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 261

ACG-CSB 080122261

Reference Number ACG-CSB 080422261

Understanding the Risk of Ransomware as a Service (RaaS)

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

Ransomware like Trojans, worms, and computer viruses is another type of malware that poses threats to individuals, private companies and even government agencies. A computer program with malicious intent, meant to encrypt a user’s data or system and demand ransom. The data or system is locked until the victim pay the ransom fee to the attacker.

Ransomware as a Service (RaaS) is a business model between ransomware operators that involves selling or renting ransomware to buyers, also known as affiliates to use ransomware tools to execute attacks. The use of RaaS enables affiliates to enter an area of extortion practices that was previously exclusive to the operators themselves.

The said ransomware is an adoption of the Software as a Service (SaaS) business model. Like all SaaS solutions, RaaS users don't need to be technically skilled or knowledgeable, to capably use the tool. The developers provide a code along with instructions on how to launch the attack. RaaS solutions, therefore, empower even the most novel hackers to execute highly sophisticated cyberattacks.

The ransomware developers need to be reputable to compel affiliates to sign up and distribute their malware. Reputable RaaS developers create software with a high chance of penetration success and a low chance of discovery.

To get started, the affiliates will pay the operator to use a skillfully coded ransomware developed by expert ransomware developers in form of cryptocurrency e.g. Bitcoin, Ethereum, etc. The affiliates can select the type of malware they wish to spread. If the attack is successful and ransom money is received, the profits are split between the developer and the affiliate. The ransom money will divided depend on the cost of revenue model.

The Four RaaS Revenue Models

Most RaaS arrangements fall under one of the four following revenue models:

- **Monthly Subscription** - Users pay a flat fee on a monthly basis and earn a small percentage of each successful ransom.

- **Affiliate Programs** - A small percent of profits go to the RaaS operator with the goal of running a more efficient service and increasing profits

- **One-time License Fee** - As the name of the model indicates, users pay a one-time fee with no profit sharing. Affiliates then have access in perpetuity.

- **Pure Profit Sharing** - Profits are divided among users and operators with pre-determined percentages upon the license purchase.

RECOMMENDATION

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

- Monitor all endpoints connection requests and establish validation processes
- Educate staff on how to identify phishing attacks
- Set up DKIM and DMARC to prevent attackers from using your domain for phishing attacks.
- Monitor and remediate all vulnerabilities exposing your business to threats
- Monitor the security posture of all your vendors to prevent third-party breaches
- Set up regular data backup sessions
- Do not solely rely on cloud storage, backup your data on external hard drives
- Avoid clicking on questionable links. Phishing scams do not only occur via email, malicious links could lurk on web pages and even Google documents.
- Use antivirus and anti-malware solutions
- Ensure all your devices and software are patched and updated.
- Provide your staff and end-users with comprehensive social engineering training
- Introduce Software Restriction Policies (RSP) to prevent programs from running in common ransomware environments, i.e. the temp folder location
- Apply the Principles of Least Privilege to protect your sensitive data.

For additional information, please refer to the following websites:

- https://www.upguard.com/blog/what-is-ransomware-as-a-service
- https://www.varonis.com/blog/ransomware-as-a-service

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.