# IssueMakersLab - Cyber Warfare Research Team

Archived: 2026-04-02 10:56:49 UTC

**1. Overview**

For about a year from June 2016 to May 2017, the estimated power of North Korea has been involved in South Korea’s 10 more organization’s websites related to diplomacy, space aviation, North Korea, unification, parliamentary, labor, finance, etc.

A Watering hole attack was conducted to distribute malware to visitors through. As direct attacks against institutions and businesses in the field became increasingly difficult, they conducted an attack against a relatively easy association compliant, and conducted a bypass penetration.

Infection vector used program was ActiveX programs from 10 domestic software, including electronic payments, authentication, encryption, reporting, webmail and groupware, to infect visitors in their respective fields. Some ActiveX programs have been installed on the PCs of many users in the country, and they distributed the malware using a vulnerability in zero day vulnerability where no patches existed at the time of distributing the malware. It was also able to distribute malwares without being detected for a long time by only distributing them for a very short period of time or identifying and distributing specific users.

The malwares were similar to those that were distributed to South Korean security agencies and large South Korean companies, which police and prosecutors concluded in 2016 were respectively responsible for North Korea. There is also a connection with malwares used in the South's ATM hacking scandal, which is suspected of being committed by North Korea but has yet to be closed. In addition, during the time of the North Korea's March 20 attack against broadcast and financial hacking (2013) incident, ActiveX vulnerabilities of the South Korean financial security module were used to infiltrate the agencies for several months, resulting in secondary damage called hard disk destruction. With this so called " Operation GoldenAxe”, it is expected to reach further damage.

**2. Target**

### 2.1. Web sites for distributing malware

The following 10 Web sites were hacked and malwares were distributed to visitors.

| | |
|---|---|
| hxxp://www[.]kcfr[.]or[.]kr | The Korea Foreign Affairs Association |
| hxxp://www[.]ksas[.]or[.]kr | Aerospace Research Institute |
| hxxp://www[.]nksis[.]com | North Korean Strategic Information Service Center |
| hxxp://www[.]tongzun[.]co.kr | A group of North Korean defectors preparing for reunification |

| | |
|---|---|
| hxxp://www[.]tongiledu[.]org | Unification Education Council |
| hxxp://kuprp[.]nodong[.]net | National Union of Public Research Workers |
| hxxp://ampcc[.]go[.]kr | The National Council of Councils |
| hxxp://www[.]wblu[.]or[.]kr | Woori Bank Branch |
| hxxp://newanticancer[.]com | Sindaeam Hospital |
| hxxp://www[.]rokps[.]or[.]kr | Hunjeonghoe of South Korea (former lawmaker) |

**2.2. ActiveX programs used to distribute malware**

The following 10 ActiveX programs were used to distribute malware.

Some ActiveX vulnerabilities used in the dissemination were exploited by zero-day vulnerabilities, with no patches present at the time of the spread of malwares.

In particular, ActiveX zero-day vulnerabilities in M2Soft's reporting solution were used in June 2016 for an organization, and were again used to distribute the malware of North Korea.

| | |
|---|---|
| EasyPayPlugin.EPplugin.1 | EasyPay Electronic Payment Plug-in Module |
| MagicLoaderX.MagicLoaderX.1 | Dream Security MagicloaderX Authentication Plug-in Modul |
| NVERSIONMAN.NVersionManCtrl.1 | Nanoom Groupware Smart Flow NVersionMan Module |
| admctrl.FileIO.1 | Dream Security Administrator Privilege Processing Component Modul |
| RDVistaSupport.VistaSupport.1 | M2 Soft Reporting Solution Report Designer Module |
| JxVistaDll.JXVistaUtil.1 | Soft 25 Zone Encryption Solution JX - CEAL Vista Module |
| JXFILEBOX.JxFileBoxCtrl.1 | Soft 25 JXFILEBOX Module |
| JXORGTREE.JXOrgTreeCtrl.1 | Soft25 Webmail JXMAIL Module |
| INIWALLET61.INIwallet61Ctrl.1 | INISYS INIWALLET Browser extension module |
| INIUPDATER.INIUpdaterCtrl.1 | Initec INISAFE Encryption Solution Update Module |

**3. Malware distributed (malware by North Korea)**

A number of malwares have been circulated, which are similar to malwares those were said to be attributed by North Korea from the investigation report of the Prosecutor's Office and National Police Office.

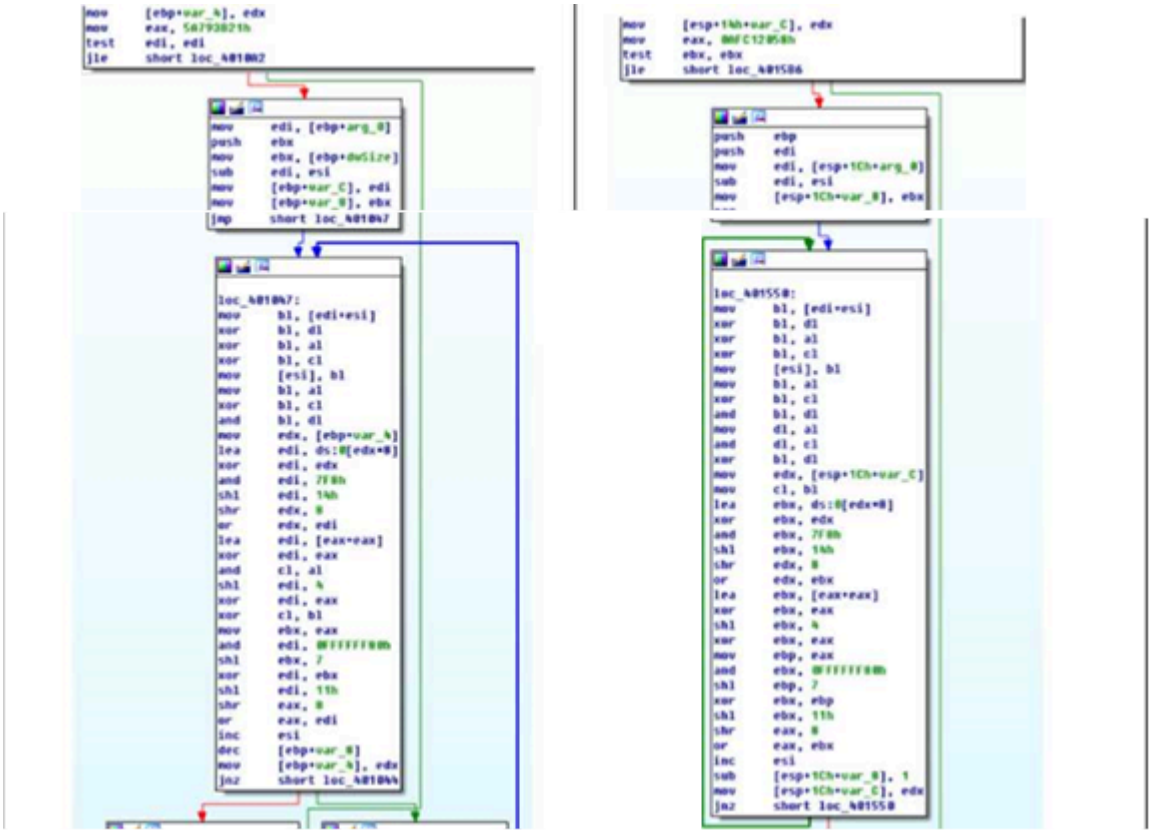
malwares allow users to remotely control their PCs to steal information or transmit additional malwares.

**3.1. Similar to the malware used for hacking to South Korea's large enterprise group**

(Source: S. Korea's National Police Office)

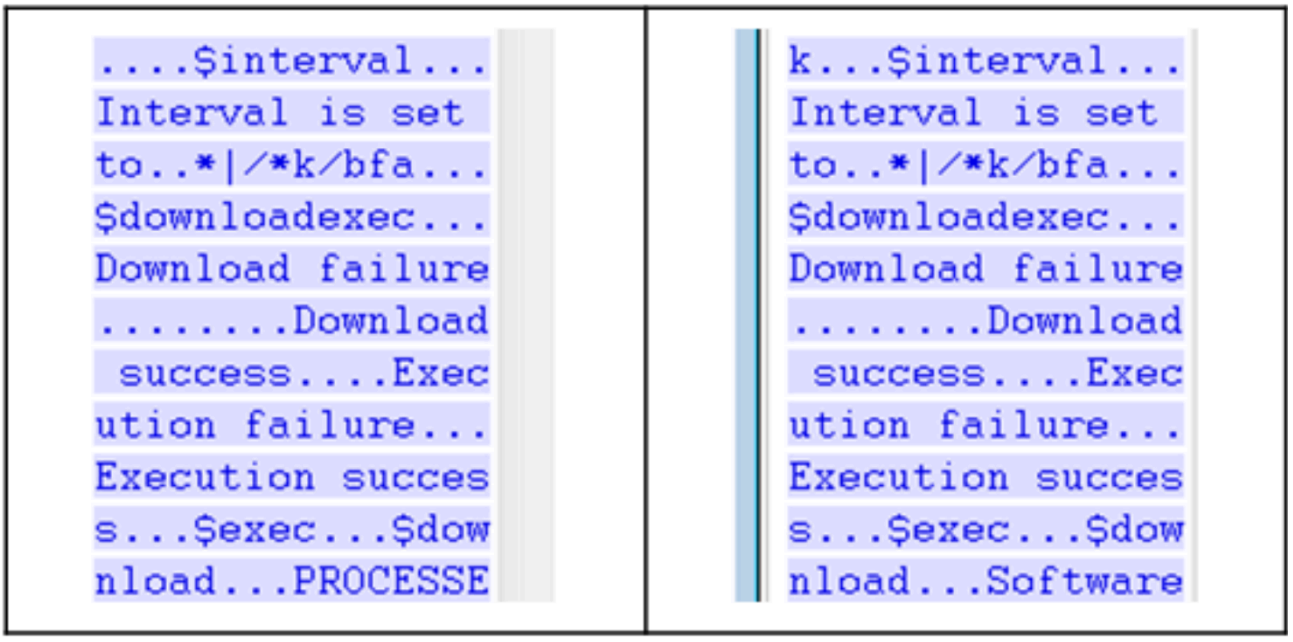
The malware on the left of the picture below is malware that was announced by the police as North Korean made, and the malware on the right was distributed in the Operation GoldenAxe. Unique Encryption/Decryption logic used in malware is identical. Other malwares found the same part of the protocol used to control & command.

**3.2. Similar to malware used for hacking of S. Korea's Security Software Companies (Source: S. Korea's Prosecutor's Office)**



The malware at the top of the picture below is malware that was announced by the S. Korean Prosecutor's Office as the act of North Korea. Two malwares use the same Encryption/Decryption method and has the same C&C command system.


When the above two malwares are decoded, the same C&C command system is used as follows.




### 3.3. Connected to malware found in S. Korea's ATM hacking (suspected North Korean actions)

The C&C server address used in the incident targeting The National Council on Public Relations (hxxp://ampcc[.]go[.]kr) that distributed malwares during this Operation GoldenAxe corresponds to that of code found in the ATM hacking incident in Korea.

#### 4. Comments/Response

North Korea is mainly using zero-day vulnerabilities in the ActiveX program of South Korean software. ActiveX is a common use by local organizations, companies, and others, and many are installed on the local users ' PCs. Also, finding an ActiveX vulnerability is fairly easy compared to other software programs, making it the best

weapon for North Korea to use in an attack spreading malware. In particular, the March 20 attack in 2013, which was found to have been committed by North Korea, was infiltrated by the vulnerability of ActiveX financial security module, which is widely used in South Korea. In the current situation where it is difficult to penetrate directly as major organizations and companies have increased security due to frequent cyberattack from North Korea, the agency and its employees are infected through associations and associations.

Therefore, it is necessary to refrain from using ActiveX, which is relatively vulnerable to security.

---