Threat Update: Nigerian Cybercriminals Target High-Impact Industries in India via Pony

By The Cylance Team

June 28, 2016

If you go strictly by the daily news headlines, you'd think that the majority of current cybercrime issues were limited to just a few ‘hot’ areas such as China, Russia and Iran. This is far from the truth, and in fact, there has always been a great deal of concerning activity that originates from outside these ‘hot’ areas. One such area is the nation of Nigeria.

When you think of Nigeria and cybercrime, the first thing that pops into your mind is probably the familiar Nigerian “419” scams. Those enticing emails that promise huge sums of money while scamming victims out of ‘advance fees’ and personal data have become something of a punchline these days. Despite being well known, they still persist and often succeed, but in reality, these are just a minor percentage of the total cybercrime activity coming out of Nigeria.

For years now there has been a more serious Nigeria-based cyberscam with a rotating cast of actors and groups. The goal of this cyberscam is primarily financial gain, with disruption of business as a welcome side benefit. The potential, however, exists for more severe actions, in terms of physical compromise or destruction of property, cargo and possibly even human life.

While this activity has received a decent amount of coverage in the past, Cylance's Research Team decided to take a closer look.

Nigerian Scams Grow in Sophistication

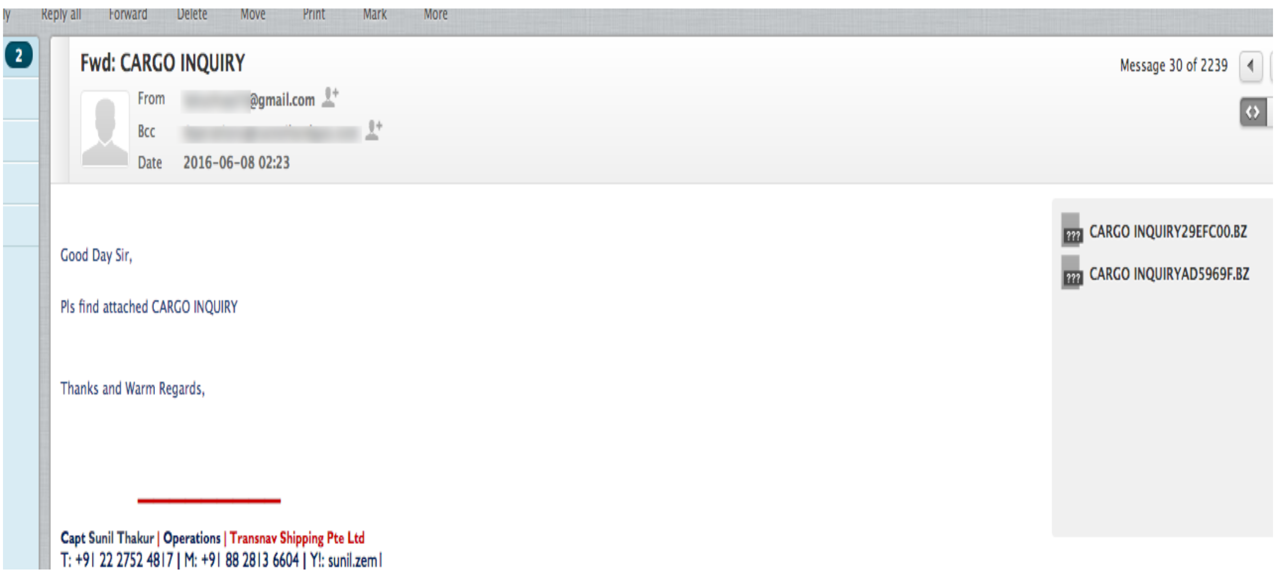
Cylance’s investigation concentrated on an ongoing campaign out of Nigeria, primarily targeting high-impact industries in India. In particular: manufacturing, shipping, freight/cargo logistics, and transportation companies were targeted.

The immediate gain from these attacks for the cybercriminals is access to a wealth of financial data. By leveraging credential-stealing tools such as Pony and Hawkeye, the attackers are able to gain access to personal and corporate email accounts as well as breaching corporate intranets and VPNs.

But rather than simply stealing data wholesale and selling it online to the highest bidder, the attackers do something unusual: they manually read through the mail in the compromised email accounts, searching for further targets (both personal and corporate) which they can leverage to infiltrate other companies or siphon money from. The level of detail to which the attackers are privy after accessing corporate email accounts is alarming. Sensitive data including employee records, banking transactions, vehicle or ocean vessel tracking info, and standard intellectual property were all targeted and exfiltrated by this group.

There have been multiple ‘waves’ observed in these attacks, primarily spanning from October 2015 to June 2016. With the Pony Loader 2.2 infrastructure in place, the attackers were able to begin the initial stages of attack. This was typically carried out via a standard spear-phish email to individuals in targeted companies. The messages all have invoice, cargo or shipment inquiry themes, and are sent from registered domains that look very similar to the domains of legitimate companies with whom the target companies typically do business.

For example:



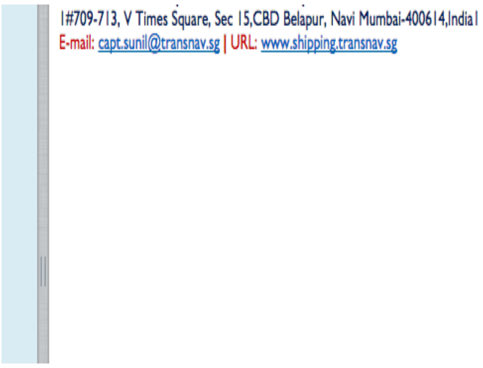
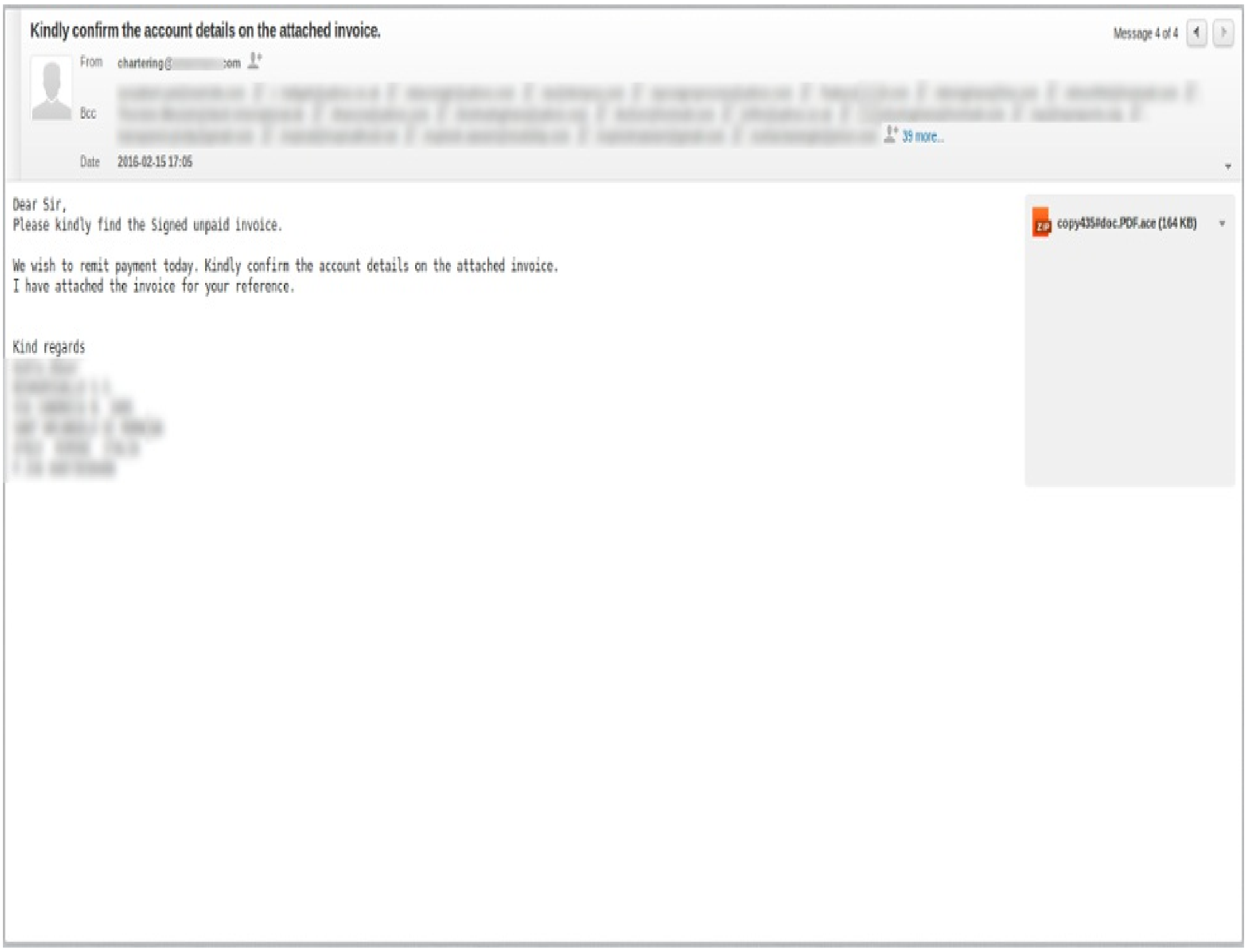

|#709-713, V Times Square, Sec 15,CBD Belapur, Navi Mumbai-400614,India|
E-mail: capt.sunil@transnav.sg | URL: www.shipping.transnav.sg

Figure 1: Phishing Email 1 - Bogus Cargo Inquiry (With Malicious Attachment)


Kindly confirm the account details on the attached invoice.
Message 4 of 4
From chartering@[redacted]om
Bcc [redacted] 39 more...
Date 2016-02-15 17:05
copy435#doc.PDF.ace (164 KB)

Dear Sir,
Please kindly find the Signed unpaid invoice.

We wish to remit payment today. Kindly confirm the account details on the attached invoice.
I have attached the invoice for your reference.

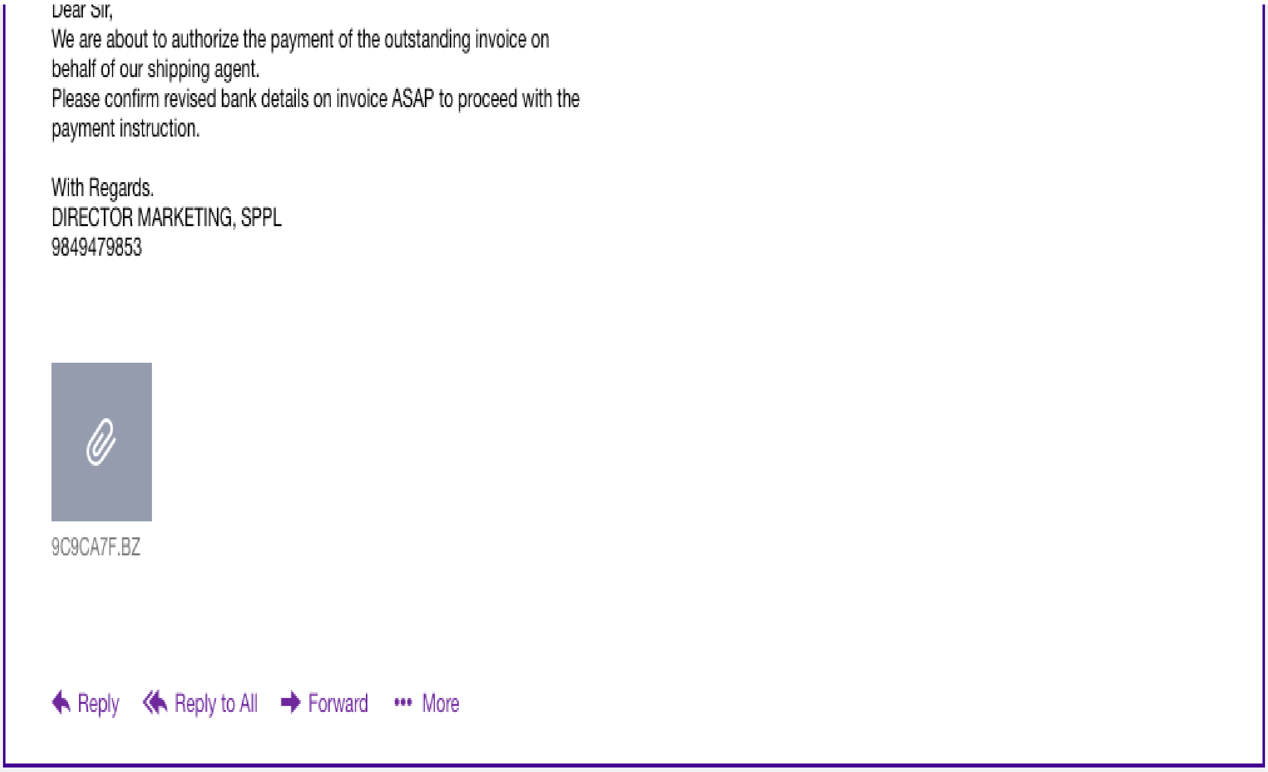
Kind regards
[redacted]

Figure 2: Phishing Email 2 - Bogus Account Details Confirmation (With Malicious Attachment)

The spear-phish emails are weaponized with either .BZ or .ACE compressed executables (extracting to either .EXE or .SCR files).

Those attachments are Pony or Hawkeye trojans, which are then used to steal even more credentials and data from the targets. Once the cybercriminals have actual legitimate credentials to work with, they send further spear-phish emails to additional targets manually identified from the compromised accounts.


Chalapathi Rao KV <kvcrao@unigas.in>
Jun 10 at 5:47 AM



Dear Sir,
We are about to authorize the payment of the outstanding invoice on behalf of our shipping agent.
Please confirm revised bank details on invoice ASAP to proceed with the payment instruction.

With Regards.
DIRECTOR MARKETING, SPPL
9849479853

9C9CA7F.BZ

Reply Reply to All Forward More

Figure 3: Phishing Email 3 - Bogus Outstanding Invoice Confirmation (With Malicious Attachment)

In some cases, Hawkeye and Pony are sent in the same email, as per the example in Figure 4, below:

Subject: Fwd: Enquiry
From: "Didik Triwaluyo" <didik.triwaluyo@asiatranslogistics.com>
Date: Thu, June 9, 2016 7:25 am
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file | View Message details

Good day,

please find attach Enquiry

My Best Regards,

Didik Tri Waluyo
Asia Trans Logistics (Batam)
Regency Park blok II No.23
Pelita - Batam
Mailing Address : -
Changi Airfreight Center
PO Box 788
Singapore 918110
HP/WA : 0821 7066 7065
Skype ID : Jowotulen

www.haegroup.com

www.cargolinkexpress.com
www.asiatranslogistics.com

All Business handled is subject to our General Trading Conditions, a copy can be made available upon request.

Attachments:

inquiryEA1B88F.BZ	197 k	[application/x-bzip]	Download
inquirybocredt231456.bz	1 M	[application/x-bzip]	Download

Figure 4: Phishing Email 4 - Changi Airfreight Center Enquiry (Note Spelling Errors) - With Malicious Pony & Hawkeye Trojan Attachments

Panels and Infrastructure

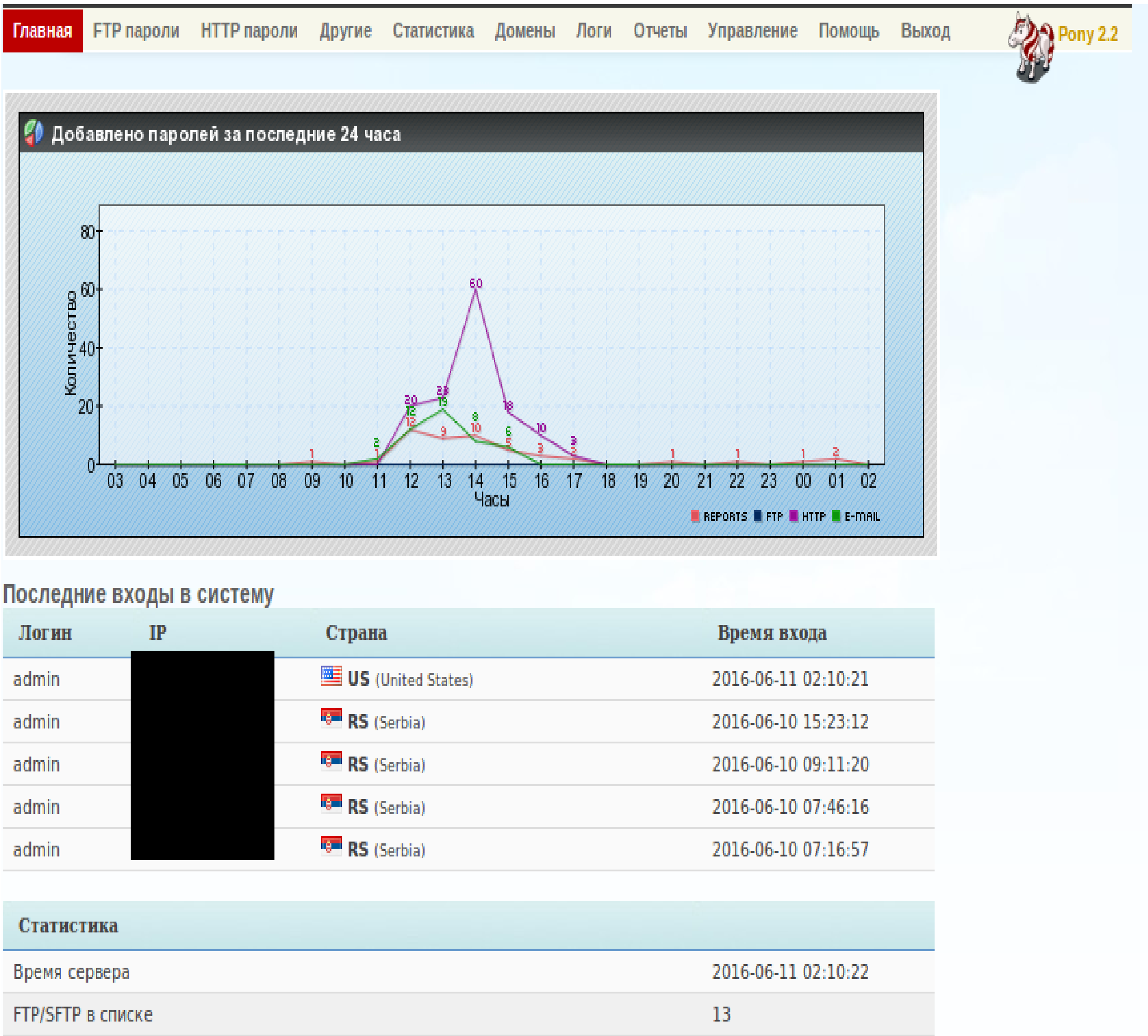


Figure 5: Pony 2.2 Control Panel - 1

Cylance's primary investigative focus with these campaigns has been the wave which started in early April 2016, and (as of this writing) is still ongoing in June 2016. In early April, the attackers set up their main infrastructure via Unlimited Web Hosting out of the UK. Multiple registered domains were immediately used to set up Pony Loader panels and host associated malware:

Initial Registered Domains:

cosmoships-gr(dot)com
equinoxdsitribution(dot)com
etaship-sg(dot)com
fortressict-nl(dot)com
friendshlp-chartering(dot)com
iwenconsultinggroup(dot)com
nevig8group(dot)com

nqvoil-sg(dot)com

octagonainternational(dot)com

pcchand(dot)com

pruship-tw(dot)com

seahorsegroup-in(dot)com

toships(dot)net

tosihps(dot)com

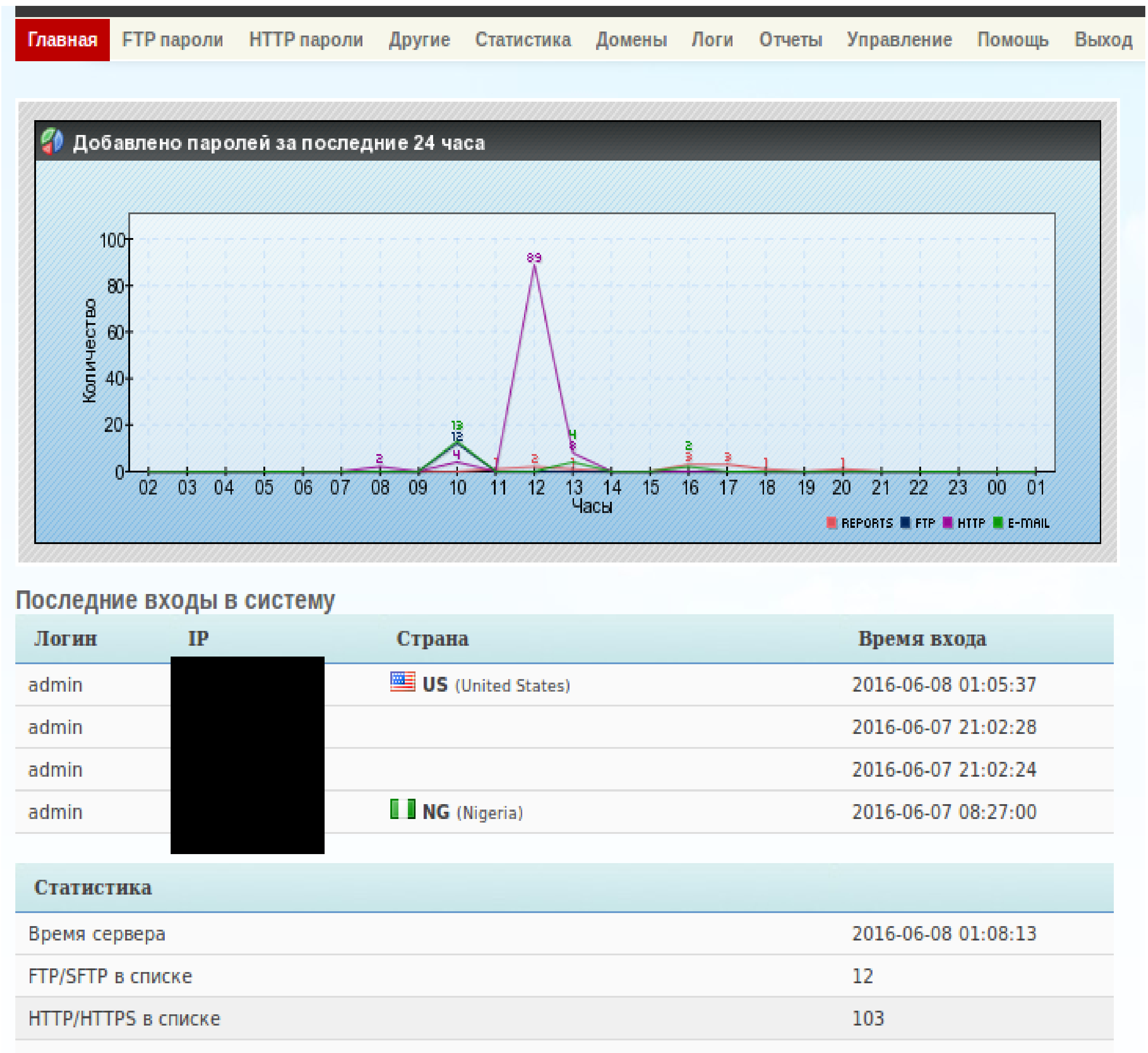
toslhips(dot)com

toslhps(dot)com

vietexcurisons(dot)com

alexbensonship(dot)com

The longest running panels (now down as of 6/14/2016) were hosted on nqvoil-sg(dot)com, and pcchand(dot)com. Pony C2s were briefly active on friendship-□ chartering(dot)com, toships(dot)net, and tosihps(dot)com. Both the Pony-hosting domains, and those not hosting Pony were observed sending out weaponized email messages, directing victims to one of the active Pony C2s:



E-mail паролей в списке	19
Сертификатов в списке	0
Кошельков в списке	0
RDP в списке	1
Уникальных отчетов	12

Figure 6: Pony 2.2 Control Panel - 2

Firefox	**6** (1.47%)

Популярность E-mail клиентов

E-mail клиент	Количество паролей
Outlook	**119** (94.44%)
Windows Live Mail	**4** (3.17%)
IncrediMail	**2** (1.59%)
Thunderbird	**1** (0.79%)

Популярность HTTP доменов

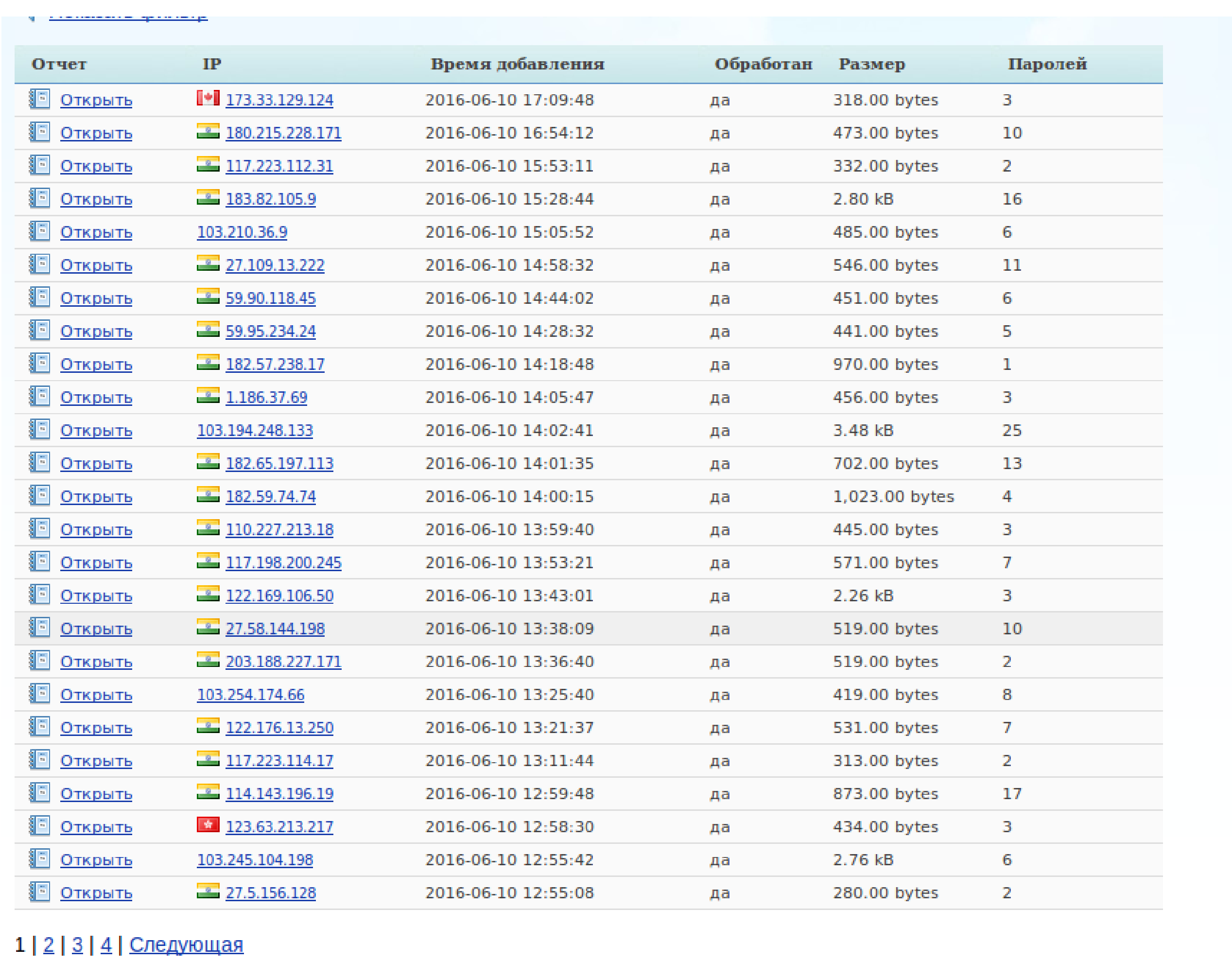
Домен	Количество паролей
accounts.google.com	**29** (19.73%)
service.mail.com	**14** (9.52%)
login.yahoo.com	**13** (8.84%)
commercialtax.gujarat.gov.in	**12** (8.16%)
www.facebook.com	**11** (7.48%)
www.mail.com	**8** (5.44%)
www.irctc.co.in	**7** (4.76%)
www.rediffmailpro.com	**6** (4.08%)
login.live.com	**6** (4.08%)
uanmembers.epfoservices.in	**5** (3.40%)
www.services.irctc.co.in	**5** (3.40%)
mail.shahinternational-in.com	**4** (2.72%)
mail.rediff.com	**4** (2.72%)
www.amazon.in	**4** (2.72%)
www.sbicard.com	**4** (2.72%)
accounts.zoho.com	**3** (2.04%)
onlineap.meeseva.gov.in	**3** (2.04%)
www.snapdeal.com	**3** (2.04%)
smartfleetonline.co.in	**3** (2.04%)
sso.secureserver.net	**3** (2.04%)

Скрыть (20)

Figure 7: Pony 2.2 Control Panel - 3

Главная FTP пароли HTTP пароли Другие Статистика Домены Логи **Отчеты** Управление Помощь Выход Pony 2.2

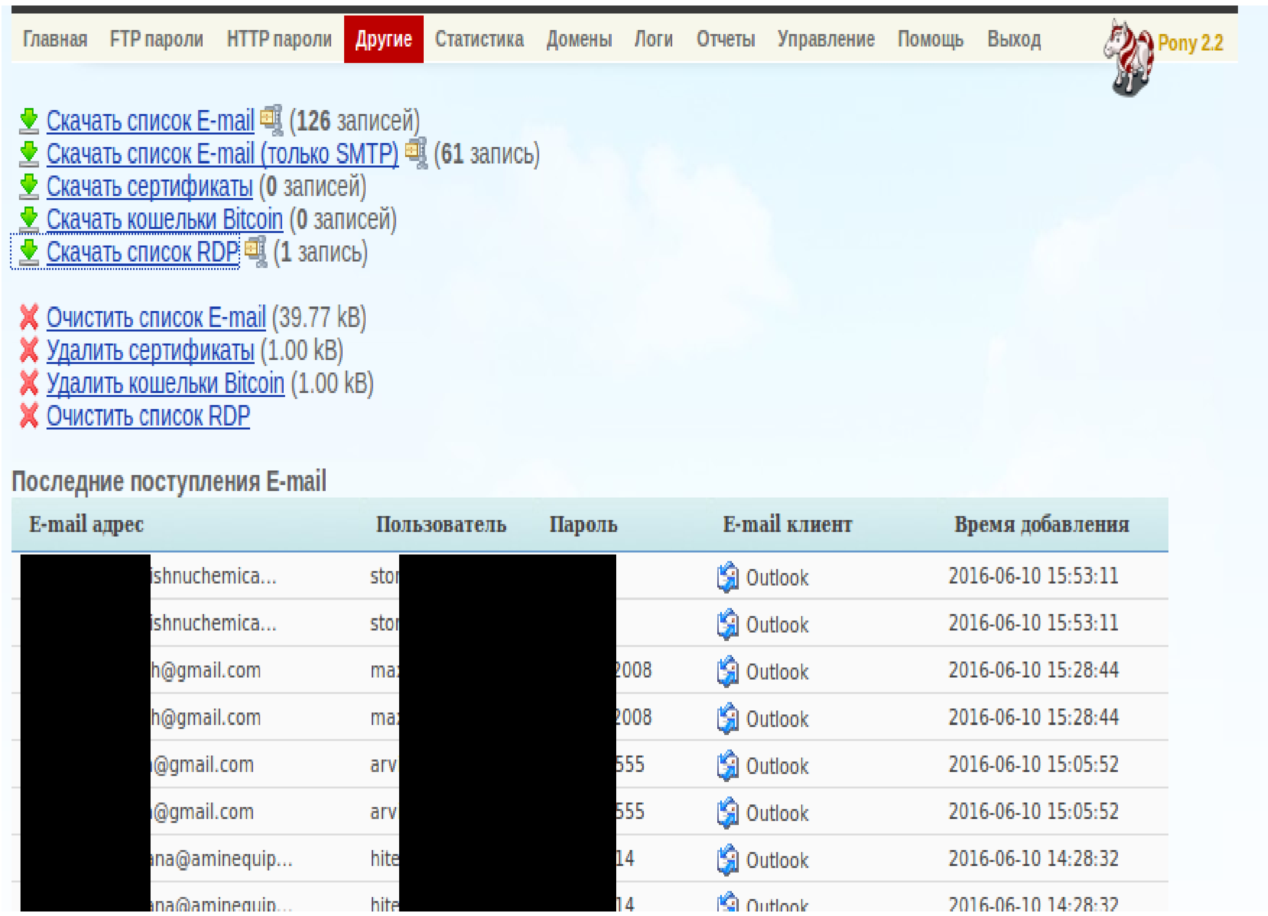
Скачать все отчеты (**140** записей, 219.29 kB)
Скачать необработанные отчеты (0 записей, 0 bytes)
Удалить все отчеты (219.29 kB)
Показать фильтр



Отчет	IP	Время добавления	Обработан	Размер	Паролей
Открыть	173.33.129.124	2016-06-10 17:09:48	да	318.00 bytes	3
Открыть	180.215.228.171	2016-06-10 16:54:12	да	473.00 bytes	10
Открыть	117.223.112.31	2016-06-10 15:53:11	да	332.00 bytes	2
Открыть	183.82.105.9	2016-06-10 15:28:44	да	2.80 kB	16
Открыть	103.210.36.9	2016-06-10 15:05:52	да	485.00 bytes	6
Открыть	27.109.13.222	2016-06-10 14:58:32	да	546.00 bytes	11
Открыть	59.90.118.45	2016-06-10 14:44:02	да	451.00 bytes	6
Открыть	59.95.234.24	2016-06-10 14:28:32	да	441.00 bytes	5
Открыть	182.57.238.17	2016-06-10 14:18:48	да	970.00 bytes	1
Открыть	1.186.37.69	2016-06-10 14:05:47	да	456.00 bytes	3
Открыть	103.194.248.133	2016-06-10 14:02:41	да	3.48 kB	25
Открыть	182.65.197.113	2016-06-10 14:01:35	да	702.00 bytes	13
Открыть	182.59.74.74	2016-06-10 14:00:15	да	1,023.00 bytes	4
Открыть	110.227.213.18	2016-06-10 13:59:40	да	445.00 bytes	3
Открыть	117.198.200.245	2016-06-10 13:53:21	да	571.00 bytes	7
Открыть	122.169.106.50	2016-06-10 13:43:01	да	2.26 kB	3
Открыть	27.58.144.198	2016-06-10 13:38:09	да	519.00 bytes	10
Открыть	203.188.227.171	2016-06-10 13:36:40	да	519.00 bytes	2
Открыть	103.254.174.66	2016-06-10 13:25:40	да	419.00 bytes	8
Открыть	122.176.13.250	2016-06-10 13:21:37	да	531.00 bytes	7
Открыть	117.223.114.17	2016-06-10 13:11:44	да	313.00 bytes	2
Открыть	114.143.196.19	2016-06-10 12:59:48	да	873.00 bytes	17
Открыть	123.63.213.217	2016-06-10 12:58:30	да	434.00 bytes	3
Открыть	103.245.104.198	2016-06-10 12:55:42	да	2.76 kB	6
Открыть	27.5.156.128	2016-06-10 12:55:08	да	280.00 bytes	2

1 | 2 | 3 | 4 | Следующая

Figure 8: Pony 2.2 Control Panel - 4



E-mail адрес	Пользователь	Пароль	E-mail клиент	Время добавления
[redacted]ishnuchemica...	sto[redacted]	[redacted]	Outlook	2016-06-10 15:53:11
[redacted]ishnuchemica...	sto[redacted]	[redacted]	Outlook	2016-06-10 15:53:11
[redacted]h@gmail.com	ma[redacted]	[redacted]2008	Outlook	2016-06-10 15:28:44
[redacted]h@gmail.com	ma[redacted]	[redacted]2008	Outlook	2016-06-10 15:28:44
[redacted]@gmail.com	arv[redacted]	[redacted]555	Outlook	2016-06-10 15:05:52
[redacted]@gmail.com	arv[redacted]	[redacted]555	Outlook	2016-06-10 15:05:52
[redacted]na@aminequip...	hite[redacted]	[redacted]14	Outlook	2016-06-10 14:28:32
[redacted]na@aminequip...	hite[redacted]	[redacted]14	Outlook	2016-06-10 14:28:32

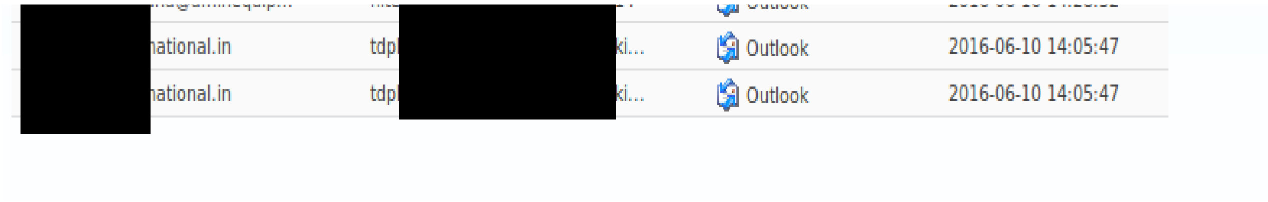


Figure 9: Pony 2.2 Control Panel - 5

Armed with ample sets of credentials, the attackers now have access to an enormous amount of sensitive information. This is perhaps the biggest takeaway of this post. Even if the attackers were only interested in the financial data, of which there is plenty, the potential for financial and physical damage via leveraging other segments of acquired data is alarming.

Not only do the cybercriminals have access to critical financial data such as account numbers, transaction IDs, bank routing numbers, SWIFT codes, IBAN codes, and so on, but in this case the attackers also have direct access to vehicle, shipping, and cargo logistics data. This data ranges from the routes and locations of delivery truck fleets, all the way to routing and cargo of commercial and government marine vessels. Examples of financial and transportation data, gathered/ monitored by the attacker, are given below:

mail.com

Re: 回复： 回复： Payment for machinery supply to China.

From: [redacted]eologist.com>
To:
Cc:
Date:

Dear Sir,

Hope you have already instruct your Bank to release the above payment for **US$ 110600**.

Kindly note down our bank details once again -
BANK ACCOUNT DETAILS:
BENEFICIARY: [redacted]
BANK:METRO BANK PLC
ADDRESS: [redacted] UNITED KINGDOM
ACCOUNT: [redacted]
IBAN: [redacted]
SWIFT CODE: [redacted]

Kind regards,

[redacted]

Figure 10: Confidential Banking Data Monitored by the Attackers - 1

Transfer Instruction

Message 11 of 12

From [redacted]

To [redacted]

Cc [redacted]

Date [redacted]

TRANSFER INSTRUCTION.docx

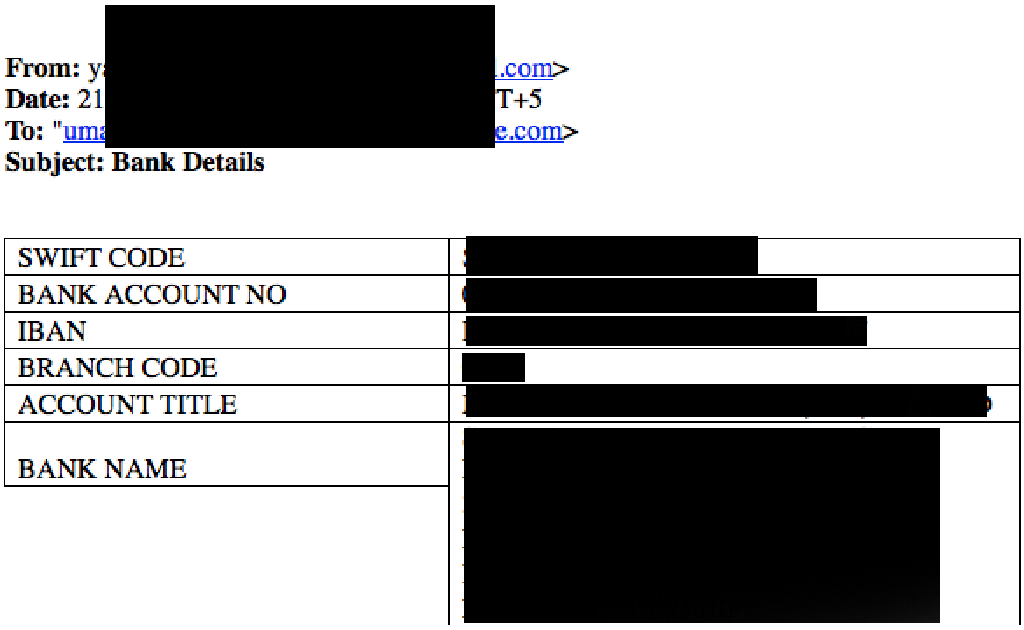
find attached,

Bank Authority for transfer & also to raised Draft for on the stated vessel.

Thank you.

For

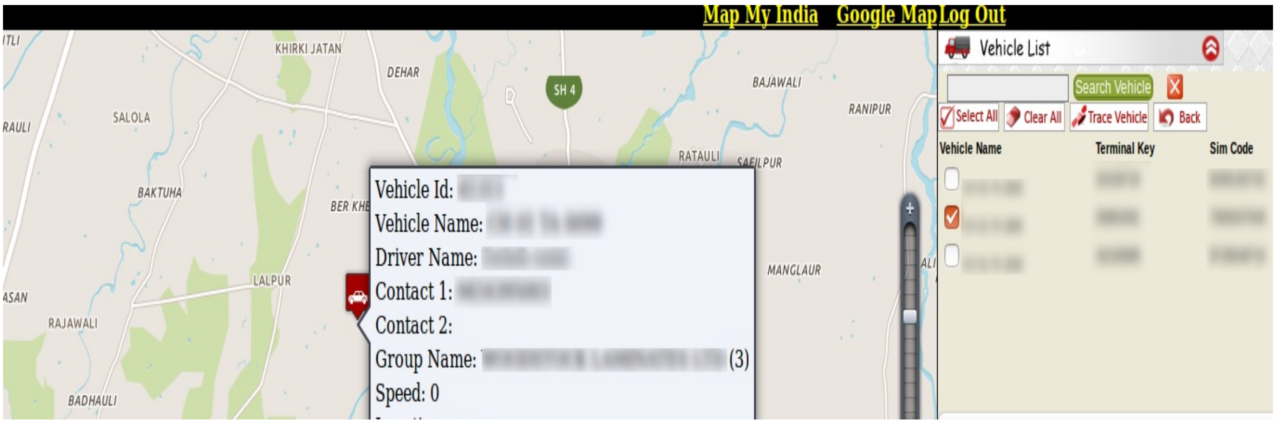
Figure 11: Confidential Data Monitored by the Attackers - 2



From: [redacted]
Date: [redacted]
To: "[redacted]
Subject: Bank Details

SWIFT CODE	[redacted]
BANK ACCOUNT NO	[redacted]
IBAN	[redacted]
BRANCH CODE	[redacted]
ACCOUNT TITLE	[redacted]
BANK NAME	[redacted]

Figure 12: Confidential Data Monitored by the Attackers - 3



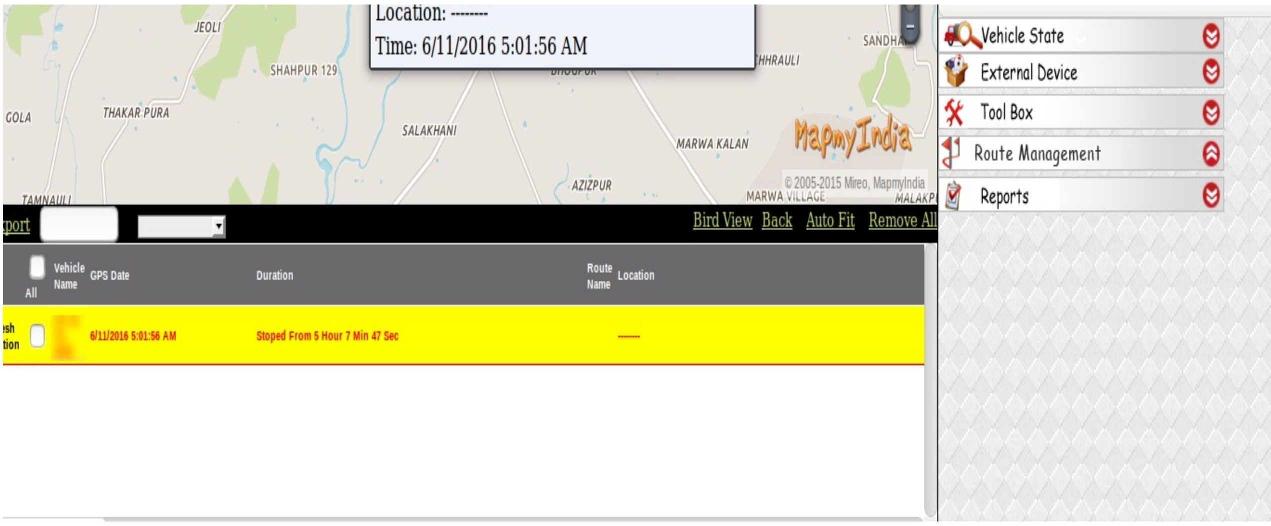
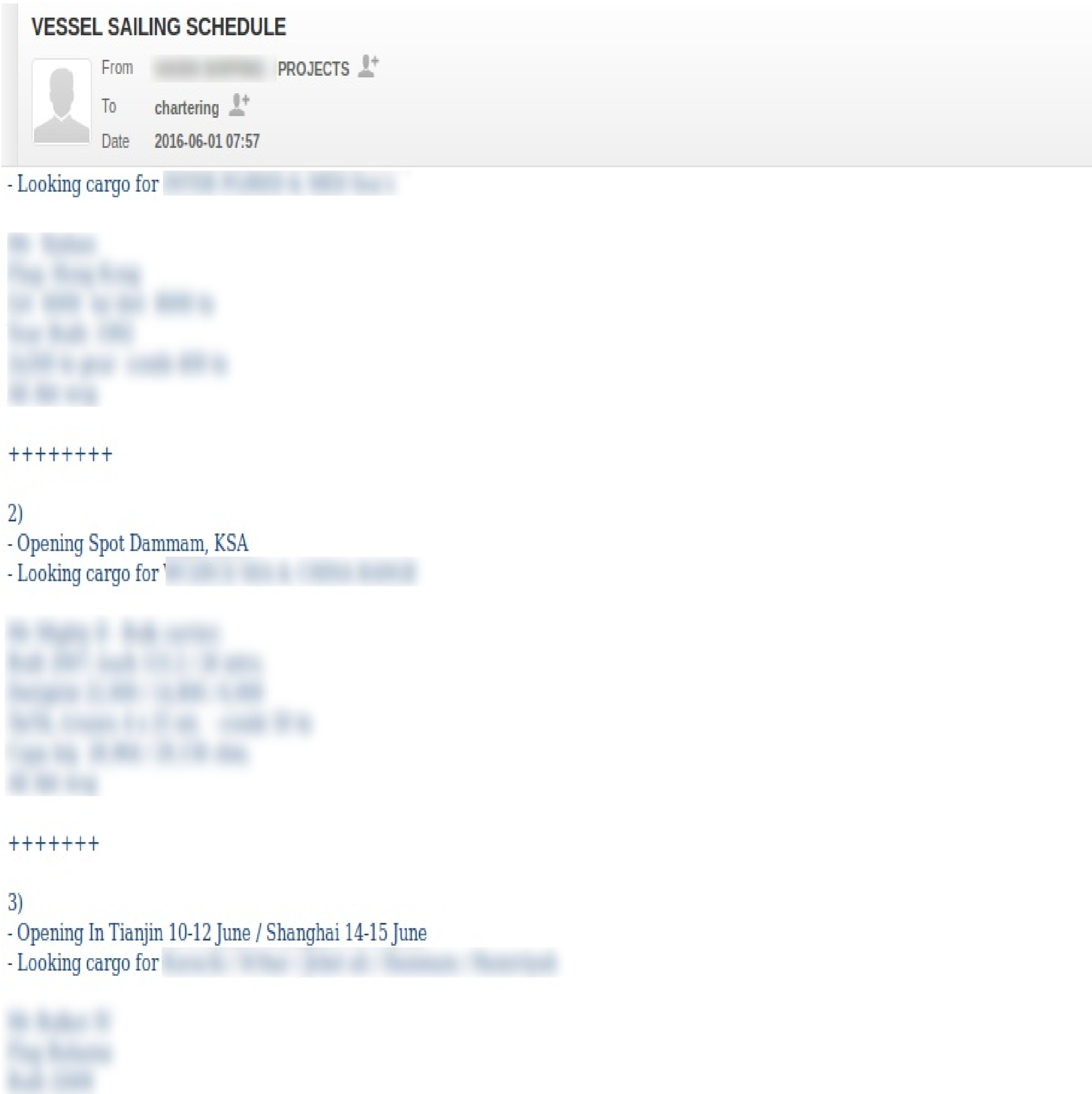


Figure 13: Vehicle/ Tracking Cargo Info Monitored by the Attackers -1



VESSEL SAILING SCHEDULE

From PROJECTS

To chartering

Date 2016-06-01 07:57

- Looking cargo for

++++++++

2)
- Opening Spot Dammam, KSA
- Looking cargo for

+++++++

3)
- Opening In Tianjin 10-12 June / Shanghai 14-15 June
- Looking cargo for

Figure 14: Vehicle / Cargo Tracking Info Monitored by the Attackers - 2

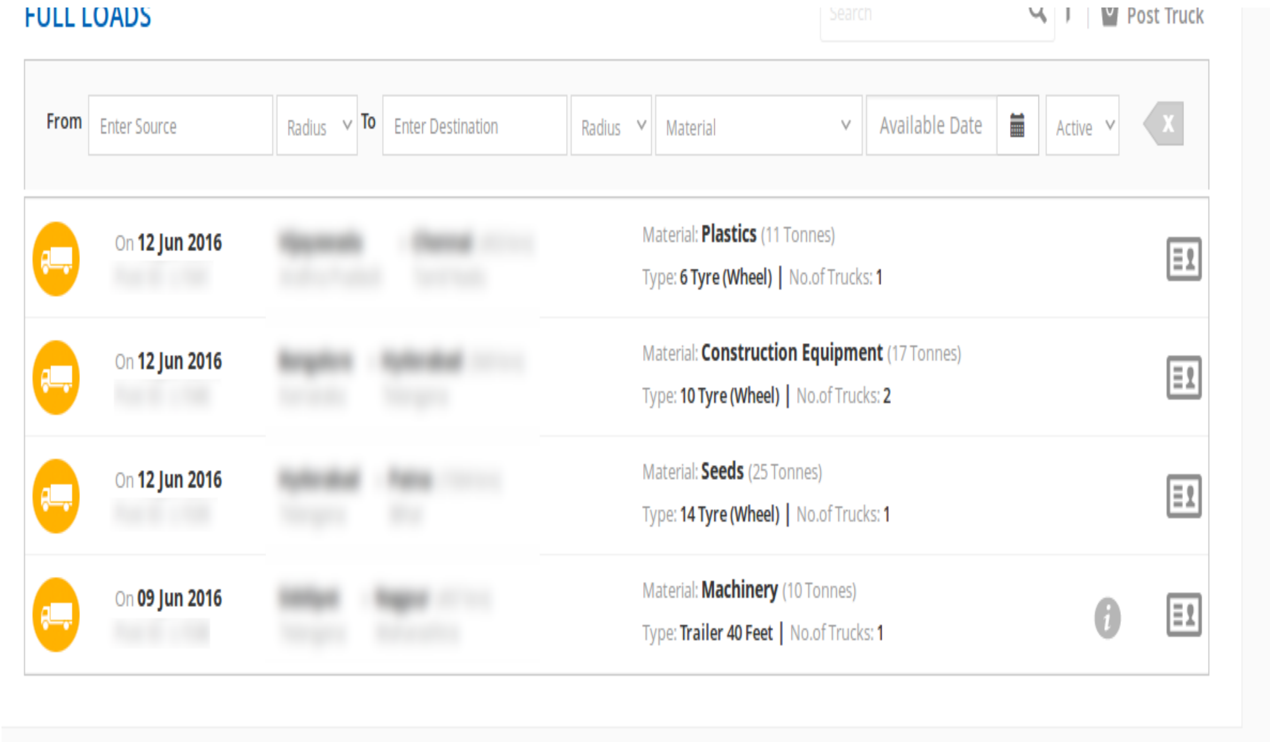


Figure 15: Vehicle/ Cargo Tracking Info Monitored by the Attackers - 3

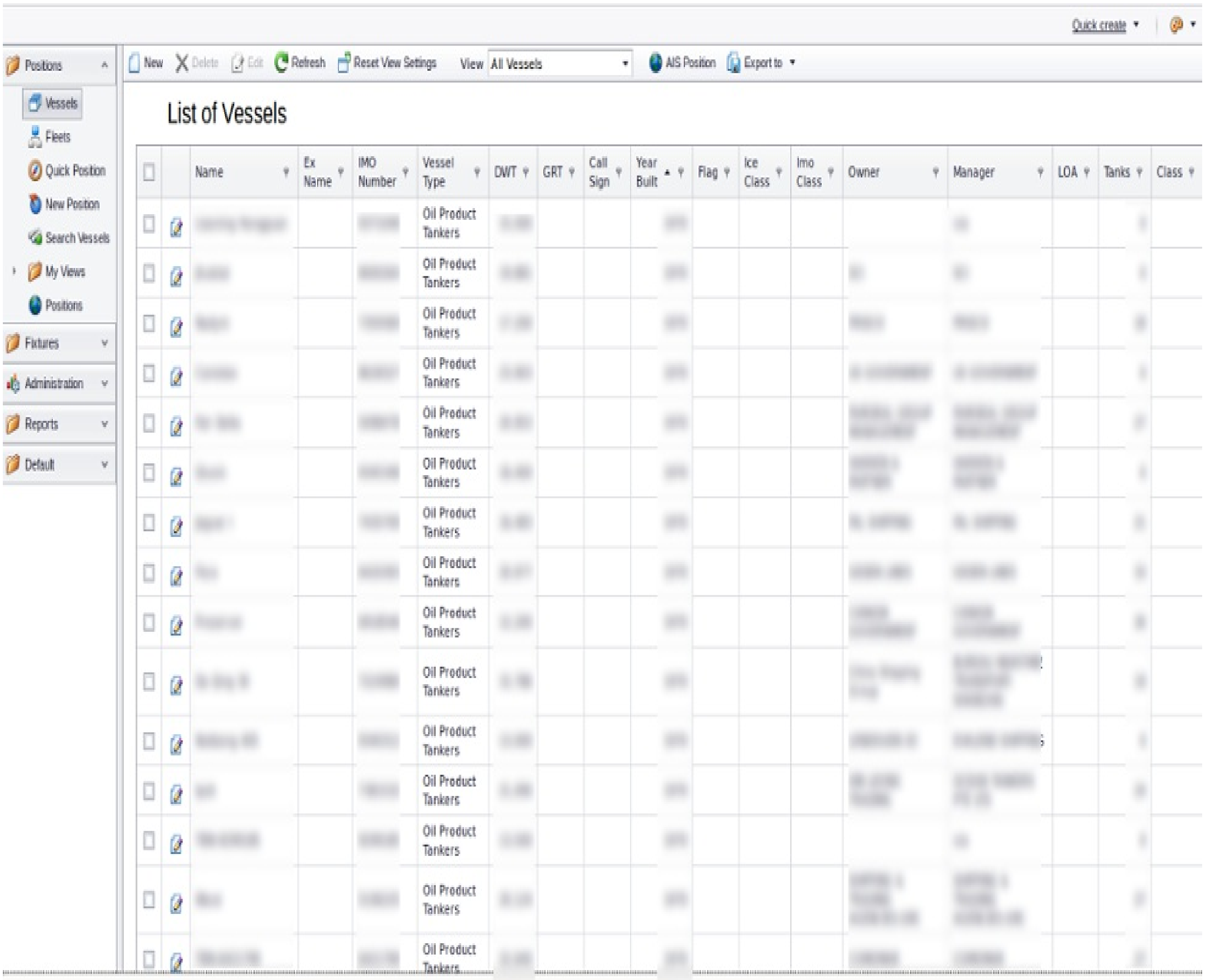


Figure 16: Monitored Vehicle/ Cargo Tracking Info - 4

Malware Used in the Attacks

Malware Used in the Attacks

The attackers are utilizing Pony Loader 2.2 almost exclusively for these attacks. There are a few specific targets where Hawkeye and/or Zeus came into play, but most of the focus and benefit comes from Pony. The Pony malware is purpose-built to harvest a prescribed set of credentials and data from the victim's machine. Pony 2.2 is capable of harvesting RDP, HTTP/HTTP, FTP, SFTP, SMTP, POP3, IMAP as well as bitcoin (including Electrum and Multibit modules).

The bitcoin theft modules are relatively new to Pony Loader. That is to say, the functionality related to theft of cryptocurrencies was introduced first in version 2.0 of Pony Loader. The password stealing modules are (in standard Pony fashion) also specific to certain products.

Global Password Module List:

```
// module_class | module_id | module_name
$global_module_list = array(
   array('module_systeminfo',          0x00000000, 'System Info'),
   array("module_far",             0x00000001, 'FAR Manager'),
   array("module_wtc",             0x00000002, 'Total Commander'),
   array("module_ws_ftp",            0x00000003, 'WS_FTP'),
   array("module_cuteftp",            0x00000004, 'CuteFTP'),
   array("module_flashfxp",          0x00000005, 'FlashFXP'),
   array("module_filezilla",          0x00000006, 'FileZilla'),
   array("module_ftpcommander",        0x00000007, 'FTP Commander'),
   array("module_bulletproof",          0x00000008, 'BulletProof FTP'),
   array("module_smartftp",          0x00000009, 'SmartFTP'),
   array("module_turboftp",          0x0000000a, 'TurboFTP'),
   array("module_ffftp",            0x0000000b, 'FFFTP'),
   array("module_coffeecupftp",        0x0000000c, 'CoffeeCup FTP / Sitemapper'),
   array("module_coreftp",            0x0000000d, 'CoreFTP'),
   array("module_ftpexplorer",          0x0000000e, 'FTP Explorer'),
   array("module_frigateftp",          0x0000000f, 'Frigate3 FTP'),
   array("module_securefx",          0x00000010, 'SecureFX'),
   array("module_ultrafxp",            0x00000011, 'UltraFXP'),
   array("module_ftprush",            0x00000012, 'FTPRush'),
   array("module_websitepublisher",     0x00000013, 'WebSitePublisher'),
   array("module_bitkinex",          0x00000014, 'BitKinex'),
   array("module_expandrive",          0x00000015, 'ExpanDrive'),
   array("module_classicftp",          0x00000016, 'ClassicFTP'),
   array("module_fling",            0x00000017, 'Fling'),
   array("module_softx",            0x00000018, 'SoftX'),
   array("module_dopus",            0x00000019, 'Directory Opus'),
   array("module_freeftp",            0x0000001a, 'FreeFTP / DirectFTP'),
   array("module_leapftp",            0x0000001b, 'LeapFTP'),
   array("module_winscp",            0x0000001c, 'WinSCP'),
   array("module_32bitftp",          0x0000001d, '32bit FTP'),
   array("module_netdrive",          0x0000001e, 'NetDrive'),
   array("module_webdrive",          0x0000001f, 'WebDrive'),
   array("module_ftpcontrol",          0x00000020, 'FTP Control'),
   array("module_opera",            0x00000021, 'Opera'),
   array("module_wiseftp",            0x00000022, 'WiseFTP'),
   array("module_ftpvoyager",          0x00000023, 'FTP Voyager'),
    array("module_firefox",            0x00000024, 'Firefox'),
    array("module_fireftp",            0x00000025, 'FireFTP'),
    array("module_seamonkey",          0x00000026, 'SeaMonkey'),
    array("module_flock",            0x00000027, 'Flock'),
```

```
array("module_mozilla",          0x00000028, 'Mozilla'),
array("module_leechftp",         0x00000029, 'LeechFTP'),
array("module_odin",             0x0000002a, 'Odin Secure FTP Expert'),
array("module_winftp",           0x0000002b, 'WinFTP'),
array("module_ftp_surfer",       0x0000002c, 'FTP Surfer'),
array("module_ftpgetter",        0x0000002d, 'FTPGetter'),
```

Figure 17: Global Password Module List -1

```
array("module_alftp",            0x0000002e, 'ALFTP'),
array("module_ie",               0x0000002f, 'Internet Explorer'),
array("module_dreamweaver",      0x00000030, 'Dreamweaver'),
array("module_deluxeftp",        0x00000031, 'DeluxeFTP'),
array("module_chrome",           0x00000032, 'Google Chrome'),
array("module_chromium",         0x00000033, 'Chromium / SRWare Iron'),
array("module_chromeplus",       0x00000034, 'ChromePlus'),
array("module_bromium",          0x00000035, 'Bromium (Yandex Chrome)'),
array("module_nichrome",         0x00000036, 'Nichrome'),
array("module_comododragon",     0x00000037, 'Comodo Dragon'),
array("module_rockmelt",         0x00000038, 'RockMelt'),
array("module_kmeleon",          0x00000039, 'K-Meleon'),
array("module_epic",             0x0000003a, 'Epic'),
array("module_staff",            0x0000003b, 'Staff-FTP'),
array("module_aceftp",           0x0000003c, 'AceFTP'),
array("module_globaldownloader", 0x0000003d, 'Global Downloader'),
array("module_freshftp",         0x0000003e, 'FreshFTP'),
array("module_blazeftp",         0x0000003f, 'BlazeFTP'),
array("module_netfile",          0x00000040, 'NETFile'),
array("module_goftp",            0x00000041, 'GoFTP'),
array("module_3dftp",            0x00000042, '3D-FTP'),
array("module_easyftp",          0x00000043, 'Easy FTP'),
array("module_xftp",             0x00000044, 'Xftp'),
array("module_rdp",              0x00000045, 'RDP'),
array("module_ftpnow",           0x00000046, 'FTP Now'),
array("module_roboftp",          0x00000047, 'Robo-FTP'),
array("module_cert",             0x00000048, 'Certificate'),
array("module_linasftp",         0x00000049, 'LinasFTP'),
array("module_cyberduck",        0x0000004a, 'Cyberduck'),
array("module_putty",            0x0000004b, 'Putty'),
array("module_notepadpp",        0x0000004c, 'Notepad++'),
array("module_vs_designer",      0x0000004d, 'CoffeeCup Visual Site Designer'),
array("module_ftpshell",         0x0000004e, 'FTPShell'),
array("module_ftpinfo",          0x0000004f, 'FTPInfo'),
array("module_nexusfile",        0x00000050, 'NexusFile'),
array("module_fs_browser",       0x00000051, 'FastStone Browser'),
array("module_coolnovo",         0x00000052, 'CoolNovo'),
array("module_winzip",           0x00000053, 'WinZip'),
array("module_yandexinternet",   0x00000054, 'Yandex.Internet / Ya.Browser'),
array("module_myftp",            0x00000055, 'MyFTP'),
array("module_sherrodftp",       0x00000056, 'sherrod FTP'),
array("module_novaftp",          0x00000057, 'NovaFTP'),
 array("module_windows_mail",      0x00000058, 'Windows Mail'),
 array("module_windows_live_mail", 0x00000059, 'Windows Live Mail'),
 array("module_becky",             0x0000005a, 'Becky!'),
 array("module_pocomail",          0x0000005b, 'Pocomail'),
 array("module_incredimail",       0x0000005c, 'IncrediMail'),
 array("module_thebat",            0x0000005d, 'The Bat!'),
 array("module_outlook",           0x0000005e, 'Outlook'),
 array("module_thunderbird",       0x0000005f, 'Thunderbird'),
```

Figure 18: Global Password Module List - 2

```
    array("module_fasttrack",          0x00000060, 'FastTrackFTP'),
    array("module_bitcoin",             0x00000061, 'Bitcoin'),
    array("module_electrum",          0x00000062, 'Electrum'),
    array("module_multibit",          0x00000063, 'MultiBit'),
    array("module_ftpdisk",             0x00000064, 'FTP Disk'),
    array("module_litecoin",          0x00000065, 'Litecoin'),
    array("module_namecoin",          0x00000066, 'Namecoin'),
   array("module_terracoin",          0x00000067, 'Terracoin'),
   array("module_bitcoin_armory",      0x00000068, 'Bitcoin Armory'),
   array("module_ppcoin",              0x00000069, 'PPCoin (Peercoin)'),
   array("module_primecoin",          0x0000006a, 'Primecoin'),
   array("module_feathercoin",         0x0000006b, 'Feathercoin'),
   array("module_novacoin",          0x0000006c, 'NovaCoin'),
   array("module_freicoin",          0x0000006d, 'Freicoin'),
   array("module_devcoin",             0x0000006e, 'Devcoin'),
   array("module_frankocoin",          0x0000006f, 'Frankocoin'),
   array("module_protoshares",         0x00000070, 'ProtoShares'),
   array("module_megacoin",          0x00000071, 'MegaCoin'),
   array("module_quarkcoin",          0x00000072, 'Quarkcoin'),
   array("module_worldcoin",          0x00000073, 'Worldcoin'),
   array("module_infinitecoin",       0x00000074, 'Infinitecoin'),
   array("module_ixcoin",             0x00000075, 'Ixcoin'),
   array("module_anoncoin",          0x00000076, 'Anoncoin'),
   array("module_bbqcoin",             0x00000077, 'BBQcoin'),
   array("module_digitalcoin",         0x00000078, 'Digitalcoin'),
   array("module_mincoin",             0x00000079, 'Mincoin'),
   array("module_goldcoin",          0x0000007a, 'Goldcoin'),
   array("module_yacoin",             0x0000007b, 'Yacoin'),
   array("module_zetacoin",          0x0000007c, 'Zetacoin'),
   array("module_fastcoin",          0x0000007d, 'Fastcoin'),
   array("module_i0coin",             0x0000007e, 'I0coin'),
   array("module_tagcoin",             0x0000007f, 'Tagcoin'),
   array("module_bytecoin",          0x00000080, 'Bytecoin'),
   array("module_florincoin",          0x00000081, 'Florincoin'),
   array("module_phoenixcoin",         0x00000082, 'Phoenixcoin'),
   array("module_luckycoin",          0x00000083, 'Luckycoin'),
   array("module_craftcoin",          0x00000084, 'Craftcoin'),
   array("module_junkcoin",          0x00000085, 'Junkcoin'),
;
```

Figure 19: Global Password Module List - 3

The RDP Capture module can be seen below, along with portions of the bitcoin processing modules:

```
// RDP

class module_rdp extends module
{
    public function import_item($stream, $id)
    {
        switch ($id)
        {
```

```
            case 0x0000:
            case 0x0001:
                $rdp_user = ztrim($stream->read_str());
                if ($id == 0x0001)
                {
                    $ip = $stream->read_dword();
                    $rdp_host = strval($ip & 0xff).'.'.
                                strval(($ip >> 8) & 0xff).'.'.
                                strval(($ip >> 16) & 0xff).'.'.
                                strval(($ip >> 24) & 0xff);
                }
                else
                {
                    $rdp_host = ztrim($stream->read_str());
                }
                $rdp_pass = ztrim_unicode($stream->read_str());
                $rdp_pass = unicode_to_ansi($rdp_pass);
                $rdp_host = str_replace('TERMSRV/', '', $rdp_host);

                $this->add_rdp($rdp_host, $rdp_user, $rdp_pass);
                break;
            default:
                $this->log->add("ERR_UNKNOWN_ITEM_TYPE");
                return false;
        }
        return true;
    }
}
```

Figure 20: RDP Capture Module -1

Below, we see how credentials are constructed from the data submitted from infected clients:

```
function extract_domain($url)
{
    if (!strlen($url))
        return '';

    // protocol
    $p = strpos($url, '://');
    if ($p !== false)
        $url = substr($url, $p+3);

    // user:pass divider
    $p = strpos($url, ':');
    if ($p !== false)
        $url = substr($url, $p+1);

    // domain part
    $p = strpos($url, '@');
    if ($p !== false)
        $url = substr($url, $p+1);

    // port
    $p = strpos($url, ':');
    if ($p !== false)
        $url = substr($url, 0, $p);
```

```php
// folder (path)
$p = strpos($url, '/');
if ($p !== false)
    $url = substr($url, 0, $p);

// folder (path)
$p = strpos($url, '\\');
if ($p !== false)
    $url = substr($url, 0, $p);

// some passwords can contain extra '@' chars
$p = strrpos($url, '@');
if ($p !== false)
    $url = substr($url, $p+1);

return $url;
```

Figure 21: RDP Capture Module - 2

Pony Loader stores data in a local MySQL database. This functionality is outlined in database.php on the server hosting the Pony DB:

```php
define('CPONY_LOG_TABLE', 'pony_system_log');
define('CPONY_USER_TABLE', 'pony_user');
define('CPONY_CERT_TABLE', 'pony_cert');
define('CPONY_WALLET_TABLE', 'pony_wallet');
define('CPONY_EMAIL_TABLE', 'pony_email');
define('CPONY_DOMAINLIST_TABLE', 'pony_domainlist');

class pony_db
{
    public $db_link;
    protected $database;
    public $state;
    public $privileges;
    public $auth_cookie;
    public $user_id;
    public $login;

    function __construct()
    {
        $this->state = true;
        $this->db_link = null;
        $this->privileges = '';
    }

    function connect($host, $user, $pass)
    {
        global   $use_mysql_persist_connections;
        if   (!isset($use_mysql_persist_connections))
            $use_mysql_persist_connections = false;

        // establish the connection
        if ($use_mysql_persist_connections)
        {
            // workaround for PHP warning: MySQL server has gone away
            $this->db_link = @mysql_pconnect($host, $user, $pass);
```

Figure 22: Pony Loader SQL Database

Here we actually see an example of the attacker leaving the MySQL credentials exposed (in the clear) in the server's config.php:

```
$mysql_host = 'localhost';
$mysql_user = 'nqvoilsg_obi';
$mysql_pass = 'obiobiobi111';
$mysql_database = 'nqvoilsg_obi';

$global_directory_slash = DIRECTORY_SEPARATOR;
$global_temporary_directory = 'temp';

// debug settings
$global_verbose_log = false; // improved verbose log, use for debugging onl
$global_allow_all_ftp = false; // disable filtering, set 'true' for testing

$global_filter_list = array(
    '127.0.0.1',
    '192.168.',
    'localhost',
    'nonymous',
    'bitshare.com',
    'depositfiles.com',
    'filesonic.com',
    'gigapeta.com',
    'hotfile.com',
    'ifolder.ru',
    'letitbit.net',
    'sms4file.com',
    'turbobit.ru',
    'uploadbox.com',
    'vip-file.com',
    'wupload.com',
);
```

Figure 23: MySQL Credentials - Exposed

Upon execution, Pony Loader will attempt to identify specific AV products running on the victim's machine, for evasion purposes. In the analyzed examples, the binaries are looking to identify running instances of antivirus products from the following companies:

* Bitdefender
* Kaspersky
* AVG

Pony binaries (associated with these campaigns) do not stray from the natively built binaries generated by the Pony Builder, with one exception. Some of the binaries are encrypted with an off-the-shelf Crypter tool called DarkEyE Protector:

Figure 24: DarkEyE Protector Logo

In one example we looked at, the license for DarkEyE Protector is bound to / associated with the email address lakashop25(at)gmail.com. (Visible as artifact embedded in the malware binary). That same email address is associated with the hosting of the Pony C2 domains.

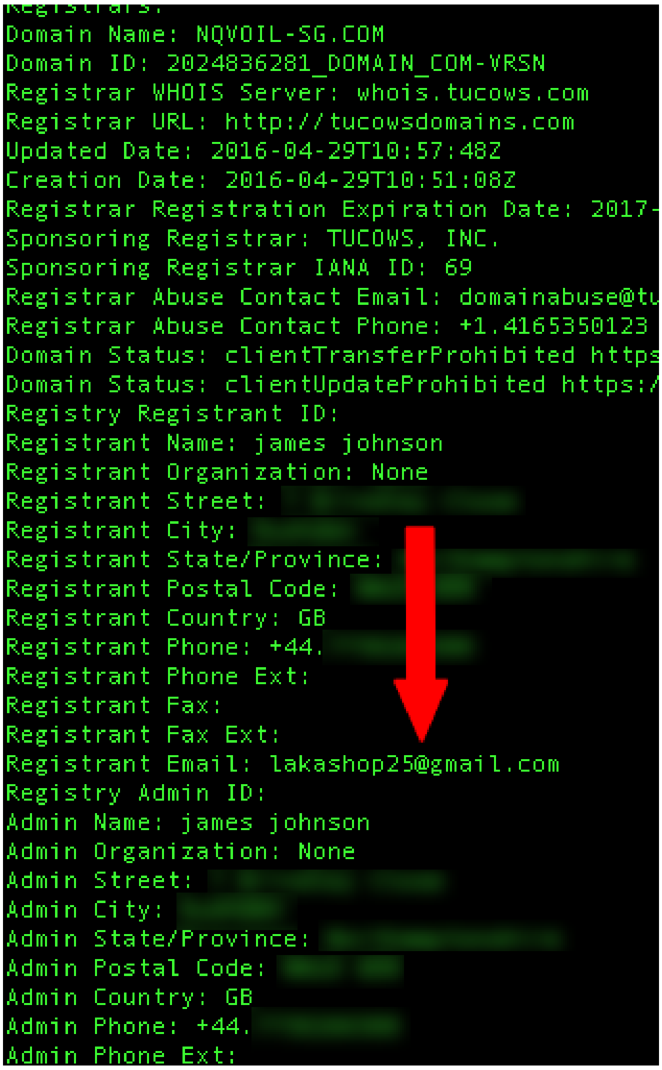

```
Domain Name: NQVOIL-SG.COM
Domain ID: 2024836281_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2016-04-29T10:57:48Z
Creation Date: 2016-04-29T10:51:08Z
Registrar Registration Expiration Date: 2017-
Sponsoring Registrar: TUCOWS, INC.
Sponsoring Registrar IANA ID: 69
Registrar Abuse Contact Email: domainabuse@tu
Registrar Abuse Contact Phone: +1.4165350123
Domain Status: clientTransferProhibited https
Domain Status: clientUpdateProhibited https:/
Registry Registrant ID:
Registrant Name: james johnson
Registrant Organization: None
Registrant Street: [redacted]
Registrant City: [redacted]
Registrant State/Province: [redacted]
Registrant Postal Code: [redacted]
Registrant Country: GB
Registrant Phone: +44.[redacted]
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: lakashop25@gmail.com
Registry Admin ID:
Admin Name: james johnson
Admin Organization: None
Admin Street: [redacted]
Admin City: [redacted]
Admin State/Province: [redacted]
Admin Postal Code: [redacted]
Admin Country: GB
Admin Phone: +44.[redacted]
Admin Phone Ext:
```

Figure 25: Domain Hosting Purchase Showing Use of Email Address: lakashop(at)gmail.com

If we go back to some of the initial spear-phish campaigns, we can actually find one where that same email account was used to send the infected message:

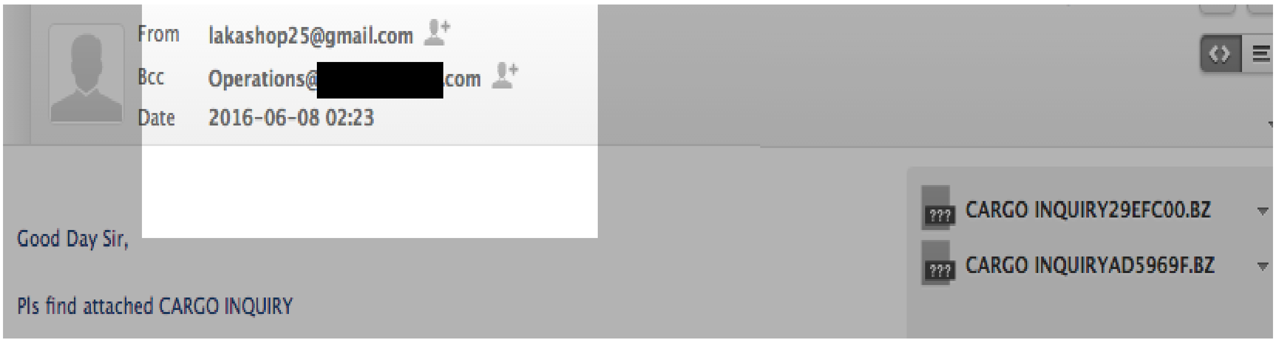
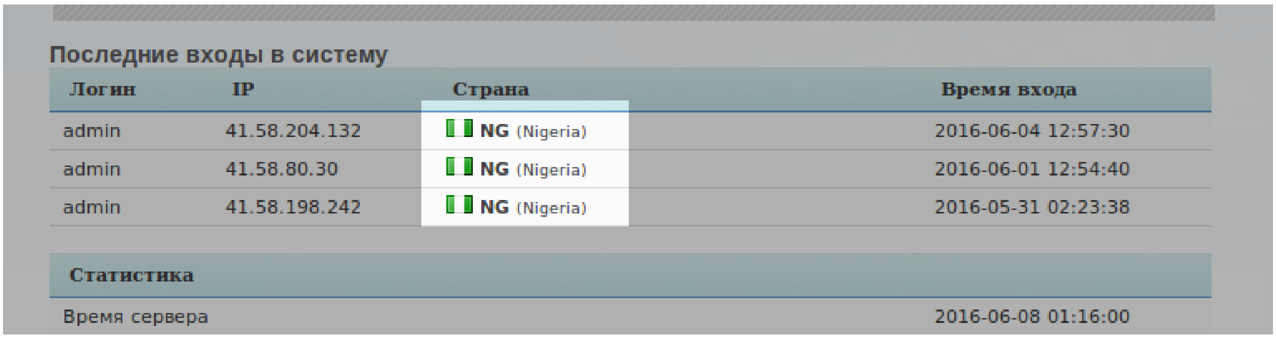


Figure 26: Spear Phish Email Showing Same Email Address Used as Domain Purchaser

Attribution

There are many aspects that point to Nigeria above and beyond the by-the-book modus operandi outlined in both this write-up and some of the past efforts previously referenced.

We also observed that most of the logins to the various Pony admin panels were tagged as being in Nigeria:



Последние входы в систему

Логин	IP	Страна	Время входа
admin	41.58.204.132	NG (Nigeria)	2016-06-04 12:57:30
admin	41.58.80.30	NG (Nigeria)	2016-06-01 12:54:40
admin	41.58.198.242	NG (Nigeria)	2016-05-31 02:23:38

Статистика	
Время сервера	2016-06-08 01:16:00

Figure 27: Pony Admin Panel Showing Logins From Nigeria

We also see consistent reuse of user names and passwords that reference Nigerian culture. These accounts appear consistently among the compromised accounts as well within the actual administrative credentials to Pony admin panels.

For example, one particular actor uses several variations of “waxxy” which is a reference to the popular Nigerian DJ known as DJ Waxxy.

EX: waxxy3:waxxysomuch
EX: waxxy3:vgwbnpcnra
EX: waxxy3:louiss33

We also see several recurring uses of “chukwuka123” and “chukwuka”. “chukwuka” is a reference to the popular Nigerian actress Chioma Chukwuka:

Figure 28: Chioma Chukwuka, Whose Name is Often Used as a Password

The term “chukwuka” is more frequently used as the password to some of the Pony admin panels, but appears as a modified password for compromised accounts as well.

Going back to the specific attribution side, we can do a little more digging around these terms to find OSINT pointing to specific individuals acting as part of this cybercrime group.

One particular username and associated email account pops up far more frequently than others. The “onyeb4real” user name is frequently observed setting up dummy/burner email accounts and using them to send out either weaponized messages, or text-only social engineering lures in attempts to lure victims into either running malicious code, or visiting sites hosting malicious code.

Examples are listed below (exact URLs obfuscated):

h x x p s / / -onyeb4real@gmail.com:hope@www.maxxxxxxxxxxxxxxxxxxxxxxxookmark
h x x p s / / -onyeb4real@yahoo.com:louiss33@www.xxxxxxxxxxxxxom/cart
h x x p s / / -onyeb4real@gmail.com:louiss33@dolxxxxxxxxxxxxxxxxxxom/join/shipping
h x x p / / -onyeb4real@gmail.com:louiss33@traclxxxxxx.xxxx/signup/
h x x p / / -onyeb4real@gmail.com:louiss33@my.fxxxxxxxxxxxxxomgnup.seam

h x x p s / / -onyeb4real@gmail.com:louiss33@wwwxxxxxxxxxxxxxxomm.ng
h x x p s / / -onyeb4real@gmail.com:Louiss33@wwxxxxxxxxxxxxxxomount/login.jsp
h x x p / / -onyeb4real@gmail.com:louiss33@www.juxxxxxxxxxxxxxom959.html
h x x p s / / -onyeb4real@gmail.com:louiss33@wwxxxxxxxxxxxxxxomm
h x x p / / -onyeb4real@yahoo.com:louiss@wwxxxxxxxxxxxxxxomos_.html
h x x p / / -onyeb4real@yahoo.com:louiss@baxxxxxxxxxxxxxxomgnin/
h x x p s / / -onyeb4real@gmail.com:louiss33@m.exxxxxxxxxxxxxxomnin
h x x p s / / -onyeb4real@gmail.com:louiss33@signin.exxxxxxxxxxxxxxomSAPI.dll
h x x p s / / -onyeb4real@yahoo.com:louiss@xxxxxxxxxxxxxxomgin.php

Oftentimes, the “onyeb4real” string is coupled with “louis33”. If we refer to the "waxxy" references outlined above, we see that there are also couplings of “louiss” (and variations of it) and both “onyeb4real” and "waxxy".

A little OSINT digging reveals numerous profiles of a specific Nigerian individual names “Louis” with a frequent handle of Waxxy or Waxxy3. The email address tied to this individual’s social media accounts is: onyeb4real(at)gmail.com.

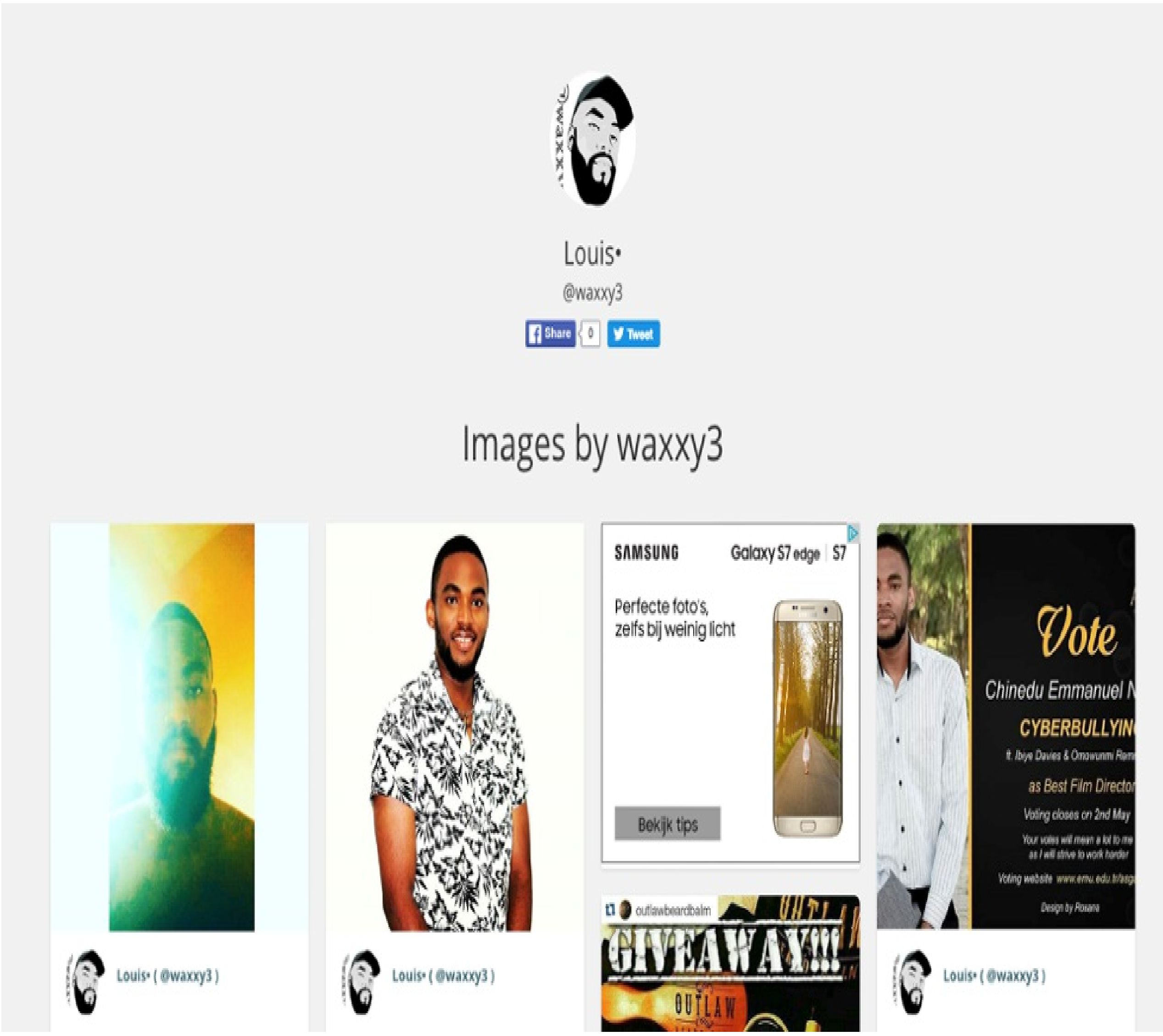


Figure 29: Instagram Account of Louis - AKA “Waxxy” 1

When cross-referencing publicly available information on this individual, we are able to collect numerous fragments of data that solidify the location of this particular actor. In the example below, we see a classified advert selling a used Blackberry:

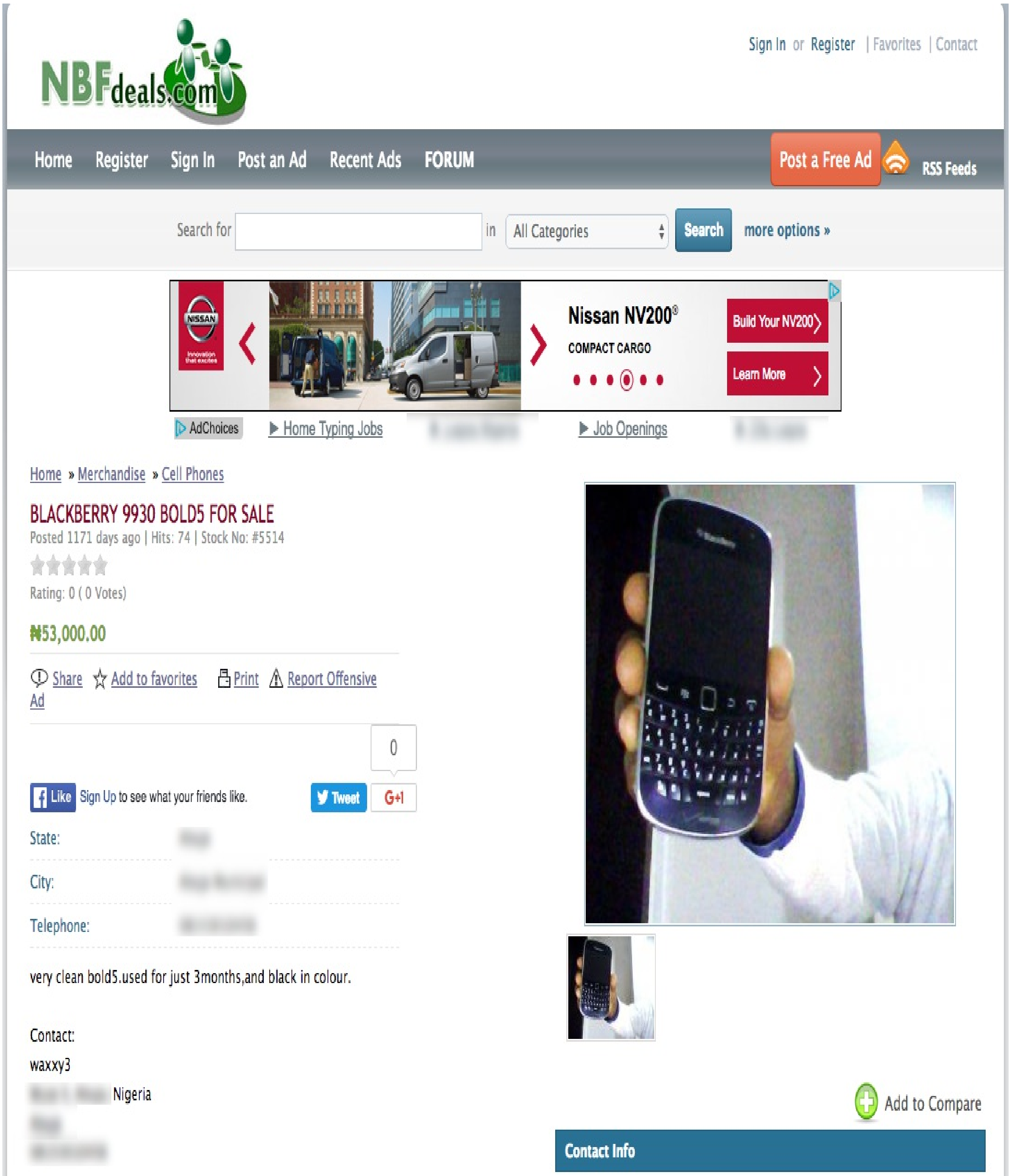


Figure 30: Blackberry Phone sold online by “Waxxy”

Meet Louis Onyeka - AKA Waxxy3 - AKA Onyeb4Real:

Figure 31: Louis Onyeka - AKA Waxxy3 - AKA Onyeb4Real

The Test – CylancePROTECT® vs. Pony Loader & Hawkeye

All of these compromises require that a Pony or Hawkeye binary be executed on the target host. It is therefore critical that any protective or preventative controls on the hosts completely prevent that binary from being executed. Now that we see how much sensitive information a small group of cybercriminals can get access to using simple stolen email credentials, we can understand how vital it is to prevent this simple theft from happening. Unfortunately, that is not always possible with traditional, signature-based, technologies running on the endpoint.

It is important to point out that some of the samples we analyzed were not 'publically available' at the time of analysis. That is to say, there were not available on any of the popular, multi-engine, scanning and analysis services which many legacy antivirus technologies and vendors rely on. Having to rely on third party services or quickly outdated signatures is not an option if you wish to prevent these kinds of attacks from occurring.

Cylance tested over 30 samples associated with these attacks using our AI based endpoint protection solution CylancePROTECT. CylancePROTECT stopped all of them cold, pre-execution. End of story.

<u>The following samples were tested against CylancePROTECT:</u>

9ece0cad4cbfe0cf2524880461d62419ed2dcc5f6531c4f4d0b88b16a8a29890
0f8995f8ece4ec14d6ad1745ec11987a02585c0e83ffa8f5c752331a16e0a02f
7009bde544c8cae66301899cd15963698fe78abf31d11b32a0e38028f3472fb9
6d53538d71e655b22a64e41dd986789fb0f81a0cec528fcfb9c7eff770f64363
1b7f600c8dbe9683e2e092e12ce6fc9a296e341c4106acfdb9fbf48c018b1fbe
d6093f98bb65a669487eb1e41f550a4cd7b0a8c30fa2a9f050eb3bb43d69e1be
35194eb171953f2df033a8941053c1f96b74a9d926ba8f991299956cf5243fe9
924fadc931ce2dd5f0b2a83e470ff7ef4ab30ccd17f99dad67103fca2dd5f2b4
7de63c48f9b5caba8855012875937a515b2a6821f230bc291884bc37bc92a62f
d49251a4909f51bac8981fde55696746572f38d463d2fb3fdfe8d7dfff973ff6
de64c7ff454cbb648091f6779eaf2351ddcb25e68087eb8853ac83848598315e
97f25bb70111fe56d3a6b788fc5a0160923fe82ec875305c10541bcff455d5d7
eb3808f586de4cadf98a9a08f303d07de63cdfd8e709181139627c15ff5bab5f
e613e0390fdbfd04d475747d84f966440f9a52a4d49170e5d35ed141bd849fb1
d70aab7549551161df985fe4bea9c00081816c529682f8e01673ca37cff73468
276286c21c93060701b4fd844be7af10b85671e90622e777ebeeeca6e44265b0
d35faedfa36e5ce25f5918e0fe4b536109d9ee49c95da7403c976189c3bcf950
b3062e772925653a6a1c52b7690854f8f26216e78ee836db295aa4c007144bea
befceb428a4f678731b368e00431d5c15e3522c03748e1980db559988c074837
f26a26ccdb91b4bd26406146858477556a5c734a0f276360d2b07fbd697f693d
495b2d3102de768ca3a8c428788777b254ff01023058bca1a1b3f19c9958564b
a7d9cd02734a49e30dfdff4d37e878831717afd9aaa0bbf04814980aea7bb65b
4c10dd2c7477ffa1921a3c646fd728a8f96210c8a984d6d4d4016ca9cf13db20
97c78d5ec6ca8b0b9af2038cb42d6d5c8c560ee11bbf7ba939f916f62b0d0f38
812284a88b8fe2b9af802aeb43d928e18443335fa4a83a62565224ff5e7bcccd
a4f362f3282a1988824fb4fcdf1faa40bb86e7c41ae813ad383753d33c6c5fc2
dd68390cba23f0a740e9cb2c44963c03ea38eb44067447a757fffd4c7a0d214d
3b8f1e963da628ebe6308fbdbbed378593242c5c9eaff9ee68e5c42f8277e608

c73fea308a2cd4c5f201c011b3ebba3466e3af0a0388b25e49680a01c3c8c61e
fb18cbe7482eccc37cca30f354a8fad710494477dd47bc0a8fb6744aeb6c3283
b9caa67341fe2c191a2fc7bc4b932c9f4c96bc4a7d4906d28871db609623e55f
72b8b03e9a0835529c4324e7d0f2c0d13e8d14e8ac1d77072407542c79705bb0
c374a14d2f95a6544acc084e78b70382b6d1294cfb47b486f757f0575d6d2fea
857f1201bd89c906cad2c4a0b9f280e0412392e82a09f5c3f5c3f032304fa34e
a5f9fb3fb839f484359e89e7043ef3739da4ebcd01fd8bc010e26905f725cc72
be882ecbe903b4b9e74d6f592053231c4ce5e653212fadf05cb5261d69bad4f4

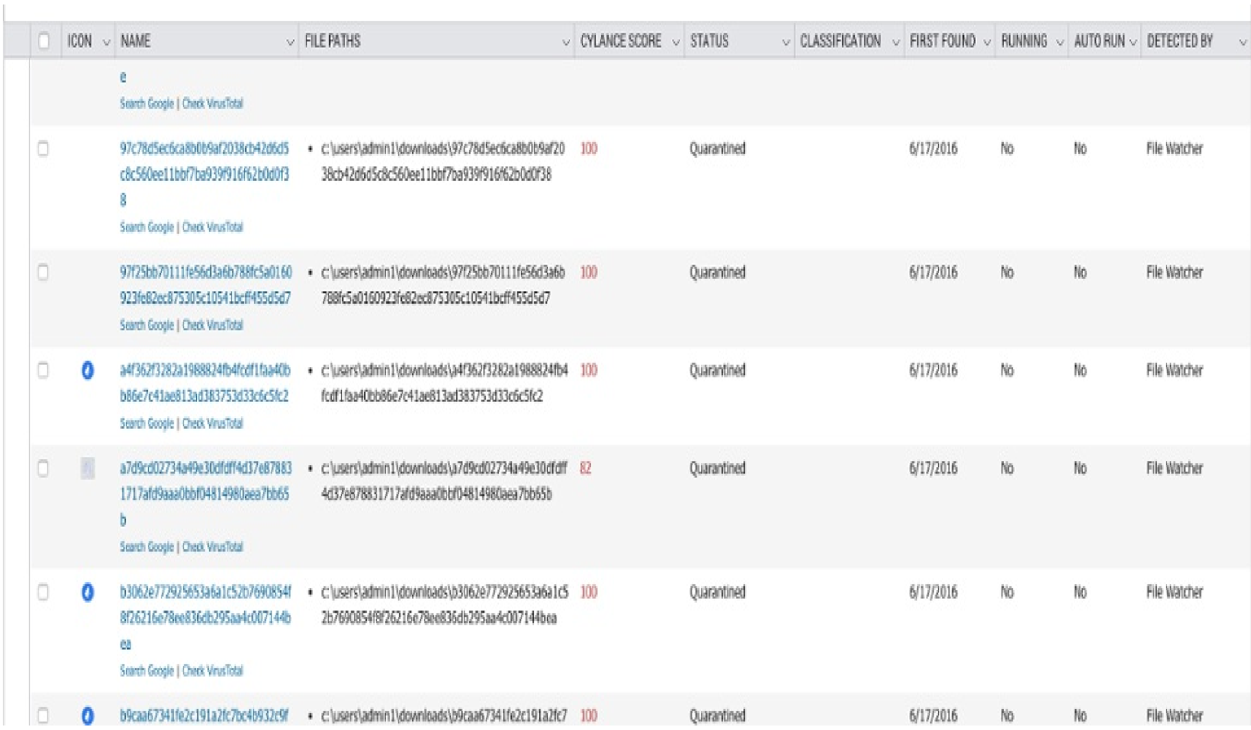
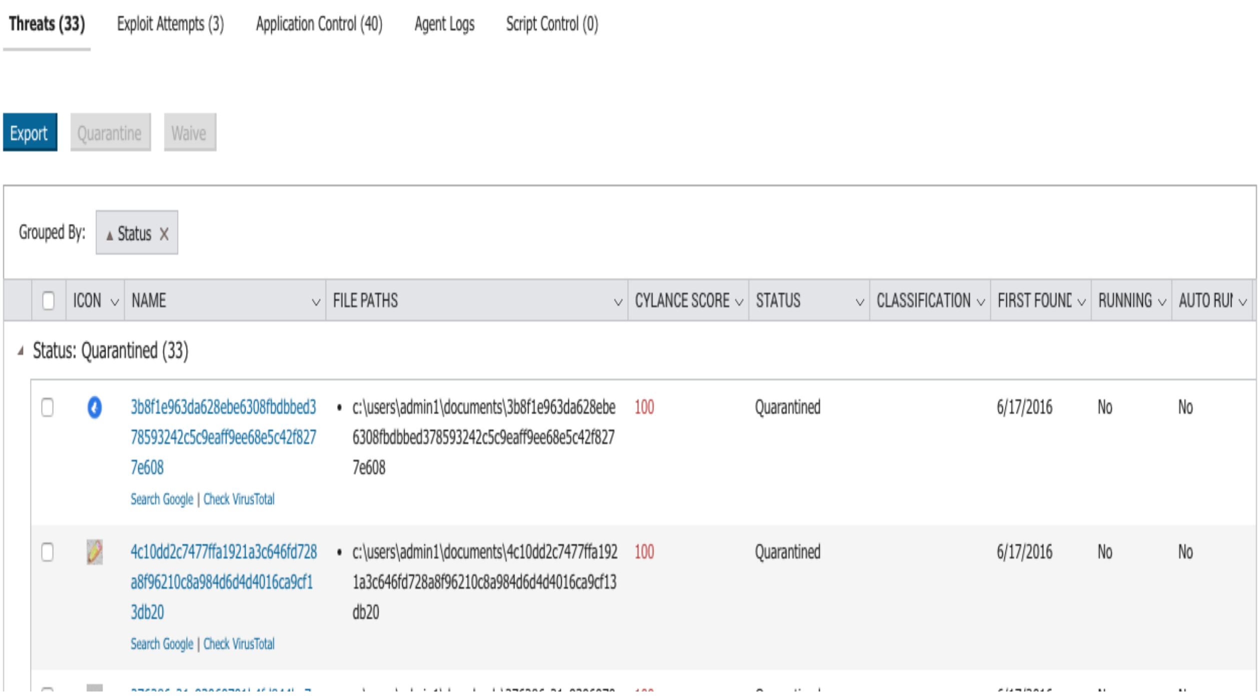


Figure 32: CylancePROTECT Dashboard, Showing Detected and Quarantined Samples Associated With the Nigerian Phishing Attacks - 1



27628bc21c93060701b4fd844be7af10b85671e90622e777ebeeeca6e44265b0 Search Google | Check VirusTotal	• c:\users\admin1\downloads\27628bc21c93060701b4fd844be7af10b85671e90622e777ebeeeca6e44265b0	100	Quarantined	6/17/2016	No	No
495b2d3102de768ca3a8c428788777b254ff01023058bca1a1b3f19c9958564b Search Google | Check VirusTotal	• c:\users\admin1\downloads\495b2d3102de768ca3a8c428788777b254ff01023058bca1a1b3f19c9958564b	100	Quarantined	6/17/2016	No	No
7009bde544c8cae66301899cd15963698fe78abf31d11b32a0e38028f3472fb9 Search Google | Check VirusTotal	• c:\users\admin1\downloads\7009bde544c8cae66301899cd15963698fe78abf31d11b32a0e38028f3472fb9	19	Quarantined	6/17/2016	No	No

Figure 33: CylancePROTECT Dashboard, Showing Detected and Quarantined Samples Associated With the Nigerian Phishing Attacks - 2

Appendix – IOCs

SHA256 Hashes

9ece0cad4cbfe0cf2524880461d62419ed2dcc5f6531c4f4d0b88b16a8a29890 pcchand

0f8995f8ece4ec14d6ad1745ec11987a02585c0e83ffa8f5c752331a16e0a02f pcchand

7009bde544c8cae66301899cd15963698fe78abf31d11b32a0e38028f3472fb9 pcchand

6d53538d71e655b22a64e41dd986789fb0f81a0cec528fcfb9c7eff770f64363 pcchand

1b7f600c8dbe9683e2e092e12ce6fc9a296e341c4106acfdb9fbf48c018b1fbe pcchand

d6093f98bb65a669487eb1e41f550a4cd7b0a8c30fa2a9f050eb3bb43d69e1be pcchand

35194eb171953f2df033a8941053c1f96b74a9d926ba8f991299956cf5243fe9 pcchand

924fadc931ce2dd5f0b2a83e470ff7ef4ab30ccd17f99dad67103fca2dd5f2b4 pcchand

7de63c48f9b5caba8855012875937a515b2a6821f230bc291884bc37bc92a62f pcchand

d49251a4909f51bac8981fde55696746572f38d463d2fb3fdfe8d7dfff973ff6 pcchand

de64c7ff454cbb648091f6779eaf2351ddcb25e68087eb8853ac83848598315e pcchand

97f25bb70111fe56d3a6b788fc5a0160923fe82ec875305c10541bcff455d5d7 nqvoil-sg

eb3808f586de4cadf98a9a08f303d07de63cdfd8e709181139627c15ff5bab5f
nqvoil-sg
e613e0390fdbfd04d475747d84f966440f9a52a4d49170e5d35ed141bd849fb1
nqvoil-sg
d70aab7549551161df985fe4bea9c00081816c529682f8e01673ca37cff73468
nqvoil-sg
276286c21c93060701b4fd844be7af10b85671e90622e777ebeeeca6e44265b0
friendship-chartering
d35faedfa36e5ce25f5918e0fe4b536109d9ee49c95da7403c976189c3bcf950
friendship-chartering
b3062e772925653a6a1c52b7690854f8f26216e78ee836db295aa4c007144bea
friendship-chartering
befceb428a4f678731b368e00431d5c15e3522c03748e1980db559988c074837
friendship-chartering
f26a26ccdb91b4bd26406146858477556a5c734a0f276360d2b07fbd697f693d
toships(dot)net
495b2d3102de768ca3a8c428788777b254ff01023058bca1a1b3f19c9958564b
toships(dot)net
a7d9cd02734a49e30dfdff4d37e878831717afd9aaa0bbf04814980aea7bb65b
toships(dot)net
4c10dd2c7477ffa1921a3c646fd728a8f96210c8a984d6d4d4016ca9cf13db20
toships(dot)net
97c78d5ec6ca8b0b9af2038cb42d6d5c8c560ee11bbf7ba939f916f62b0d0f38
toships(dot)net
812284a88b8fe2b9af802aeb43d928e18443335fa4a83a62565224ff5e7bcccd
toships(dot)net
a4f362f3282a1988824fb4fcdf1faa40bb86e7c41ae813ad383753d33c6c5fc2
tosihps(dot)com
dd68390cba23f0a740e9cb2c44963c03ea38eb44067447a757fffd4c7a0d214d
tosihps(dot)com
3b8f1e963da628ebe6308fbdbbed378593242c5c9eaff9ee68e5c42f8277e608
tosihps(dot)com
c73fea308a2cd4c5f201c011b3ebba3466e3af0a0388b25e49680a01c3c8c61e
tosihps(dot)com
fb18cbe7482eccc37cca30f354a8fad710494477dd47bc0a8fb6744aeb6c3283
tosihps(dot)com
b9caa67341fe2c191a2fc7bc4b932c9f4c96bc4a7d4906d28871db609623e55f
tosihps(dot)com
72b8b03e9a0835529c4324e7d0f2c0d13e8d14e8ac1d77072407542c79705bb0

tosihps(dot)com
c374a14d2f95a6544acc084e78b70382b6d1294cfb47b486f757f0575d6d2fea
tosihps(dot)com
857f1201bd89c906cad2c4a0b9f280e0412392e82a09f5c3f5c3f032304fa34e
tosihps(dot)com
a5f9fb3fb839f484359e89e7043ef3739da4ebcd01fd8bc010e26905f725cc72
nqvoil-sg
be882ecbe903b4b9e74d6f592053231c4ce5e653212fadf05cb5261d69bad4f4
shit(dot)exe, various hosts

Domains

cosmoships-gr(dot)com
etaship-sg(dot)com
prisheimpex(dot)com
toships(dot)net
seahorsegroup-in(dot)com
viatexcursions(dot)com
iwenconsultinggroup(dot)com
nevig8group(dot)com
vsuil(dot)com
rightltd-gr(dot)com
vrmeritime(dot)com
transegrldmcc(dot)com
vietexcurisons(dot)com
vietaxcursions(dot)com
toslhps(dot)com
pcchand(dot)com
arcadieshipping(dot)com
tosihps(dot)com
pruship-tw(dot)com
friendshlp-chartering(dot)com
toslhips(dot)com
alexbensonship(dot)com

IP Addresses

149.255.58.2
149.255.58.4
149.255.62.53

149.255.62.54

Believe the Math!!!

Convinced that the next generation of endpoint security is right for your organization? Contact a Cylance expert to get started!

Tags: Nigerian Scams, Hawkeye, Pony, Pony Loader

« **Back to Blog**

Blog

No More Sacrificial Lambs

by Chad Skipper

The Unbelievable Tour

18201 Von Karman, Suite 700
Irvine, CA 92612
USA

Call Us: 1-844-CYLANCE
1-844-295-2623

Get Support: 1-866-699-9689
Incident Response: 1-877-973-3336