Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City

ACG-CYBER SECURITY BULLETIN NR 199

ACG-CSB 110520190

Reference Number ACG-CSB 110520199

Beware of LokiBot Malware

The following information was obtained from different cyber security sources for notification to all parties concerned pursuant to the mandate of the Philippine National Police Anti-Cybercrime Group (PNP ACG) and classified as “Restricted” pursuant to the PNP Regulation 200-012 on Document Security and Impact Rating as high based on PNP Information Communication Technology (ICT) Security Manual s.2010-01 p. 22 and p.129.

SUMMARY

LokiBot also known as Lokibot, Loki PWS, and Loki-bot—employs Trojan malware to steal sensitive information such as usernames, passwords, cryptocurrency wallets, and other credentials.

Lokibot can also create a backdoor into infected system to allow an attacker to install additional payloads.

Malicious cyber actors typically use LokiBot to target Windows and Android operating systems and distribute the malware via email, malicious websites, text, and other private messages.

LokiBot is a dangerous Trojan, which drops malicious objects all over the system. It can not only delete files, but also hijack registries, turn core processes idle, block anti-virus, and perform other tasks that are not restored after Trojan infection.

It usually infiltrates devices using malicious phishing emails, which are massively sent by bots employed by hackers or can be downloaded as a fake application from third-party websites. LokiBot Trojan can attack Windows and Android users It is difficult to determine what the collected data is used for, since LokiBot is not particularly advanced malware. Nevertheless, it can cause serious problems for the user. Fortunately, most reputable anti-virus/anti-spyware suites are capable of detecting and removing LokiBot. Therefore, we strongly advise you to have this software installed and running at all times. You are also advised to periodically run full system scans to check for any infections that have found their way into your system.

In addition to prevent this situation, be very cautious when browsing the Internet and downloading/installing software. Think twice before opening email attachments. If the file seems irrelevant or has been received from a suspicious/unrecognizable email address, do not open it. These emails should be deleted immediately, without reading. Furthermore, download your software from official sources only, using direct download links. Third party downloaders/installers often include rogue applications that can cause chain infections, and thus should never be used. Download Android applications from Google Play only. In addition, be very cautious - we strongly advise you to read the user reviews and see if there are any negative responses although applications in Google Play are scanned before being posted, there still are some that are classed as rogue.

All PNP personnel as well as the public are advised to be aware of Lokibot Malware to avoid being a victim of cybercrime:

RECOMMENDATION

The public are advised to follow these tips in order to prevent being victimized of Lokibot malware, to wit:

- Download software from official sources;
- Scan all downloaded from the internet prior to executing;
- Maintain up-to-date antivirus signatures and engine;
- Enforce a strong or multifactor authentication and password; and
- Change your passwords regularly;
- Keep operating system patch updated.

For additional information, please refer to the following websites:

- https://www.2-spyware.com/remove-lokibot-virus.html
- https://us-cert-.cisa.gov/ncas/alerts/aa20-259a
- https://arstechnica.com/information-technology/2020/09/lokibot-the-malware-that-steals-your-most-sensitive-data-is-on-the-rise/
- https://www.zdnet.com/article/new-lokibot-trojan-malware-campaign-comes-disguised-as-a-popular-game-launcher/

POINT OF CONTACT

Please contact **PMAJ JOSEPH ARVIN L VILLARAN**, Police Communication Relation thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 7230401 local 3562 for any inquiries related to this CYBER SECURITY BULLETIN.