The Day After Patch Tuesday: Effects Observable in IP Darkspace Traffic

Tanja Zseby[1,2], Alistair King[2], Nevil Brownlee[2,3], and kc Claffy[2]

[1] Fraunhofer Institute FOKUS, 10589 Berlin, Germany
[2] CAIDA, UCSD, San Diego, CA 92093, USA
[3] The University of Auckland, Auckland, New Zealand

Abstract. We investigated how Patch Tuesday affects the volume and characteristics of malicious and unwanted traffic as observed by a large IPv4 (/8) darkspace monitor over the first six months of 2012. We did not discover significant changes in overall traffic volume following Patch Tuesday, but we found a significant increase of the number of active hosts sending to our darkspace monitor the day after Patch Tuesday for all six investigated months. Our early results suggest the effects of Patch Tuesday are worth deeper investigation. Detecting time intervals during which new sources become active can help tune sampling methods toward activity periods that likely contain more interesting information (i.e., many new malicious sources) than other time periods.

Microsoft releases accumulated security patches on the second Tuesday of each month, termed "Patch Tuesday" (PT). Attackers can use the released patch information to exploit vulnerabilities on machines that have not yet been patched or to check whether security holes previously exploited are still open. Launching new malware immediately after Patch Tuesday also maximizes the potential lifetime of an exploit before a patch is deployed.

We investigated how Patch Tuesday affects the volume and characteristics of malicious and unwanted traffic as observed by a large IPv4 (/8) darkspace monitor [1] over the first six months of 2012. We used the tools corsaro [5], MATLAB and Wireshark to analyze packet counts, number of unique source addresses, top destination ports and packet content. We used the *IATmon* tool [3] to classify IP source hosts that contributed to observed darkspace traffic into 18 mutually exclusive source types. The classification is based on protocol and temporal patterns across a configured (in our case 1 hour) time interval.

First we analyzed the overall traffic without distinguishing among source types. The overall packet count did not reveal any unusual behavior at all at or around Patch Tuesday. But when we looked at the number of unique source IP addresses we found an interesting pattern that was consistent across all six months, shown in Figure 1. Specifically, immediately at midnight after PT, i.e., the first hour of "Exploit Wednesday" (EW), there was consistently a significant increase in the overall number of active sources, which typically remained elevated above its baseline value for several hours.

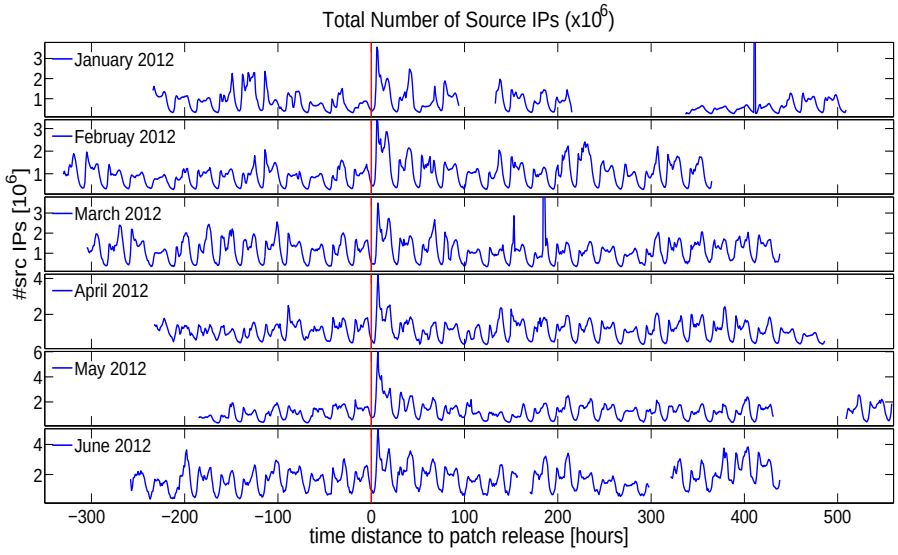

Fig. 1. Total number of unique source IP addresses per hour for 6 months. x-axis shows the time distance (in hours) from the patch release. Each month exhibits a significant increase in the number of unique source IPs shortly after PT. January and March have two other large peaks many days later that are truncated in the graph.

The *IATmon* source type analysis revealed that for all six months, the increase of active sources after Patch Tuesday is mainly caused by sources of the types '1 or 2 packets', i.e. all sources that send fewer than 3 packets, and 'UDP unknown', i.e. UDP sources that send more than 2 packets and target multiple destination addresses and destination ports (see [3]). In some months we also saw a significant increase of other source types on Exploit Wednesday, e.g., UDP probes in February and May, UDP vertical scans in July, UDP horizontal scans in May and μTorrent sources in April. But only the 'UDP unknown' and '1 or 2 packets' sources consistently increased on EW for all six months.

We saw only a few potential Patch Tuesday effects in our analysis of the packet count per source type. We saw an increase in UDP horizontal scans on EW in June and an increase of packets from 'TCP and UDP' sources on EW in July. The packet count for source type '1 or 2 packets' increased in all six months on EW, but just as a direct effect of the increase of the number of sources of this type. The source analysis also showed that 32% (in June) up to 56% (in March) of all darkspace packets originated from sources that performed TCP horizontal scans to port 445, a long-standing behavior that became even more common since the Conficker outbreak [2]. Between 13% (in January) and 42% (in April) of all observed packets were TCP backscatter (TCP-ACK, TCP-RST).

In January 2012 we saw a significant reduction of DNS backscatter traffic directly after PT. A DNS name server sent 4 to 6.5 million DNS backscatter

packets per hour throughout the 45 hours before PT in January and suddenly stopped sending within 2 hours after PT. These packets were standard DNS query response packets with a format error, sent in response to a name request for a porn web page. We assume that the queries to the name server were sent with spoofed source addresses, because the response packets have destination addresses in the darkspace. One possible explanation for this sudden drop in backscatter is that a patch was deployed that prevented compromised hosts (in a botnet) from continuing to participate in a DDoS attack against the name server sending us backscatter traffic.

In order to see whether the sources that caused the peaks in the overall source count aimed at specific vulnerabilities, we investigated how many of the sources were targeting specific destination ports. We analyzed the destination ports for all packets from sources of type 'UDP unknown' and from those sources of type '1 or 2 packets' that sent only UDP packets. Since some ports are generally more popular than others, we first calculated, as a baseline, the median number of sources per destination port over the whole month. We then looked at the number of sources per destination port on EW (midnight UTC) and PT (patch release time), and compared it to the median. We saw a broad distribution of destination ports targeted on EW; no ports had an especially high number of sources across all six months. We looked at the payload for some of the UDP packets sent to the top ten ports of the sources that became active every EW in all six months. We did not discover any new or surprising pattern, just more sources sending UDP packets that looked similar to those we see at other times.

Although we have only analyzed a slice of data, our preliminary results indicate that Patch Tuesday effects merit further investigation, ideally on multiple sources of darknet data or in combination with data from networks with active hosts. Longitudinal trends of malicious behavior related to Patch Tuesday may help quantitative assessments of the health of one component of the Internet. Information about source activity patterns can also help to optimize measurement methods, e.g. by tuning sampling techniques toward time periods with high source activities. The data used in this analysis is available at [4].

References

1. UCSD Network Telescope, 2010. `http://www.caida.org/data/passive/network_telescope.xml`.
2. Emile Aben. Conficker/Conflicker/Downadup as seen from the UCSD Network Telescope. Technical report, CAIDA, February 2009. `http://www.caida.org/research/security/ms08-067/conficker.xml`.
3. Nevil Brownlee. One-way Traffic Monitoring with iatmon. In *13th Passive and Active Measurement Conference (PAM 2012)*, 2012.
4. CAIDA. Patch Tuesday Dataset. `http://www.caida.org/data/passive/telescope-patch-tuesday.xml`, 2012.
5. Alistair King. Corsaro. http://www.caida.org/tools/measurement/corsaro/, October 2012.