What’s Next in Malware After Kuluoz?

researchcenter.paloaltonetworks.com/2015/08/whats-next-in-malware-after-kuluoz/

Ryan Olson August 10, 2015

By Ryan Olson

August 10, 2015 at 4:00 AM

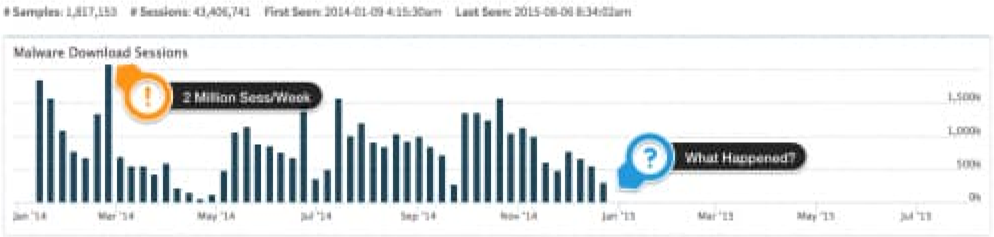
Category: Malware, Unit 42

Tags: Asprox, AutoFocus, CryptoWall, Dyre, kuluoz, Threat Landscape Review, Trojan, Upatre, WildFire

Regular readers of this blog have heard all about the infamous Kuluoz malware. This family was the latest evolution of the Asprox malware and at its peak in 2014 it accounted for 80% of all malware sessions we observed in WildFire. When the team published our Threat Landscape Review in December of last year, we highlighted this family as a scourge that impacted nearly every company Palo Alto Networks protected in 2014. Kuluoz was primarily distributed through e-mail, which means we saw large numbers of SMTP sessions, but also downloads over a variety of webmail clients.

Even if you didn’t read our blogs, you probably dealt with Kuluoz. Throughout 2014, most of the waves of spam e-mails carrying fake court notices, voicemail messages and package delivery alerts carried a Kuluoz attachment. If you opened these attachments you quickly became part of the botnet, sending copies of the malware to other victims while the botmaster silently installed additional malicious software on your system.

Given all of this activity, we were quite surprised when the malware all but disappeared at the end of December 2014.



Samples: 1,817,153 # Sessions: 43,406,741 First Seen: 2014-01-09 4:15:30am Last Seen: 2015-08-06 8:34:02am

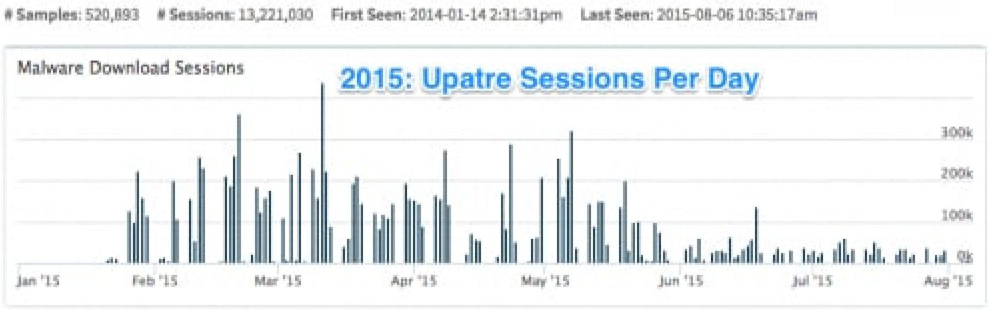
The screenshot above shows the number of malware sessions per week that we tagged as “Kuluoz” in the AutoFocus service. When we first noticed the drop-off, our suspicion was that we were “missing” the new Kuluoz samples. Just weeks earlier we published a report that highlighted their tactics -- a tactical shift in response would not have been unprecedented.

As weeks turned into months, we found that Kuluoz didn't return. We weren't the only ones who noticed; Brad Duncan wrote a blog for the SANS indicating that the e-mails which had previously carried Kuluoz were now just…spam.

Based on the data we've collected, the Kuluoz command and control infrastructure largely shut down in January and the botnet is no more. We continue to capture new samples of Kuluoz in WildFire as orphaned infections continue sending out newly-crypted variants of the malware, but the numbers are a tiny fraction of Kuluoz at its peak.

The original Asprox botnet has gone through multiple incarnations since it came online in 2007. We've not yet seen any indication that the individuals behind these attacks have been arrested or forced to stop operating, so it's likely that they've shut down this botnet to regroup and redeploy after they've found ways to evade the detections deployed by the security industry. After all, sending 80% of all malware puts you pretty high on everyone's list of priorities.

If you are wondering what malware has replaced Kuluoz as our top family, the reigning champion is Upatre, which is a downloader that typically installs the Dyre banking Trojan or the CryptoWall Ransomware. It's not nearly as prevalent as Kuluoz, but it's certainly making an impression:



Get updates from Palo Alto Networks!