The Rising Vietnamese Cybercriminal Landscape

The Backdrop

Vietnam is a burgeoning economic force in the Asia-Pacific arena, with growth projected at 6.5 percent through 2020. Its one-party government has committed to an aggressive economic growth strategy, searching for advantages it can gain over the more established regional economic powerhouses – China, Japan, South Korea, and neighboring Southeast Asian countries like Singapore. Recent investments in the domestic development of technology have attracted skilled tech workers from foreign countries to Vietnam.

This rapid economic growth and expansion naturally attracts undesirable attention in the form of cybercrime and cyber espionage. Regional cyber threat actors have targeted foreign multinational organizations operating inside Vietnam with increased frequency, and one group appears to be acting in support of Vietnam’s interests by creating economic advantages through cyberattacks on competitors.

The Impact of Vietnam’s Law on Cybersecurity

In June 2018, the Vietnamese National Assembly passed a new cybersecurity law requiring companies like Facebook and Google to open offices in Vietnam, store local user data in Vietnam, and hand over any information the government requests. The law also enforces censorship of social media, with which internet companies have one year to comply. As part of the government’s censorship initiative, it created a cyber offensive unit of 10,000 members called “Force 47” to combat proliferation of views it deems inappropriate or toxic.

Force 47’s goal is to combat “wrongful” opinions on the clear web. The cyber unit actively monitors unsavory content – as deemed by the Vietnamese government – and blocks Vietnamese users’ access to websites that are considered to be run by dissidents. Force 47 frequently requests Facebook and YouTube remove content it does not approve of, threatening to block all internet users from accessing those platforms entirely. Given that half of the country’s population of 93 million now actively uses the internet, these social media giants will be put in a precarious position, as they must decide whether or not to comply with forced censorship of their user base or to withdraw to reinforce their support of free speech and lose those users entirely. As Vietnamese authorities strengthen their grip via censorship, there has been an observed increase in Vietnamese-language internet traffic and activity on the deep and dark web. Thousands of users are migrating to Vietnamese-language forums to seek information on technology, cryptocurrencies, and cybercrime opportunities.

The influx of Vietnamese users on the dark web is growing more obvious, as hundreds of new posts in Vietnamese populate well-known hacker forums and cybercriminal hangouts every day. Hacker Vietnam Association (HVA) was a hacking website with over 14,000 members before it was shut down, and it still has almost 30,000 followers on its Facebook page. A number of hacking forums have since taken the place of HVA since it was shut down, with common discussion topics including carding, hacking, Tor usage, tutorials, cryptocurrency, and other methods to enable users to carry out cybercriminal activities.

The Vietnamese government’s recent censorship legislation – adopted in the name of bolstering cybersecurity for users – threatens to stifle the voice of a young and growing middle class. This law has been condemned by free speech advocates around the world, and is inadvertently shepherding the younger generations into underground communities.
OceanLotus (APT32)

One of the most notorious advanced cyber threats in Asia, APT32, also known as OceanLotus, is believed to be working on behalf of the Vietnamese government. The group targets foreign governments, businesses, and dissidents for financial gain and to equip the regime with intelligence on its adversaries. OceanLotus has gained notoriety for its large-scale attacks in recent years, including watering hole attacks against Vietnamese and Cambodian media outlets last year. OceanLotus was also credited with attacks on numerous automotive manufacturers in advance of Vietnam’s first domestic auto company’s planned debut in September 2019.

Tools, Tactics, and Procedures

Watering Holes:
In 2018, OceanLotus launched a watering hole campaign on at least 21 websites in Southeast Asia, including important foreign government sites. Other targets included news and media sites based in Vietnam and Cambodia. While OceanLotus has used watering hole attacks many times in the past, this instance stood out because it did not target specific enemies; rather, it used public interest sites to lure unsuspecting victims.

Steganography:
In April 2019, OceanLotus used steganography to hide encrypted payloads inside of .png images. These payloads deploy backdoors that imitate legitimate files to fool detection tools, culminating in full access to the system.

Script Injections:
As part of their watering hole attacks, OceanLotus injects Javascript codes onto the targeted website’s server, allowing them to redirect traffic to their own malicious sites. Once a user is rerouted to these sites, a second script serves as a reconnaissance tool, giving the attackers detailed information about the user’s system.

Malicious Spam:
While this attack type is by no means unique to Vietnam, it is very commonly used by the prominent Vietnamese threat actors. OceanLotus uses spam messages to lure unsuspecting users into clicking on malicious links and downloading malware.

The Targets

Economic Threats:
OceanLotus carried out cyberattacks against foreign governments that could conceivably threaten Vietnam’s economic growth – namely Cambodia. Last year’s watering hole campaign targeted a number of Cambodian government sites, like the Ministry of Defense and Ministry of Foreign Affairs and International Cooperation. Eliminating economic competition appears to be a primary motive for OceanLotus, indicating a high likelihood they could be associated with the Vietnamese government.
The Rising Vietnamese Cybercriminal Landscape

Multinational Automotive Companies:
One of OceanLotus’ top priorities for 2018 was targeting global and multinational auto companies. As part of a large-scale malware and espionage campaign, the APT group sent malicious lures to auto organizations around the world, including Toyota. Vietnam’s first domestic auto company, VinFast, is slated to release its first line of vehicles in September 2019. This development is crucial to the country’s economic growth. The simultaneous timing of the OceanLotus attacks is a strong indicator of their objectives: To gather intelligence on the competition and potentially disrupt their business operations.

Media Outlets:
Included in the 2018 watering hole attacks, OceanLotus targeted Vietnamese and Cambodian media outlets. Most of the targets were publications that had expressed criticism of the Vietnamese government. Due to the widespread use of these news sites in the region, this campaign compromised unsuspecting users in addition to the intended targets. The malware used in these attacks revealed OceanLotus’ growing sophistication in development of native malware and their ability to evade detection and analysis.

The Takeaways

While Vietnam may not yet have the resources to combat world superpowers – like China or the U.S. – in traditional warfare or economic stature, cyber warfare is an opportunity to level the playing field. Vietnam has the potential to develop into a cybercriminal outpost, as its government continues to censor the public and push its youthful middle class toward the fringes with its strict internet legislation. The omnipresent Force 47 threatens to further restrict public access to information, and the results are clear: Increasing numbers of Vietnamese internet users are choosing anonymity through the deep and dark web, and are seeking information on cryptocurrencies, dark web usage, and access to cybercrime jobs.

Ocean Lotus has ramped up their efforts in recent years, attacking foreign economic competitors and governments alike. While the Vietnamese regime has not claimed accountability for OceanLotus, it appears likely that the APT is working to fulfill the government’s priorities. Vietnam’s technological and economic growth serves as an attractive environment for cybercriminals, and it is highly likely that the government will recruit talent from this growing pool.

Forum Statistics

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Threads:</td>
<td>32,642</td>
</tr>
<tr>
<td>Posts:</td>
<td>536,689</td>
</tr>
<tr>
<td>Members:</td>
<td>14,246</td>
</tr>
<tr>
<td>Threads Last 24 Hours:</td>
<td>17</td>
</tr>
<tr>
<td>Posts Last 24 Hours:</td>
<td>93</td>
</tr>
<tr>
<td>Members Last 30 Days:</td>
<td>374</td>
</tr>
</tbody>
</table>

A snapshot of usership for a cryptocurrency forum with a strong Vietnamese presence

IntSights continues to monitor the dynamic cyber threat landscape in Vietnam as the economy grows, APT’s become more sophisticated, and the cyber and crypto communities expand in the underground.