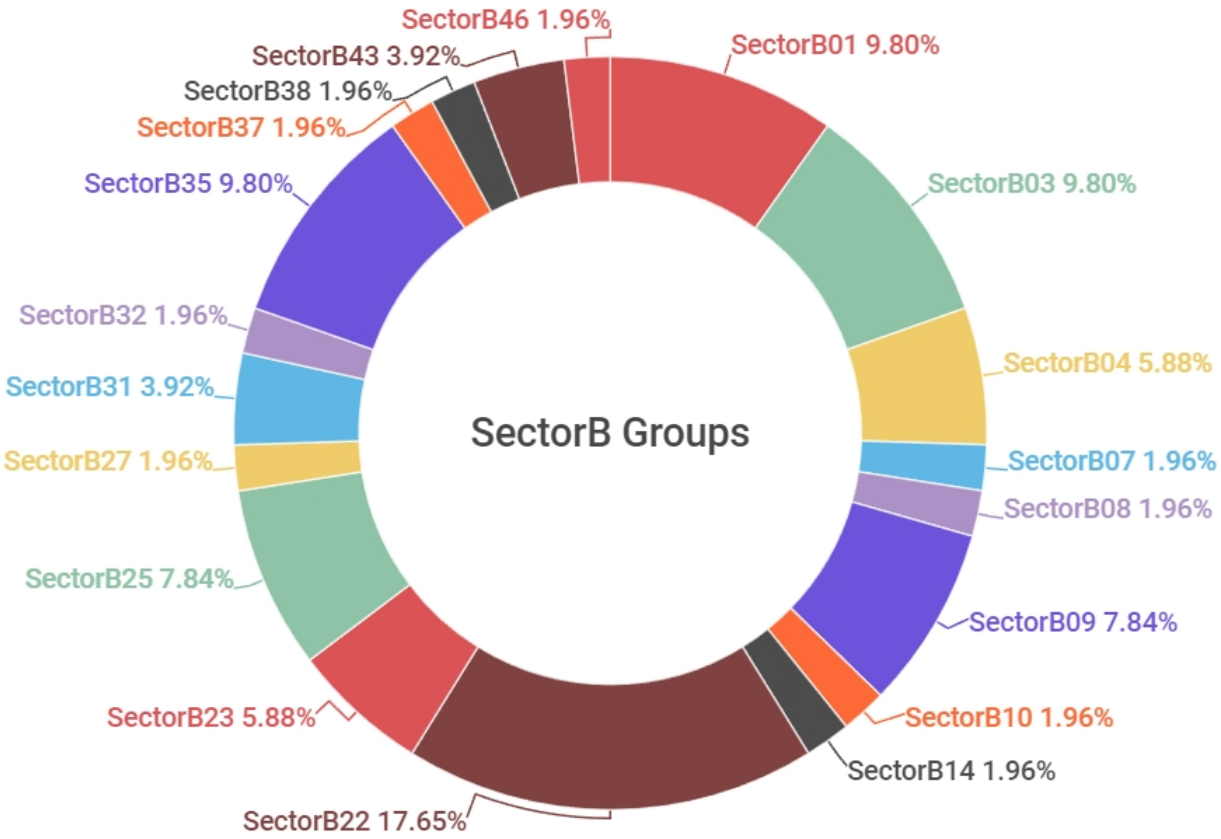
Hacking activity of SectorB Group in 2021

redalert.nshc.net/2022/04/14/hacking-activity-of-sectorb-group-in-2021/

Chinese government supported hacking group SectorB

SectorB is a hacking group supported by the Chinese government in which 48 subgroups have been identified as of now. They carry out hacking activities targeted on the entire world with the purpose of collecting advanced information regarding political, diplomatic activities of governments. The subgroups show a trend of sharing malwares or vulnerabilities among themselves for their hacking activities.

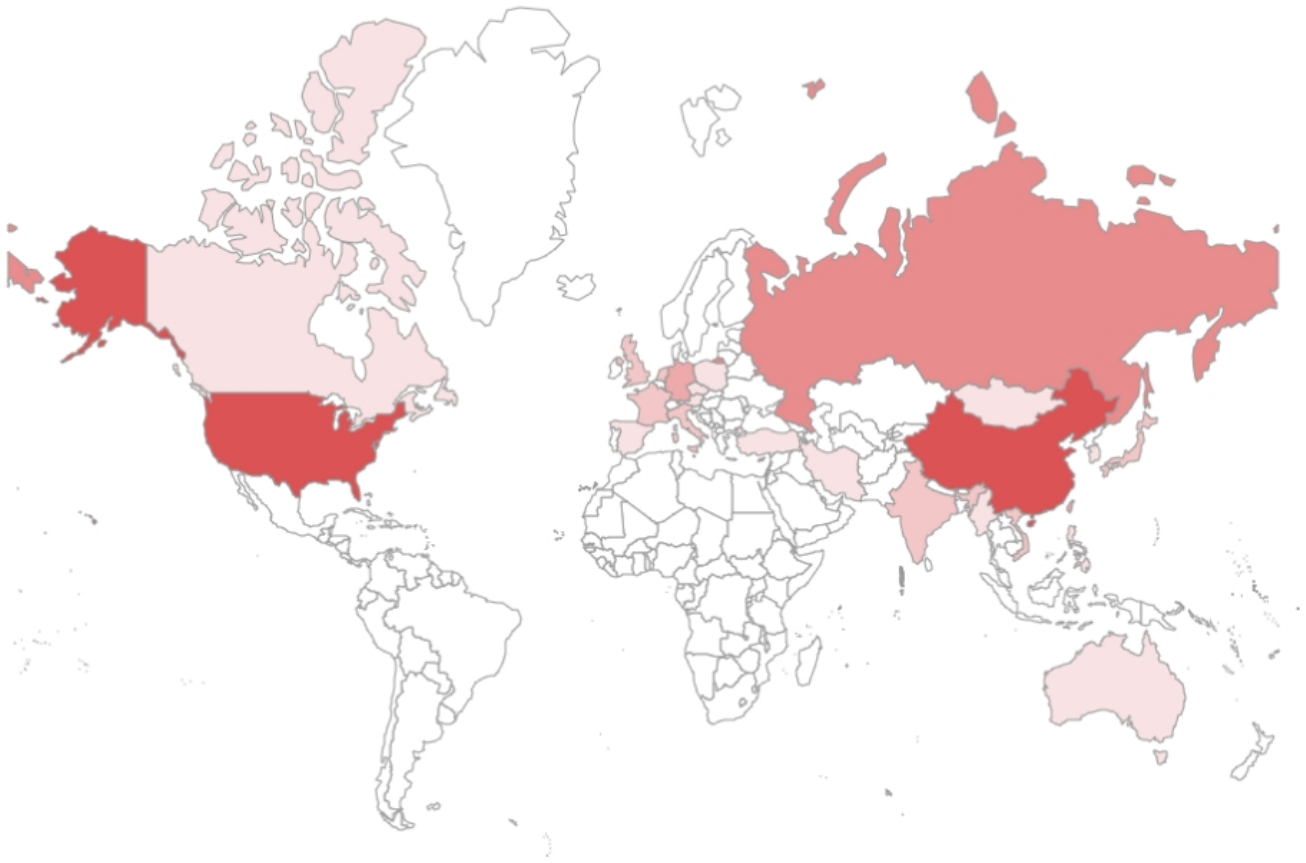


[Figure 1 : SectorB subgroup activities identified in 2021]

They targeted their attacks on workers of government institutions and national defense to collect advanced information and were identified to have been expanding their targets to national finances and IT industries related to “One Belt and One Road”, the Chinese diplomatic and economic policy.

Among the 48 subgroups of SectorB, hacking groups that showed most activities in 2021 was SectorB22 group, followed by SectorB01 group, SectorB03 and SectorB35 groups.

The following figure is the map of targeted countries of SectorB groups in 2021. A darker shade of red represents a higher number of attacks.



[Figure 2 : Map of mainly targeted countries by SectorB groups in 2021]

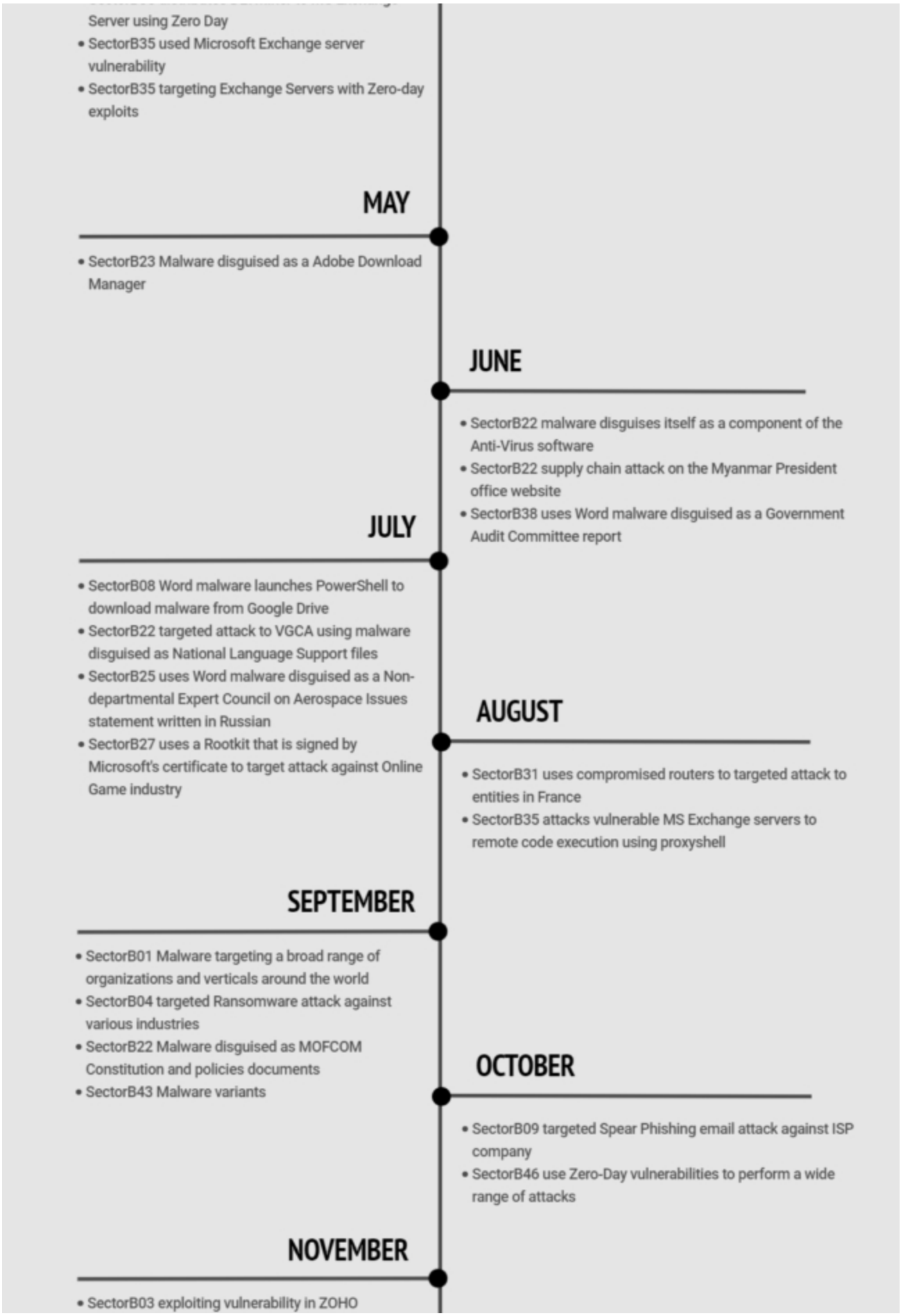
From the results, it could be deduced that SectorB carried out the greatest number of hacking activities targeted on Hong Kong, a neighboring country of China, followed by the United States and Russia.

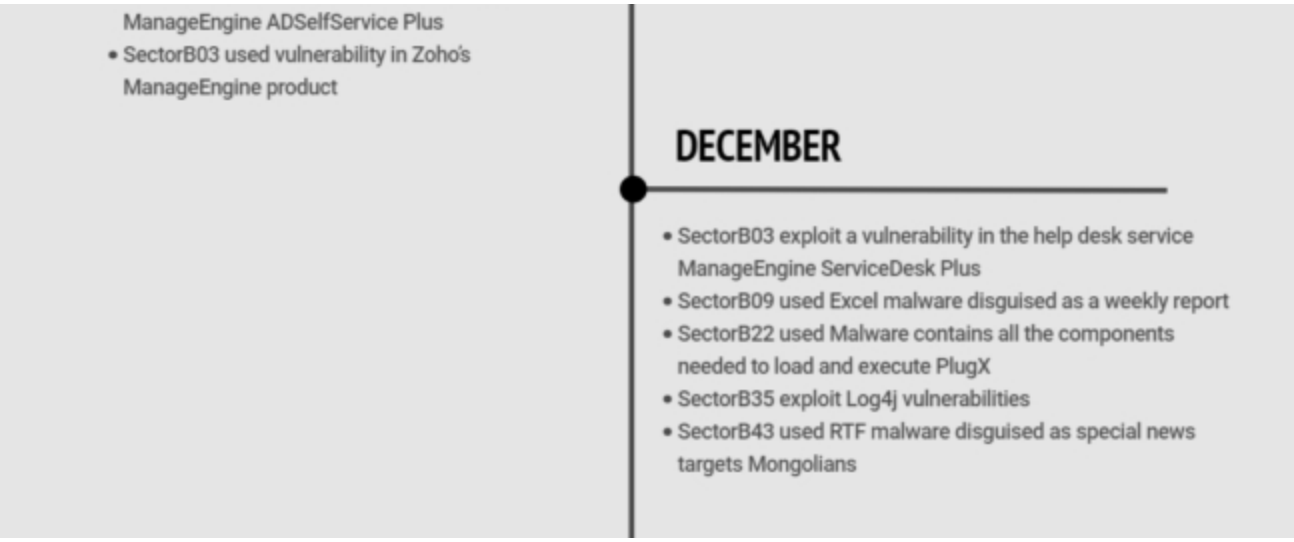
Hong Kong has been independent of China in terms of political and economic fields, but recently, democracy movements have emerged in the country against introduction of China's socialist political system. With regards to this, some of the hacking groups supported by the Chinese government launched hacking activities targeted on Hong Kong's liberalist personnel for surveillance purposes.

Additionally, China launched hacking attacks on Russian research institutions with the purpose of stealing advanced science technologies related to latest military technologies such as aircraft carriers and jet planes.

Activity details of SectorB groups in 2021

The following is the timeline and monthly activity details of hacking activities by SectorB groups identified in 2021.


Server using Zero Day
• SectorB35 used Microsoft Exchange server vulnerability
• SectorB35 targeting Exchange Servers with Zero-day exploits
MAY
• SectorB23 Malware disguised as a Adobe Download Manager
JUNE
• SectorB22 malware disguises itself as a component of the Anti-Virus software
• SectorB22 supply chain attack on the Myanmar President office website
• SectorB38 uses Word malware disguised as a Government Audit Committee report
JULY
• SectorB08 Word malware launches PowerShell to download malware from Google Drive
• SectorB22 targeted attack to VGCA using malware disguised as National Language Support files
• SectorB25 uses Word malware disguised as a Non-departmental Expert Council on Aerospace Issues statement written in Russian
• SectorB27 uses a Rootkit that is signed by Microsoft's certificate to target attack against Online Game industry
AUGUST
• SectorB31 uses compromised routers to targeted attack to entities in France
• SectorB35 attacks vulnerable MS Exchange servers to remote code execution using proxyshell
SEPTEMBER
• SectorB01 Malware targeting a broad range of organizations and verticals around the world
• SectorB04 targeted Ransomware attack against various industries
• SectorB22 Malware disguised as MOFCOM Constitution and policies documents
• SectorB43 Malware variants
OCTOBER
• SectorB09 targeted Spear Phishing email attack against ISP company
• SectorB46 use Zero-Day vulnerabilities to perform a wide range of attacks
NOVEMBER
• SectorB03 exploiting vulnerability in ZOHO



[Figure 3 : Timeline of main activities by SectorB group in 2021]

January Hacking Activities

Among the SectorB groups supported by the Chinese government, activities by a total of 4 hacking groups were identified this January, and the groups are SectorB01, SectorB07, SectorB22 and SectorB31 groups.

SectorB01 group was found to be active in China, Hong Kong, and the Philippines. In this activity, user mode Rootkit malwares created to attack Linux systems were identified.

SectorB07 group was found to be active in China and Brazil. The attackers used MS Word document malwares disguised as resumes, using the template injection technique for their attacks.

SectorB22 group was found to be active in Australia. In this activity, a modified PlugX malware used by the attackers were identified.

SectorB31 group was found to be active in Germany. In this activity, IP addresses used in hacking activities targeted on Germany's public and governmental institutions were identified.

February Hacking Activities

Among the SectorB groups supported by the Chinese government, activities by a total of 3 hacking groups were identified this February, and the groups are SectorB04, SectorB22 and SectorB32 groups.

SectorB04 group was found to be active in Japan, Turkey, and the United States. The main targets of this activity were Japanese corporations located in Japan or having overseas branches, and the attacker used vulnerabilities of SSL-VPN as their initial access methods.

SectorB22 group was found to be active in Taiwan, Hong Kong, Sri Lanka, Uganda, Poland, and Canada. The attackers intruded the update process of NoxPlayer, an Android emulator, to lead the users to download update programs containing malicious functions.

SectorB32 group was found to be active in Russia. LNK format malwares were identified in this activity, which carries out various commands through PowerShell upon execution. The LNK file was disguised as a regular program using the file name ‘adobeagent.lnk’.

March Hacking Aactivities

Among the SectorB groups supported by the Chinese government, activities by a total of 7 hacking groups were identified this March, and the groups are SectorB01, SectorB03, SectorB10, SectorB22, SectorB23, SectorB25 and SectorB35 groups.

SectorB01 group was found to be active in India, Taiwan, the United States, the Philippines, Indonesia, and Iran. The group attacked main infrastructures such as India’s electricity providing power plants, and multiple domains deduced to have been used in the attacks were identified. During this period, attacks using vulnerabilities of MS Exchange were found, and along with the previously used ShadowPad malware, various tools such as Mimikatz were found to have been used by SectorB01 groups in the attack.

SectorB03 group was found to be active in Hong Kong, Taiwan, China, and the United States. The group also used MS exchange server vulnerabilities, along with SysUpdate backdoor, tools to search NETBIOS name servers and tools to serve HTTP Tunneling functions.

SectorB10 group used the vulnerabilities of MS exchange server, and malwares written in Delphi that were used by the group in the past were identified together.

SectorB22 group was found to be active in Pakistan and Vietnam. The group also used MS exchange server vulnerabilities to attack public resource providing companies. In this attack, they used malwares disguised as installation programs of Adobe Flash Player.

SectorB23 group was found to be active in Germany. The group also used MS exchange server vulnerabilities for their attacks, and PlugX malware was identified in the attack as well.

SectorB25 group was found to be active in Netherlands and Russia. The group also used MS exchange server vulnerabilities for their attacks targeted on cybersecurity consulting companies in Eastern Europe.

SectorB35 group was found to be active in India, Italy, Canada, Iran, Belgium, the United States, Spain, Switzerland, Finland, Arab Emirates, Israel, Netherlands, Poland, Austria, Turkey, Germany, Hungary, China, and South Korea. The group used MS exchange server vulnerabilities to disseminate Cryptomining malwares. They used the same vulnerability with the intent to disseminate ransomware and botnet malwares as well.

April Hacking Activities

Among the SectorB groups supported by the Chinese government, activities by a total of 5 hacking groups were identified this April, and the groups are SectorB09, SectorB14, SectorB23, SectorB25 and SectorB37 groups.

SectorB09 group was found to be active in Taiwan and Germany. The group used PLEAD malwares in ELF (Executable and Linkable Format) format to collect system information from infected systems and used OpenSSL to communicate with the encrypted C2 server.

SectorB14 group was found to be active in Germany, Spain, China, Hong Kong, Slovakia, and Vietnam. The group used MS word documents with various subjects such as COVID-19, and the macro inserted in the document executes a normal executing program, a malware in DLL format, a normal document, and a CAB file including the encoded data. In the final stage, the normal executable program loads the malicious DLL file and communicates with the C2 server.

SectorB23 group was found to be active in Nepal, Russia, Macedonia, Australia, Kazakhstan, Switzerland, Ukraine, the United States, Afghanistan, Italy, India, and Czech Republic. The group used MS exchange server vulnerabilities to attack various industries. They distributed PlugX malwares in the infected systems, and most of the domains used in the activity were registered using a specific hosting company.

SectorB25 group was found to be active in Russia, the United States and Mongolia. The group used spear phishing emails attached with RTF (Rich Text Format) files with vulnerabilities and served hacking activities targeted on a submarine designing company in Russia.

SectorB37 group was found to be active in Czech Republic, Bangladesh, and China. The group used MS word documents with macro scripts inserted for their attacks, disguised as a document about expressway of a certain country in Southeast Asia. The VBS file created by the macro script was encoded using Microsoft script encoder and uses WMI service to collect system information and serves encrypted C2 communications upon execution of the file.

May Hacking Activities

Among the SectorB groups supported by the Chinese government, activities by a total of 1 hacking group was identified this May, and the group was SectorB23 group.

SectorB23 group was found to be active in China, Hong Kong, and Italy. The group used malwares written through Pyinstaller, and disguised the file as an Adobe Flash Player installation file. Upon execution of the malware, communication with C2 server is established and additional files related to network tunneling are downloaded.

June Hacking Activities

Among the SectorB groups supported by the Chinese government, activities by a total of 2 hacking groups were identified this June, and the groups are SectorB22 and SectorB38 groups.

SectorB22 group was found to be active in Myanmar, Japan, Netherlands, Taiwan, the Philippines, China, Singapore, Thailand, and the United States. Supply chain attacks targeted on the official website of Myanmar's president was identified, and ZIP format malwares were disseminated on the website.

SectorB38 group was found to be active in Vietnam and China. The group used MS word malwares with reports by audit committee of the Vietnamese government as the subject, which uses the template injection technique to download RTF (Rich Text File) including MS office equation editor vulnerabilities from a remote server.

July Hacking Activities

Among the SectorB groups supported by the Chinese government, activities by a total of 4 hacking groups were identified this July, and the groups are SectorB08, SectorB22, SectorB25 and SectorB27 groups.

SectorB08 group was found to be active in Taiwan. The MS word malware identified in this activity contained a macro script, which, in the final stage, executes PowerShell to download malwares uploaded in Google drives, and uses normal WinRAR programs to extract the downloaded files.

SectorB22 group was found to be active in Vietnam, South Korea, and China. In this activity, malware like the malware used in supply chain attacks on the Vietnamese government certification authority in December 2020 was identified. Malwares identified in these two activities have a similar code structure, Rich Header hash, PDB (Program Database) path, and both uses service DLL files disguised as NLS (National Language Support) extension.

SectorB25 group was found to be active in Russia, Japan, France, and England. In this activity, RTF documents written in Royal Road were found, and the document disguised as "Statement by non-departmental expert committee on Aerospace" contains equation editor vulnerabilities.

SectorB27 group was found to be active in the United States, Russia, and China. In this activity, Netfilter Rootkit malware signed by Microsoft were found, and the hacking group was deduced to have created the malware to target on online game industry. The malware was signed and disseminated using Microsoft and other companies' certifications.

August Hacking Activities

Among the SectorB groups supported by the Chinese government, activities by a total of 2 hacking groups were identified this August, and the groups are SectorB31 and SectorB35 groups.

SectorB31 group was found to be active in France and China. In this activity, attacks affecting numerous institutions in France were identified. Various custom opensource tools were used to steal information, and ELF malwares were used to make use of the router's vulnerabilities.

SectorB35 group was found to be active in Spain, Ireland, Italy, and England. The group used ProxyShell vulnerabilities often used against Microsoft exchange servers, and used CVE-2021-31207, CVE-2021-34523 and CVE-2021-34473 vulnerabilities to execute their remote code in the Microsoft exchange servers.

September Hacking Activities

Among the SectorB groups supported by the Chinese government, activities by a total of 4 hacking groups were identified this September, and the groups are SectorB01, SectorB04, SectorB22 and SectorB43 groups.

SectorB01 group was found to be active in Canada, India, England, France, Austria, Luxembourg, Hong Kong, Bahrain, the United States, South Korea, and Singapore. The group targeted their attacks on workers of various fields such as government institutions, academy, religion, and IT. They used .NET loaders to load malware in the memory of infected user system to serve their attacks.

SectorB04 group was found to be active in England, the United States, Hong Kong, Germany, France, and India. The group took advantage of vulnerabilities to launch attacks on various industries such as manufacturing, finance, travelling and tourism. They used MS exchange serves to connect to the target's network and continuously monitors their victims.

SectorB22 group was found to be active in Japan, England, and the United States. The group used documents disguised as China's national meeting and constitutional laws to serve their attacks. The malware delivered in the form of compressed files used DLL side loading techniques to load malicious DLL on a normal program to serve their functions, to avoid suspicion from users.

SectorB43 group was found to be active in Russia. In this activity, a malware was found to be continuously updated by a certain user at a specific time interval. New updates are added to the malware in every update and serves various RAT (Remote Administration Tool) functions.

October Hacking Activities

Among the SectorB groups supported by the Chinese government, activities by a total of 2 hacking groups were identified this October, and the groups are SectorB09 and SectorB46 groups.

SectorB09 group launched attacks on a certain company in this activity and used malwares using the MFC (Microsoft foundation class) libraries. The malware contained functions to collect information from the infected system and to download and execute additional malwares.

SectorB46 group was found to be active in Russia. The group used Zero-day vulnerabilities in the Window Kernel drive to launch attacks targeted on workers of defense industries and diplomatic institutions.

November Hacking Activities

Among the SectorB groups supported by the Chinese government, activities by a total of 1 hacking group was identified this November, and the groups was SectorB03 group.

SectorB03 group was found to be active in China, Czech Republic, and the United States. The group used vulnerabilities of password management solutions to distribute payload containing malwares to workers in various industries such as defense industry, energy, education, and consulting services.

December Hacking Activities

Among the SectorB groups supported by the Chinese government, activities by a total of 5 hacking groups were identified this December, and the groups are SectorB03, SectorB09, SectorB22, SectorB35 and SectorB43 groups.

SectorB03 group was found to be active in Hong Kong, Denmark, and Netherlands. The group used vulnerabilities of corporate IT operation and service managing software to launch their attacks on medical, electronics and IT industries.

SectorB09 group was found to be active in China. The group used MS excel format malwares disguised as weekly work reports in this activity.

SectorB22 group was found to be active in Vietnam, Taiwan, Myanmar, and Russia. The group used malwares in compressed file formats disguised as Adobe library files in this activity.

SectorB35 group was found to be active in the United States. The group used RCE (Remote Code Execution) vulnerabilities that allows one to execute unknown codes in the framework of Apache software.

SectorB43 group was found to be active in Mongolia. In this activity, the group used RTF (Rich Text File) format malwares containing equation editor vulnerabilities, which were disguised as featured news.

The full report detailing each event together with IoCs (Indicators of Compromise) and recommendations is available to existing NSHC ThreatRecon customers. For more information, please contact RA.global@nshc.net