

[Bad Sites](#)
[Botnets](#)
[CTO Insights](#)
[Exploits](#)
[Internet of Things](#)
[Mac](#)
[Malware](#)
[Mobile](#)
[Social](#)
[Spam](#)
[Targeted Attacks](#)
[Vulnerabilities](#)

[blog.trendmicro.com Sites](#) > [TrendLabs Security Intelligence Blog](#) > [Exploits](#) > [Hacking Team Flash Attacks Spread: Compromised TV and Government-Related Sites in Hong Kong and Taiwan Lead to PoisonIv](#)

Jul28 [Hacking Team Flash Attacks Spread: Compromised TV and Government-Related Sites in Hong Kong and Taiwan Lead to PoisonIv](#)

2:01 pm (UTC-7) | by [Joseph C Chen \(Fraud Researcher\)](#)

[f Share](#) [f Recommend](#) 441

A recent campaign compromised Taiwan and Hong Kong sites to deliver Flash exploits related to Hacking Team and eventually download PoisonIv and other payloads in user systems. This campaign started on July 9, a few days after the Hacking Team announced it was **hacked**.

The actors compromised the sites of a local television network, educational organizations, a religious institute, and a known political party in Taiwan; and a popular news site in Hong Kong. Note that the affected sites have consistent followers given the nature of their content. The affected educational organizations, for instance, are used to deliver employment exams for government employees. The Taiwanese television network involved has been producing and importing TV shows and movies for a decade.

We have notified the owners of the sites that are affected by the campaign; however, three sites are still compromised as of this writing.

Traces of Hacking Team Still Out There

The actors initially delivered a **Flash Player exploit** (CVE-2015-5119) found in the Hacking Team dump into pre-compromised sites a few days after the company announced it was **hacked** (July 5) and **Adobe patched** the flaw (July 7). The actors delivered a second wave of attack by delivering **another Flash zero-day exploit** (CVE-2015-5122) related to the Hacking Team.

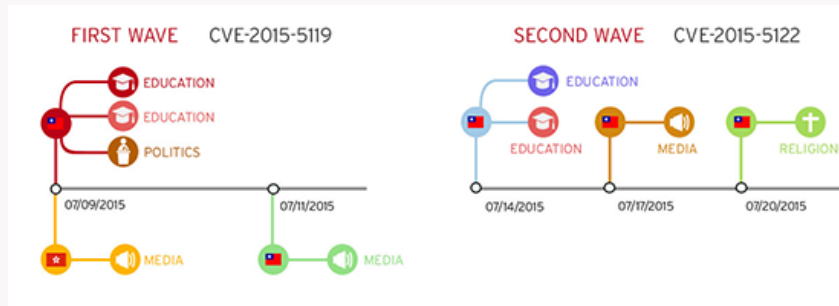


Figure 1. Timeline of Flash exploits related to Hacking Team delivered to Taiwan and Hong Kong sites

Note that, at the start of the first and second wave of attacks, the actors included the same two educational organizations' websites in Taiwan among its targets.



Search our blog:

Zero-Day Alerts

- ❏ **CVE-2015-2426:** Hacking Team Leak Uncovers Another Windows Zero-Day, Fixed In Out-Of-Band Patch
- ❏ **CVE-2015-2425:** "Gifts" From Hacking Team Continue, IE Zero-Day Added to Mix
- ❏ **CVE-2015-5123:** New Zero-Day Vulnerability in Adobe Flash Emerges from Hacking Team Leak
- ❏ **CVE-2015-2590:** Trend Micro Discovers New Java Zero-Day Exploit Linked to Pawn Storm
- ❏ **CVE-2015-5122:** Another Zero-Day Vulnerability Arises from Hacking Team Data Leak
- ❏ **CVE-2015-5119:** Unpatched Flash Player Flaw, More POCs Found in Hacking Team Leak

Hacking Team Leak

- ❏ Hacking Team Flash Attacks Spread: Compromised TV and Government-Related Sites in Hong Kong and Taiwan Lead to PoisonIv
- ❏ Hacking Team RCSAndroid Spying Tool Listens to Calls; Roots Devices to Get In
- ❏ Hacking Team Leak Uncovers Another Windows Zero-Day, Fixed In Out-Of-Band Patch
- ❏ Fake News App in Hacking Team Dump Designed to Bypass Google Play
- ❏ "Gifts" From Hacking Team Continue, IE Zero-Day Added to Mix
- ❏ Hacking Team Uses UEFI BIOS Rootkit to Keep RCS 9 Agent in Target Systems
- ❏ New Zero-Day Vulnerability (CVE-2015-5123) in Adobe Flash Emerges



Figure 2. Screenshot of a religious organization's site in Taiwan compromised to deliver CVE-2015-5122

PoisonIvy and Other Payloads

We found that all the compromised sites, save for the official site of a known Taiwanese political party, were injected with a malicious SWF using iframe which leads to the remote access tool (RAT) PoisonIvy, detected here as BKDR_POISON.TUFW, as the final payload. **PoisonIvy** is a popular RAT backdoor available in the underground market and typically used in targeted attacks. This backdoor has been known to capture screenshots, webcam images, and audio; log keystrokes and active window; delete, search, and upload files; and perform other intrusive routines.

The party's site, on the other hand, has been observed to deliver a different payload embedded in a picture and detected as TROJ_JPGEMBED.F. The party's site sends collected information to the same server as the other sites (223.127.143.132), leading us to believe that it is part of the same campaign.

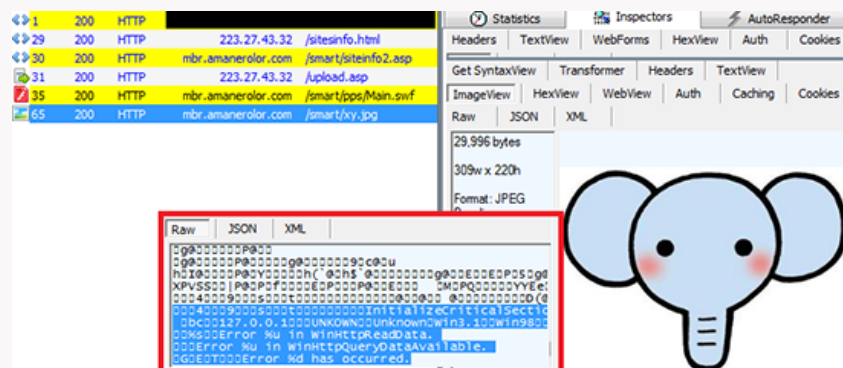


Figure 3. Photo where a final payload of Hacking Team Flash exploit campaign is embedded

Although analysis is still ongoing to determine if this campaign is a targeted attack, we have found a suspicious domain `wut[.]mophecbr[.]com` embedded in the payload which was listed in the command-and-control (C&C) list of a previously reported targeted attack dubbed "Tomato Garden."

Recommendations

To protect machines from exploits and unwanted backdoor access, users should update Adobe Flash Player. You can verify if you're using the latest version by checking the [Adobe Flash Player page](#). It also helps to keep yourself updated with the latest news on popular software. Read more about recent Flash-related incidents and what users and companies can do on our blog post, "[The Adobe Flash Conundrum: Old Habits Die Hard.](#)"

Trend Micro detects all malware and exploits related to this incident. The SHA1s are outlined below:

- SWF_CVE2015122.A
d4966a9e46f9c1e14422015b7e89d53a462fbd65
- SWF_CVE2015122.B
fdcdf30a90fa22ae8a095e99d80143df1cc71194
- SWF_CVE2015122.C
9209fee58a2149c706f71fb3c88ef14b585c717
- BKDR_POISON.TUFW
2dc1deb5b52133d0a33c9d18144ba8759fe43b66

from Hacking Team Leak

- Another Zero-Day Vulnerability Arises from Hacking Team Data Leak (CVE-2015-5122)
- Hacking Team Flash Zero-Day Tied To Attacks In Korea and Japan... on July 1
- Hacking Team Flash Zero-Day Integrated Into Exploit Kits
- A Look at the Open Type Font Manager Vulnerability from the Hacking Team Leak
- Unpatched Flash Player Flaw, More POCs Found in Hacking Team Leak

Recent Posts

- MMS Not the Only Attack Vector for "Stagefright"
- Flash Threats: Not Just In The Browser
- FuTuRology: Wearables and Smart Medical Devices, Gears for a Data-Driven Healthcare Future

Calendar

July 2015						
S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	
« Jun						

Email Subscription

Email Subscription

Your email here

Subscribe

About us

Share this article



Get the latest on malware protection from TrendLabs




This entry was posted on Tuesday, July 28th, 2015 at 2:01 pm and is filed under [Exploits](#), [Targeted Attacks](#), [Vulnerabilities](#) . You can [leave a response](#), or [trackback](#) from your own site.



Trend Micro Discovers Vulnerability That Renders Android Devices Silent The Russian Underground—Revamped

Other Trend Micro blogs

-  [CTO Insights](#)
-  [CounterMeasures Blog](#)
-  [Cloud Security Blog](#)
-  [Consumerization Blog](#)
-  [Fearless Web](#)
-  [Internet Safety for Kids & Families](#)
-  [Simply Security News](#)
-  [Trend Micro Blog \[German\]](#)
-  [TrendLabs Security Blog \[Japan\]](#)
-  [Cloud Security APAC](#)



Do you have a product-related question? [Visit our eSupport website.](#)