FireEye
SECURITY REIMAGINED

SPECIAL REPORT

EMAIL CAMPAIGNS DURING THE 2015 HOLIDAY SEASON

FireEye Labs

CONTENTS

EMAIL CAMPAIGN TRENDS

Banker Malware

- Dridex remains one of the most widely distributed malware families.
- We observed shifts in Dridex's malware delivery techniques as well as a widespread infection campaign.

Ransomware

- TeslaCrypt has been increasingly active using malicious JavaScript as its downloader infection vector.
- The JavaScript files used are highly unique due to the ease of updating their script-based downloaders.

New Malware

- Nivdort is a malware family worth paying attention to as it is becoming increasingly aggressive.
- The mobile messaging app WhatsApp is often used as a phishing topic to socially engineer users into opening the malicious attachments.

Email phishing remains one of the primary infection **vectors used by threat actors to deliver malware.**

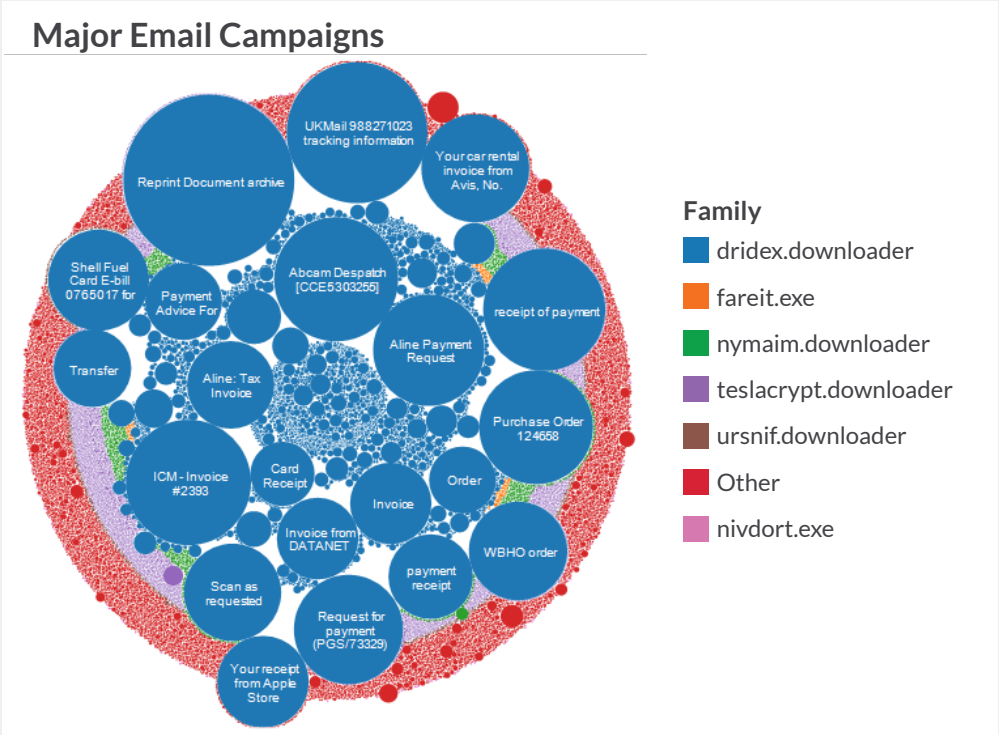
OVERVIEW

The holidays are that time of the year when cyber criminals relentlessly look for more effective and fortuitous opportunities to spread threats and launch criminal activities. The holiday season is known historically to herald a significant number of email-borne threats, often using relevant themes such as merchant sales or package deliveries to attack unsuspecting users and trick even the keenest ones.

FireEye Labs has collected data on the most prominent malware families delivered via email campaigns this holiday season. This report focuses on different varieties of malicious emails laced with Dridex, Nivdort, Fareit, Nymaim, UrSnif and TeslaCrypt malware.

Figure 1 shows the major email campaigns that we will discuss.

Figure 1: The Prevalence of the Various Malware Family Campaigns



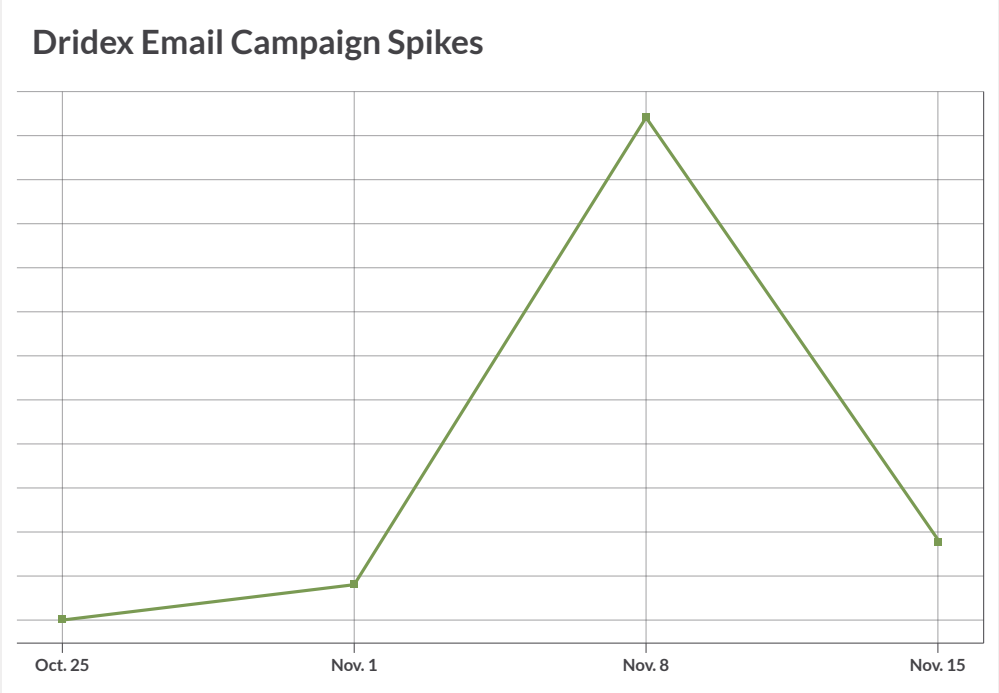
DRIDEX

TAKING a commanding lead is the notorious Dridex[1] — a highly prevalent strain of banking Trojan whose primary goal is to steal credentials and obtain money from the victim's accounts. Dridex is known to be highly dynamic and adaptive to increase its chance of infecting users. Dridex is mainly distributed though phishing emails using malicious Word or Excel attachments or malicious hyperlinks.[2] However, we noticed a recent change in its distribution methods.

Soon after the arrest of a major Dridex operator in mid-October 2015, we saw a Dridex campaign picking up in the third week of October. We also observed a shift from the typical Dridex distribution method of using malicious Word macros to using malicious Excel macros and exploit kits.[3]

As shown in Figure 2, we noted a sharp spike in malicious Excel infection activity with at least a tenfold increase in volume during the week of Nov. 8, 2015. We believe that this noticeable shift in the attackers' activity and techniques was intended to help them regain control of their lost turf.

Figure 2: Timeline of Dridex Distributed Using Malicious Excel Attachments



[1] https://www.fireeye.com/blog/threat-research/2015/06/evolution_of_dridex.html
[2] https://www.fireeye.com/blog/threat-research/2015/10/macros_galore.html
[3] https://www.proofpoint.com/us/threat-insight/post/dridex-shifu-give-spam-bots-day-off

EMAIL messages used to deliver Dridex in recent weeks have attempted to fool recipients by spoofing content from courier and logistics giant UK Mail, rental car service Avis, and petrochemical company Shell (see Figure 3 and Figure 4). Dridex capitalized further on the holidays by sending fake Christmas-themed invoices from networking company Knowledge Network West shortly before Christmas.

Figure 3: Dridex Avis Campaign

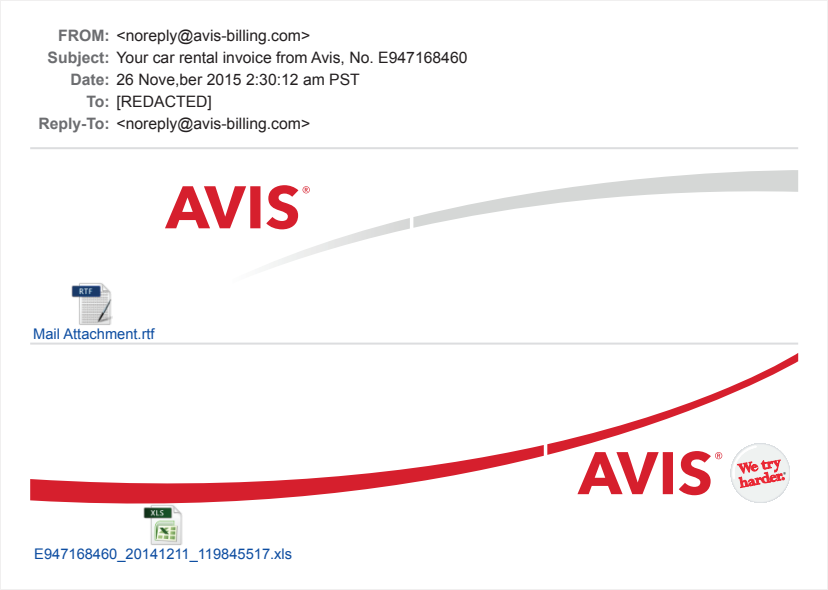


Figure 4: Dridex Email Samples

Below are some email subjects used by Dridex campaigns during this timeframe:

- Reprint Document Archive
- UKMail XXXXXXXXX tracking information
- Your car rental invoice from Avis, No. XXXXXXXXXX
- Abcam Despatch [XXXXXXXXXX]
- ICM - Invoice #XXXX
- Shell Fuel Card E-bill XXXXXXX for Account B500101 DD/MM/YYYY
- Purchase Order XXXXXX
- Request for payment (PGS/XXXXX)
- Your receipt from Apple Store
- Aline Payment Request

For Dridex Indicators of Compromise (IOCs), please see APPENDIX 1.

FAREIT

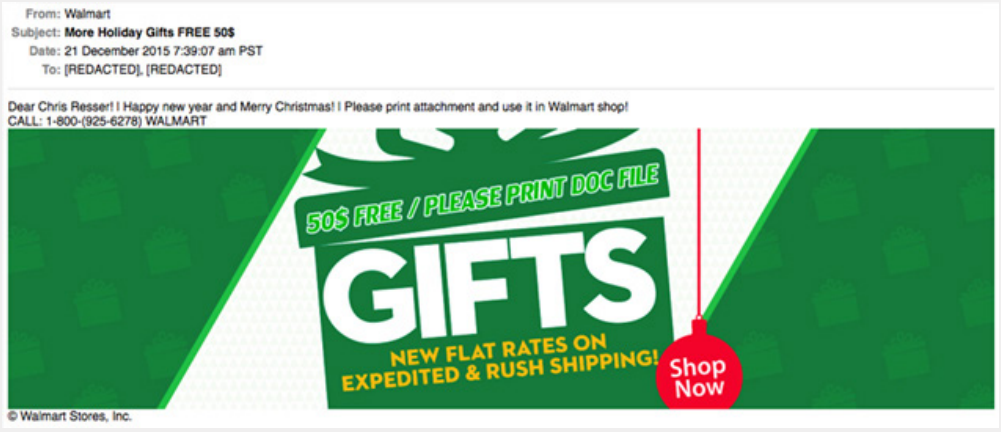
Fareit, also known as Pony Loader, has been around for several years. Its main goal is to collect credentials from File Transfer Protocol (FTP) applications, browser caches and cryptocurrency wallets such as Bitcoin, Bytecoin and Litecoin.

Historically, Fareit is installed as a second-stage downloader by other malware, including fake antivirus Trojans such as FakeScanti and Backdoor, Cycbot, Trojans such as Zeus, and ransomware such as Cryptolocker. Recent developments suggest that Fareit is now using malicious spam campaigns as the infection vector in attacks.

During this holiday season, we noticed that Fareit abused Walmart – one of the top retailers in the United States – by using fake emails saying that Walmart was giving away gift cards just a few days before Christmas (see Figure 5).

Fareit also leveraged the travel aspect of the holiday season by using email messages with itineraries and reservations. Some of the emails were designed to appear to come from American Airlines and luxury travel company Abercrombie and Kent Travel (see Figure 6).

Figure 5: Fareit Walmart Campaign

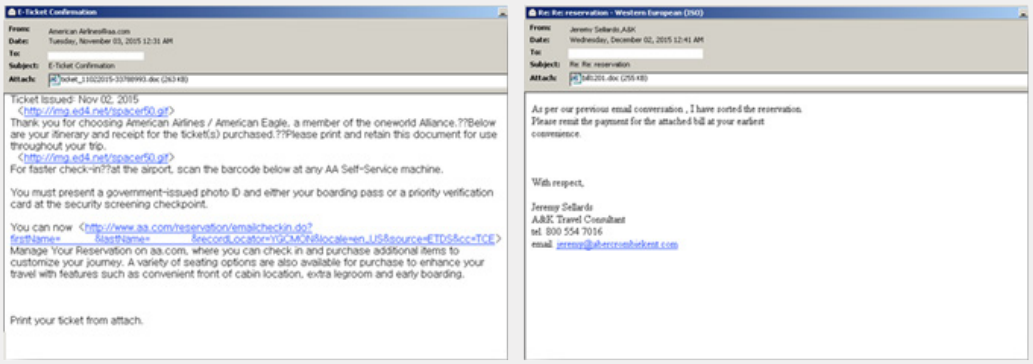


Below are some email subjects used by Fareit campaigns during this timeframe:

- E-Ticket Confirmation
- Re: Re: Reservation
- Re: New Year Order
- More Holiday Gifts FREE 50$
- More Holiday Gifts
- Walmart FREE 50$ On Giftcards
- Walmart Present FREE 50$
- Gift from Walmart
- Gift from Walmart!
- Walmart FREE Bonus On Giftcards
- Walmart Present FREE 50$

For Fareit IOCs, please see APPENDIX 2.

Figure 6: Fareit Email Samples



The holiday season is historically known to bring a significant number of email-borne threats, many using relevant themes such as merchant sales or package deliveries to attack unsuspecting users and trick even the keenest ones.

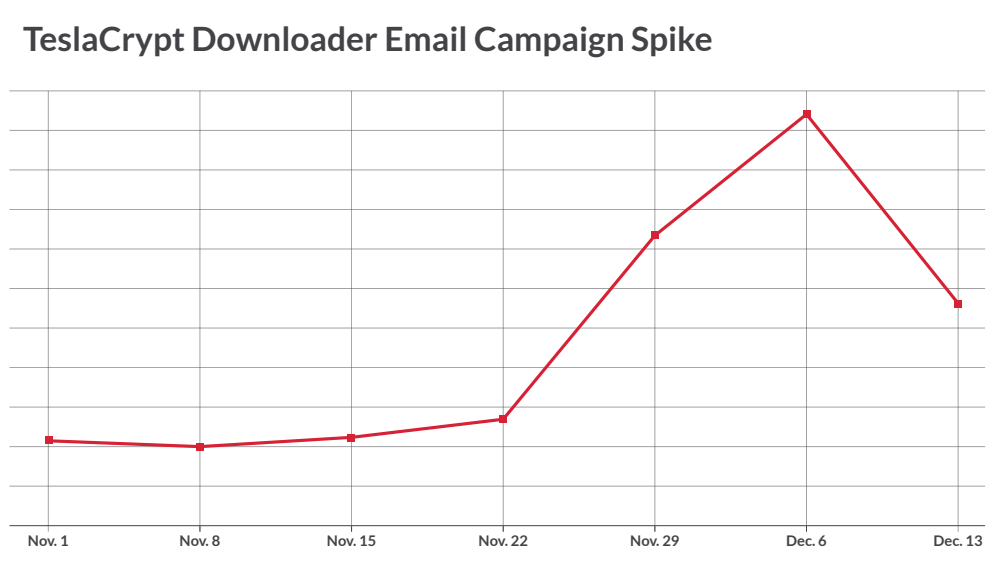
TESLACRYPT CAMPAIGNS

TESLACRYPT is a ransomware first observed in February 2015. It is spread via the Angler Exploit Kit,[4] and has since become one of the most active ransomware families. TeslaCrypt has been known in the past as AlphaCrypt.

FireEye Labs observed a rapid increase in TeslaCrypt-related malicious email activity in the weeks leading up to the holiday season (see Figure 7). Email messages used to deliver TeslaCrypt are similar to those associated with UrSnif in that they are very generic. TeslaCrypt campaigns only spoofed brand names or well-known companies on very few occasions. The malicious email campaigns leveraged Donoff macro downloaders. These downloaders are famous for delivering other malicious payloads such as Dridex, which delivers TeslaCrypt in parallel with JavaScript downloaders. The downloader scripts themselves are sometimes named Nemucod.

We also observed that the malicious script-based downloaders used by Telsacrypt were often unique in terms of their hash (MD5 sum); this is very different than in other spam campaigns where a unique malicious downloader is delivered in bulk. We believe that this could be due to the ease of creating new malicious samples using certain generators.

Figure 7: TeslaCrypt Downloader Email Campaign Spike



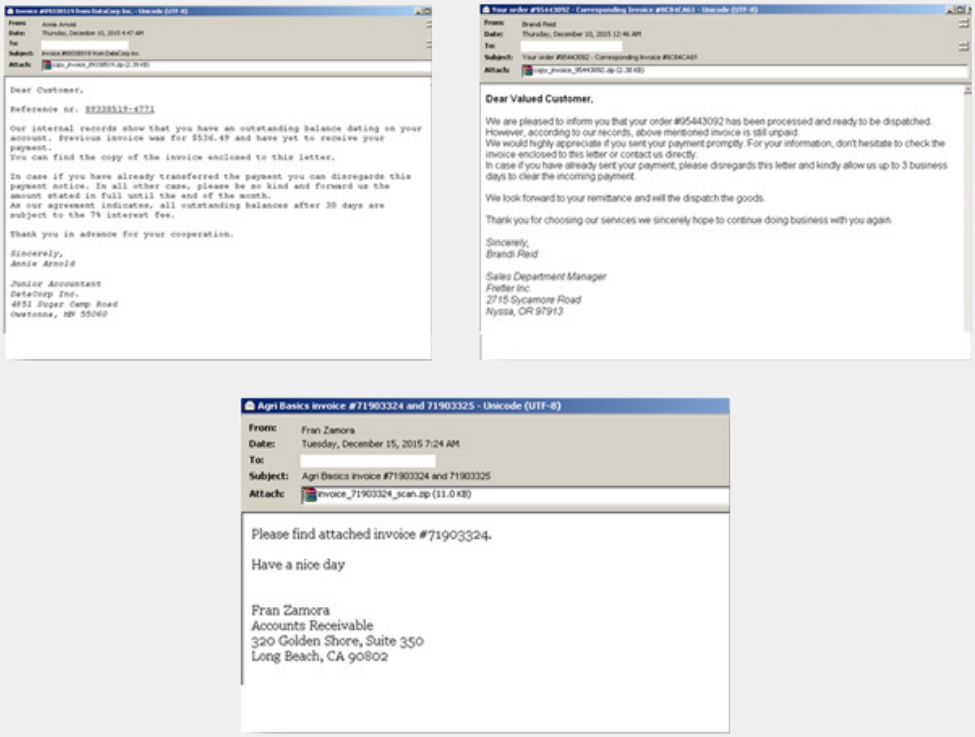
[4] https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=TrojanSpy:Win32/Nivdort.P

Below are some email subjects used by TeslaCrypt campaigns during this timeframe:

- Your order #XXXXXXXX - Corresponding Invoice #XXXXXXXX
- Your order #XXXXXXXX
- Your account has a debt and is past due
- Reference Number #XXXXXXXX, Last Payment Notice
- Payment Request, Ref. nr: XXXXXXXX/YYYY
- Payment Nr: XXXXXXXX/XXXXXXXX
- Invoice from PASSION BEAUTY SUPPLY LTD
- Invoice #XXXXXXXX from DataCorp Inc.
- Agri Basics invoice # XXXXXXXX and XXXXXXXX

For TeslaCrypt IOCs, please see APPENDIX 3.

Figure 8: TeslaCrypt Email Samples



NIVDORT

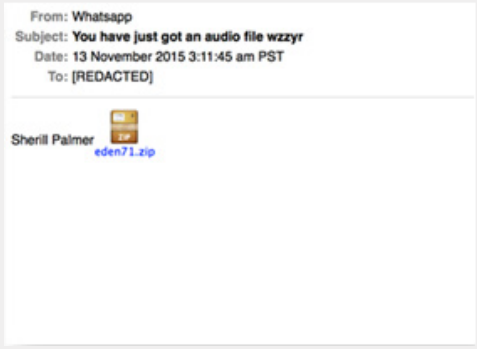
COMPARED to the other malware described in this paper, Nivdort is a less widely observed threat.[5] In general, its activity pattern is erratic, which makes it interesting. Commonly observed arriving as a ZIP attachment from email spam, Nivdort's behavior is similar to that of TrojanSpy. The malware may sniff sensitive HTTP information by: (1) redirecting traffic intended for legitimate websites to an attacker-controlled IP address by modifying the infected computer's

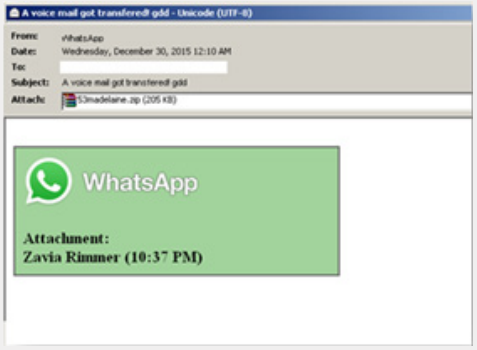
[5] https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=TrojanSpy:Win32/Nivdort.P

hosts file, or (2) reducing the infected machine's security level by disabling firewall notifications. Nivdort sends information about the victim's computer system to a remote server used for malicious purposes. When run, Nivdort creates a random folder and drops several copies of itself inside the folder before setting the attribute as "hidden," then uses the usual Startup folder for persistence.

For recent campaigns, Nivdort used email messages that spoofed cross-platform mobile messaging and voice communications brands WhatsApp Messenger and LINE, and social networking heavyweight Facebook. The malicious emails used to distribute Nivdort were in different languages – including German, French and Romanian – to target a wider audience (see Figure 9).

Figure 9: NivDort Email Samples





Below are some email subjects used by Nivdort campaigns during this timeframe:

- A brief vocal memo has been missed
- A short audible recording has been delivered. XXXX
- A short voice recording has been received
- A sound email has been downloaded
- A vocal warning has been transfered!
- Ati primit acum ceva timp un mesaj audio. XXXX
- Du hast vor kurzem eine akustische Notiz aufgenommen!
- Sie haben neulich einen vernehmlichen Bescheid angenommen! XXXX
- You got a video e-mail! XXX
- You recently obtained an audio note!
- You've got a video notice
- You've got an audible warning! XXX
- You've got an audio e-mail.
- You've missed a voice note!
- Youve just missed a brief vocal announcement. XXXXX
- Un document acoustique tait rceptionn
- Please verify our payment. XXXXXX
- I am sending you my booking details, please approve XXXXX
- I am emailing you my booking information, please approve. XXXX
- Please verify our payment. XXXXXXX
- Please approve my booking! XXXX

For Nivdort IOCs, please see APPENDIX 4.

URSNIF

URSNIF is considered as multifaceted malware because it has various behaviors and has a high adaptation and evolution rate. UrSnif is similar to Fareit; it is a password-stealing malware that has been around for almost a decade and has been recently observed being downloaded by Dridex.[6] Similar to Fareit, UrSnif collects sensitive information such as certificates, clear-text passwords transmitted over the network from FTP, POP3, IMAP and TELNET traffic, and other STET credentials.

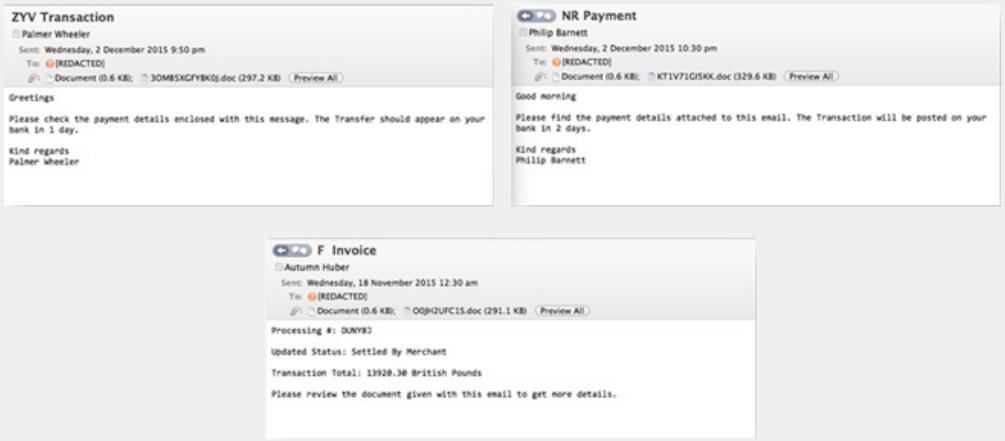
Unlike other campaigns that used major brand names or holiday-related events, UrSnif used year-round yet operations-relevant themes in its attacks. Transactions, payments and invoices are the usual baits seen in email distributing URSNIF. The design of the malicious emails is very simple and generic, with little to no graphics (see Figure 10).

Below are some email subjects used by URSNIF campaigns during this timeframe:

- F Invoice
- ZYV_Transactions
- NR_Payment

For UrSnif IOCs, see APPENDIX 5.

Figure 10: UrSnif Email Samples



[6] https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=TrojanDownloader:Win32/Drixed.B

NYMAIM

NYMAIM's notoriety stems from its complex obfuscation techniques that make it quite difficult to reverse engineer. Nymaim is a two-stage ransomware variant; the first executable, or first stage, downloads and runs the second executable, or the second stage. Nymaim also has a downloader component. It has been tied to other crimeware families in the past, most prominently BlackHole and DarkLeech. In other campaigns, Nymaim has been observed being downloaded along with families such as Pony, Sirefef and Urausy.

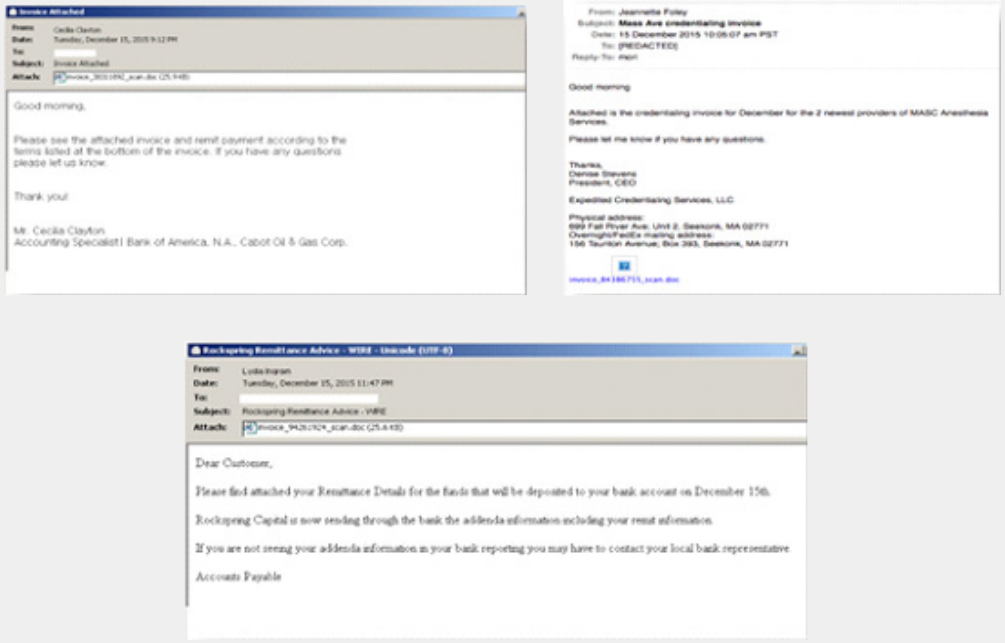
NYMAIM used fake remittance payments from Texas-based investment firm Rockspring Capital and banking giant Bank of America, as well as fake invoices pretending to be from credentialing company Expedited Credentialing Services. One distinct feature of the emails used to distribute this malware was that they encouraged potential victims to contact the sender, which is meant to build a sense of trust (see Figure 11).

Below are some email subjects used by Nymaim campaigns during this timeframe:

- Mass Avenue credentialing invoice
- Invoice Attached
- Rockspring Remittance Advice

For Nymaim IOCs, please see APPENDIX 6.

Figure 11: Nymaim Email Samples



CONCLUSION

Email phishing remains one of the primary infection vectors used by threat actors to deliver malware. Detecting these email campaigns continues to be challenging, as delivery methods and downloader forms continue to evolve.

It is interesting to see the evolution of the tricks and techniques associated with various malware families' infection attempts. Dridex conducted a large-scale attack using new delivery methods in a suspected attempt to obtain new victims following an October takedown. Fareit continues to be creative in its social engineering techniques to entice targets. And TelsaCrypt uses scripts that could easily be modified, which makes each sample highly dynamic in its content and techniques.

Given such a complex landscape, the threat is not going to end. We expect that threats will persist and continue to adapt through new social engineering techniques, delivery methods and the complexity of their attacks. Hence, it is important for organizations to remain vigilant with user education, proactive detection technologies and security policies that help prevent new threats.

APPENDIX 1: DRIDEX IOCS

1. Abcam Despatch [XXXXXXXXXX]

Malicious servers observed:

- biennalecasablanca.ma
- diabeteshelptoday.com
- villmarkshest.no

Callbacks observed:

- GET /7745gd/4dgrgdg.exe HTTP/1.1
- GET /~esterdj3/7745gd/4dgrgdg.exe d

Attachment names:

- invoice_1366976_08-01-13.xls

2. Aline Payment Request

Malicious servers observed:

- allfirdawhippet.com
- pivarimb.wz.cz
- sebel.fr

Callbacks observed:

- GET /4367yt/p0o6543f.exe HTTP/1.1

Attachment names:

- Statement_1973_1357257122414.doc

3. ICM - Invoice #XXXX

Malicious servers observed:

- ante-prima.com
- vinsdelcomtat.com
- www.ofenrohr-thermometer.de

Callbacks observed:

- GET /u5y432/h54f3.exe HTTP/1.1

Attachment names:

- order_2393.doc

4. Purchase Order XXXXXX

Malicious servers observed:

- det-sad-89.ru
- c-noda.1pworks.com
- terrazzo-beton.de
- vanoha.webzdarma.cz
- wal1.kns1.al
- gentlemenradio.com
- alfa-motor.com

Callbacks observed:

- GET /4367yt/p0o6543f.exe HTTP/1.1

Attachment names:

- P-ORD-C-10156-124658.xls

5. Reprint Document Archive

Malicious servers observed:

- pr-clanky.kvalitne.cz
- buzmenajerlik.com.tr
- irisbordados.com

Callbacks observed:

- GET /65y3fd23d/87i4g3d2d2.exe HTTP/1.1

Attachment names:

- pmB3A6.doc

6. Request for payment (PGS/XXXXX)

Malicious servers observed:

- cru3lblow.xf.cz
- data.axima.cz
- rotulosvillarreal.com
- timjokin.pp.fi
- lyk-kokkinochoria-amm.schools.ac.cy
- vasickovabanda.wz.cz

Callbacks observed:

- GET /6543f/9o8jhdw.exe HTTP/1.1
- GET /~clientes/6543f/9o8jhdw.exe HTTP/1.1
- GET /~krejcir/6543f/9o8jhdw.exe HTTP/1.1

Attachment names:

- 3-6555-73329-1435806061-3.doc

7. Shell Fuel Card E-bill XXXXXXX for Account B500101 DD/MM/YYYY

Malicious servers observed:

- allfirdawhippet.com
- sebel.fr

Callbacks observed:

- GET /4367yt/p0o6543f.exe HTTP/1.1

Attachment names:

- ebill0765017.doc

8. UKMail XXXXXXXXX tracking information

Malicious servers observed:

- cr9090worldrecord.wz.cz
- lyk-kokkinochoria-amm.schools.ac.cy
- timjokin.pp.fi
- vasickovabanda.wz.cz
- www.capodorlandoweb.it
- xsnoiseccs.bigpondhosting.com

Callbacks observed:

- GET /u654g/76j5h4g.exe HTTP/1.1
- GET /6543f/9o8jhdw.exe HTTP/1.1

Attachment names:

- 988271023-PRCL.xls
- 988271023-PRCL.doc

9. Your car rental invoice from Avis, No. XXXXXXXXXX

Malicious servers observed:

- domainregistrationthailand.com
- ht-savoie.com
- naceste2.czechian.net

Callbacks observed:

- GET /76t89/32898u.exe HTTP/1.1

Attachment names:

- E947168460_20141211_119845517.xls

10. Your receipt from Apple Store

Malicious servers observed:

- anetliberec.cz
- steveyuhas.com
- www.maklu.be

Callbacks observed:

- GET /87tr65/43wedf.exe HTTP/1.1
- GET /~steveyuhas/87tr65/43wedf.exe HTTP/1.1

Attachment names:

- emailreceipt_20150130R2155644709.xls

APPENDIX 2: FAREIT IOCS

1. E-Ticket Confirmation

Malicious servers observed:

- eextensions.co
- thetedrenre.ru
- unlaccothe.ru
- wicytergo.ru
- www.10203040.at
- www.eshtari.me

Callbacks observed:

- GET /m.exe HTTP/1.0
- POST /gate.php HTTP/1.0
- POST /sliva/gate.php HTTP/1.0

Attachment names:

- ticket_11022015-33788993.doc

2. More Holiday Gifts FREE 50$ and similar

Malicious servers observed:

- aningmasule.ru
- cameratranquoc.com
- ceas.md
- dorenledint.ru
- thehintitcal.ru
- www.camasirsepetiniz.com

Callbacks observed:

- GET /system/logs/hsg.exe HTTP/1.0
- POST /sliva/gate.php HTTP/1.0

Attachment names:

- giftcard_9684983.doc

3. Re: New Year Order

Malicious servers observed:

- 196.0.35.21
- 122.168.100.184
- 118.163.246.18
- 46.105.103.219

Callbacks observed:

- GET /kuvi/sam/x987/specification.exe HTTP/1.0
- POST /kuvi/sam/x987/gate.php HTTP/1.0
- GET /sobakavolos.gif?698483=* HTTP/1.1

Attachment names:

- Purchase_Order.exe

4. Re: reservation

Malicious servers observed:

- divatisestore.com
- ebbabogados.com
- hindistanvizesi.com.tr
- meletwihi.ru
- ressparromi.ru
- ruathanhep.ru

Callbacks observed:

- POST /gate.php HTTP/1.0
- GET /wp-content/plugins/cached_data/ff.exe HTTP/1.0

Attachment names:

- bill1201.doc

APPENDIX 3: TESLACRYPT IOCS

1. MM/DD/YYYY HH:MM:SS {A,P}M

Malicious servers observed:

- 46.151.52.197
- 5.39.222.193
- 74.117.183.84
- aawraa.com
- ifyougowegotoo.com

Callbacks observed:

- GET /73.exe?1 HTTP/1.1
- GET /80.exe?1 HTTP/1.1
- GET /85.exe?1 HTTP/1.1
- GET /94.exe HTTP/1.1
- GET /wp-includes/theme-compat/73.exe?1 HTTP/1.1

Attachment names:

- doc_KH7U42GpGYF.jsdoc_sQwBgn, doc_DZBvmZYItyW.js
- doc.zip, doc.js
- part1.zip, part1.js

2. Get your early access to our pre-Christmas sale

Malicious servers observed:

- soft2webextrain.com

Callbacks observed:

- GET /89.exe?1 HTTP/1.1

Attachment names:

- generation.zip, click_to_generate.js

3. Your account has a debt and is past due

Malicious servers observed:

- iamthewinnerhere.com
- whatdidyaysay.com

Callbacks observed:

- GET /80.exe?1 HTTP/1.1
- GET /97.exe HTTP/1.1
- GET /97.exe?1 HTTP/1.1

Attachment names:

- SCAN_INVOICE_33399796.zip, invoice_SCAN_s7Srp.js
- SCAN_INVOICE_87030810.zip, invoice_SCAN_uICpK.js
- SCAN_INVOICE_99796811.zip, invoice_SCAN_xr1To.js
- SCAN_INVOICE_37046986.zip, invoice_CO8AEJ.js
- SCAN_INVOICE_51882587.zip, invoice_copy_N7Wb8z.js

APPENDIX 4: NIVDORT IOCS

1. Please verify your payment and similar

Malicious servers observed:

- classdistance.net
- degreebrought.net
- difficultniece.net
- forwardairplane.net
- forwardmethod.net

Callbacks observed:

- GET /index.php HTTP/1.0

Attachment names:

- info.exe
- maddison.exe
- simons.exe
- merrill.exe

2. You got a video e-mail! XXX and similar

Malicious servers observed:

- classdistance.net
- degreebrought.net
- difficultniece.net
- forwardairplane.net
- forwardmethod.net

Callbacks observed:

- GET /index.php HTTP/1.0

Attachment names:

- eden71.zi

APPENDIX 5: URSNIF IOCS

1. F Invoice, ZYV_Transaction, NR_ Payment

Malicious servers observed:

- xcelgraphic.com

Callbacks observed:

- GET /media/cal.jpg HTTP/1.1

Attachment names:

- 0DOXM1M2A.doc
- 230WBU9UCXLL.doc
- 2C11WJOG3DTPG.doc
- 3OMB5XGFYBK0J.doc
- 3VN6TJG3O.doc
- 4RNLS36C16.doc
- 6S77B7W2652.doc
- 8RVH3R01C4G1V4.doc

APPENDIX 6: NYMAIM IOCS

1. Mass Ave credentialing invoice

Malicious servers observed:

- arengtynd.com
- cujamslud.com
- induscursa.net
- niseisyrma.com
- yeukydrant.com

Callbacks observed:

- POST /h908/bvn4854.exe HTTP/1.1
- POST /h908/ayuijo74.exe HTTP/1.1
- POST /h908/ckgigrj48.exe HTTP/1.1
- POST /h908/dkormv83.exe HTTP/1.1
- POST /h908/egidjd87.exe HTTP/1.1

Attachment names:

- invoice_17022757_scan.doc
- invoice_22314984_scan.doc
- invoice_23498256_scan.doc
- invoice_27982737_scan.doc
- invoice_53092133_scan.doc
- invoice_61427115_scan.doc
- invoice_65686829_scan.doc
- invoice_75416769_scan.doc
- invoice_79854936_scan.doc
- invoice_84386755_scan.doc
- invoice_99057008_scan.doc

For additional technical discussions on threat research, cyber attacks and threat intelligence from the FireEye Labs team, visit:

https://www.fireeye.com/blog/threat-research.html

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**