Stonefly: North Korea-linked Spying Operation Continues to Hit High-value Targets

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage

Threat Hunter TeamSymantec

The North Korean-linked Stonefly group is continuing to mount espionage attacks against highly specialized engineering companies with a likely goal of obtaining sensitive intellectual property.

Stonefly specializes in mounting highly selective targeted attacks against targets that could yield intelligence to assist strategically important sectors such as energy, aerospace, and military equipment. Virtually all of the technologies it appears to be interested in have military as well as civilian uses and some could have applications in the development of advanced weaponry.

History of ambitious attacks

Stonefly (aka DarkSeoul, BlackMine, Operation Troy, and Silent Chollima) first came to notice in July 2009, when it mounted distributed denial-of-service (DDoS) attacks against a number of South Korean, U.S. government, and financial websites.

It reappeared again in 2011, when it launched more DDoS attacks, but also revealed an espionage element to its attacks when it was found to be using a sophisticated backdoor Trojan (Backdoor.Prioxer) against selected targets.

In March 2013, the group was linked to the Jokra (Tojan.Jokra) disk-wiping attacks against a number of South Korean banks and broadcasters. Three months later, the group was involved in a string of DDoS attacks against South Korean government websites.

In recent years, the group's capabilities have grown markedly and, since at least 2019 Symantec has seen its focus shift solely to espionage operations against select, high-value targets. It now appears to specialize in targeting organizations that hold classified or highly sensitive information or intellectual property. Stonefly's operations appear to be part of a broader North Korean-sponsored campaign to acquire information and intellectual property, with Operation Dream Job, a more wider-ranging trawl across multiple sectors, being carried out by another North Korean group, Pompilus.

Latest target

The most recent attack discovered by Symantec, a division of Broadcom Software, was against an engineering firm that works in the energy and military sectors. The attackers breached the organization in February 2022, most likely by exploiting the Log4j vulnerability (CVE-2021-44228) vulnerability on a public-facing VMware View server. The attackers then moved across the network and compromised 18 other computers.

17 hours later: Shortly after compromising the initial server, the attackers installed an updated version of Stonefly's Backdoor.Preft malware (aka Dtrack, Valefor). The attackers then used a masqueraded version (file name: pvhost.exe) of PuTTY's PSCP command line application, presumably to exfiltrate data from the infected machine. Shortly after PSCP was executed, the credential-dumping tool Mimikatz (masquerading under the file name pl.exe) was run.

Day 2: Malicious activity resumed when 3proxy tiny proxy server, a publicly available proxy tool (file name: svhost.exe) was executed. Use of this tool continued for the next four days. A second suspected proxy tool was installed two days into this four day period (file name: tapi.exe). Several hours afterwards, a copy of the Preft backdoor (file name: svchost.exe) was installed. Two days later, WinSCP, an open-source SSH file-transfer tool was used, presumably to exfiltrate or upload data to the compromised computer.

Day 3: The next phase of the intrusion began on the following day, when Preft was executed and the attackers began moving latterly across the organization's network, using Invoke-TheHash, a publicly available PowerShell pass-the-hash utility (file name: rev.ps1), and wmiexec.py, a publicly available Impacket tool used to run WMI commands (file name: notepad.exe).

Updated Preft backdoor

The attackers used an updated version of Stonefly's custom Preft backdoor. Analysis of the backdoor revealed that it is a multistage tool:

Stage 1 is the main binary. A python script is used to unpack the binary and shellcode.

Stage 2 is shellcode. It performs the following actions:

- Sleeps for 19,999 seconds, probably in an attempt to evade sandbox detection
- Opens a mutex, with the name specified in the Stage 3 shellcode
- Instead of loading an executable file, it starts Internet Explorer (iexplore.exe) or explorer.exe and injects the Stage 3 shellcode into either. It sets up a named pipe ("\.\pipe\pipe") for communication. The file name of the main binary is sent over the pipe.

Stage 3 is more shellcode.

Stage 4 is the payload. It is an HTTP remote access tool (RAT) that supports various commands, including:

1. Download (Download a file and save locally)
2. Upload (Upload a file to a C&C server)
3. Set Interval (Change C&C server query interval - in minutes)
4. Shell Execute (Execute a command in the shell)
5. Download Plugin
6. Update (Download a new version and replace)
7. Info (Return debug information about the current infection)
8. Uninstall
9. Download Executable

The malware can support four different kinds of plugins: executable files, VBS, BAT, and shellcode. It supports three different persistence modes: Startup_LNK, Service, Registry, and Task Scheduler.

Custom information stealer

Along with the Preft backdoor, Stonefly also deployed what appears to be a custom developed information stealer (infostealer). Analysis of this malware revealed that it is a three-staged threat. The main binary extracts and decrypts the encrypted shellcode with a modified RC4 algorithm.

Stage 2 is shellcode which retrieves the payload and decrypts it with the same modified RC4 algorithm. The decrypted payload is an executable file that is loaded in-memory. It is designed to search the infected computer for files using pre-configured parameters. These are then copied to temporary files before being copied to a single .zip file and the temporary files are removed. The ZIP file path is %TEMP/~[XXXXXXXX].tmp, where XXXXXXXX is a simple hash of the computer name (eight uppercase hex digits).

Curiously, this ZIP file is not automatically exfiltrated. It is possible that the exfiltration functionality was removed and the attackers planned to use an alternative means of exfiltration.

High-value targets

While Stonefly's tools and tactics continue to evolve, there are some common threads between this recent activity and previous attacks, such as its ongoing development of the Preft backdoor and heavy reliance on open-source tools.

The group's capabilities and its narrow focus on acquiring sensitive information make it one of the most potent North Korean cyber threat actors operating today.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file is available to us, Symantec Endpoint products will detect and block that file.

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.