photos!

1- Secret photos – Could be used to undermine the control of the supreme leader

2- Secret base locations – Could be used for an attack against the empire and prove our involvement in nuclear weapon development

3- True soldier count – this could prove or disprove our true strength or weakness in a combat environment

4- Reserve counts - this could prove or disprove our true strength or weakness in a combat environment

5- Military Secrets – These could be used against the Empire to prove access to nuclear weapons and that the supreme leader poops every morning at 0600

6- Organizational Data – This is the chain of command, who is in what position and why

7- Personnel Records – This is all the information about each individual in the NKPA

8- Internal Communications – How they communicate and what levels of security

3.3. Impact Attributes:

- Confidentiality:
  - Only those authorized can see the data
- Integrity:
  - No unauthorized changes
- Availability:
  - Accessible when needed

3.4. Impact Values:

High

- Reveals Locations of Nuclear weapons
- Reveals images of Mr. Jung-un (severely inappropriate)
- Leads to the arrest or death of international criminal
- Prevention of loss of 10 or more lives
- Rate payer power outage of greater than 5 days
- South Korean invasion of North Korea
- A negative article in the New York Times.

Medium

- Secret Files
- Collection of attack plans
- Collection of reserve files to include mon power and trained soldiers.
- Creates chaos within internal networks
- A negative article in the LA Times

Low

- Any downtime on National North Korean networks
- Loss of less than $100,000,000 in revenue
- Prevention of loss of up to 2 lives
- Loss of employee PII
- A negative article in the Colorado Springs Gazette

3.5. Organizational Information Criticality Matrix:

Type	Confidentiality	Integrity	Availability
Secret Photos	High	High	High
Base Locations	High	High	High
Active Soldiers	Low	Low	Medium
Reserve Soldiers	Medium	Low	Medium
Military Secrets	High	High	High
Organizational Data	Low	Low	Low
Personnel Records	High	Low	Medium
Internal Communications	Medium	Medium	Medium
High Watermark			
	High	High	Medium

Figure 2 Criticality Matrix (Organizational)

3.6. System Information Criticality

3.6.1. FACTS

FACTS	Confidentiality	Integrity	Availability
Military Secrets	H	H	H
Active Soldiers	L	L	M
Personnel Records	H	L	M

3.6.2. SNOOP

SNOOP	Confidentiality	Integrity	Availability
Military Secrets	H	H	H
Personnel Records	H	L	M

3.6.3. Physical Description of components

The section is a complete system description/configuration, including the number of workstations, PCs, etc., the hardware platform, and the software being used on the system. It can also include the number of active accounts and the number of users, if available. The types of features used on the system should also be included (i.e., TCP/IP, TELNET, SMTP, FTP, etc.), as well as what firewalls, if any, are implemented by the company and how they are implemented.

The description should state what connections the company has in place. Also included is brief description of the connection (i.e., 256kb leased carrier line, cisco routers, firewalls, etc.). Is the connection through an organization headquarters or direct? Include a description of the organization's modem connections. The number of modems, types of modems, hours of operation, modem access, I&A requirements, dial-back capability, etc. should all be included in this section.

4. Infosec Analysis

The INFOSEC Analysis includes all of the findings from the assessment. Each finding has a corresponding discussion, describing more details about the vulnerability the finding represents, and recommendation, presenting mitigation mechanisms or procedures.

4.1. High Findings

Finding: 1

Title: Data base servers can be accessed remotely.
Rating: High
CVE: CVE-2016-1525
CVSS: 8.6
Description: This vulnerability is ranked high because the ability to access the databases servers remotely can lead to major problems for NKPA. It could lead to several different kinds of files being compromised; everything from project timelines, to employee records and payroll are accessible remotely.

Recommendation: Currently there is no fix for the CVE, so Dirty Sanchez inc. recommends refraining from using this service until a fix is found. Fix it.

Finding: 2

Title: Microsoft Office / COM Object DLL planting.
Rating: High
CVE: CVE-2016-0016
CVSS: 7.8
Description: NKPA systems are vulnerable to this CVE. It allows a user to gain elevated privileges. This could crash the entire system or create a loss of critical data.

Recommendation: We recommended that NKPA updates to the newest version of Microsoft Office as well as all system updates for all devices. Updating will apply the patch that Microsoft issued. Updating is our first recommendation, another would be to remove Microsoft Office from NKPA systems. This would also remove the vulnerability from NKPA's hardware.

Finding: 3

Title: Adobe Flash vulnerability.
Rating: High
CVE: CVE-2015-8635
CVSS: 8.8
Description: NKPA's systems where outdated allowing possible remote code execution. Once the system is infected it can be used to launch arbitrary code. It would do this by corrupting or replacing freed memory data with the new malicious code or data.

Recommendation: NKPA will update their systems allowing the created patch by Adobe to be applied. Since NKPA was made aware of our discovery they have started the updating process, and is .0002% complete. We also provided NKPA with a secondary plan to uninstall Adobe Flash from all systems.

4.2 Other Findings 5-7

5- Pictures

   a. We were able to find numerous photos of several top ranking officials taking a crap.
   b. This was a scary finding, there were 1000's of photos.
   c. Most photos were found on the internet, some on secure servers
      i. VERY HIGH RISK

6- Passwords

   a. We were able to locate, crack and use 156 passwords of upper officials.
   b. The passwords gave us access to the photos found in findings 1.
   c. The password findings were due to weak security protocols when creating them.
   d. A complete lack of organization and preparedness were the most critical mistakes.
      i. VERY HIGH RISK

7- Locations

   a. By using found passwords, we were able to find several locations of bases
   b. They were secret
      i. VERY HIGH RISK

5. Conclusion

After 6 months of testing and assessment we at Traken Analytics have demonstrated that the North Korean People’s Army is completely unsatisfactory. There are security risks at every corner. There were violations at every instance of the assessment and in no way could we address every issue within the timeframe given to us be the Supreme Leader. There were several known CVE’s found that would give nearly every hacker a way into the network and gain access to nearly every level of internal security possible. There were several files found that would completely discredit the Supreme Leader. In the current state, I would say the attack surface of the NKPA is very large and could be victim to countless attacks if the issues are not addressed.

Recommendations:

The most important thing here is to understand what constitutes as good security habits and what will help or hurt your organization. The start was getting this assessment, the next step would be to fix as many of the findings as possible and have the assessment redone with another company to verify that your ‘Fixes” have actually helped your security posture.

APPENDIX A – Assessment Plan

Assessment Plan Outline

I IMPORTANT POINTS-OF-CONTACT

Daniel Sanchez, 480-555-1234, d.sanchez.dsjobs.com

II MISSION

To hide and protect critical secret information based on vulnerable procedures, processes, software and training deficiencies. The end goal to conduct discrete clandestine missions around the world without the fear of being caught, up to and including be hacked by other countries.

III ORGANIZATIONAL INFORMATION CRITICALITY

Secret photos – Could be used to undermine the control of the supreme leader
Secret base locations – Could be used for an attack against the empire and prove our involvement in nuclear weapon development
True soldier count – this could prove or disprove our true strength or weakness in a combat environment
Reserve counts - this could prove or disprove our true strength or weakness in a combat environment
Secret Files – These could be used against the Empire to prove access to nuclear weapons and that the supreme leader poops every morning at 0600

	Confidentiality	Integrity	Availability
Secret Photos	High	High	Low
Base Locations	High	High	Medium
Active Soldier	High	High	Low
Reserve Soldier	High	High	Low
Secret Files	High	High	Low
High Watermark			
	High	High	Medium

IV SYSTEM(S) INFORMATION CRITICALITY

Mobile devices
Email
Server based computing
Desktop
Laptop
Vehicle communications

	Confidentiality	Integrity	Availability

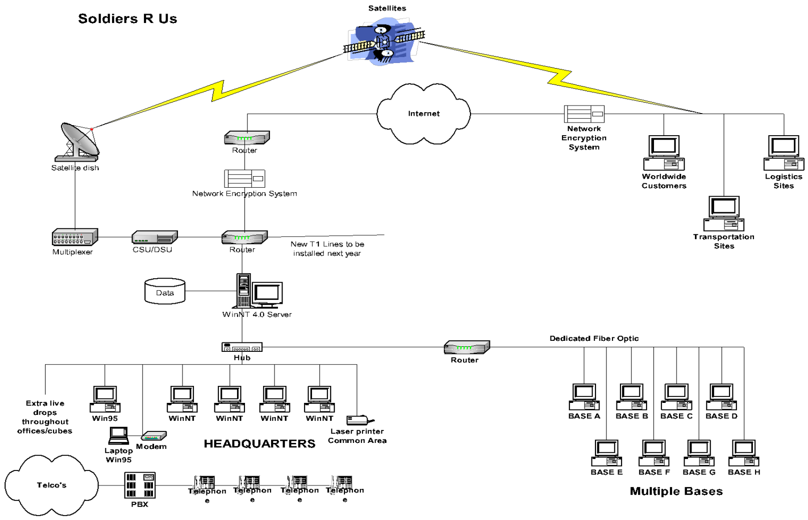
Mobile Devices	Low	High	Low
Email	High	High	Low
Servers	High	High	Low
Computers	High	High	Low
Radios	High	High	Low
High Watermark			
	High	High	Low

V CUSTOMER CONCERNS

(Special considerations, concerns, and/or constraints levied by the customer organization)

VI SYSTEM CONFIGURATION

This network would use some of the following devices in daily operations; laptops, cell phones, tablets, encrypted radios, desktop computers, satellites, internet, servers, routers, switches, and email.



VII INDIVIDUALS AND POSITIONS TO BE INTERVIEWED

SL – Supreme Leader – Kim Juan-Un, Highest Level “GOD like”
CO – Commanding Officer – Lee U, Leader of troops, logistics
XO – Executive Officer – Fu Mea, Low level control of daily troop care
DBA – Database Admin – Jon Sun, Chin Low, Hi Chu, network, database control
ROM - Communications Operator – Sue Ti Lie, all commo, radio, digital, physical
SSO – System Security Officer – Tie Ree Ree, All network and digital security
PSO – Physical Security Officer – Shin Mi Chin, Physical security, national security

VIII DOCUMENTS REVIEWED

Concept of Operations (CONOPS)
Recovery and backup procedures
Security Administrator’s Manual
Security CONOPS
Security Features User’s Guide
Security Policy
Security Test Plans
Standard Operating Procedures (SOPs)
User’s Guide
Vendor documentation

IX TIME-LINE OF EVENTS

	Date	Time	Completed
Contract	02/01/2016	0600	NLT 09/01/2016
Pre-Assessment	02/08/2016	1400	02/08/2016 1800
Assessment	03/01/2016	0600	TBD
Post Assessment	TBD	0800	NLT 09/01/2016

APPENDIX B – System Diagrams

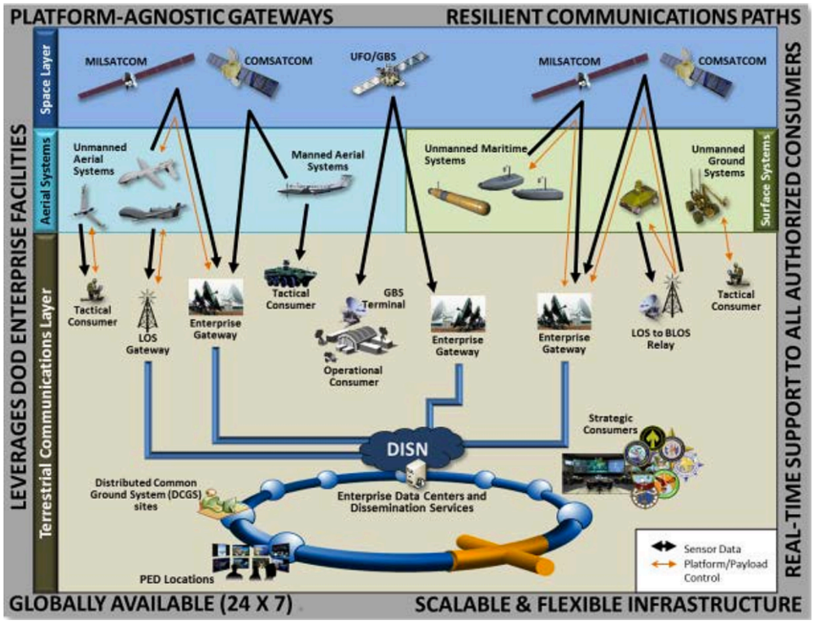


Figure 3 Public Sector IT: Search Results. (n.d.). Retrieved April 25, 2016

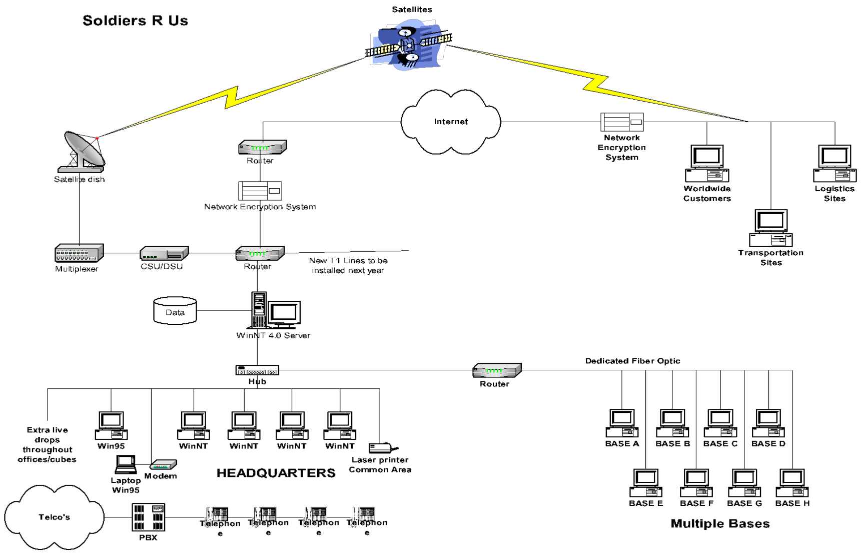


Figure 4 Network Diagram

APPENDIX C – Organizational Vulnerability Criticality Matrix

OVCM Organizational Vulnerability Criticality Matrix	Finding Number	Severity	CVSS Rating	Vulnerability Impact Attributes	High			High			High		
					Military Secrets Confidentiality	Military Secrets Integrity	Military Secrets Availability	Secret Photos Confidentiality	Secret Photos Integrity	Secret Photos Availability	Base Locations Confidentiality	Base Locations Integrity	Base Locations Availability
CVE-2016-1525	1	H	8.6	CIA	10	7.9	9.1	N/A	N/A	N/A	N/A	5.5	N/A
CVE-2016-0016	2	H	7.8	CIA	N/A	6.5	N/A	8	7	9.2	N/A	N/A	N/A
CVE-2015-8635	3	H	8.8	IA	N/A	N/A	6.7	N/A	N/A	N/A	8.9	9.1	7.4