*Note: The details in this fictional simulated scenario are for academic purposes only and are not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*

---

**Department of Homeland Security**
**Preliminary Report on Moonrok Attacks**
**May 26, 2014**

## Summary

The Department of Homeland Security is taking the lead in the investigation into an ongoing cyber attack that began on May 18, 2014. The attack started with escalating distributed denial-of-service (DDoS) attacks targeting US and Republic of Korea (ROK) financial institutions, followed by the emergence of destructive malware disrupting critical systems and requiring costly and logistically challenging replacement of hardware. The attack is currently affecting trading platforms in every major US financial institution across every US exchange and is impacting the ability of exchanges to clear and settle transactions of securities worldwide. Analysis of affected computer systems indicates that equipment malfunction was caused by a piece of malware called 'Moonrok' after a word embedded in its code.

## Background

• *The US, Japan, and ROK carry out a routine military exercise.*
On 05/18, South Korea and Japan joined the US in a two-day joint military drill off the southern coast of the Korean peninsula. The drill involved the nuclear-powered aircraft carrier USS George Washington docked at the port of Busan, guided-missile ships, anti-submarine helicopters, early warning aircraft, and B52 bombers making flights over South Korea. Planned in accordance with a newly signed and updated contingency plan "designed to counter future North Korean provocations," US and ROK officials have described the drill as a search and rescue exercise to improve readiness for humanitarian disasters.

• *US and ROK financial sectors are the victim of DDoS attacks by unknown actors.*
Beginning on 05/18, a still-unverified group waged DDoS attacks to overwhelm financial-industry websites with traffic from hijacked computers. The attack flooded bank websites with 10 to 20 times more Internet traffic than normal, rendering them unavailable to consumers and disrupting transactions for hours at a time over a period of several days. The nature of this attack is sophisticated enough that even the largest of the financial institutions are finding it difficult to defend against.

• *Attacks evolve from disruptive to destructive.*
New attacks emerging on 05/23, with the introduction of the 'Moonrok' malware, sought to destroy data and take over or shut down financial networks that provide accurate pricing information and run trading platforms. Unlike viruses that aim to hit as many targets as possible, this one appears designed to cripple computers on specific networks identified by the culprits. Moonrok appears to be exclusively targeting companies in the financial sector and involve inject vectors that are previously unseen, fully-autonomous, and widely undetectable.

• *US financial sector significantly affected.*
By 10:00 AM on 05/23, every major financial institution was reporting computer irregularities in their trading platforms and massive trading disruptions. Citing exigent and unprecedented circumstances, the Securities Exchange Commission suspended trading on many Fortune 100 companies, including "MajorBank Corporation." The inability of exchanges to price securities and clear and settle transactions affected every US exchange market, some suffering a record 10% loss in value. By the end of the day, every US market had voluntarily halted trading before the normal closing bell.

• *North Korea claims responsibility.*
On 05/26 as a "show of force," the North Korean government claimed responsibility for the crippling attacks on U.S. financial institutions. They cite recent joint U.S., Japan, and ROK military exercises as motivation for retaliation. While these claims cannot be proven, North Korean officials released a block of I.P. addresses targeted in the attack on Pastebin, a website often used by hackers to claim responsibility for attacks. While these addresses could only have been gathered by the perpetrators of the attack, DHS continues to investigate. Additionally, it is unlikely that North Korea has the capability to create malware of the level of sophistication of Moonrok.

• *State Department mobilizing diplomatic resources.*
While not directly involved in the investigation, the State Department is working closely with DHS and the Department of Defense to coordinate requests for information sharing with other governments. The Secretary of State and the ambassadors to China and the UN are being briefed on the situation regularly in preparation for possible diplomatic action. Additionally, China's leadership has offered to act as a mediator in any potential conflict on the Korean peninsula, an act that has the potential to greatly strengthen the future of US and China's diplomatic relationship.

• *All options are on the table.*
Military as well as diplomatic options were weighed at a high level White House meeting this week, including possible retaliation and counterattacks against self-identified attackers, North Korea. Overall, the financial services industry is still split over whether a response should take on a more forceful role. Some argued that any response should go after the hackers, while others cautioned that offensive action could lead to retaliation, additional attacks against the banks, or unforeseen consequences. Other options include government action in the form of complaining through diplomatic channels.

• *Private sector engagement.*
Bank officials are asserting that financial firms have spent millions of dollars responding to the attacks and that they can't be expected to fend off attacks from a foreign government without violating existing US domestic laws. A number of affected financial institutions would like the government to let the private sector block the attacks or even take down the network of computers mounting attacks.

**Analysis**

• *Attacks appear to be for sabotage.*
Previous DDoS attacks proved to have been cover for looting bank accounts and stealing customers' or employees' personal information, but there's no evidence so far that the latest attack has included theft. It appears that this time, the attackers' aim is not espionage but sabotage. Most attacks against American companies—especially those coming from China—have been attempts to obtain confidential information, steal trade secrets, and gain competitive advantage.

• *Attacks are distributed and appear to be from somewhere in Asia.*
The attackers are using a network of tens of thousands of infected computers running corporate websites, coming from computers that could have legitimate reasons to communicate with the banks. Roughly half of those computers are overseas and out of the reach of US law enforcement. Although pinpointing a specific source of the attacks is tricky, some believe that China—itself the victim of multiple computer attacks—may have played a role. There is no conclusive forensic evidence, because by design, Moonrok covers its tracks by erasing data on computer hard drives. We are still not certain exactly where the attacks are coming from, or whether they are state-sponsored or the work of hackers or criminals, but the source seems to be somewhere in Asia.

• *Threat may not be limited to financial sector.*
Moonrok poses an ongoing threat to national cybersecurity. Moonrok's ability to spread via network connections and USB devices could result in widespread computer infections, meaning that critical infrastructure could be at risk. If the financial industry, which spends more on Internet security than any other industry and has its largest and most extensive defenses, can't handle this, it is unclear whether any critical infrastructure industry can.

• *The attacks may not be over.*
Cybersecurity and data storage companies believe that additional infections involving Moonrok remain a possibility. Interdependencies between telecommunication and financial sectors require that operations not be segregated from a company's internal communications network, the primary method of infection. While the immediate focus is on work replacing the hard drives of tens of thousands of its PCs, finance executives are unsure that the internal communications networks can't be used to hit again.

**Conclusions**

Moonrok poses the single biggest threat to US cybersecurity witnessed to date. Stopping Moonrok and mitigating its damage will take a concerted effort from both public and private entities. In what is regarded as the most destructive act of computer sabotage to date, the malware erased data—documents, spreadsheets, emails, files—on three quarters of PCs of exchanges, financial institutions, trading platforms, and financial regulators. The challenge will be managing our nation's offensive and defensive capabilities requiring a very broad engagement across the private sector.

At the moment, DHS cannot identify the attacker conclusively. However, indications are that this is very likely a state-supported attack, with significant evidence pointing to the involvement of North Korea. DHS will coordinate further with the Department of State, the Department of Defense, and intelligence services to develop more information on the origin of the attack.

*Note: The details in this fictional simulated scenario are for academic purposes only and are not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*

**UNITED STATES OF AMERICA**
**Before the**
**SECURITIES AND EXCHANGE COMMISSION**
**May 23, 2014**

**In the Matter of**

**MajorBank Corporation,**

**File No. 912-1**

ORDER OF SUSPENSION OF TRADING

It appears to the Securities and Exchange Commission that there is a lack of current, accurate, and adequate information concerning the securities of MajorBank Corp. because of potential market manipulation, and the inability of exchanges to clear and settle transactions of securities across multiple exchanges.

The Commission is of the opinion that the public interest and the protection of investors require a suspension of trading in all securities the above-listed company. Therefore, it is ordered, pursuant to Section 12(k) of the Securities Exchange Act of 1934, that trading in the securities on the above-listed company are suspended from 2:45 p.m. EST on May 23, 2014 through 11:59 p.m. EST on June 6, 2014.

By the Commission.

Klara Jordan
Assistant Secretary

*Note: The details in this fictional simulated scenario are for academic purposes only and are not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*

---

**Joint Security Awareness Report (JSAR-14-912-01A)**
**Moonrok/ Malware (Update A)**
**Original release date: May 23, 2014 | Last revised: May 26, 2014**

## Overview

"Moonrok," is an information-stealing malware that also includes a destructive module. Moonrok renders infected systems useless by destroying the BIOS as well as data overwriting the Master Boot Record (MBR), the partition tables, and most of the files with random data. Once overwritten, the data are not recoverable.

Based on initial reporting and analysis of the malware, no evidence exists that Moonrok specifically targets industrial control systems (ICSs) components or U.S. government agencies.

According to multiple cybersecurity and ICS companies, Moonrok has three primary functional components:

- Dropper—the main component and source of the original infection. It installs a number of other modules.
- Wiper—this module is responsible for the destructive functionality of the malware.
- Reporter—this module is responsible for reporting infection information back to the attacker.
- After the initial infection, Moonrok spreads via network shares to infect additional machines on the network. Multiple cybersecurity companies first detected Moonrok on May 23, 2014, and estimates infections existing worldwide are limited to only few companies (less than 100).

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT and US-CERT for tracking and correlation against other incidents.

## Impact

Because of the highly destructive functionality of the Moonrok "Wiper" module, an organization infected with the malware could experience operational impacts including loss of intellectual property (IP), disruption of critical systems, and damage requiring costly and logistically challenging replacement of hardware. Actual impact to organizations may vary, depending on the type and number of systems impacted.

*Note: The details in this fictional simulated scenario are for academic purposes only and are not meant to represent the views of the competition organizers, authors, or any affiliated organizations.*

**The US Times (May 26, 2014)**

## North Korea Claims Responsibility for Devastating Cyber Attack

The North Korean government on May 26 claimed responsibility for a series of crippling attacks on U.S. financial institutions, and experts say that current evidence supports the veracity of these claims.

On the morning of May 23 a trickle of traders began reporting computer irregularities in their trading platforms. By 10:00 AM, the levy had broken and reports from every major financial institution and securities exchange indicated massive trading disruptions -- it was clear that a critical problem, impacting all U.S. financial markets, had occurred.

After a record 10% plunge in nearly every exchange market, the Securities Exchange Commission suspended trading on many Fortune 100 companies, including "MajorBank Corporation," before the scheduled close of business on May 23. Initial reports from the SEC indicated that an unprecedented cyber attack on the U.S. financial markets had been perpetrated by assailants using previously unknown malware called "Moonrok." Government official have been unable to say who initiated this assault on the U.S. economy and why.

The answer to these questions may have just been offered by the perpetrators themselves. In a forceful statement issued Monday morning, Kim Jong-un, the supreme leader of the Democratic People's Republic of Korea, claimed responsibility for the attacks and condemned U.S. arrogance and imperialism for instigating the assault.

After Jong-un's remarks, North Korean officials released blocks of I.P. addresses on Pastebin, a Web site often used by hackers to claim responsibility for their attacks. The officials claimed that these I.P. addresses belong to computers that they infected with the Moonrok malware.

North Korea's claim for responsibility for the attacks come after a week of escalating distributed denial-of-service (DDoS) attacks and other threats of retaliation for recent joint U.S., Japan, and Republic of Korea military exercises held around the Korean peninsula from May 18 to 19.

The now familiar threats leveled by North Korea in response to periodic military exercises included threats of preemptive strikes and assertions that the 1954 armistice has been invalidated. In addition, the Supreme Command of the North Korean military said, "we will put on the highest alert all the field artillery units, including strategic rocket units and long-range artillery units, which are assigned to strike bases of the U.S. imperialist aggressor troops in the U.S. mainland."

On May 20 North Korea renewed warnings to the United States of a "horrible disaster" resulting from the recently concluded military exercise and put its troops on alert. The United States is "wholly accountable for the unexpected horrible disaster" that was coming to its "imperialist aggression forces," a North Korean military spokesman said.

In a separate statement, Jong-un said, "[U.S. leaders] must bear it in mind that reckless provocative acts would meet our retaliatory strikes and lead to an all-out war of justice for a final showdown with the United States." Jong-un said that he will not beg for peace and will protect his nuclear-armed nation against all enemies with strong self-defense measures.

In response to questions over the decision to publicly take credit for the largest and most damaging cyber attack in history, Jong-un responded that the show of force was to "demonstrate North Korea's power as the greatest cyber warrior, even greater than the might of its nuclear strength."

Though a large scale cyber strike against the U.S. does not fit neatly with the threats levied by North Korea, the country has lashed out online before. After new U.N. sanctions and the March 2013 joint military exercise, the South Korean financial sector was hit with DDoS attack later attributed to North Korean hackers.

North Korea's latest announcement comes after some experts previously speculated that Pyongyang may initiate an attack on the U.S. economy, inspired during Dennis Rodman's recent visit with Jong-un. John Junper, a former member of the Wall Street Warbucks professional basketball team who accompanied Rodman on his recent visit to North Korea, told the US Times about an exchange he overheard during an official dinner in January.

"Rodman looked over to Kim [Jong-un] and said, 'Man, if you really want to win in the U.S. you've got to take down Wall Street,'" Junper said. "I thought he was hassling me and my old team, but after the banks all went down. . . Well I just don't know."