New htpRAT Gives Complete Remote Control Capabilities to Chinese Cyber Threat Actors

riskiq.com/blog/labs/htprat/

October 26, 2017

External Threat Management Labs

October 26, 2017

By Yonathan Klijnsma

HtpRAT, a newly discovered Remote Access Trojan (RAT) extends the capabilities of traditional RATs by providing complete remote execution of custom commands and programming. htpRAT, uncovered by RiskIQ cyber investigators, is the newest weapon in Chinese cyberattackers' campaign against Association of Southeast Asian Nations (ASEAN).

Most RATs can log keystrokes, take screenshots, record audio and video from a webcam or computer microphone, install and uninstall programs and manage files. They support a fixed set of commands operators can execute with different command IDs —'file download' or 'file upload,' for example—and must be completely rebuilt to have different functionality.

htpRAT, on the other hand, serves as a conduit for operators to do their job with greater precision and effect. On the Command and Control (C2) server side, cyber threat actors can build new functionality in commands, which can be sent to the malware to execute. This

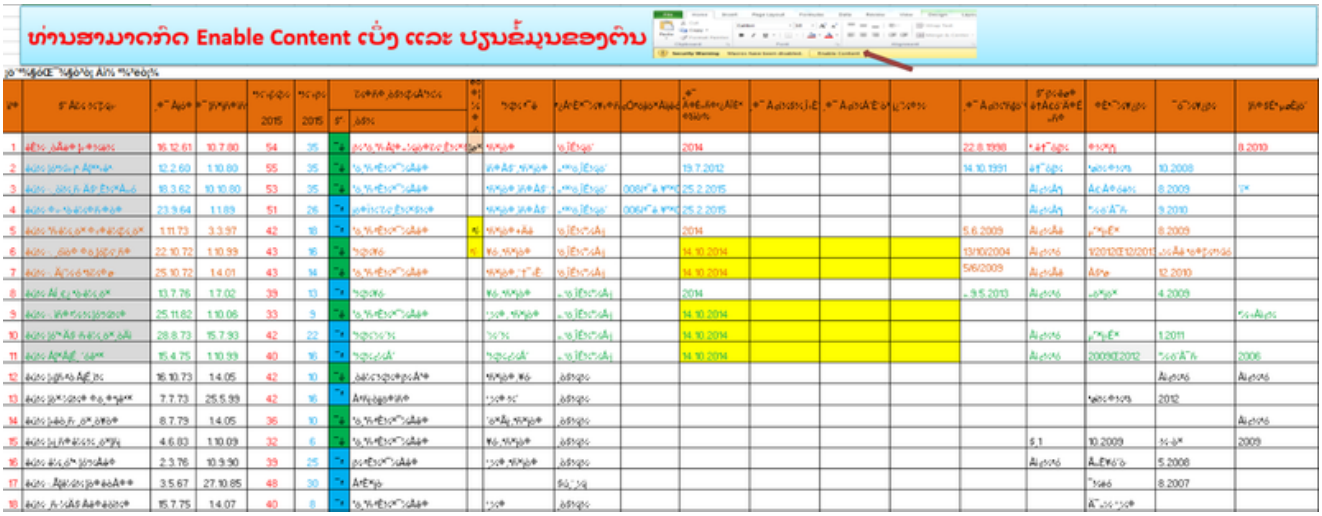
capability makes htpRAT a small, agile and incredibly dynamic piece of malware. Operators can change functionality, such as searching for a different file on the victim network, simply by wrapping commands.

ASEAN countries endure complicated and often contentious relations with one another, especially over China's economic influence and its claim over disputed territory in the South China Sea. As a way to spy on and disrupt rivals, China has sponsored several documented cyberattacks against its neighbors. Use of htpRAT elevates an attacker's capabilities to a new level.

Unfortunately, most ASEAN countries have notoriously underdeveloped cybersecurity practices and levels of awareness, both in the public and private sectors, making government and business organizations easy pickings for hackers—especially those from highly skilled and experienced attackers commissioned by the Chinese government. A 2015 survey by ESET Asia found that 78% of internet users in Southeast Asia had not received any formal education on cybersecurity. Another study revealed that Asia-Pacific companies spent 47% less on information security than North American firms in 2015.

As a result, many of these countries are already under siege. In a cybercrime operation led by Interpol, nearly 9,000 C2 servers and hundreds of compromised websites were identified across the ASEAN region for carrying out cyber attacks on local organizations. Another study, revealed that in Myanmar, Thailand, and Vietnam, more than 20% of computers running Windows were targeted by cyber attacks, compared with the global average of 9%.

Laos, which is ranked 77th in the world in its response to online threats in the International Telecommunication Union Cybersecurity Index, is also vulnerable. On November 8, 2016, RiskIQ discovered that a non-disclosed Laotian entity was spear-phished by what seems to be--based on the tooling and its links to other attacks--a Chinese government threat group. A clever email attempted to get victims to download a nefarious RAT that includes a back door for administrative control over the target computer via a link shown in the attached file below.



Spear phishing has, of course, become a favorite vector for cyber threat actors who try to fool people within specific organizations into giving up sensitive information by clicking on malicious links or downloading malicious files with fake emails purporting to be from someone the victim may know. Typically, they do this by spoofing an email address and mimicking the language, behaviors, and processes used in the day-to-day operations of the organization.

In this case, the malicious file encourages the recipient, in both Lao and English, to click a link to "Enable Content," with an added image showing how to enable macros in the document. The top part containing Lao and English "u0e97u0ec8u0eb2u0e99u0eaau0eb2u0ea1u0eb2u0e94u0e81u0ebbu0e94 Enable Content u0ec0u0e9au0eb4u0ec8u0e87 u0ec1u0ea5u0eb0 u0e9bu0ebdu0e99u0e82u0ecdu0ec9u0ea1u0eb9u0e99u0e82u0eadu0e87u0e95u0ebbu0e99" roughly translates to "You can click 'Enable Content' to (see/change) the data."

Once the machine is infected, we noticed something remarkable. Chinese state-sponsored hackers are known for old, reliable tooling (PlugX malware is one example), but htpRAT enables cyber threat actors to create new commands from the C2 server side which can be sent to the malware on the infected host to execute.

Connections to Other Attacks

Hackers associated with China like to employ the same malware over and over, which is part of what makes htpRAT so unique. Older samples connected to the C2 domain used in the htpRAT campaign link to a variety of PlugX malware samples and Hacking Team exploit activity. One especially interesting connection is a piece of malware called ‘MyHNServer,’ which is a packaged PlugX payload linked to another piece of malware called ‘MyCL’ via its C2 server, which has been widely used in other attacks in Vietnam.

Looking at the registration information for the C2 domain, we found a link to a more recent attack against the Vietnamese government. The domain is registered to a person with the same email address that was also used to register a domain imitating an official military domain in Vietnam.

These findings and others reveal a significant escalation in state-sponsored cyber warfare and could become standard fare for advanced cybercriminal attacks on businesses and organizations around the world. If effectively used, the new tools could make detection more difficult and could help attackers move beyond the theft of data and secrets to more data or system manipulation or other kinds of sabotage.

Download the report for a full analysis of the malware, including details of the investigation, IOCs, and infrastructure analysis.

Subscribe to Our Newsletter

Subscribe to the RiskIQ newsletter to stay up-to-date on our latest content, headlines, research, events, and more.

Base Editor