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 252

ACG-CSB 060622252

Reference Number ACG-CSB 060622252

Understanding the Risk of GameOver Zeus 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

GameOver Zeus (GOZ), a variant of the Zeus family of bank credential-stealing malware, uses a decentralized network infrastructure of compromised personal computers and web servers to execute command-and-control. 0GOZ, which is often propagated through spam and phishing messages, is primarily used by cybercriminals to harvest banking information, such as login credentials, from a victim’s computer. Infected systems can also be used to engage in other malicious activities, such as sending spam or participating in distributed denial-of-service (DDoS) attacks.

Prior variants of the Zeus malware utilized a centralized command and control (C2) botnet infrastructure to execute commands. Centralized C2 servers are routinely tracked and blocked by the security community. GOZ, however, utilizes a P2P network of infected hosts to communicate and distribute data, and employs encryption to evade detection. These peers act as a massive proxy network that is used to propagate binary updates, distribute configuration files, and to send stolen data. Without a single point of failure, the resiliency of GOZ’s P2P infrastructure makes takedown efforts more difficult.

The botnet is primarily used to steal large sums of money through fraud by taking over thousands of banking customers' banking sessions. These fraudulent methods are performed in real time. Additionally, the cyber criminals are crafty and will often distribute the malware via email that looks like an invoice, ultimately tricking the customer into thinking it is from their bank. They are also targeting HR departments through Monster and CareerBuilder in an attempt to set up fake employees and access baking data that way. Once the deed is done the virus has infected the computer and waits until the user accesses their banking website. Gameover then identifies and intercepts their online session using a technique commonly known as man-in-the-browser (MITB). The malware also has the ability to bypass two-factor authentication and can display malicious banking security messages to weasel out secure information to authorize transactions and fraudulently claim their victim's money.

The end goal of the Gameover Zeus group is to make a profit from the fraudulent information they receive from the botnet. The P2P Zeus crew primarily makes a profit from the botnet through large Automated Clearing House (ACH) transactions and wire transfers. In order for this malware ring to function the gang must siphon funds from compromised bank accounts and work with other cyber criminals to complete the transfers. Just like drug cartels, these accomplices are known as money mules and are often located in the same areas as the victims. This reduces the risk of detection and allows them to complete the transaction much more smoothly.

RECOMMENDATION

All PNP personnel as well as the public are advised to follow these tips to avoid being a victim of Revil Ransomware:

- **Use and maintain anti-virus software** - Anti-virus software recognizes and protects your computer against most known viruses. It is important to keep your anti-virus software up-to-date.
- **Change your passwords** - Your original passwords may have been compromised during the infection, so you should change them.
- **Keep your operating system and application software up-to-date** - Install software patches so that attackers can't take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.
- **Use anti-malware tools** - Using a legitimate program that identifies and removes malware can help eliminate an infection. Users can consider employing a remediation tool that will help with the removal of GOZ from your system.

For additional information, please refer to the following websites:

- https://www.cisa.gov/uscert/ncas/alerts/TA14-150A
- https://www.knowbe4.com/gameover-zeus
- https://heimdalsecurity.com/blog/zeus-gameover/
- https://www.fbi.gov/news/stories/gameover-zeus-botnet-disrupted

POINT OF CONTACT

Please contact **PMAJ JUN-JUN S DAGURO**, Police Community Relations Officer thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 8723-0401 local 7483 for any inquiries related to this CYBER SECURITY BULLETIN.