Vietnamese Malware Gets Very Personal

By Eva Galperin and Morgan Marquis-Boire

Published: 2014-01-19 · Archived: 2026-04-05 14:50:08 UTC

As encryption has become more prevalent in online communications as a countermeasure against surveillance, attackers have sought to circumvent these measures by covertly installing malware on targeted computers that can log keystrokes, remotely spy on users with their own webcams, record Skype calls, and listen in on the computer's built-in microphone. Sometimes the attacker is a criminal, such as the hacker who used a remote access tool (RAT) to take blackmail photos of Miss Teen USA. Sometimes the attacker is acting in support of a state, like the pro-Assad hackers whose malware campaigns against opposition supporters EFF has been tracking for the last two years. Sometimes the attacker is the government or a law enforcement agency. For example, the NSA's Tailored Access Operations unit uses covertly-installed malware to spy on targets.

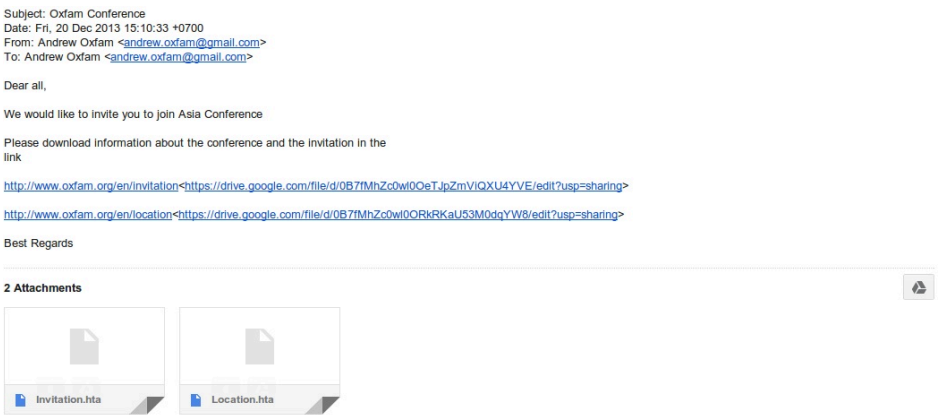
Malware is a tool that most states have their toolbox, and Vietnam is no exception. For the last several years, the communist government of Vietnam has used malware and RATs to spy on journalists, activists, dissidents, and bloggers, while it cracks down on dissent. Vietnam's Internet spying campaign dates back to at least March 2010, when engineers at Google discovered malware broadly targeting Vietnamese computer users. The infected machines were used to spy on their owners as well as participating in DDoS attacks against dissident websites. The Vietnamese government has cracked down sharply on anti-government bloggers, who represent the country's only independent press. It is currently holding 18 bloggers and journalists, 14 from a year earlier, according to a report issued by the Committee to Protect Journalists in 2013.

EFF has written extensively about the worsening situation for bloggers in Vietnam, supporting campaigns to free high-profile bloggers such as Le Quoc Quan and Dieu Cay, and criticizing Vietnam's Internet censorship bill. This report will analyze malware targeting EFF's own staff, as well as a well-known Vietnamese mathematician, a Vietnamese pro-democracy activist, and a Vietnam-based journalist at the Associated Press.

A Campaign Targeting EFF and Associated Press

We will begin with the attack targeting EFF staffers. This marks the first time we have detected a targeted malware attack against our organization by what appear to be state-aligned actors.

On December 20th, 2013, two EFF staffers received an email from "Andrew Oxfam," inviting them to an "Asia Conference," and inviting them to click on a pair of links which were supposed to contain information about the conference and the invitation itself. These links were especially suspicious because they were not hosted on Oxfam's domain, but instead directed the invitee to a page hosted on Google Drive, seen below. In addition, this email contained two attachments purporting to be invitations to the conference.



This targeting is especially interesting because it demonstrates some understanding of what motivates activists. Just as journalists are tempted to open documents promising tales of scandal, and Syrian opposition supporters are tempted to open documents pertaining to abuses by the Assad regime, human rights activists are interested in invitations to conferences. For greater verisimilitude, the attacker should have included an offer to pay for flights and hotels.

Both attachments are the same:

> 351813270729b78fb2fe33be9c57fcd6f3828576171c7f404ed53af77cd91206 Invitation.hta
> 351813270729b78fb2fe33be9c57fcd6f3828576171c7f404ed53af77cd91206 Location.hta

The detection rate for this malware is very low, using VirusTotal, we see only one anti-virus vendor out of a possible 47 detecting this as of 19 January 2014.

The same malware was also sent to an Associated Press reporter, masquerading as a Human Rights Watch paper.

From: HRW Asian <human.rights.watch.asian@gmail.com>
Date: 7 November 2013 13:48:26 GMT+8
To: HRW Asian <human.rights.watch.asian@gmail.com>
Subject: Human Rights White Paper

Dear every body,

We sent to you the Human Rights White Paper VietNam

please see link: https://docs.google.com/HRW/document/WhitePaper

HRW

In this attack, clicking the link in the email takes the user to the malicious HTML application (.hta) file.

The file meta-data reveals the following information:

> Invitation.hta: Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Template: Normal, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:00, Create Time/Date: Mon Nov 19 05:02:00 2012, Last Saved Time/Date: Mon Nov 19 05:02:00 2012, Number of Pages: 3, Number of Words: 395, Number of Characters: 2258, Security: 0

This HTML application contains an encoded executable and also contains a Microsoft Word document named “baviet.doc”:

When the recipient runs the attachment it drops the following files:

> C:\Users\admin\AppData\Local\Temp\baiviet.doc
> C:\Users\admin\AppData\Local\Temp\xftygv.exe

When "baviet.doc’ is displayed and "xftygv.exe" is run, it causes the following files to be installed:

> C:\Program Files\Common Files\microsoft shared\ink\InkObj.dat
> C:\Users\admin\AppData\Local\Temp\1959.tmp
> C:\Users\admin\AppData\Local\Temp\19A8.tmp
> C:\Users\admin\AppData\Local\Temp\1A65.tmp
> C:\Users\admin\AppData\Local\Temp\1D72.tmp
> C:\Users\admin\AppData\Roaming\HTML Help\help.dat
> C:\Users\admin\AppData\Roaming\KuGou7\status.dat
> C:\Users\admin\AppData\Roaming\Microsoft\Media Player\PLearnL.DAT
> C:\Users\admin\AppData\Roaming\Microsoft\Werfault\WerFault.exe
> C:\Windows\Performance\WinSAT\DataStore\Formal.Assessment.WinSAT.xml
> C:\Windows\Performance\WinSAT\ShaderCache.vs_3.0
> C:\Windows\System32\api-ms-win-core-xstate-l1-1-0.bin
> C:\Windows\System32\odbccr64.dll

Several registry changes are made to enable the malicious implant to persist after reboot and the file api-ms-win-core-xstate-l1-1-0.bin is written into the process space of explorer.exe which then instantiates an outbound connection on port 443 to yelp.webhop.org.

At the time of the report, this domain pointed to 62.75.204.91 which hosted the following domains:

> tripadvisor.dyndns.info, neuro.dyndns-at-home.com, foursquare.dyndns.tv, wowwiki.dynalias.net, yelp.webhop.org

This has been used as a command and control server for other Vietnamese-affiliated malware:

> 82f0db740c1a08c9d63c3bb13ddaf72c5183e9a141d3fbd1ffb9446ce5467113 bai viet.hta
> 9c07d491e4ddcba98c79556c4cf31d9205a5f55445c1c2da563e80940d949356 Unhotien.doc

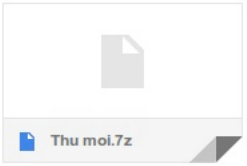
Examining this malware reveals a relationship to earlier campaigns targeting Vietnamese activists.

Targeting of Vietnamese Bloggers

In February of 2013, a Vietnamese blogger and mathematics professor, received the following email:

--------- Message transféré ---------
De : "nguoiviet diendan" <diendannguoiviet.us@gmail.com>
Date : 23 févr. 2013 06:27
Objet : Thư mời
À : <[redacted]>

Kính gửi anh Nguyễn Tiến Dũng thư mời
Trân trọng



Like the malware targeting the EFF and the Associated Press, the attachment was an HTML Application. In this case, the attachment was compressed with 7zip.

> 2fa7ad4736e2bb1d50cbaec625c776cdb6fce0b8eb66035df32764d5a2a18013 Thu moi.7z

extracted:

> dd100552f256426ce116c0b1155bcf45902d260d12ae080782cdc7b8f824f6e1 Thu moi.hta

The file meta-data reveals the following information:

> Thu moi.hta: Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Author: pluto, Template: Normal, Last Saved By: pluto, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Total Editing Time: 07:00, Create Time/Date: Thu Mar 1 05:02:00 2012, Last Saved Time/Date: Thu Jan 24 09:28:00 2013, Number of Pages: 3, Number of Words: 277, Number of Characters: 1584, Security: 0

As with the EFF and AP attacks, the HTML application contains an encoded executable (“zzpauvooos.exe”) and a document (“Doc loi.doc”).

Running “Thu moi.hta” displays “Doc loi.doc” and also drops the following files:

> C:\Users\admin\AppData\Local\Temp\Doc loi.doc
> C:\Users\admin\AppData\Local\Temp\zzpauvooos.exe

When "‘zzpauvooos.exe" is run, it drops the following file:

> C:\Users\admin\AppData\Local\Temp\C947.tmp

And then following command is run:

> "C:\Users\admin\AppData\Local\Temp\C947.tmp" --helpC:\Users\admin\AppData\Local\Temp\zzpauvooos.exe D1DF15E4D714BFDB764ECF92AE709D14BCA3E0E6C759CF7C675BE26D0296A63C3B147110AC79543CC31527651D66787152102A66C3371

Then the following files are dropped onto the system and the original executable is deleted:

> C:\Users\admin\AppData\Roaming\Common Files\defrag.exe
> C:\Users\admin\AppData\Roaming\Identities\{116380ff-9f6a-4a90-9319-89ee4f513542}\disk1.img
> C:\Windows\Tasks\ScheduledDefrag.job
> C:\Windows\Tasks\ScheduledDefrag_admin.job

Values are inserted into the Windows registry for persistence and the main implant, disk1.img, contacts the remote command and control domain, static.jg7.org, on port 443/tcp.

A prominent Vietnamese pro-democracy blogger living in California was successfully targeted by this attack, which led to the compromise of her blog and the invasion of her private life.

The group behind these attacks appears to have been operating since late 2009, and has been very active in the targeting of Vietnamese dissidents, people writing on Vietnam, and the Vietnamese diaspora. The appears to be the work of a group commonly known as “Sinh Tử Lệnh” and while it has been anecdotally claimed to be the work of Chinese actors, it seems to be more likely the work of Vietnamese targeting Vietnamese.

EFF is greatly disturbed to see targeted malware campaigns hitting so close to home. While it is clear that this group has been targeting members of the Vietnamese diaspora for some time, these campaigns indicate that journalists and US activists

are also under attack. And while longtime activists and journalists might expect to be targeted by a state they regularly criticize, it appears that a single blog post is enough to make you a target for Vietnamese spying.
