September 13, 2024

Pro-Russian Hacktivists Target Organizations in Taiwan With DDoS Attack Campaign

Overview

- Pro-Russian threat actors NoName057(16), RipperSec and Cyber Army of Russia (aka People's Cyber Army) have launched DDoS attacks on Taiwanese targets.
- The attacks are a reaction to Taiwan President Lai Ching-te's comment in an interview with Taiwanese media that China should also take back land from Russia.
- The attack campaign started on September 9 and continues against over 50 targets including government sites, airports, financial services and Taipei Stock Exchange.

Motivation

The attacks are a reaction to what Taiwan President Lai Ching-te said in an interview with Taiwanese media. NoName057(16), a pro-Russian threat actor and one of the most active hacktivist groups, announced: "Last week, the President of Taiwan suggested that China take away land in the Far East from Russia. This statement reflects the 'virtual reality' in which such satellite countries are immersed. Taiwan clearly feels its impunity, which is why it allows itself such attacks. One of our tasks is to remind such Taiwanese that they are just a pawn in this game, benefiting from US protectionism in the international arena. Moreover, Beijing's control over the island is only a matter of time. We remind you that this 'chip country' is part of China, we put Taiwanese sites and pass the baton to our friends from the [People's CyberArmy]."

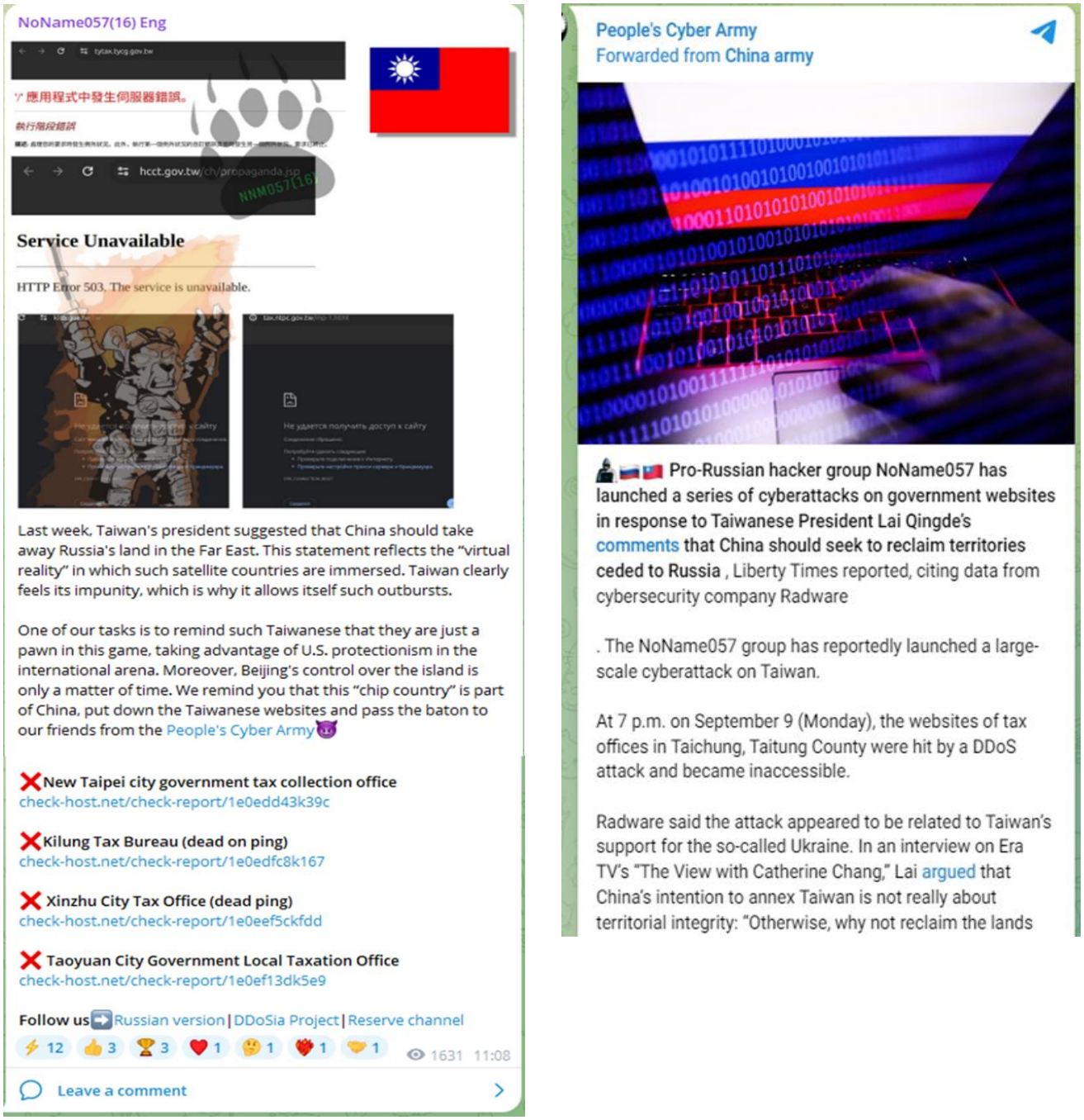


Figure 1: NoName057 and People's Cyber Army announce their attack campaign through Telegram

Threat Actors

NoName057(16) is a pro-Russian hacker group known for its cyberattacks on Ukrainian, American and European websites of government agencies, media and private companies. It is regarded as a well-organized pro-Russian hacktivist group with over 2.5 years of experience targeting countries that support Ukraine or speak badly about Russia.

RipperSec is a pro-Muslim hacktivist group operating from Malaysia. Their operations are politically motivated and are often coordinated through Telegram channels. The group has been involved in several high-profile DDoS attacks, including disruptions during significant geopolitical events.

Cyber Army of Russia is a decentralized pro-Russian hacktivist group that mainly targeted Ukraine at first. More recently, the group has started to align its targets more closely with NoName057(16). The group uses DDoS attacks to target governments and corporations perceived as oppressive or corrupt. They coordinate through social media platforms and Telegram, rallying support during geopolitical tensions.

It is common to see like-minded threat actors make ad-hoc alliances and collaborate on campaigns to increase their impact.

Attack Tools

Threat actors have mastered their ability to generate highly evasive and sophisticated HTTPS flood attacks that are hard to detect and mitigate.

The tools used by the aforementioned threat actors are known and have been reviewed by Radware:

- **NoName057(16):** Project DDoSia
- **RipperSec:** MegaMedusa

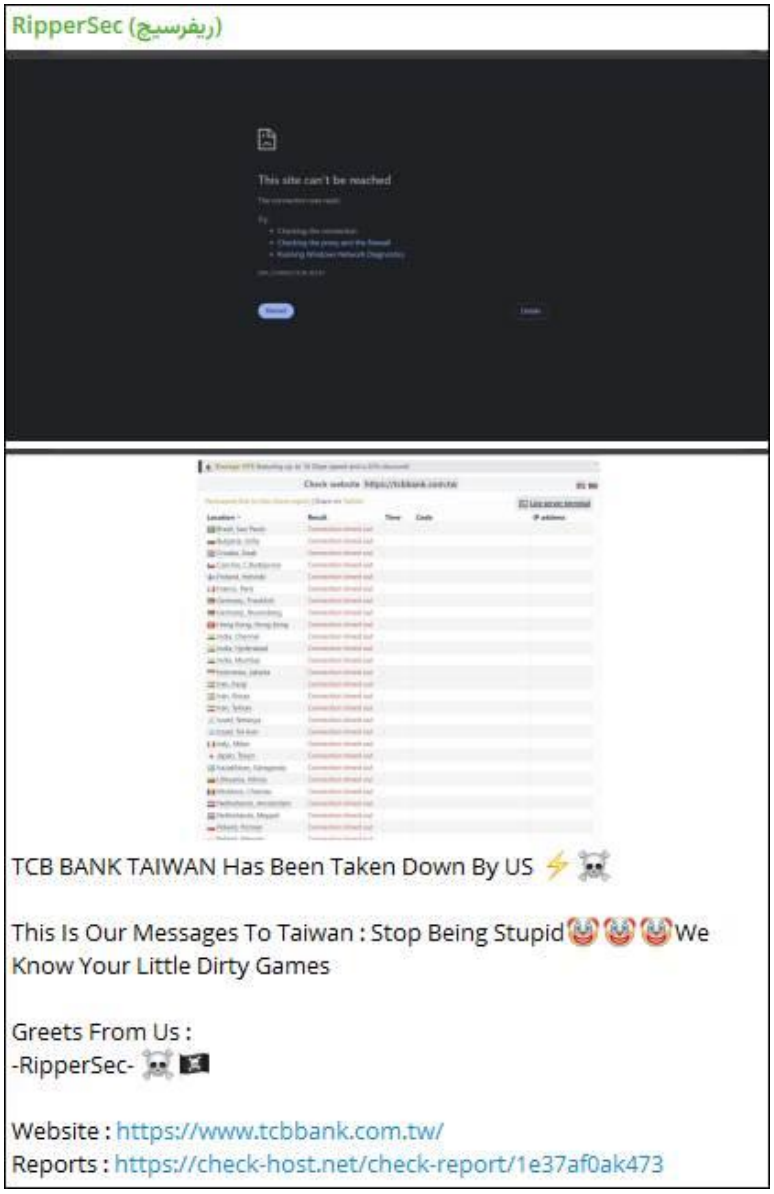
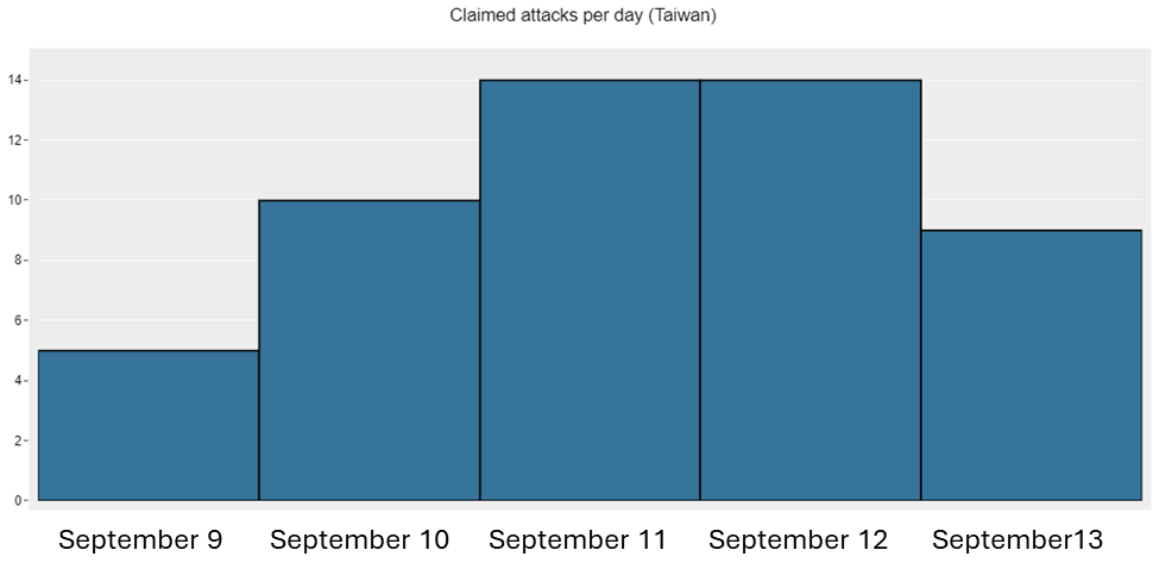
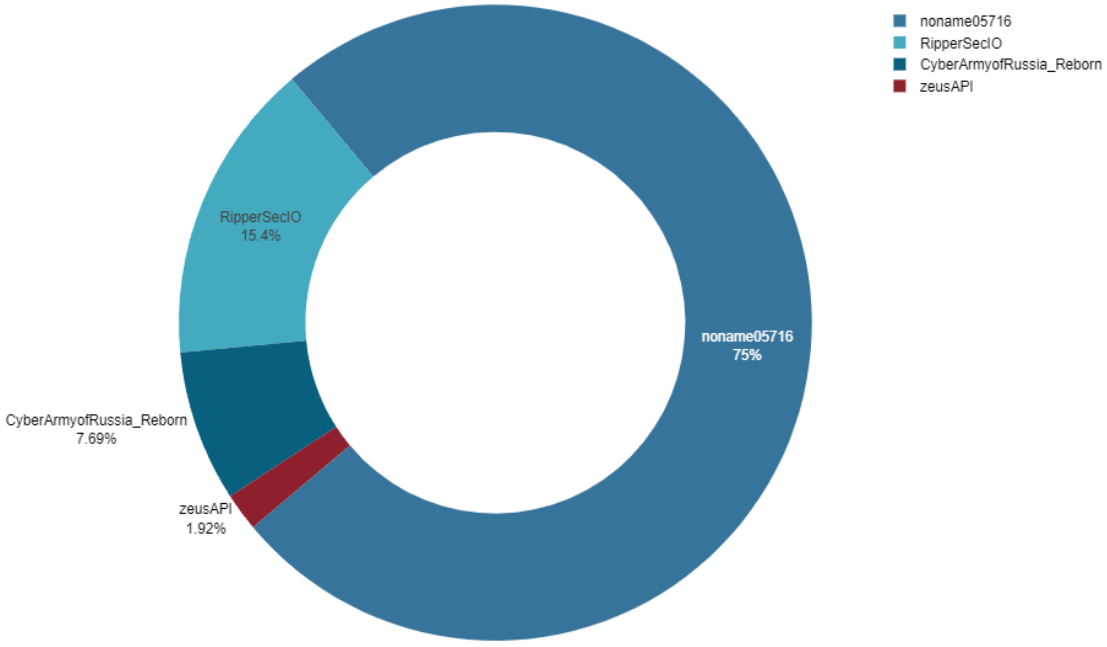


Figure 2: RipperSec claims an HTTPS flood attack on the web services of TCB Bank Taiwan. The Check Host page shows the victim resources were offline

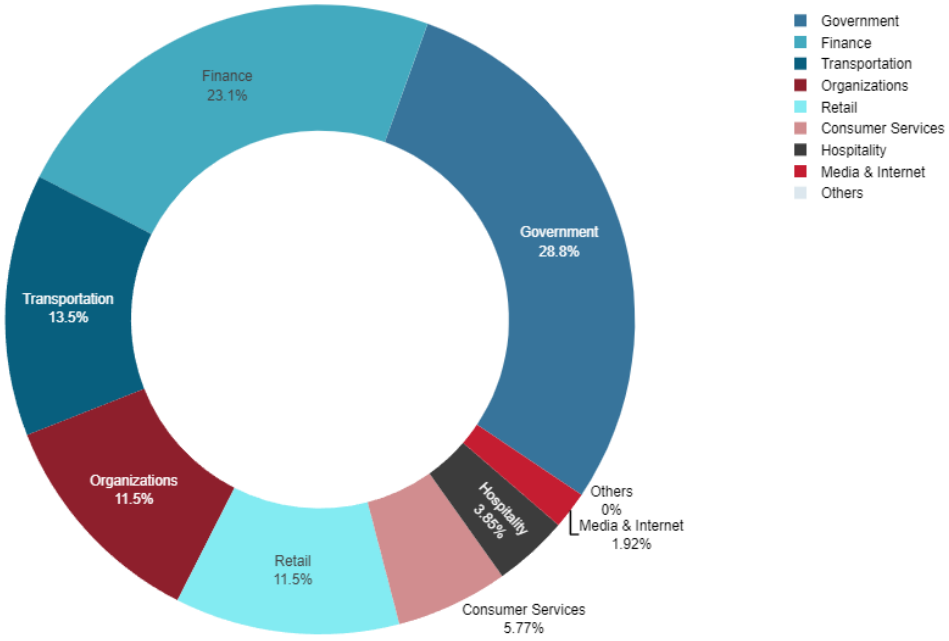
Attack Timeline



Claiming Actors



Targeted Industries



EFFECTIVE DDOS PROTECTION ESSENTIALS

Behavioral-Based Detection – Leverage Radware's advanced behavioral analysis to quickly and accurately identify and block anomalous bot activity while allowing legitimate traffic.

Real-Time Signature Creation – Utilize Radware's ability to promptly create and deploy signatures to protect against emerging threats and zero-day attacks.

AI-Powered Content Analysis – Implement Radware's AI-driven solutions to detect and mitigate sophisticated disinformation campaigns across multiple platforms.

Cross-Platform Monitoring – Employ Radware's comprehensive monitoring tools to track influence operations across various digital channels.

Rapid Response Capabilities – Leverage Radware's 24/7 Emergency Response Team to swiftly address and mitigate emerging threats.

For further network and application protection measures, Radware urges companies to inspect and patch their systems to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options including on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.

REPRESENTATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES THAT THIS REPORT IS ERROR-FREE OR ANY IMPLIED WARRANTIES REGARDING THE ACCURACY, VALIDITY, ADEQUACY, RELIABILITY, AVAILBILITY, COMPLETENESS, FITNESS FOR ANY PARTICULAR PURPOSE OR NON-INFRINGEMENT. USE OF THIS REPORT, IN WHOLE OR IN PART, IS AT USER'S SOLE RISK. RADWARE AND/OR ANYONE ON ITS BEHALF SPECIFICALLY DISCLAIMS ANY LIABILITY IN RELATION TO THIS REPORT, INCLUDING WITHOUT LIMITATION, FOR ANY DIRECT, SPECIAL, INDIREC, INCIDENTAL, CONSEQUENTIAL, OR EXAMPLARY DAMAGES, LOSSES AND EXPENSES ARISING FROM OR IN ANY WAY RELATED TO THIS REPORT, HOWEVER CAUSED, AND WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHER THEORY OF LIABILITY, EVEN IF IT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, LOSSES OR EXPENSES. **CHARTS USED OR REPRODUCED SHOULD BE CREDITED TO RADWARE**