Committee: Cybersecurity

Main Sponsor: Norway

Signatories: Russian Federation, Poland, France, Costa Rica, China, Canada, Sweden, USA

Topic: Increase in PowerShell attacks and other file less malware attacks

General Assembly,

Deeply concerned with the malicious malware attacks of Windows PowerShell,

Fully aware that these attacks are based off using tools that are built into the software such as PowerShell instead of using installations of a software on the target's machine – making it fileless,

Welcoming all means of protection that will protect against these fileless attacks such as Cybereason,

1. Recommends the use of Cybereason which distinguishes between both legitimate and malicious PowerShell operations:
    a. Reviews action taken by the code running the PowerShell engine,
    b. Asks behavioral questions in order to identify the fileless attacks,
    c. Uses key requirements such as:
        i. Addressing all versions of PowerShell,
        ii. Handling all types of invocation (command line, interactive, script loading of System.Management.Automation.dll),
        iii. Not affecting or interfering with user experience,
        iv. Notifying analysts about attacks and providing details – who's involved and what machines are involved;
2. Notes that file less attacks do not create a file which makes file-based detections ineffective therefore should instead:
    a. Conduct security hygiene checks on applications to search for vulnerabilities,

    b. Use application control to prevent internet browsers from spawning script interpreters,
    c. Invest in MDR services to look for malicious application behavior,
3. Suggests the utilization of INTERPOL operated teams of apprehended cyber criminals that survey and assist in the development of antivirus software by:
    a. Performing mock hacks on a nation's security system as most of the antiviral software's have small holes in the system that can allow a hacker access into the protected computer,
    b. Recognizing If a flaw is found in the system, then deploying certified group of UNIT members that will work to patch the system to ensure that it is up to international standards,
4. Recommends the UN to promote a policy of training for all corporations which utilize or plan on utilizing Microsoft's Powershell;
    a. Training would be in the form of a short class for current and new employees about how to prevent the infiltration of file less malware operations.
5. Creates a Cyber Response Team (CRT), consisting of a team of professionals in the cyber-field, comprised of qualified officials from every nation to identify perpetrators of attacks, and to prevent future attacks:
    a. Rotating panel of experts in the academics of data sciences, informational studies, and international security,
    b. Works with existing task forces of trained personnel to:
        i. Establish zonal observatories in areas of defense and security,
        ii. Study and observe the source and process of cyber-attacks,
        iii. Collaborate with Ministries of Defense to develop cyber security branches;
6. Calls for the creation of a failsafe which would include:
    a. Layering security walls that will be able to immediately shut down a system when a hacker is detected – each layer will be used if one were to be infiltrated,
    b. Redirecting the information to this failsafe as a hacker is attempting to infiltrate these layers of security,

    c. Will be implemented through the help from FIRST or Forum of Incident Response and Security Teams because of:
        i. Its wide variation of computer security incident response teams that can range from government to commercial or educational organizations,
        ii. Its ability to act quickly and respond to incidents;
7. Calls upon the creation of an international watchdog called the United Nations Cybercrime Defense and Supervision Agency (UNCDSA) under the CRIPT Treaty:
    a. The committee will supervise and look over cyber-crimes committed by both individuals and governments under a certain severity,
    b. UNCDSA will enforce international laws unto perpetrators of international cyber laws, does not supervise sovereign states without evidence, and will supervise countries and individuals that are accused of cybercrime;
8. Calls for consumers to be educated on protecting themselves against file less malware attacks by:
    a. Regularly check security logs for the amounts of data leaving the network which could potentially be going to a hacker,
    b. Updating software regularly;
9. Further recommends that organizations also take preventative steps from these file less malware attacks such as:
    a. Patching systems to avoid vulnerabilities,
    b. Limit administrative tools such as PowerShell and should only be used based on reasonable need but otherwise should be disabled,
    c. Investing in products from reputable companies that add protection against these file less malware attacks such as:
        i. Symantec,
        ii. Trend,
        iii. McAfee,
        iv. Kaspersky,
    d. Using application controls on endpoint computers that will ensure that only approved applications are used;
10. Suggests two-part plan to protect citizens from the occurrence of a cyber-attack:

a. The first step is to have each country identify which companies are most important to the economy - these important companies would purchase standardized cyber insurance policies,
b. Each country would then securitize its insurance pool on the private market - these pools would help companies reach a higher level of coverage and provide high risk insurance.

11. Expresses its hope for collaboration with domestic and private sector businesses, as well as civil society, in order to educate the necessity for protective data and preparedness against cyber-attacks:
    a. Private-public partnership with top tier companies to promote temporary campaigns through advertisements and features that will educate its current and prospective customers on the importance of cybersecurity and preparedness against cyberwarfare,
    b. Hold lessons and workshops in educational institutions to achieve a 40% increase in firewall programming and the related career fields,
    c. Collaborate with the Ministries of Defense in willing states to develop a potential cyber security branch,
    d. Help establish zonal observatories in each area of defense and security.