Targeted Malware Attacks against NGO Linked to Attacks on Burmese Government Websites

October 16, 2015

Tagged: Burma, Targeted Threats, Tibet

Categories: Adam Senft, Irene Poetranto, Katie Kleemola, Masashi Crete-Nishihata, Reports and Briefings, Research News

By: Katie Kleemola, Masashi Crete-Nishihata, Adam Senft, and Irene Poetranto

Summary

- This report analyzes a campaign of targeted attacks against an NGO working on environmental issues in Southeast Asia.
- The email messages used in the attacks leverage themes related to economic development and politics in Burma, which is relevant to the work of the NGO.
- Our analysis reveals connections between these attacks, recent strategic web compromises against Burmese government websites, and previous campaigns targeting groups in the Tibetan community.

Background

For many years, Burma was known as one of the world's most heavily restricted information environments. Internet censorship was pervasive, connectivity was prohibitively expensive, and media publication laws created a climate of self-censorship. Recently, however, the country has been undergoing a process of political and economic transformation. Online censorship has decreased, the introduction of two large foreign telecom providers has sparked competition and reduced barriers to access, and the draconian 1962 Printers and Publishers Registration Law has been replaced.

On November 8, 2015, Burma will hold a general election, the first since a nominally civilian government took power in 2011. The participation of opposition leader Aung San Suu Kyi's National League for Democracy party, the religious strife and ongoing armed conflict with ethnic armies and rebel groups, as well as the disruptive effects of increased foreign investment have set the stage for a highly contentious election.

Burma is a resource-rich country, known for its oil, gas, minerals (e.g., zinc, copper, tin, tungsten), jade and other gemstones, and forest products (e.g., timber). Burma also has large hydro power potential, with 302 projects currently ongoing to deliver electricity to the entire population. The process of liberalization has cast a spotlight onto these resources, which many have been eyeing for commercial exploitation, especially neighbouring countries like China and India, and yet they are situated in the midst of armed conflict. China's demand for natural resources has led it to invest heavily in Burma, providing backing for infrastructure projects such as pipelines, dams, highways, and railways. This undertaking is not without controversy, as these development projects cut across territories known for being political hotspots and have resulted in concerns regarding their significant environmental and human rights impact.

The Kyaukpyu Shwe Gas Pipeline, for instance, transports crude and natural gas overland from the Bay of Bengal, traversing the conflict-ridden Arakan and northern Shan States, and finally to the city of Kunming, the capital of China's Yunnan province which borders Burma. The project has been criticized for draining the country of natural resources, damaging the environment, and producing minimal benefit to the local community. The Shwe Gas project has enabled the establishment of related projects, such as the creation of a Kyaukpyu Special Economic Zone (SEZ) and a 950-kilometre railway, running parallel to the pipeline, that will link Kyaukpyu township with Yunnan province. Kyaukpyu, situated in Arakan State, has been mired by ethnic unrest, with minority Muslim Rohingyas being targeted by non-Muslims. Pictures from the township obtained by Human Rights Watch following a week that violence broke out in 2012 showed that more than 811 buildings and houseboats had been razed. Clashes have also continued to occur between Burma's

army and rebel groups fighting in the predominantly ethnic Chinese area of Kokang in northern Shan State.

As Burma's economy further develops, with China as one of its main trading partners, the number of China-backed projects in the country is likely to increase. Simultaneously, political reforms and better access to information and communication technologies have facilitated citizens' expression of discontent. Civil society organizations are also working towards improving transparency and accountability in resource management, as the government and ethnic rebel groups strive to establish a nationwide ceasefire agreement. The ongoing interaction of these factors will carry wide-ranging implications for Burma's transition to democracy.

Pre-Reform Targeted Attacks

Burmese civil society and media organizations have faced targeted online attacks both before and after the current liberalization process. During the last years of the military junta (1962-2011), Burmese independent media groups experienced waves of distributed denial-of-service (DDoS) and defacement attacks, often around the anniversary of the 2007 "Saffron Revolution," a period of mass protests during which authorities shut down national access to the Internet. While activists generally suspected the military junta of being behind the DDoS and defacements, attribution around these attacks is inconclusive.

Reports of targeted malware attacks during this period are less frequent. In 2000, Burmese political activists reported receiving malware attacks, and accused the government of engaging in an organized attack campaign.

Post-Reform Targeted Attacks

Since the beginning of the reform period, a number of reports have emerged of targeted malware attacks against journalists and Burmese government targets that are contextually related to the energy sector and industrial development issues in the country.

Beginning in 2013, a number of domestic and foreign journalists working in the country received warnings from Google that their Gmail accounts might have been targeted by "state-sponsored attackers". Government spokespeople denied that the Burmese government had engaged in these activities. Similar Gmail warnings were reported in 2014, and appeared to indicate attacks on journalists covering news about the Kyaukpyu Shwe Gas Pipeline.

In May 2015, Palo Alto Networks reported that the website of the President of Myanmar was compromised by attackers who injected an Inline Frame (IFRAME) into a JavaScript file in the site's Drupal theme. This IFRAME served visitors a variant of the Evilgrab malware family. The Evilgrab malware has typical RAT capabilities including collecting screenshots, recording keystrokes, and capturing video and audio from the webcam and microphones of compromised devices. This kind of attack, in which attackers compromise normally trusted websites and serve malicious code to specific visitors, is often referred to as a strategic web compromise.

Palo Alto Networks identified the compromise after a computer belonging to a "globally recognized organization in the oil and gas industry" visited the URL containing the malicious code. While the report does not attribute the attack to a specific actor, it notes that the choice of the President's website as a vector suggests that individuals or organizations engaged in political relations with Burma may have been the intended target.

In August 2015, Arbor Networks released a report documenting a similar strategic web compromise against a Myanmar Ministry of Information website (`http://www.moi.gov[.]mm`) hosting content related to the Myanmar Motion Picture Development Department. Similar to the previous attack against the President of Myanmar website, an IFRAME was injected into the site that pointed to a malicious file in the Drupal themes folder. The malware in this attack is from the PlugX malware family, which has similar RAT functionality as EvilGrab.

The malware used "Kpsez-htday" as a Command and Control (C2) authentication string, which may be a reference to the Kyaukpyu Special Economic Zone. Arbor Networks also identified common C2 domains used by this malware, and the Evilgrab malware reported by Palo Alto Networks:

```
usafbi.websecexp[.]com
usacia.websecexp[.]com
webhttps.websecexp[.]com
appeur.gnway[.]cc
```

Arbor Networks further identified PlugX malware hosted on the website of the Union Election Commission (`http://www.uecmyanmar[.]org`), a national level electoral commission in Burma.

PlugX uses a technique called DLL sideloading, in which a legitimate executable runs a malicious DLL. This malicious code then decrypts and decompresses the binary file in memory which contains the main malicious functionality. Since the malicious code is being run by a signed, legitimate executable, and the payload never exists unencrypted on disk, it is more difficult for antivirus programs to detect the malware. The PlugX sample found on the Union Election Commission

website used a legitimate executable signed by McAfee.

The overlapping C2 servers that link the PlugX attacks to the previous Evilgrab reported by Palo Alto Networks suggest that either the same attack group is responsible for the two attacks, or that multiple groups are using the same infrastructure.

Targeted Attacks on an Environmental NGO

This report analyzes two targeted malware attacks against an NGO working on environmental issues in Southeast Asia. These attacks have technical and contextual links to previously reported attacks on Burmese government websites, and are also linked to attack campaigns against Tibetan groups. We conclude that at least two scenarios are possible: these attacks are being conducted by the same attackers, or multiple attack groups are sharing infrastructure and development resources.

Attack 1

On June 5, 2015, staff members of the NGO received an email with the subject "Japanese firms apply to operate in SEZs Permit." This subject line matches the title of an article published by online news organization Eleven Myanmar about Japanese insurance companies activities' in Burma's Thilawa Special Economic Zone.

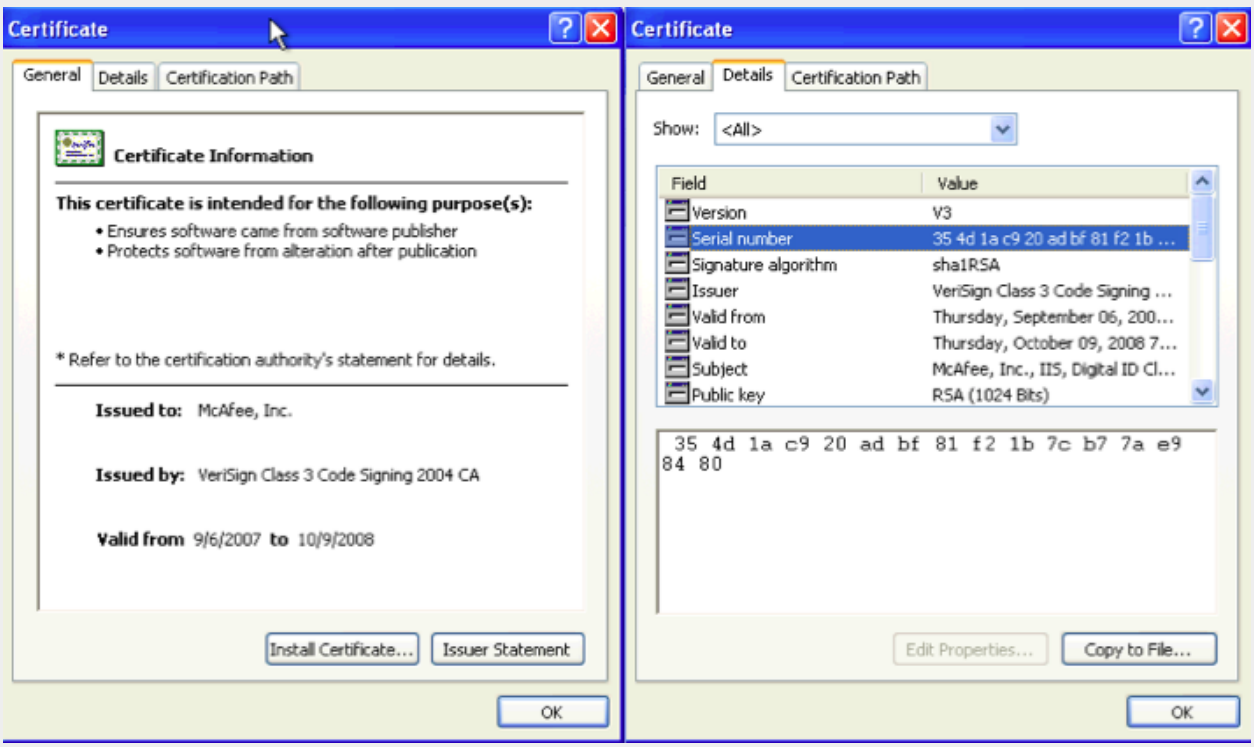
The email body contained the following content:

> "Dear all,
> Japanese firms apply to operate in SEZs Permit.
> [Redacted Google Drive link]

The NGO was suspicious of the email, as it appeared to be sent from an email address that closely resembled (but did not match), the address of an individual in the organization.

The Google Drive link in the body connects to a file 'Permit.zip'. This zip folder contains `Permit.jpg.lnk`, a shortcut that opens a command prompt to download and run `ca-bundle.exe` from the Chinese forum site `hjclub.info` (hxxp://www.hjclub.info/bbs/uploadfiles/45/ca-bundle.exe',' %TEMP%\ca-bundle[.]exe). When executed, `ca-bundle.exe` drops a self-extracting archive (`AwViewWx.exe`) that contains the three components of PlugX, a signed legitimate executable, a malicious DLL, and a binary file containing the main payload.

In this case the malware uses a McAfee Oem module as its legitimate executable (`MD5: 884d46c01c762ad6ddd2759fd921bf71`) with a certificate that expired in 2008. This executable is the same one used in the PlugX sample reported by Arbor Networks.



The malware connects to the C2 `t2.mailsecurityservice[.]com` and `t1.mailsecurityservice[.]com`, which resolve to `118.193.212.98`, a server registered to a customer in Shanghai, China, according to WHOIS results. We found an additional malware sample (`MD5:15c926d2602f65be0de65fa9c06aa6c6`) hosted on the C2 at the address

`hxxp://client.mailsecurityservice.com/ViewClient/connect.php?n=zxishanchu1106[.]exe`. This sample also uses `t2.mailsecurityservice[.]com` as a C2.

Attack 2

On August 16 2015, the same NGO received an email with the subject "Burma Gags Media Linked to Shwe Mann, Adding to Concerns About Reforms." This subject line is the title of an article published by Reuters that reports on an effort by Burma's government to limit public discussion of Shwe Mann, a parliamentary speaker who was purged from the ruling party in August 2015.

The email body contained the following content:

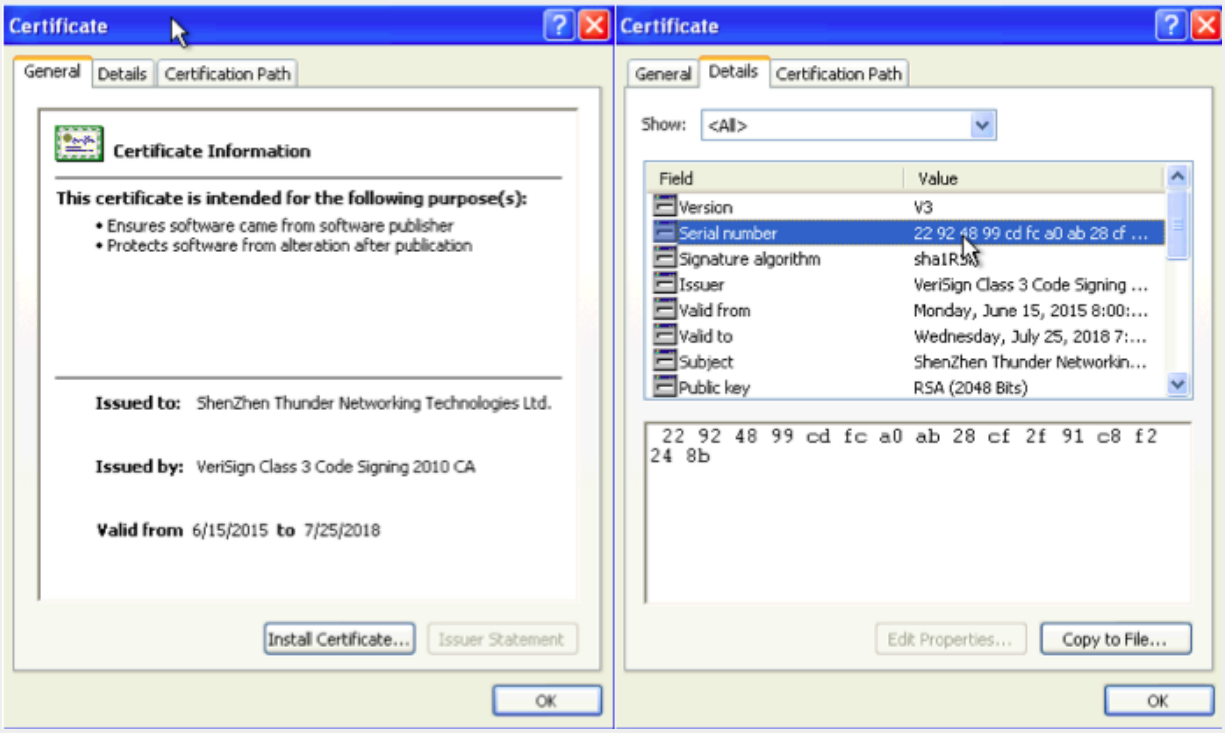
> Burma Gags Media Linked to Shwe Mann, Adding to…
> [Redacted Google Drive link]

The Google Drive link connects to a zip file "Burma Gags Media Linked to Shwe Mann, Adding to Concerns About Reforms.zip". The zip archive includes two files: a benign document "Burma Gags Media Linked to Shwe Mann, Adding to Concerns About Reforms.docx." and a Windows Screensaver file that contains malware "Burma Gags Media Linked to Shwe Mann, Adding to Concerns About Reforms.scr". The .scr file includes a Microsoft document icon to trick recipients into thinking it is a document file. The file is actually a self extracting RAR archive that drops three files: a legitimate executable, a malicious DLL, and a binary file with the payload.

While these three components are similar to the structure of PlugX, the malware used in this attack is the 3102 variant of the 9002 malware family. The variant is labeled 3102, because it always uses the string "3102" in its first communications with a C2 server.

The legitimate executable is labeled "lsass.exe" presumably to make it appear to look like a Windows system file when it is run. What appears to be a DLL used for error handling XLBugHandler.dll is actually malicious.

To bypass certificate warnings, the malware uses a genuine code-signing certificate signed by Shenzhen Thunder Networking Technologies Ltd. on August 3 2015, which relative to other attacks we have observed is an unusually recent signature.



The malware connects to the C2 `198.44.190.85`. This IP is a Virtual Private Server (VPS) hosted in the US and owned by VpsQuan, a company that markets international IP addresses (thus helping to bypass China's Great Firewall) to Chinese citizens.

Connections with Previously Reported Attacks

The attacks against the environmental NGO share features with the recent strategic web compromises against Burmese government websites and to campaigns targeting the Tibetan diaspora.

Connections to Campaigns Targeting Burmese Government Websites

The PlugX malware used in Attack 1 shares common features with the malware identified by Arbor Networks on the websites of the Myanmar Ministry of Information and the Union Election Commission. Similar to the malware used in Attack 1, the PlugX samples found on the Ministry of Information website also rely on a McAfee Oem module for the DLL side loading attack. The sample found on the Union Election Commission website has closer similarities, as it uses the same legitimate McAfee executable (MD5 884d46c01c762ad6ddd2759fd921bf71) that we found in Attack 1.

In addition, the time frame of the attacks (May and August 215) and the campaigns identified by Arbor Networks and Palo Alto Networks are broadly similar (June and August 2015).

Connections to Campaigns Targeting Tibetan Groups

Our analysis of Attacks 1 and 2 uncovered similarities in attack vectors, infrastructure, and malware with campaigns against groups in the Tibetan diaspora.

The use of Google Drive in the environmental NGO attacks is interesting as we have seen the same tactic used to deliver malware to Tibetan organizations during campaigns over May to July 2015. The use of Google Drive in these campaigns occur as Tibetan groups are promoting Google Drive as an alternative to sending file attachments to prevent infection from document-based malware. Beyond this common tactic, we also see infrastructure overlap that links the attacks to previous campaigns against Tibetan groups.

The C2 domain `mailsecurityservice.com` that was used in Attack 1 was registered with the same email (`wojiaojilao2@sohu.com`) as another C2 domain `iyouthen.com` that we identified on VirusTotal. Passive DNS records from PassiveTotal show that in March 2015, both domains also resolved to the same IP address 103.20.222.0. We found an Evilgrab sample uploaded to VirusTotal in March 2014 that connects to `gmail.iyouthen.com` (a subdomain of `iyouthen.com`). This sample is signed with a revoked certificate from Qindao Ruanmei Network Technology.

A March 2012 report from Alienvault on attacks against Tibetan NGOs and the Central Tibetan Administration, found a variant of the Gh0St RAT malware family that includes an embedded executable that drops `fxsst.dll`, which is signed by the same revoked certificate. In addition to this similarity, in April 2012 we received an Evilgrab sample from an attack targeting a Tibetan NGO that connected to the C2 `59.44.49.88`, which was also used in the campaigns analyzed by Alienvault.

Conclusion

Far from being an isolated campaign, the attacks that targeted this NGO are linked to recent campaigns against Burmese Government websites. The Palo Alto Networks report suggests that these attacks have also affected industry groups interested in the region. Our analysis provides yet another example of a civil society group targeted as part of a wider campaign that includes government and the private sector. The threat actors responsible appear to be interested in monitoring the activities of groups with a stake in international investment and natural resource development in Burma. However, while industry groups and governments may benefit from well-resourced enterprise security support, civil society organizations typically do not have access to the same resources.

The further connections to previous campaigns against Tibetan organizations can be interpreted in two ways: either the attack group is the same, or there is a degree of infrastructure and tool sharing between multiple threat actors. Sharing between groups could be informal, or be coordinated via what Ned Moran describes as a "digital quartermaster," which maintains and supplies threat infrastructure and malware development resources to multiple groups. Based on our current findings, we are unable to make a definitive conclusion on which of these scenarios is most likely.

Acknowledgements

Thanks to John Scott-Railton for comments on the post.

Indicators

Attack 1

Attachment

File name: `Permit.zip`
MD5: `53f81415ccedf453d6e3ebcdc142b966`

Drops

File name: `ca-bundle.exe`
MD5: `c4c147bdfddffec2eea6bf99661e69ee`

File name: `mcf.exe`
MD5: `884d46c01c762ad6ddd2759fd921bf71`

File name: `mcutil.dll`
MD5: `56f0e67d981024ddcc215543698f44fb`

File name: `mcf.ep`
MD5: `7e0081fba718fcd71753d3199a290f03`

Command and Control Server

`t1.mailsecurityservice[.]com`
`t2.mailsecurityservice[.]com`

Attack 2

Attachment

File name: `Burma Gags Media Linked to Shwe Mann, Adding to Concerns About Reforms.zip`
MD5: `6701662097e274f3cd089ceec35471d2`

File name: `Burma Gags Media Linked to Shwe Mann, Adding to Concerns About Reforms.scr`
MD5: `699b3d90b050cae37f65c855ec7f616a`

Drops

File name: `lsass.exe`
MD5: `5710d567d98a8f4a6682859ce3a35336`

File name: `XLBugHandler.dll`
MD5: `cec071424d417a095221bf8992819388`

File name: `xlbug.dat`
MD5: `49ceba3347d39870f15f2ab0391af234 c`

Command and Control Server

`198.44.190.85`

Post a Comment

Your email is *never* shared. Required fields are marked *

Name *

Email *

Website

Comment

Post Comment