Black Friday Cyber Threats

Last year, Black Friday was a big day – for shoppers and hackers alike.

With Black Friday 2016 being days away, our partners at Recorded Future decided to analysize the trends during the 2015 holiday period. Their research found that targeted threats against shoppers and retailers increase as the volume of shoppers multiplies.

So how can you stay safe during this season?

Watch out for key attack methods used over the Black Friday holiday period. These include:

- Phishing/Smishing/Spam
- Malvertising
- Pre-Installed Malware
- POS Malware
- Service Disruption Attacks
- Account Takeovers

There are also recent advances in threat actor TTPs, including:

- Updated POS Malware such as FastPOS
- Increased service disruption potential following the Mirai botnet 1.2TB DDoS attack.

Analysis

Black Friday sales and deals extend to Cyber Monday nowadays and attacks can be seen for the whole weekend or even the whole holiday season. Akamai reports the Black Friday to Cyber Monday weekend is becoming as popular and important for retailers and e-commerce sites in Europe as it is in America[1].

Looking at Recorded Future's history of reported incidents around the holiday period during 2015, it is clear there is heightened attention around Black Friday campaigns (seen in Figure 1). Details of the common attack methods seen are described below.

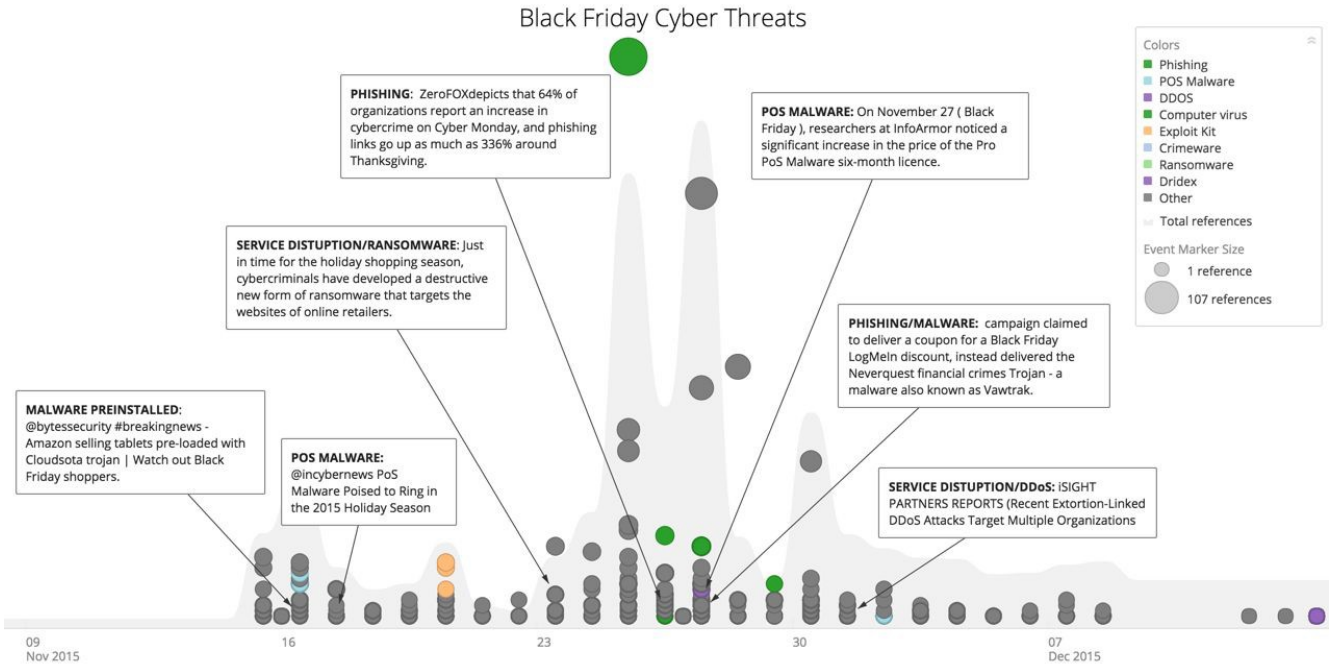

Figure 1: Recorded Future Cyber Threats around Black Friday Weekend 2015

Phishing/Smishing/Spam

- According to security firm ZeroFox phishing links go up as much as 336% around Thanksgiving[5]. Email, text message and social media messages all may containscams to dupe customers.
- Themes included: payment related fraudulent emails purporting to be from PayPal[3], delivery confirmation email claiming a package is being delivered, coupons promoting products or retailers, and fake refunds[2]. Phishing kits even have holiday packages to help fraudsters lure customers[4].

Malvertising

- Malvertising attacks use online ads to distribute malware via reputable Web sites. Invincia reports Yahoo!, eBay UK, and Huffington Post visitors were all hit with malvertising prior to the 2015 holiday season[9,17].

Pre-Installed Malware

- Reports of pre-installed malware on tablets purchased from various retailers including Amazon were seen ahead of the Black Friday sales[8]. It is not the first case of this type of threat with Android, Lenovo and other smartphones having been infected in the past[14].

POS Malware

- Reports on Point of Sale Malware, for stealing credit card details directly from retailers, were released ahead of the 2015 holidays. ModPOS[6] and Pro PoS[7] were two variants of the malware reported by security firms to be actively used and targeting retailers. Symantec states the most common attack route against POS systems is through the corporate network. Once an attacker gains access to the corporate network, for example through a vulnerable public-facing server or spear-phishing email, the attacker could traverse the network until they gain access to an entry point to the POS network. This entry point is often the same as a corporate administrator would utilize to maintain the POS systems[26].

Service Disruption Attacks

- According to Akamai[1], Distributed Denial of Service (DDoS) attacks are a consistent threat for retailers during the holidays. DDoS attacks can take down a retailer's online site during the busiest shopping days of the year and often come with an extortion threat.

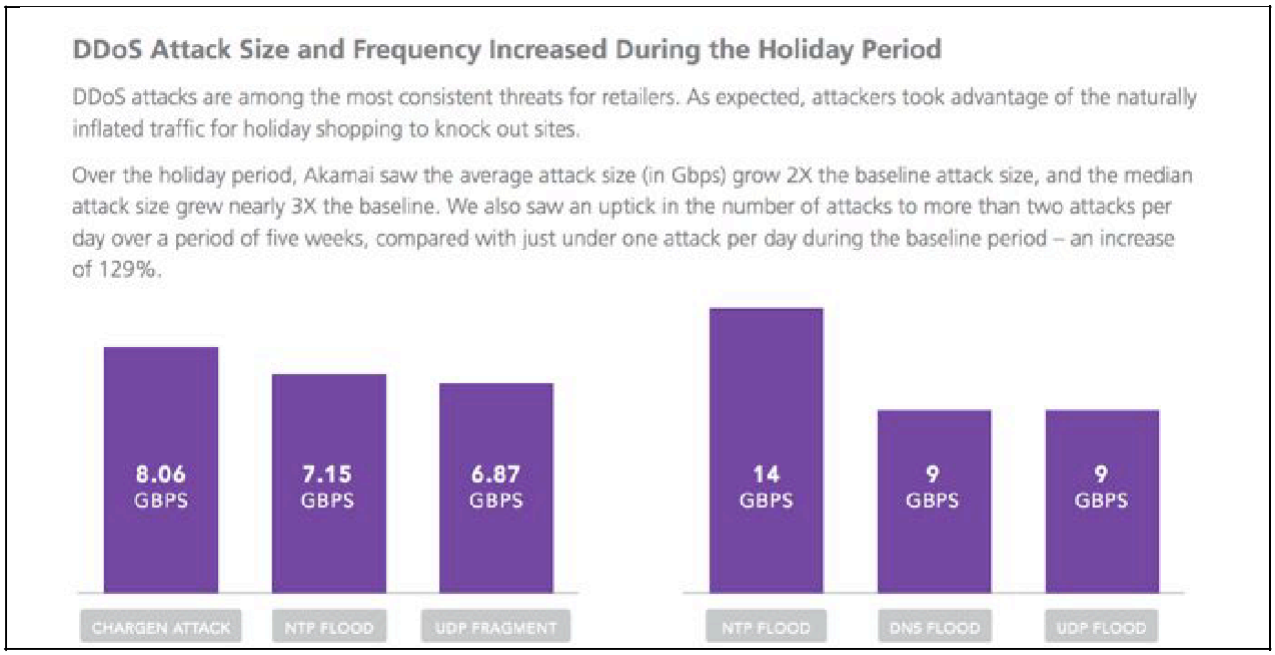

Figure 2: Akamai 2015 Online Holiday Shopping Trends and Traffic Report[1]

- Additionally according to independent security journalist Brian Krebs, fraudsters have developed new ransomware – dubbed 'Linux.Encoder.1' – that targets websites to essentially hold the site's files, pages and images for ransom[28].

Account Takeovers

- Account takeover is big business for criminal actors, and they're targeting more than bank information. Accounts such as mobile phone contracts, PayPal and Uber can sell for much

more than stolen credit card details on the underground market.[22,23] ThreatMatrix Q4 2015 report states there was a large increase in account creation and account takeover fraud driven by the increased availability of stolen identities in the wild, harvested from massive breaches. The overall attacks increased by over 100% compared to the previous year. Additionally it is mentioned there was an 80% increase in attacks over Q4 2014; and 250% increase in attacks on retailers during the peak shopping days.[21]

Expectations for 2016

We do envision more of the same types of attacks as threat actors advance and enhance their TTPs.

- Holiday-Themed Phishing/Smishing/Spam – Dynamoo's security blog is currently reporting many cases of Locky malware being spread. This is likely to continue over the holidays.[11]
- POS Malware - FastPOS was just reported to be updated in October ahead of the holiday season.[12]
- DDOS attacks – The Mirai 'Internet-of-Things' (IoT) botnet attack that took many websites offline via attacking DNS service provider Dyn on October 21st is likely to be a large threat over the holidays especially as the source code has been released.[13] Criminal botnet operators will likely use Mirai's success as a way to extract blackmail payments from online retailers and banks with threats of interfering with online shopping.
- Pre Installed Malware – this year preinstalled malware have already been seen on CCTV devices and cheap noname Android devices.[15,16]
- Malvertising – Big mainstream sites like the BBC and the New York Times have already been found to be serving malware via malvertising this year.[27] More recently Spotify and Google AdWords have been spreading malware via adds.[18,19]
- Account Takeover – There have been many data breaches in the press already this year.[24] Some may have occurred years ago (like Yahoo[25]) but data is being openly shared now. This type of personal data can be used by threat actors to facilitate account takeovers. Some breaches may contain full credentials that are being sold on the underground market.

In addition to the threats above, there have been recent warnings of fake apps being pushed ahead of this holiday season to the Apple App Store. The New York Times reports: Hundreds of fake retail and product apps have popped up in Apple's App Store in recent weeks — just in time to deceive holiday shoppers.[20]

References

1. https://www.akamai.com/uk/en/multimedia/documents/content/white-paper/akamai-2015-online-holiday-shopping-traffic-re port-white-paper.pdf
2. https://us.norton.com/busylife-black-friday-scams/article
3. http://www.redeszone.net/2015/12/02/nueva-campana-phishing-de-paypal-tras-el-black-friday-y-el-cyber-monday/
4. http://community.spiceworks.com/topic/1307915-new-holiday-campaign-with-9-new-simulated-phishing-templates?utm_campaign=item&utm_medium=rss&utm_source=global
5. https://www.zerofox.com/blog/cyber-monday-breeds-cyber-crime-infographic/
6. https://www.fireeye.com/blog/threat-research/2015/11/modpos.html
7. https://infoarmor.com/wp-content/uploads/2016/04/Pro-POS-Solution-FINAL.pdf
8. http://www.cmcm.com/blog/en/security/2015-11-09/842.html
9. https://www.invincea.com/2015/12/invincea-holiday-shopping-safety-and-survival-guide/
10. https://twitter.com/poshcricketer/statuses/687199579314483200
11. http://blog.dynamoo.com/
12. https://www.cin7.com/alert-fastpos-malware-threat/
13. http://arstechnica.co.uk/security/2016/10/that-botnet-of-things-malware-is-getting-a-nasty-makeover/
14. http://www.scmagazineuk.com/chinese-android-smartphones-now-shipping-with-pre-installed-malware/article/436631/
15. http://thehackernews.com/2016/04/home-security-system.html
16. http://hungrygizmo.com/2016/06/27/the-danger-of-no-name-android-devices-pre-installed-malware/
17. http://business-reporter.co.uk/2015/12/21/malvertising-expected-to-triple-and-ransomware-on-the-rise-in-2016/
18. https://www.scmagazine.com/spotify-serving-malicious-ads-to-freemium-users/article/527585/
19. http://www.darkreading.com/attacks-breaches/google-adwords-malvertising-campaign-targets-apple-macs-/d/d-id/132735 7
20. http://www.nytimes.com/2016/11/07/technology/more-iphone-fake-retail-apps-before-holidays.html?_r=0
21. https://www.threatmetrix.com/whitepapers/threatmetrix-cybercrime-report-Q42015-en-us.pdf?_ga=1.105819655.526295316.1479140011
22. http://www.darkreading.com/endpoint/anatomy-of-an-account-takeover-attack/a/d-id/1324409
23. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-follow-the-data.pdf
24. http://www.crn.com/slide-shows/security/300081491/the-10-biggest-data-breaches-of-2016-so-far.htm
25. http://arstechnica.com/security/2016/11/yahoo-admits-some-staff-knew-of-mega-breach-in-2014/
26. https://www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf
27. https://www.theguardian.com/technology/2016/mar/16/major-sites-new-york-times-bbc-ransomware-malvertising
28. https://krebsonsecurity.com/2015/11/ransomware-now-gunning-for-your-web-sites/