Holiday lull? Not so much

proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much

January 12, 2018

Blog
Threat Insight
Holiday lull? Not so much

January 12, 2018 Proofpoint Staff

Overview

For at least the last two years, Proofpoint researchers have observed a seasonal lull in activity around the Thanksgiving holiday and during the weeks between Christmas and Russian Orthodox Christmas (January 7). Activity during the Thanksgiving 2017 holiday, however, was higher than in previous years, with multiple campaigns targeting a variety of regions. Examining year-over-year differences in malicious message volumes for the period of December 15 through January 12 revealed that, while activity dropped during this period, it remained significantly higher than what we observed the previous year and returned to near pre-holiday levels more quickly after January 7 than in 2017.

Analysis

Figure 1 shows a year-over-year comparison of message volume for the period of December 15-January 12. The week leading up to Christmas 2016 had significantly higher volumes than during the same week in 2017, primarily due to Locky ransomware campaigns distributed by TA505. Just before, we observed a slight jump in traffic around Christmas 2017 relative to both previous weeks in 2017 and the same week in 2017. Unlike in 2016, some actors seemingly worked through that week during which we generally expect very limited activity.

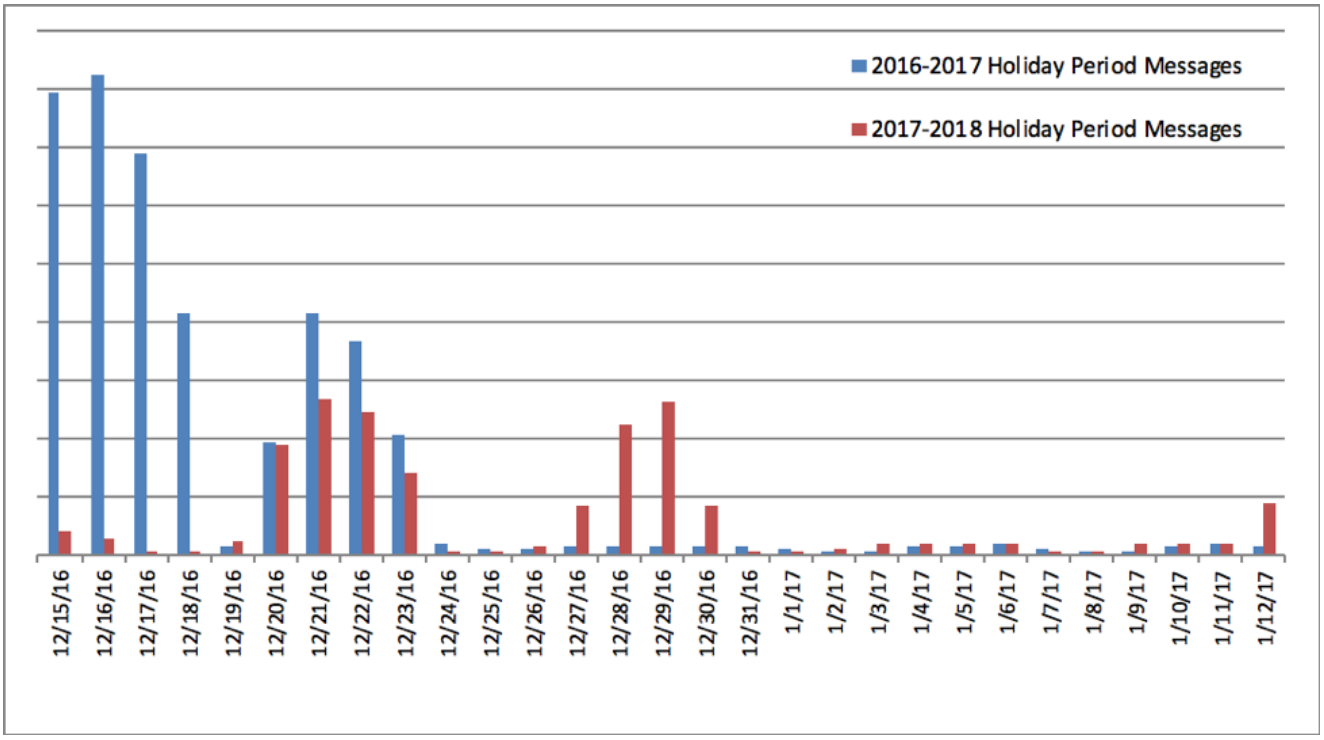

Figure 1: 2016 vs 2017 volumes for malicious messages during the holidays

Because the activities of threat actor TA505 tend to obscure the campaigns of other threat actors, breaking down activity during this period by actor gives a better sense of the nature and diversity of malware involved in these campaigns over the holidays. The following actors were actively conducting campaigns after December 22, 2017, but were inactive the year before between December 22, 2016, and January 2, 2017:

TA542 – We began tracking the actors behind Emotet in April of 2017 and as a result, did not track them during the 2016 holiday season. TA542 campaigns have appeared consistently since they emerged in April and, during the Christmas week, we observed Emotet distributed via URLs that led to malicious Microsoft Word documents with embedded macros used to download the malware. On at least one occasion during the Christmas week, Emotet also downloaded Zeus Panda. This instance of Zeus Panda primarily targeted online retail sites during the holiday season.

TA505 - The actors behind the massive Locky and Dridex campaigns of the last two years also passed up the full two-week Christmas break this year, relying heavily on malicious VBScript and JavaScript files in 7-Zip archives to deliver primarily GlobeImposter ransomware, with two separate large campaigns on December 27 and 28. In early 2017, TA505 took a nearly three month hiatus before resuming campaigns; this year, their campaigns resumed on January 11 after less than a two-week break around the Russian Orthodox Christmas. It is worth noting that TA505 activity is highly dependent on the Necurs botnet, so some of their quiet periods may relate to botnet disruptions or maintenance. However, we observed increases in activity from multiple actors this season, suggesting that this is not an artifact exclusively related to TA505 distribution.

TA544 – We observed a campaign targeting Japanese users dropping URLZone from malicious Microsoft Excel documents, which eventually led to a final Ursnif payload. This was the first time in several months that we had seen this particular infection chain.

TA543 – We identified another Ursnif campaign, this time targeting Australian users, via malicious Microsoft Word documents during the Christmas season. The campaign utilized a familiar theme, namely a billing notification lure using stolen branding for a widely recognized New Zealand-based accounting software company.

Conclusion

For years, threat actors typically avoided sending large, broad-based campaigns on major American and UK holidays and weekends. However, that tendency appears to be changing, perhaps because of widening geographical targets, attempts to have malspam waiting in crowded inboxes when users return from holidays, or attempts to deliver malware when defenders within organizations are more likely to be out of the office. Moreover, the heightened threat actor activity of the 2017-2018 holiday period reflects the broader trend of 2017 as whole, a year that saw fewer sustained disruptions in campaign activity by major threat actors. Whatever the reason for the change, it appears that some seasonal trends may be shifting such that defenders and end users should be prepared at all times to deal with both high-volume and targeted campaigns across geographies. Of particular note are campaigns from TA505 -- because this actor frequently drives a large percentage of global malicious spam, their much more rapid return to activity following the Russian Orthodox Christmas compared to 2016-2017 as well as higher levels of activity around the western Christmas holiday at the end of 2017 stands out as a potential indicator of a change in tactics.