Phishing Campaign Leverages WOFF Obfuscation and Telegram Channels for Communication

fireeye.com/blog/threat-research/2021/01/phishing-campaign-woff-obfuscation-telegram-communications.html

Breadcrumb

Threat Research

Bernard Sapaden, Mohammed Mohsin Dalla, Rahul Mohandas, Sachin Shukla, Srini Seethapathy, Sujnani Ravindra

Jan 26, 2021

5 mins read

Threat Research

FireEye Email Security recently encountered various phishing campaigns, mostly in the Americas and Europe, using source code obfuscation with compromised or bad domains. These domains were masquerading as authentic websites and stole personal information such as credit card data. The stolen information was then shared to cross-platform, cloud-based instant messaging applications.

Coming off a busy holiday season with a massive surge in deliveries, this post highlights a phishing campaign involving a fake DHL tracking page. While phishing attacks targeting users of shipping services is not new, the techniques used in these examples are more complex than what would be found in an off-the-shelf phishing kit.

This campaign uses a WOFF-based substitution cypher, localization specific targeting, and various evasion techniques which we unravel here in this blog.

Attack Flow

The attack starts with an email imitating DHL, as seen in Figure 1. The email tries to trick the recipient into clicking on a link, which would take them to a fake DHL website. In Figure 2, we can see the fake page asking for credit card details that, if submitted, would give the user a generic response while in the background the credit card data is shared with the attackers.

Figure 1: DHL phishing attempt

Figure 2: Fake website imitating DHL tracking

This DHL phishing campaign uses a rare technique for obfuscating its source page. The page source contains proper strings, valid tags, and appropriate formatting, but contains encoded text that would render gibberish without decoding prior to loading the page, as seen in Figure 3. Typically, decoding such text is done by including script functions within the code. Yet in this case, the decoding functions are not contained in the script.

Figure 3: Snippet of the encoded text on page source

The decoding is done by a Web Open Font Format (WOFF) font file, which happens upon loading the page in a browser and will not be visible in the page content itself. Figure 4 shows the substitution cipher method and the WOFF font file. The attacker does this to evade detection by security vendors. Many security vendors use static or regex signature-based rules, so this method will break those naïve-based conditions.

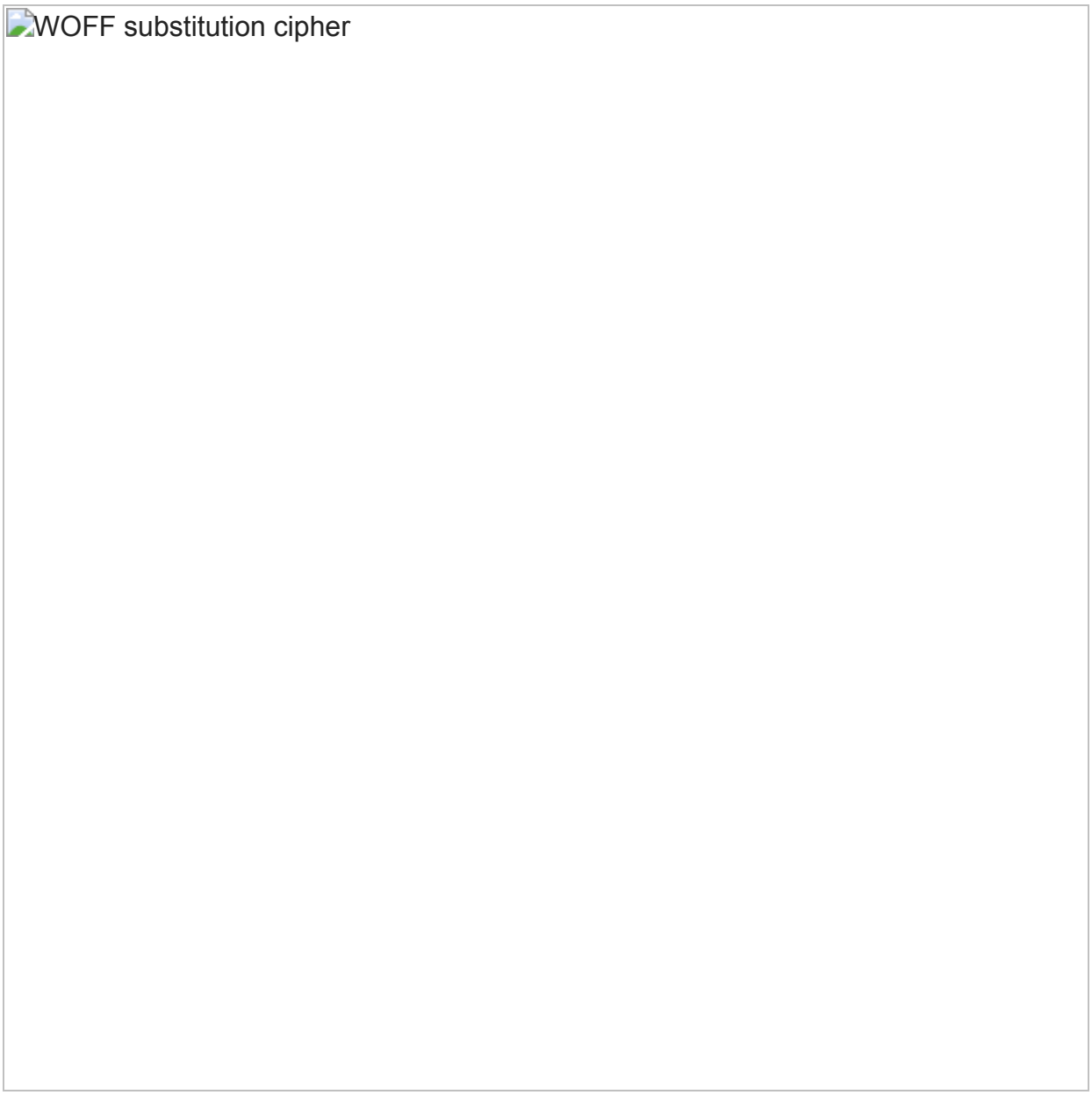

Figure 4: WOFF substitution cipher

Loading this custom font which decodes the text is done inside the Cascading Style Sheets (CSS). This technique is rare as JavaScript functions are traditionally used to encrypt and decrypt HTML text.

Figure 5: CSS file for loading WOFF font file

Figure 5 shows the CSS file used to load the WOFF font file. We have also seen the same CSS file, style.css, being hosted on the following domains:

- hxxps://www.lifepointecc[.]com/wp-content/sinin/style.css
- hxxps://candyman-shop[.]com/auth/DHL_HOME/style.css
- hxxps://mail.rsi-insure[.]com/vendor/ship/dhexpress/style.css
- hxxps://www.scriptarticle[.]com/thro/HOME/style.css

These legitimate-looking domains are not hosting any phishing websites as of now; instead, they appear to be a repository for attackers to use in their phishing campaigns. We have seen similar phishing attacks targeting the banking sector in the past, but this is newer for delivery websites.

Notable Techniques

Localization

The phishing page displays the local language based on the region of the targeted user. The localization code (Figure 6) supports major languages spoken in Europe and the Americas such as Spanish, English, and Portuguese.

Figure 6: Localization code

The backend contains PHP resource files for each supported language (Figure 7), which are picked up dynamically based on the user's IP address location.

Figure 7: Language resource files

Evasion

This campaign employs a variety of techniques to evade detection. This will not serve up a phishing page if the request came from certain blocked IP addresses. The backend code (Figure 8) served the users with a "HTTP/1.1 403 Forbidden" response header under the following conditions:

- IP has been seen five times (AntiBomb_User func)
- IP host resolves to its list of avoided host names ('google', 'Altavista', 'Israel', 'M247', 'barracuda', 'niw.com.au' and more) (AntiBomb_WordBoot func)
- IP is on its own local blocklist csv (x.csv in the kit) (AntiBomb_Boot func)
- IP has seen POSTing three times (AntiBomb_Block func)

Figure 8: Backend evasion code

After looking at the list of blocked hosts, we could deduce that the attackers were trying to block web crawlers.

Data Theft

The attackers behind this phishing campaign attempted to steal credentials, credit card data, and other sensitive information. The stolen data is sent to email addresses and Telegram channels controlled by the attacker. We uncovered a Telegram channel where data is being sent using the Telegram Bot API shown in Figure 9.

Figure 9: Chat log

While using php *mail()* function to send stolen credentials is quite common, in the near past, encrypted instant messaging applications such as Telegram have been used for sending phished information back to command and control servers.

We were able to access one of the Telegram channels controlled by the attacker as shown in Figure 10. The sensitive information being sent in the chat includes IP addresses and credit card data.

Figure 10: Telegram channel with stolen information

Conclusion

Attackers (and especially phishers) are always on the hunt for new ways to evade detection by security products. Obfuscation gives the attackers an edge, and makes it harder for security vendors to protect their customers.

By using instant messaging applications, attackers get user data in real time and victims have little to respond once their personal information is compromised.

Indicators of Compromise (IOC)

FireEye Email Security utilizing FAUDE (FireEye Advanced URL Detection Engine) protects customers from these types of phishing threats. Unlike traditional anti-phishing techniques dependent on static inspection of phishing URL content, FAUDE uses multiple artificial intelligence (AI) and machine learning (ML) engines to more effectively thwart these attacks.

From December 2020 until the time of posting, our FAUDE detection engine saw more than 100 unique URLs hosting DHL phishing pages with obfuscated source code, including:

- hxxps://bit[.]ly/2KJ03RH
- hxxps://greencannabisstore[.]com/0258/redirect-new.php

- hxxps://directcallsolutions[.]co[.]za/CONTACT/DHL_HOME/
- hxxps://danapluss[.]com/wp-admin/dhl/home/
- hxxp://r.cloudcyberlink[.]digital/<path> (multiple paths using same domain)

Email Addresses

- medmox2k@yandex[.]com
- o.spammer@yandex[.]com
- cameleonanas2@gmail[.]com

Telegram Users

- @Saitama330
- @cameleon9

style.css

- Md5: 83b9653d14c8f7fb95d6ed6a4a3f18eb)
- Sha256: D79ec35dc8277aff48adaf9df3ddd5b3e18ac7013e8c374510624ae37cdfba31

font-woff2

- MD5: b051d61b693c76f7a6a5f639177fb820
- SHA-256: 5dd216ad75ced5dd6acfb48d1ae11ba66fb373c26da7fc5efbdad9fd1c14f6e3

Domains

Pradosdemojanda[.]com
global-general-trackks.supercarhiredubai[.]com
tracking-dhi.company
Tapolarivercamp[.]com
Rosariumvigil[.]com
Mydhlexpert[.]com
Autorepairbyfradel[.]com

URLs

hxxps://wantirnaosteo[.]com[.]au/logon/home/MARKET/F004f19441/11644210b.php

hxxps://ekartenerji[.]com[.]tr/wp-admin/images/dk/DHL/home.php

hxxps://aksharapratishthan[.]org/admin/imagess/F004f19441/sms1.php

hxxps://royalgateedu[.]com/wp-content/plugins/elementor/includes/libraries/infos/package/F004f19441/00951124a.php

hxxps://vandahering[.]com[.]br/htacess

hxxps://hkagc[.]com/man/age/F004f19441/11644210b.php

hxxps://fiquefitnes[s]comsaude[.]com/.well-known/MARKET/MARKET/F004f19441/11644210b.php

hxxps://juneispearlmonth[.]com/-/15454874518741212/dhl-tracking/F004f19441/00951124a.php

hxxps://www.instantcopywritingscript[.]com/blog/wp-content/22/DHL/MARKET

hxxps://isss[.]sjs[.]org[.]hk/wp-admin/includes/F004f19441/11644210b.php

hxxps://www.concordceramic[.]com/fr/frais/F004f19441/11644210b.php

hxxps://infomediaoutlet[.]com/oldsite/wp-content/uploads/2017/02/MARKET/

hxxps://wema-wicie[.]pl/dh/l/en/MARKET

hxxps://www.grupoindustrialsp[.]com/DHL/MARKET/

hxxps://marrecodegoias[.]com[.]br/wp-snapshots/activat/MARKET/F004f19441/11644210b.php

hxxps://villaluna[.]de/wp-content/info/MARKET/F004f19441/11644210b.php

hxxp://sandur[.]dk/wp-content/upgrade/-/MARKET/

hxxps://chistimvse[.]com/es/dhl/MARKET/

hxxps://detmayviet[.]com/wp-includes/widgets/-/MARKET/F004f19441/11644210b.php
hxxps://dartebreakfast[.]com/wp-content/plugins/dhl-espress/MARKET/
hxxps://genesisdistributors[.]com/-/Tracking/dhl/Tracking/dhl-tracking/F004f19441/00951124a.php
hxxps://www.goldstartechs[.]com/wp-admin/js/widgets/102/F004f19441/11644210b.php
hxxps://universalpublicschooltalwandisabo[.]com/DHL
hxxps://intranet[.]prorim[.]org[.]br/info/MARKET/F004f19441/11644210b.php
hxxps://administrativos[.]cl/mail.php
hxxps://nataliadurandpsicologa[.]com[.]br/upgrade/MARKET/F004f19441/11644210b.php
hxxps://tanaxinvest[.]com/en/dhl/MARKET/
hxxps://deepbluedivecenter[.]com/clear/item/
hxxps://keystolivingafulfilledlife[.]com/wp-admin/includes/daspoe99i3mdef/DOCUNTRITING
hxxps://juneispearlmonth[.]com/-/15454874518741212/dhl-tracking/F004f19441/00951124a.php