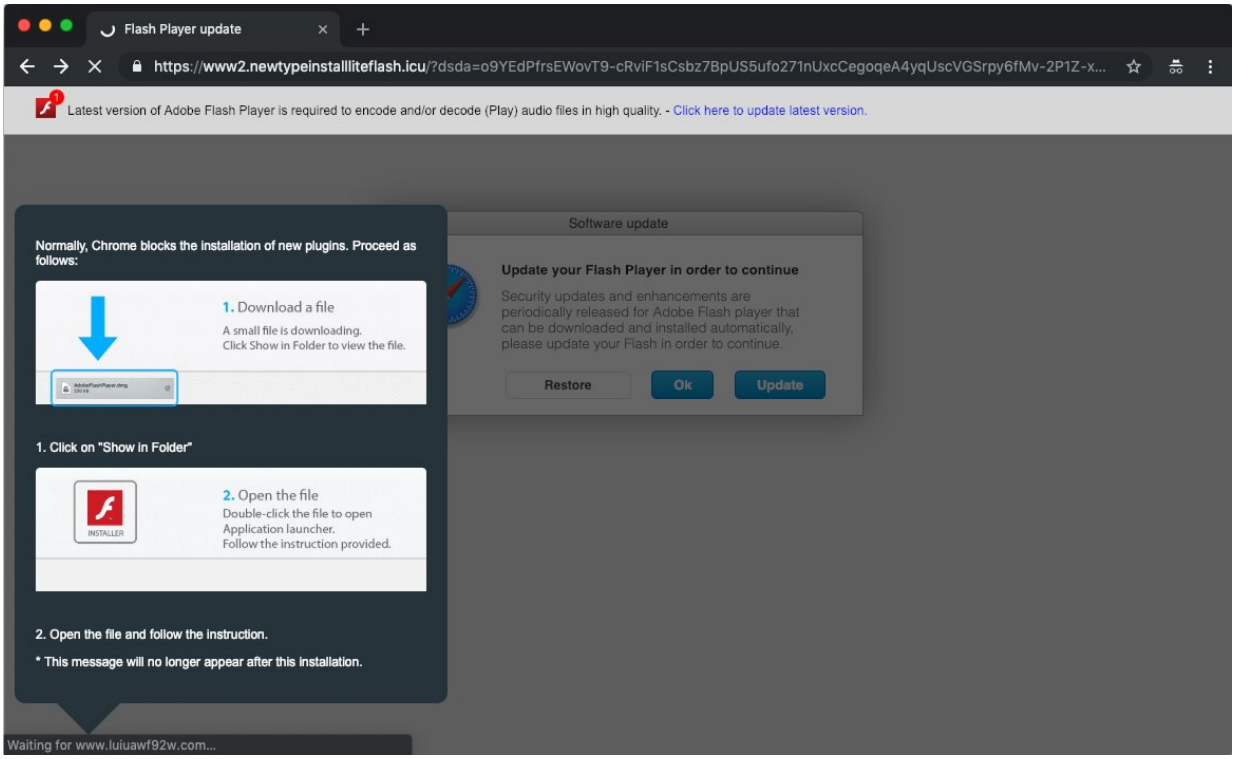
VeryMal: Campaign in image-based malware spotted

January 27 2019, by Nancy Cohen



Credit: Confiant

By this time, news stories have made words like bugs, viruses and malware familiar and by all means frequent, as computer users scramble to self-educate on how to avoid falling victim to a range of security invasions.

Now "Malvertisers" can be added to the list of mischief-makers who keep security watchers on their toes. *Ars Technica*'s headline was a case in point. "Malvertisers target Mac users with steganographic code stashed in image." HTML5 coding helped malicious ads avoid scanners. Eliya Stein of Confiant explained what we are now facing. According to the Confiant blog, it was Confiant and Malwarebytes which spotted this steganography-based ad payload.

Confiant named the payload as VeryMal. Confiant reported brazenly run display ads under the guise of Flash updates and PC repair software.

Shaun Nichols in *The Register* presented the problem as "a malvertising operation that spreads through poisoned ad images."

Dan Goodin in *Ars Technica* reported that "a two-day blitz triggered as many as 5 million times per day. At the core of the storm was "highly camouflaged JavaScript stashed in images to install a trojan on visitors' Macs."

Ionut Ilascu in *BleepingComputer* similarly reported Confiant said that this recent VeryMal campaign "lasted for two days between January 11-13, and targeted only US visitors."

The sneaky feats were taking advantage of a JavaScript vulnerability on Macs to redirect browsers to a site "where you get the opportunity to install a Flash 'update'. It looks to have been most active between January 11th and 13th, but evidence suggests it was active since December," said *PC Perspective*.

BleepingComputer reported: "An analysis from Adam Thomas of Malwarebytes shows that the phony update is a macOS adware installer known as Shlayer."

Reports said this was a steganography-based ad payload dropping a Shlayer Trojan on people using Macs.

Shlayer Trojan? You may have read about this last year when researchers discovered OSX/Shlayer, Mac malware. In a security blog last year, Joshua Long, a security analyst at Intego, said while malware disguised as an update to Adobe Flash Player was nothing new, some incarnations of fake Flash Player installers had a method of downloading additional content.

Stein responded to a reader's question: "In order to be infected by the malware, you had to have seen an ad from attacker's campaign. Not everyone who sees the ad gets redirected to the malware installer, but the few that fit the mold of what the attacker is looking for will."

Meantime, the Confiant site provided a sobering rundown of maladvertisers' effects on business. What happens due to these malicious impressions? The Confient blog examined the impact.

"You have the publisher who loses money directly from the interrupted user sessions, and loses future money from the increased ad blocking usage and user trust loss. There are the ad exchanges who had their inventory access cut off while they battled the infection and will have had some publishers pull their inventory out permanently. The advertisers will get hit with the resulting ad fraud from the infected devices. And let's not disregard the user, who now has an infected device."

Confiant benchmarked the cost impact for a January 11th peak adding up to over $1.2 million.

Looking for a longer-range estimate on malicious code stashed inside ad images? Catalin Cimpanu in *ZDNet* noted a GeoEdge report from last

November: Malicious code hidden inside ad images caused financial losses to ad networks estimated at around $1.13 billion in 2018.

More information: blog.confiant.com/confiant-mal … -on-mac-cd31e885c202

Citation: VeryMal: Campaign in image-based malware spotted (2019, January 27) retrieved 20 April 2024 from https://techxplore.com/news/2019-01-verymal-campaign-image-based-malware.html