OnionDog is not a Targeted Attack—It's a Cyber Drill

Published: 2017-08-09 · Archived: 2026-04-05 13:55:11 UTC

Alleged attacks from North Korean actors are a hot security research topic. The infamous Sony Pictures hack in 2014open on a new tab, for instance, was reported by some to be the work of North Korean threat actors. There is a lot of interest in Lazarus too, which is purportedly a North Korea-linked groupopen on a new tab responsible for a couple of global bank heists that attempted to steal staggering amounts of money.

In this blog post, we will look into smaller scale attacks in which an actor group allegedly attacked high profile targets working in the energy and transportation sector of South Korea for more than three years in a row. These attacks, which are known as OnionDog, received some publicity in the media. A perfunctory look into these actors' activities might easily lead to hasty conclusions on attribution. We had a more thorough look, in which we reached an interesting conclusion: OnionDog is not a targeted attack. OnionDog is a cyber drill.

OnionDog is a Cyber Drill

OnionDog was first observed in 2013. When it was reported in 2016, it was attributed to be behind attacks on South Korean energy and transportation companies that went as far back as 2013. We know of about 200 unique OnionDog samples. At first sight, it looked like the work of a small but still-significant threat actor group. A reportopen on a new tab from the Qihoo 360's Helios Team has the most detailed analysis of OnionDog. It included indicators of compromise (IoCs) such as hashes of malicious files along with eight specific command-and-control (C&C) IP addresses. The IP addresses are indeed callback addresses for malware-infected computers. Their purpose doesn't look malicious but merely meant to record which targets fell victim to a cybersecurity drill. We looked up historical domain resolutions of these eight IP addresses and found these:

IP	Domain	Active
221[.]149[.]223[.]209	korea[.]kr[.]ncsc[.]go[.]kr	June 2011—August 2011
112[.]169[.]154[.]65	cyber[.]ncsc[.]go[.]kr	June 2011—August 2011
221[.]149[.]32[.]213	drill12[.]ncsc[.]go[.]kr	July 2012—August 2012
220[.]85[.]160[.]3	dril113[.]ncsc[.]go[.]kr	August 2013
222[.]107[.]13[.]113	drill12[.]ncsc[.]go[.]kr	August 2013

Table 1: Historic passive DNS data of hardcoded OnionDog C&C IP addresses

IP1	Domain IP1	IP2	Domain IP2
218[.]145[.]131[.]130	None	220[.]85[.]160[.]3	dril113[.]ncsc[.]go[.]kr
218[.]153[.]172[.]53	None	221[.]149[.]223[.]209	korea[.]kr[.]ncsc[.]go[.]kr

Table 2: Two pairs of OnionDog C&C IP addresses with the same HTTP response in July and August 2014. These responses were unique in historical Internet-wide HTTP scans by Rapid7.

The ncsc.go.kr domain belongs to the National Cyber Security Center (NCSC) of South Korea, indicating the five IP addresses in table 1 belonged to the NCSC of South Korea. Two more C&C IP addresses cited in the report had virtually unique digital fingerprints based on their response to basic HTTP requests. This convinced us that these were controlled by the South Korean NCSC in 2014 too. So seven out of the 8 IPs listed in the report clearly linked back to NCSC at some point in the past. This alone already made us think that the OnionDog samples were related to cyber drills.

We found about 200 files in the wild related to OnionDog, which means the cyber drills' tools were not contained in a controlled environment. This potentially poses problems—after all, no one wants these methods and tools to become public, especially when they were specifically intended for the drill.

Below are some of the samples belonging to OnionDog:

SHA256	**Compile Time**	**Hardcoded C&C**
dbb0878701b8512daa057c93d9653f954dde24a25306dcee014adf7ffff0bdb4	13/08/13 07:47	dril113[.]ncsc[.]go[.]kr
f8c71f34a6cfdc9e3c4a0061d5e395ffe11d9d9e77abe1a5d4b6f335d08da130	13/08/13 07:47	dril113[.]ncsc[.]go[.]kr
7564990506f59660c1a434ce1526b2aea35a51f97b8a490353eece18ec10b910	10/10/13 11:35	221[.]149[.]223[.]209
8b91cfd40529b5667bbdab970d8dba05fca0952fffba8ccbb1ad9549d204ba85	10/10/13 11:58	221[.]149[.]223[.]209
e20d0a8e1dec96ed20bd476323409f8f5c09531777207cfeda6b7f3573426104	13/07/14 11:43	dril113[.]ncsc[.]go[.]kr
7461e8b7416bf8878d20a696a27ccf378c93afc6c8f120840c3738b9508839d2	15/07/14 04:43	221[.]149[.]223[.]209
04e87e473d34974874dd0a5289433c95ef27a3405ba9ad933800b1b855e6e21a	15/07/14 04:45	221[.]149[.]223[.]209
caf4b03118e5c5580c67b094d58389ade565d5ae82c392bb61fc0166063e845a	12/08/14 06:52	drill14[.]kr[.]ncsc[.]go[.]kr
46fb5bcea417d7ff38edff7e39982aa9f89f890a97d8a0218b6c0f96a5e9bad2	12/08/14 06:52	drill14[.]kr[.]ncsc[.]go[.]kr
1ffa34f88855991bdc9a153e01c9e18074ba52a773f4da390c4b798df6e6dc4e	12/08/14 06:52	drill14[.]kr[.]ncsc[.]go[.]kr
fa5799c25b5ea2ecb24ee982a202e68aad77db7e6b18f37151fa744010f69979	12/08/14 06:52	drill14[.]kr[.]ncsc[.]go[.]kr

1e926d83c25320bcc1f9497898deac05dff096b22789f1ac1f63c46d2c1c16a7	12/08/14 06:52	drill14[.]kr[.]ncsc[.]go[.]kr
65d226469d6bdb1e7056864fe6d3866c8c72613b6b61a59547ef9c36eda177dd	10/07/15 11:51	.onion.city domains
0ea456fd1274a784924d27beddc1a5caa4aa2f8c5abdf86eb40637fe42b43a7f	10/07/15 11:51	.onion.city domains
b35b7a1b437d5998b77e10fdbf166862381358250cf2d1b34b61cf682157ff19	26/07/16 01:27	.onion.city domains
1e926d83c25320bcc1f9497898deac05dff096b22789f1ac1f63c46d2c1c16a7	27/07/16 04:46	.onion.city domains

Table 3: Hashes and C&C domains of typical OnionDog samples

The oldest samples from 2013 did not hide ownership of the C&C domains at all. From 2015 onwards, the cyber drills started to use .onion.city domains. This means that the actual callback addresses of the malware are hosted on Tor hidden servers. The compile dates of the samples are mostly in the summer and fall of 2013, 2014, 2015 and 2016.

Analyzing OnionDog Samples

There have been different sets of OnionDog samples throughout the years, but they are all related. The latest ones using .onion.city C&C domains go deep inside the affected system. They install a Windows service that sends basic information to the Tor hidden C&C domains. It can also download second-stage payloads from there.

The file with SHA256 hash "65d226469d6bdb1e7056864fe6d3866c8c72613b6b61a59547ef9c36eda177dd" is one of the OnionDog files from 2015 that connects to a .onion.city C&C domain. When executed it will open an HWP document as shown below:

Figure 1: Decoy document displayed by an OnionDog sample.

The title page of the decoy HWP document roughly translates to “Plan to check the performance of public discipline and code of conduct during summer vacation in 2015”. This hints that the malware is being used as part of a cyber drill that was held in the summer of 2015.

After displaying the HWP document it extracts and executes its first resource named 101 (SHA256:6dd79b5b9778dc0b0abefa26193321444236a1525d03227f150e6e968999fea5) in a temporary folder. Two other resources are then extracted: 103 and 111. For Windows versions prior to Vista (dwMajorVersion < 6), it injects its code into the *explorer.exe* process. For newer versions, it extracts the resources to temporary folders and executes then deletes them.

Figure 2: The three binaries within .rsrc section of the main dropper

It’s uncommon for real malware to print error messages, and the main dropper includes debug messages in case it doesn’t get the code injected into *explorer.exe* process:

Figure 3: Debug messages

101 (SHA256: 6dd79b5b9778dc0b0abefa26193321444236a1525d03227f150e6e968999fea5) is a dynamic-link library (DLL) that can bypass User Account Control (UAC) in order to execute the two other binaries created in the temporary folder.

103 (SHA256: 999c1d4c070e6817c3d447cf9b9869b63e82c21c6e01c6ea740fbed38b730e6e) installs a Windows service called either “Microsoft Display Agent” or “Windows 10 Upgrader”. All traces left are deleted using a batch file script.

This Windows service (SHA256: 19e3aa92bc16915d9f3ff17731caf43519169fddda4910ad5becb71ef87a29d5) will execute at a certain date (July 13, 2015) and download another executable from the C&C server. It also drops and runs another executable file (SHA256: fd03f3f65979ec7b8b6055f92f023b08f57c3095557d1f00d88f01f4d4cb46b7), which happens to be a cleaner program that uninstalls the service and removes all files created by the program, regardless of the current date. Though the OnionDog malware doesn’t do any real harm to the systems, it uses tricks of real malware and it is not clear why they're necessary for a cyber drill.

The 2013 samples with the hardcoded drill C&C servers, highlighted in the screenshot below, clearly convey they are part of a drill. These samples include a MessageBox that would present itself if it's run within a specific time range.

Figure 4: Older OnionDog samples show a pop-up when the sample is run within a certain time range

Figure 5: An OnionDog-related pop-up message showing the target is a victim of an Ulchi cyber drill

The pop-up roughly translates to: “[2013 Ulchi drill cyber threat response training] Please let your administrator know you are infected with malicious code.” Ulchi appears to refer to the Ulchi Freedom Guardian Drills, a joint military exercise between South Korea and the United States that dates back to 1976. The exercise is annually held from August to September. We have listed the specific dates they were conducted from 2010 to 2016.

Start	**End**
August 22, 2016	September 2, 2016
August 17, 2015	August 28, 2015
August 18, 2014	August 29, 2014
August 19, 2013	August 30, 2013
August 20, 2012	August 31, 2012
August 16, 2011	August 26, 2011
August 16, 2010	August 26, 2010

Table 4: Dates of Ulchi Freedom Guardian drills

These dates correspond with the time ranges where the OnionDog samples were active. According to the United States Army's websiteopen on a new tab, the Ulchi Freedom Guardian Exercise helps guard cyber networks for communications. This shows that during the months of August and September, it is likely that some of the alerts, messages, and other indicators may be part of an exercise to help prepare high-profile South Korean targets for a real cyberattack. In military terms, what went on is a live-fire exercise—with malware as munitions that go deep and download additional malware components into computer systems that serve as a practice area or battleground.

Dangers of using real malware in exercises

Based on the data we have collected, the malware samples referred to as OnionDog have all been part of a cyber drill that is conducted every year. Protections have been put in place to limit the malware from doing anything outside of the time window of the exercises themselves. While the malware really doesn't do anything nefarious, some of the newer samples look like invasive penetration tests into systems—and they use a lot of tricks. There are risks of using real malware during security drills.

We have found 200 unique OnionDog samples in the wild. This means that the specific tools and methodologies used in the drill are in the public arena and can be researched by bad actors as well. It's possible that these actors could pick up some of the behavior and mimic it, causing Incident Response teams to think that they might be responding to the drill, and take less care responding to it.

The dangers and risks of using live malware, or even simulated malware, lie in the ability to contain them. In small exercises, for instance, if the person responsible for the malware goes out for the day for any reason—there's nothing to help stop it if things go out of control. Penetration testing tools such as Threatcareopen on a new tab, which is based off vSploit from Metasploit, can help with testing the capabilities of your incident response team to see their effectiveness via simulated communications of known threats.

This is not limited to large-scale, multi-country exercises like the Ulchi Freedom Guardian. These kinds of exercises are actually conducted by enterprises worldwide to test their preparedness in the event of an actual attack.

Attribution is hard

While OnionDog received limited media attention, it still made it to the media. Even limited media exposure on mistakenly attributed cyberattacks could lead to wrong conclusions and escalate tensions. While it is very easy to get caught up in the need to identify the country behind an attack, shown here are some of the reasons why Trend Micro did not go to that level of attribution. In this case, what looked to be a very targeted attack against specific sectors was an exercise to test the response of the nation, and that of the specific sectors being targeted.

The list of SHA256 is in this appendixopen on a new tab.
