38 NORTH

Negotiations With North Korea May Have Cyber Consequences

BY: ADAM MEYERS
MARCH 13, 2018

As unprecedented talks between the US and North Korean leaders promise to unfold in the next few months, the US has said it will continue to apply pressure on the North Korean regime to ensure favorable odds at the negotiating table. While the North Koreans have reportedly agreed to a moratorium on missile and nuclear tests during inter-Korean and US-DPRK talks, they are likely to see clandestine offensive cyber operations as a potential response to continued debilitating sanctions, as well as for further intelligence gathering. Given the North's capabilities and past targets, future offensive cyber campaigns are likely to focus on western financial, media, and government sector targets, including the defense industrial base.

North Korea's Seasoned Cyber Warriors

In June 2014, the North Korean regime launched cyber retaliation in response to the film "The Interview," which starred Seth Rogen and James Franco as two fictional tabloid TV hosts who are selected to interview Kim Jong Un and subsequently recruited by the CIA to assassinate him. Numerous outlets quoted an unnamed North Korean official cited by KCNA who said "*Making and releasing a movie on a plot to hurt our top-level leadership is the most blatant act of terrorism and war and will absolutely not be tolerated*." What happened in the months that followed is now a stark reminder of the offensive cyber capabilities that North Korea has at its disposal.

Retrospective analysis of the November 2014 destructive cyber event that took place within the networks of Sony Pictures Entertainment (SPE) indicates that the attackers penetrated the network sometime in the late summer/early fall 2014 and wormed their way through the infrastructure, ultimately attaining sufficient privilege and reach to initiate a destructive payload across most of SPE's systems and putting a stop to their on-going operations. The catastrophic event was further exacerbated by the claims of a previously unknown, and subsequently never heard from again group calling themselves the Guardians of Peace (GOP). In the cyber domain, unknown groups performing a complex and sophisticated attack are rare; generally the actors behind these attacks spend years developing and honing their capabilities and techniques. The development of this tradecraft generally leaves behind a history of what they have done and where they have learned to adapt. Information security professionals track these groups and their development in a discipline called cyber threat intelligence (CTI).

In December 2014, the US Computer Emergency Response Team (USCERT) released a report *(https://www.us-cert.gov/ncas/alerts/TA14-353A)* detailing a Server Message Block (SMB) Worm/Tool equipped with a Listening Implant, Lightweight Backdoor, Proxy Tool, Destructive Hard Drive Tool, and Destructive Target Cleaning Tool. Analysts who reverse engineered the code were able to link it to the activity of a group labeled Lazarus *(https://www.bankinfosecurity.com/british-security-services-tie-north-korea-to-wannacry-a-10005)* by many in the information security community. Others track this group's activity under the name Silent Chollima *(https://www.crowdstrike.com/blog/unprecedented-announcement-fbi-implicates-north-korea-destructive-attacks/)*. The technical experts performing analysis linked shared source code used to build these tools to attacks that occurred dating back years. In addition to similarities in code base, the tool chain used to build that source code into a program that was capable of running on the victim machines left a fingerprint unique enough to link it to previous attacks against financial, media, government and defense targets. The technical similarities were not the only element of those attacks tying them together, in attacks dubbed Dark Seoul *(https://www.theguardian.com/world/2013/mar/20/south-korea-under-cyber-attack)* previously unknown groups calling themselves Whois Team and the New Romanic Cyber Army Team took credit for the attacks. As with the GOP, neither of these groups have been heard from since.

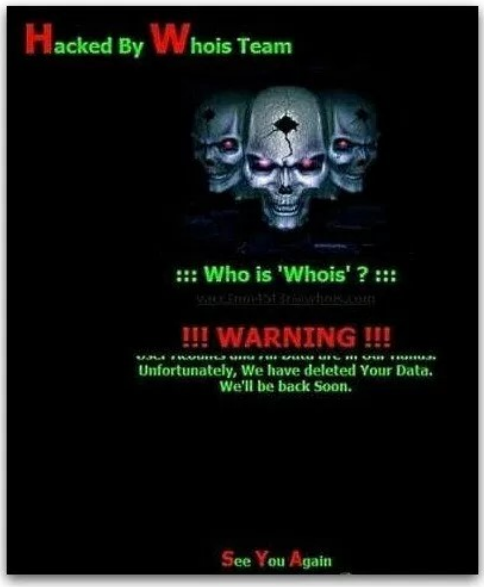
In the wake of the destructive attack at Sony, files from the victim were leaked to the internet. Included in these leaks were movies that were yet to be released, and sensitive emails that contained private and in some cases embarrassing correspondence between the leadership of SPE. The weaponization of data by the GOP was further devastating to SPE, which was paralyzed without the use of any of their systems and infrastructure to formulate a response to the rapidly devolving public relations fiasco.

DPRK Cyber Attack Options

In response to the most recent round of UN sanctions, a spokesman of the North Korean Ministry of Foreign Affairs stated *(https://www.washingtonpost.com/news/worldviews/wp/2017/12/24/north-korea-declares-latest-u-n-sanctions-an-act-of-war/?utm_term=.9b2a9bf31c47)*: *"We define this 'sanctions resolution' rigged by the U.S. and its followers as a grave infringement upon the sovereignty of our republic and as an act of war violating peace and stability in the Korean Peninsula and the region.*" This initial reaction, now that the ebullience of the PyeongChang 2018 Winter Olympics has passed, should put the world on notice that the Kim regime may see offensive cyber operations as a proportional response to the increasing chokehold of international sanctions. What might such an attack look like?

North Korean operators have been observed over the past several months targeting a variety of organizations that might be seen as viable targets for a retaliation, including financial organizations and defense contractors. North Korean operators would likely use an existing penetration as a jumping off point looking for a high-profile target to inflict damage upon as a show of force. Attacks that occurred during 2016 demonstrated DPRK actors had the capability to penetrate a financial institution and use their processes against them in a currency generation scheme *(https://www.bloomberg.com/news/articles/2017-10-17/north-korean-hacker-group-linked-to-taiwanese-bank-cyberheist)* that netted millions of dollars in currency. Based on several other high- profile attacks that followed this watershed event, it is possible that DPRK actors already possess access to organizations *(https://www.cnbc.com/2017/10/11/north-korean-hackers-target-us-electric-companies-with-malicious-emails.html)* that may meet their needs. If a suitable penetration is not present, a new one would be targeted, likely using spear phishing emails or a "watering hole" attack (compromising a legitimate website likely to attract targets of interest who would then be infected with malware). Both techniques have been leveraged by DPRK cyber operators successfully in the past.

Once initial access is attained, DPRK cyber operators would need to escalate their security privileges to that of a system or domain administrator. With elevated privileges, they will be able to move across the network, if they are not identified or stopped in the initial access. (This is the phase where they will be most exposed, because data exfiltration can consume large amounts of bandwidth and administrative account activities may attract the attention of a diligent system manager.) During the operational phase, data will likely be stolen, and logic bombs will be planted and left to detonate at a specific time or command. The victim of such an attack, if they are unable to identify and prevent it, will likely be confronted one day with a terrifying scene—all or most of the computers in the enterprise will be non-functioning and may even contain a warning image on the disabled devices.



As the organization realizes that they have become the victim of an attack, law enforcement and commercial incident response personnel will be called in to perform an investigation and remediation. As the pieces start to come together for those teams, if the opportunity presented itself, data may begin leaking including sensitive emails or proprietary information.

Targeting of financial institutions and government would certainly feel like a proportional response for the North Koreans; other targets of interest may include media, military/government organizations, or potentially critical infrastructure. In October 2017, attacks were observed targeting US electrical utilities that were associated with DPRK actors. In December 2015 and again in December 2016 attacks associated with the adversaries linked to the Russian Federation targeted Ukraine including a disruptive attack manipulating electrical transmission equipment that resulted in blackouts across that country. Such an attack against US critical infrastructure would be of interest to North Korean leadership seeking to cause fear and disruption across the US. In addition to intrusion activity including destructive or disruptive elements, distributed denial of service (DDoS) attacks may be leveraged by DPRK actors to further enhance the effects of other attacks by knocking online media or response websites offline, compounding potential disruptive effect.

North Korean cyber operators have demonstrated the ability to successfully breach sensitive systems and organizations. Offensive cyber operations provide an asymmetric tool for DPRK leadership and an alternative to military provocations when responding to what they perceive as an attack their sovereignty. Such actions are hard to attribute to specific actors and, as such, may become more common in the coming months.