New ransomware infections are the worst drive-by attacks in recent memory

reader comments

50 with 41 posters participating

Share this story

An ongoing operation that’s installing ransomware and other malware on the computers of unsuspecting website visitors is one of the most potent drive-by attack campaigns researchers have seen in recent memory.

The attacks install three pieces of malware using an exploit kit called GreenFlash Sundown, which researchers identified in 2015 and have continued to follow since. Attacks in recent weeks have spiked again as ShadowGate—one of the names given to the hacker group behind the campaign—has unleashed a highly revamped version of the exploit kit on hacked ad servers run by Web publishers. The most notable compromise is of an ad server belonging to onlinevideoconverter[.]com, a site with more than 200 million visitors per month that converts YouTube videos into video files that can be stored on a computer hard drive.

“They are ongoing and with a scale we haven’t seen in a couple of years when it comes to exploit kit-related attacks,” Jérôme Segura, a Malwarebytes researcher tracking the campaign, said of the attacks on onlinevideoconverter[.]com visitors. “We literally noticed a huge spike in our telemetry starting a few

days ago, which is very unusual. Given what we see in our telemetry, this is the most successful drive-by campaign we have seen in quite a while, so we can infer many people were affected by it.”

A significant escalation

Segura reported the revived campaign on Wednesday in a post that said the attacks were one of the first times the attackers had actively targeted people in Europe and North America. Previously, he said, the group had largely limited attacks to South Korea.

In an analysis published Thursday, researchers from Trend Micro echoed the assessment that the new campaign represents a significant escalation by the once-regional group.

“This is the most notable activity we have seen from this group since 2016,” Trend Micro’s Joseph C. Chen wrote. “Despite their low profile over the past couple of years, it seems that they have been continuously developing and evolving their exploit kit.”

Among the innovations in the new kit: well-obfuscated JavaScript hidden inside a fake GIF image that redirects people to fastimage[.]site, one of the attacker-controlled sites used to serve the exploit code. Another improvement is a fingerprinting mechanism that works on multiple levels to carefully select a subset of visitors to be exploited.

The first level of fingerprinting is performed at the network level. It filters out devices visiting from IP addresses assigned to virtual private networks and similar services, to ensure only users of residential IPs are targeted. Another round of fingerprinting uses a PowerShell script to gather details about the visitors’ devices, including their operating system, user name, video card, hard disk, and any antivirus products.

Crypto is hard

Yet another recently added feature is the use of public key encryption to protect the payloads carried by their exploit. Before targets are infected, the exploits generate a secret key that's unique to each computer. The secret key is encrypted with a public key and sent to the attackers. The attackers then use the decrypted secret key to encrypt the payloads. In theory, because the secret key is supposed to reside only in the memory of the targeted computer—and never written to disk or transmitted in plaintext—it should be hard for people reverse-engineering the exploits to analyze or identify the payloads.

Trend Micro researchers were able to defeat the encryption by exploiting a crucial weakness. A cryptographic nonce used in the generation of the unique secret key was reused as a separate encryption key and was sent in plaintext when the targeted computer communicated with one of the attacker servers. Once Trend Micro researchers obtained the nonce, they were able to reproduce the secret key that allowed them to decrypt the payload, or at least parts of it.

The ongoing compromise of onlinevideoconverter[.]com is one of a series of attacks researchers from both Malwarebytes and Trend Micro have observed the group carrying out on self-hosted ad servers running Revive Adversever. (This is an open rsource package that sometimes goes by its old name OpenX Source.)

Representatives of onlinevideoconverter[.]com didn't respond to an email seeking comment for this post.

The best way to protect against this campaign is to be sure to keep browsers, browser add-ons, and operating systems updated, since the attackss this group is known to use almost always exploit known vulnerabilities for which patches are available. Antivirus protection is also effective, since most engines

detect both the exploits and the payloads. Additionally, it’s almost never a bad idea to uninstall stand-alone versions of Flash.

Segura said the campaign is installing three separate pieces of malware, including the SEON ransomware, botnet malware known as Pony, and software that mines cryptocurrency on infected computers. The ransomware is particularly pernicious, since it deletes any shadowcopy files used for backup. The exploits are currently targeting only Windows computers that run outdated versions of Adobe’s Flash media player. Segura said visitors who have been infected will know immediately.

“The ransomware payload is the indication you were infected,” he told Ars. “It pops up a ransom note, and indeed, all the files have been encrypted.”

https://arstechnica.com/?p=1528735