

KeyBase Threat Grows Despite Public Takedown: A Picture is Worth a Thousand Words

 unit42.paloaltonetworks.com/keybase-threat-grows-despite-public-takedown-a-picture-is-worth-a-thousand-words/

Jeff White

February 25, 2016

By [Jeff White](#)

February 25, 2016 at 5:00 AM

Category: [Malware](#), [Threat Prevention](#), [Unit 42](#)

Tags: [Alibaba](#), [AutoFocus](#), [KeyBase](#), [Keylogger](#)

Be the first to receive the latest news, cyber threat intelligence and research from Unit 42. [Subscribe Now.](#)

In June 2015, Unit 42 [reported](#) on a keylogger malware family known as KeyBase, which had first appeared in February 2015. The author has since taken down its website and supposedly ceased selling the software, while also renouncing the tool's use for any malicious purposes. However, as of this writing, the software is still readily available for download with minimal effort on multiple websites. What's more, while development of KeyBase appears to have stopped, the usage of this malware has increased significantly since June. In our initial report, we identified approximately 1,500 sessions carrying KeyBase and approximately six months later we have seen over 4,900 different samples and 44,200 sessions within Palo Alto Networks AutoFocus.

One interesting discovery, identified by Unit 42 malware researcher [Josh Grunzweig](#) was that while the KeyBase web panel requires authentication for access, the part of the KeyBase web panel which saves screenshots from the infected computers is not properly locked down, thus requiring no authentication and allowing anyone on the Internet to freely access it. This lack of security on the miscreants' part opens up a window to perform target analysis of the infected machines.

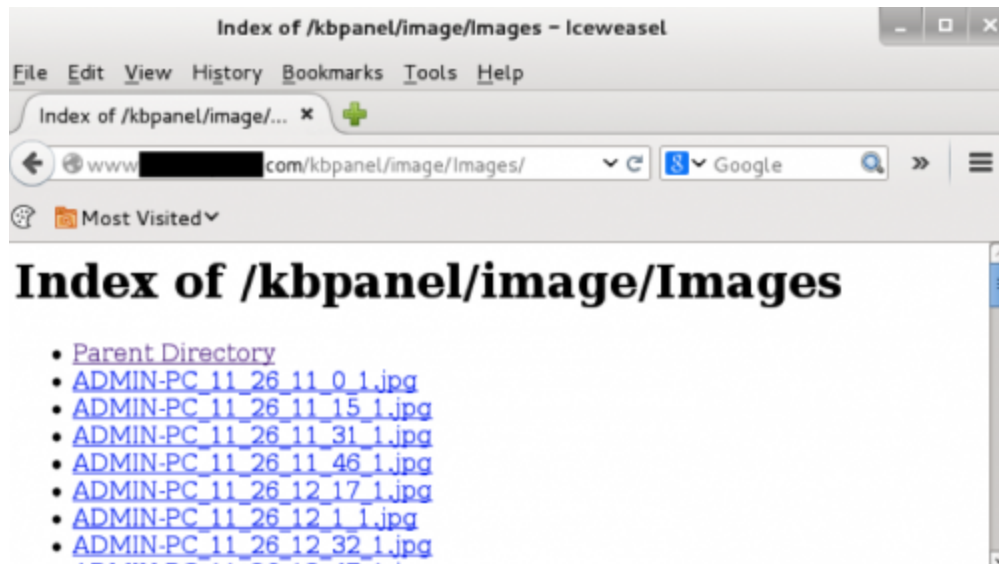


Figure 1 - Open /Images/ directory

By leveraging the visibility within AutoFocus along with KeyBase web panels identified through information sharing groups, 64 websites have been identified hosting 82 active KeyBase web panels with a total of 933 infected Windows systems accounting for 125,083 screenshots. These images give us a glimpse into what attackers see when they infect systems, what information they obtain outside of the normal keystroke and clipboard logging capabilities of the malware, and how that information may be used for malicious activity. This blog post will explain our findings in detail, but here is a short summary of what you'll see if you read through to the end.

- India, China, South Korea and the United Arab Emirates are most targeted with KeyBase, but the impact is global.
- Companies in the manufacturing and transportation industries see the most KeyBase infections.
- Attackers captured screenshots of sensitive e-mails, bank account transfers, security cameras and hotel management systems.

Attackers who (accidentally) infected their own systems revealed the tactics, tools and procedures they used to launch their attacks.

Defining terms & the analysis process

Before we dive into the data, it must be said that since we are analyzing images, we are making some assumptions. For example, if an image shows an e-mail being composed and the e-mail has a signature at the footer with a company name and position, we assume this to be an indicator of the company and user's role. Similarly, if we see images showing three different Facebook accounts logged in during the course of the infection, we assume the system is a shared resource among multiple people. More often than not, we needed to combine information from multiple screenshots to determine the user or company.

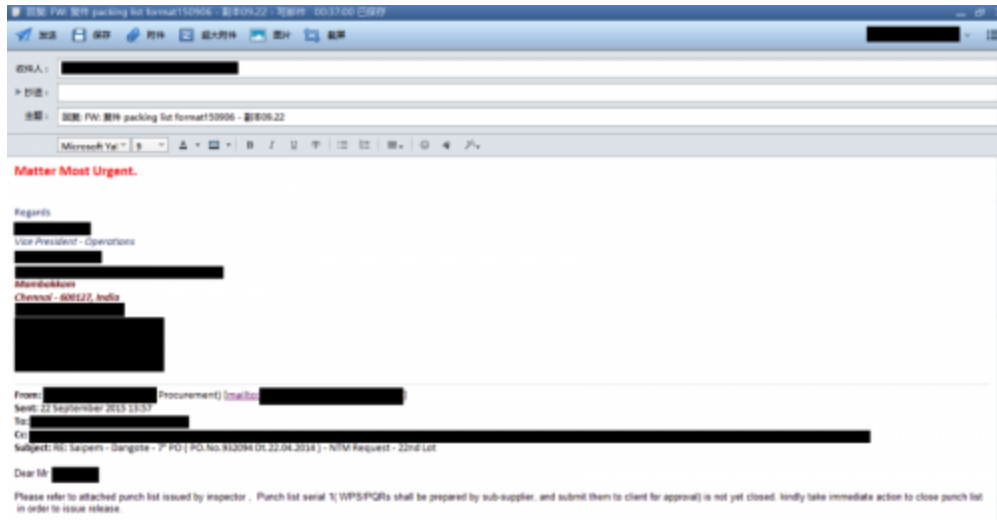


Figure 2 - Signature based identification on e-mail being composed

Throughout the analysis of the more than 125,000 images, we defined a number of data points to track across all infections. Below is a listing of the categories that will be referenced throughout the rest of this post and a brief definition of what we looked for during analysis.

- **Geographic location** – Country in which the infected user was located. Typically determined via e-mail signature, local events, e-mail content, or corporate location.
- **Industry** – Standard industry category names, taken from AutoFocus. Typically determined by outside company look-up via the Internet.
- **Company name** – Official company name. Typically determined via e-mail signatures, corporate documentation, desktop images, applications, or logged in accounts.
- **Corporate title** – The corporate title displayed by the user of the infected system. Typically determined via e-mail signature or corporate documentation.
- **Corporate data** – Information that appears to be internal to the company, such as budgets, research, salaries, roadmaps, inventory, and logistical information. Typically determined via e-mail content and corporate documentation.
- **Client data** – Information that appears to be related to the corporate business but exposes information of third parties, such as purchase orders, client details, contracts, and legal documents. Typically determined via e-mail content, internal applications, or corporate documentation.
- **Shared usage** – When the infected system was clearly used by more than one individual. Typically determined via non-corporate e-mail usage, social media accounts, and chat applications.
- **Personal usage** – When the infected system appeared to be used for non-corporate activity, such as social media, watching movies, or playing games. Typically determined via browser activity or application usage.
- **Bank usage** – When the infected system was used to conduct online banking activities. Typically determined via browser activity of online banking websites.

- **Lure Subject/Name/Address** – Details on phishing e-mails used to deliver the KeyBase malware. Typically determined via e-mail activity.
- **Archive/File Name** – Details on archives or files used to deliver the KeyBase malware. Typically determined via e-mail activity or archive applications.

The Rise of KeyBase

Palo Alto Networks began detecting an increase in KeyBase delivery sessions at the beginning of August 2015 and it began escalating quickly thereafter, with thousands of unique samples coming in per month.

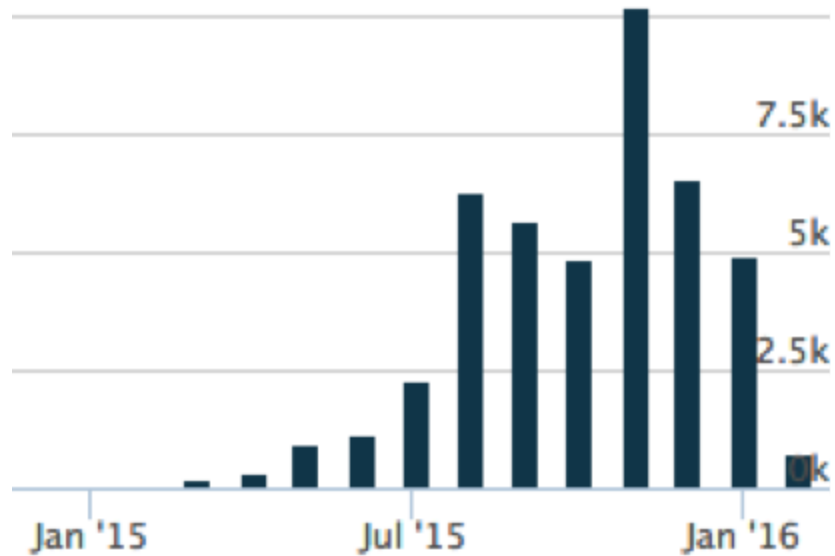


Figure 3 – KeyBase malware samples in AutoFocus increase in August 2015

When looking at the dates and volumes of images collected, it matched up with the above image data curve, with thousands of screenshots being sent back to KeyBase web panels on a daily basis.

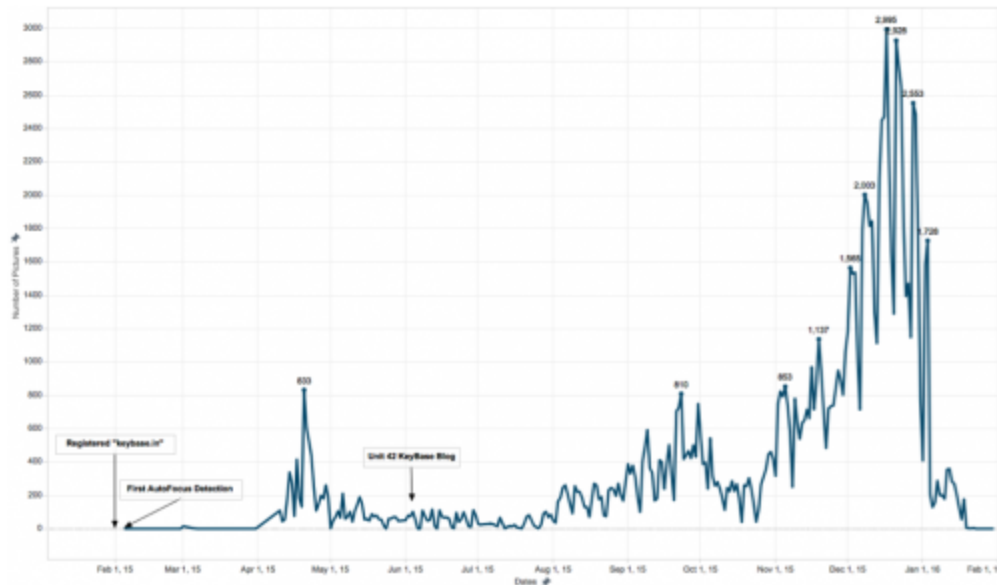


Figure 4 – Volume of images collected per day from KeyBase web panels

Since the KeyBase builder was leaked, more miscreants have gained access to the software and we see this reflected in its proliferation. A side effect, of course, is that once it has entered the easily accessible tool population, you have a wide variety of actors using it, with different intentions and different techniques. This is where target analysis becomes valuable as patterns begin to emerge and you can attempt to discern targeted attacks from opportunistic ones.

Across the set of extracted images, there was an average of 133 images per infection, with the minimum being 1 and the maximum being 5,029; sometimes all that was needed to convey a story was 1 image, while other times hundreds may not be sufficient.

When the KeyBase builder generates a new variant of the malware, the user of the application has the ability to specify how often screenshots should be taken, along with the option of doing “InstaLogging” screenshots for specific websites, such as Facebook or Google. We commonly saw screenshot intervals at 1 minute (default), 10 minutes, or 30 minutes – effectively giving us 1 hour, 1 day, or 2 days of average visibility into a user’s activity.

One of the challenges faced -- assuming periods of inactivity for user sleep or PC shutoff, along with the time between screenshots -- is that our sample set of useful data can be quite small, so every screenshot needs to be assessed for minute details. As such, the following sections are based on observations made during the analysis of the more than 125,000 KeyBase screenshots.

One final point before getting any further into the analysis is that we are looking at pictures from infected systems and, while we can speculate on how the data might be used, at the end of the day we really have no idea how its being used based solely on this information.

Are the miscreants really interested in salaries, inventories, design blueprints, research, cargo manifests, and internal e-mails with devious plans to exploit the data? Or are they just looking to steal someone's Facebook password to sell for a quick buck? Towards the end of this blog we'll also take a look at a number of people who infected themselves with KeyBase, whether for testing or by accident, and see what the bad guys are up to.

Observations

Where in the world?

We found that infected systems are located primarily in Asia Pacific, Europe, Middle East, and Africa with the largest infection bases found in India, China, South Korea, and the United Arab Emirates. The below image represents 342 of the 933 infected systems, identifiable by location, and their respective volume of images per country.



Figure 5 – Geographic spread of KeyBase malware

Taking a look at Industry, there were 27 different categories identified, with Manufacturing, Transportation & Logistics, Wholesale & Retail, and Engineering making up the majority of infected PC's with corporate data.

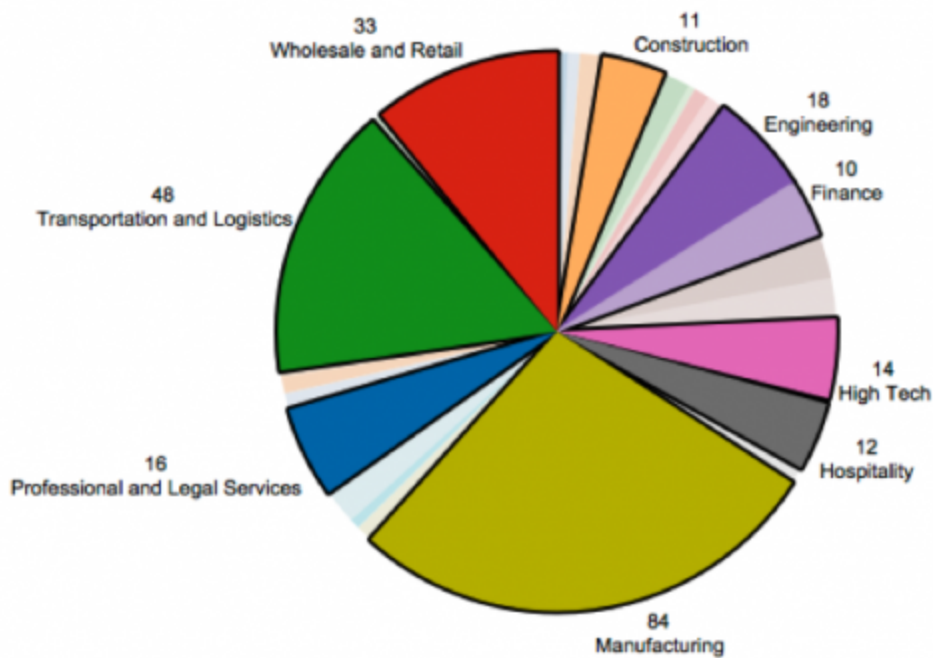


Figure 6 – Industry breakdown

Combining this information and overlaying industry data on top of geographic data, we can see certain countries stand out, possibly implying a concentrated effort to target industries in those locations. More often than not, the screenshots seemed to indicate the infected system was used for company activity versus purely personal usage.

Manufacturing

For the manufacturing industry we see a large concentration in South and East Asia, totaling 46 different infections across 45 different companies. These companies are heavily focused on metal materials and products throughout the region. This is not surprising given three of the top five manufacturing economies are based in this geographic area.



Figure 7 – Manufacturing: Infection Distribution

What stood out across this industry was the usage of websites to buy materials or sell manufactured products. One website that stood out in particular was [Alibaba](#), which is similar to an eBay for manufacturers and suppliers. However, making global trading easier isn't possible without communication and each company has a profile page with a link to contact the business.



Figure 8 - Requests for goods on Alibaba.com

It's plausible, given the number of companies infected in the same region, in the same industry, that targets may have been selected via Alibaba or similar websites and delivered malware through their respective listed contact addresses. For the data we have available, we saw corporate titles for the recipients of the malware in five sales roles, three in purchasing/supplies, and one in exports.

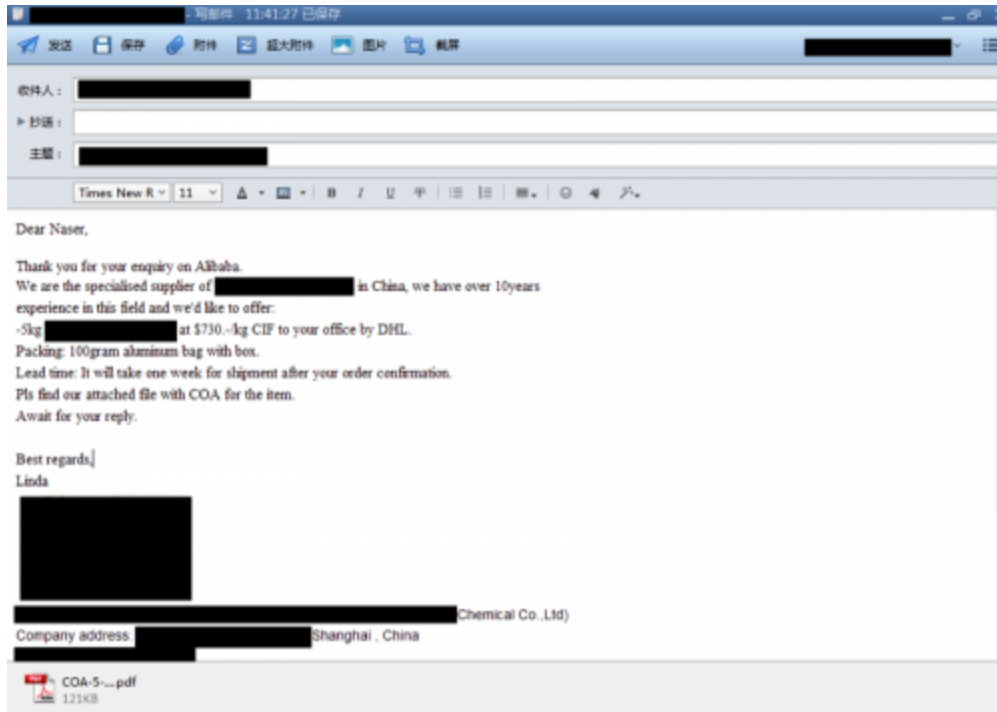


Figure 9 - E-mail reply to an Alibaba message

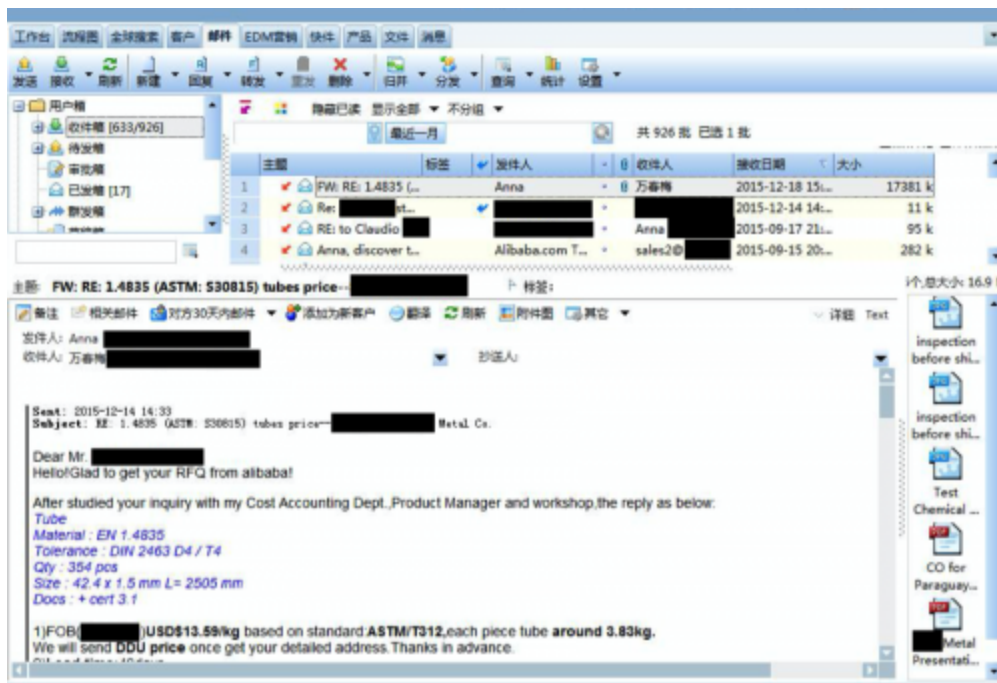


Figure 10 - E-mail reply to an Alibaba message

The type of data an attacker would see varied greatly for this industry, but it wasn't uncommon to see purchase orders, invoices, quotes, client/customer information, inventories, or even designs for products.

19/08/2015 Invoice Wise Sale
From 01/05/2015 To 31/05/2015

DATE	INV #	DISPATCH #	CUSTOMER NAME	AMOUNT
27/05/2015	SI-31691	29721	[REDACTED]	56,271.92
27/05/2015	SI-31692	29722	[REDACTED]	66,386.52
27/05/2015	SI-31693	29723	[REDACTED]	97,920.00
27/05/2015	SI-31694	29724	[REDACTED]	23,709.72
27/05/2015	SI-31695	29725	[REDACTED]	32,302.20
27/05/2015	SI-31696	29726	[REDACTED]	12,960.00
27/05/2015	SI-31697	29727	[REDACTED]	85,113.60
27/05/2015	SI-31698	29728	[REDACTED]	163,518.60
28/05/2015	SI-31699	29741	[REDACTED]	1,439,608.80
28/05/2015	SI-31700	29729	[REDACTED]	79,444.80
28/05/2015	SI-31701	29730	[REDACTED]	219,672.00
28/05/2015	SI-31702	29731	[REDACTED]	576,979.20
28/05/2015	SI-31703	29732	[REDACTED]	31,850.88
28/05/2015	SI-31704	29733	[REDACTED]	6,075.00
28/05/2015	SI-31705	29734	[REDACTED]	24,300.00
28/05/2015	SI-31706	29735	[REDACTED]	67,813.20
28/05/2015	SI-31707	29736	[REDACTED]	12,906.48

Figure 11 - Invoice data for multiple customers with values

Dear Mr. [REDACTED]

Tomorrow we shall quote you considering you will provide us tools.

If we have to develop the tools we shall quote tools cost at the the time of finalisation of roder.

Your early action in the above matter will be highly appreciated.

Thanks & regards,

[REDACTED]

Mobile: [REDACTED] / What's App No.: [REDACTED]

Web: [REDACTED]

[REDACTED]

Mfrs. Of Industrial [REDACTED] & HI-Tech [REDACTED] Products

An ISO 9001-2008 Certified Company

Figure 12 - Drafting document/e-mail for an upcoming quote for their product

主题: Re: RE: Re: Enquiry No 15130 // 3-way 16" control Valve CL150

发件人: [REDACTED] 收件人: [REDACTED]

【伊程】 发送时间: 2013-09-18 10:05 当前时间: 2013-09-21 13:17

Dear Nancy,

Sorry for the late response. Actually the client did not accept the drawing type. For your reference please consider the below sample. Please accordingly provide your drawing based on in order we could get the client's approval.

Any sooner feedback would be thankful.



Figure 13 - E-mail with designed valve details for client approval

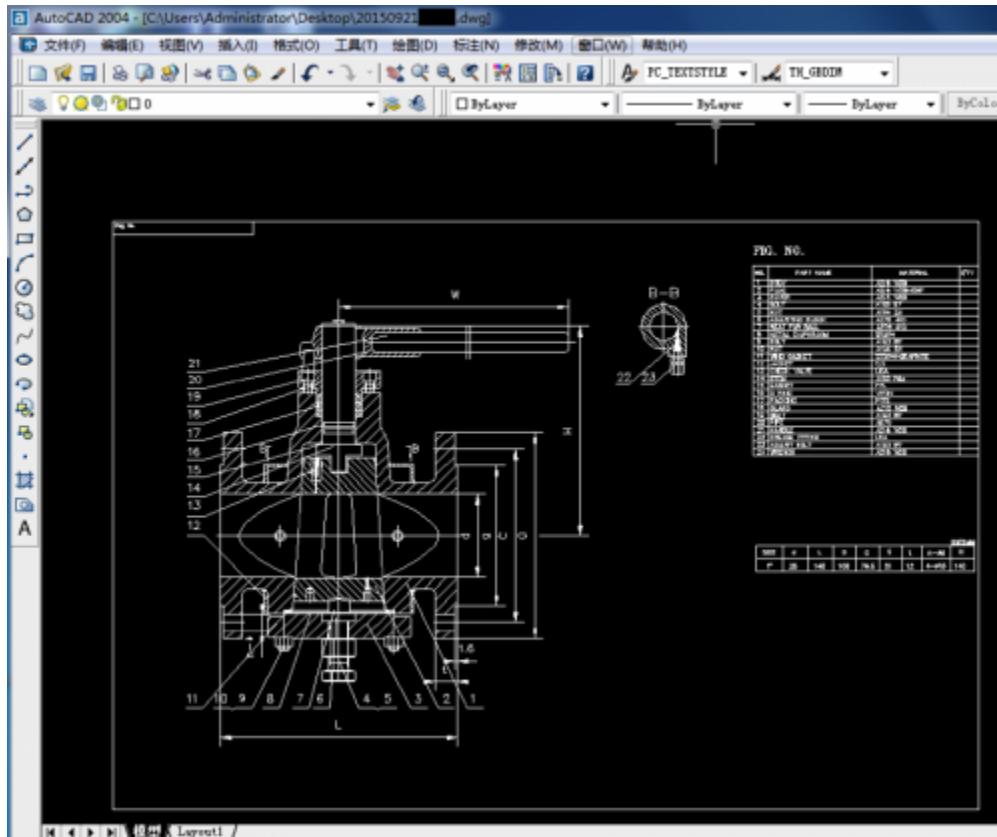
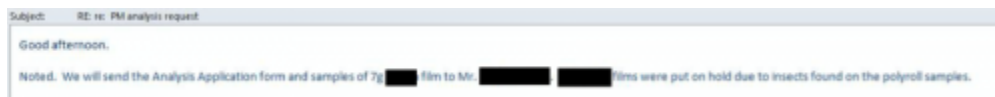


Figure 14 - Sales drawing for another product

There was also at least one seasoning mix that was...well, a little too seasoned as you'll see below...



Transportation and Logistics

The second major industry that showed a large set of KeyBase infections is Transportation and Logistics. Clustered more dominantly in the Middle East and East Asia, this mainly included companies specializing in the shipment of freight for import and export.



Figure 15 – Transportation and Logistics

It is unknown exactly how a miscreant might use the information from these machines, or whether they have any intent to exploit it, but it does provide interesting data for analysis.

To illustrate, there were three separate infected systems that showed users logged into Pakistan’s customs clearing system with the role of “Customs Agent” or “Trader”. Information that the miscreants would see includes container status, goods held within, the recipient, the sender, their location in port and vessel, the value of the goods, etc.

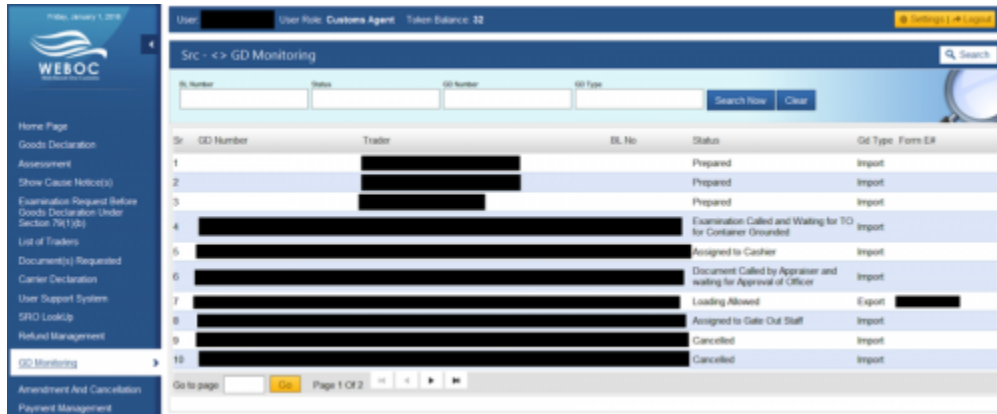


Figure 16 - Pakistan Web Based One Customs – “Customs Agent”

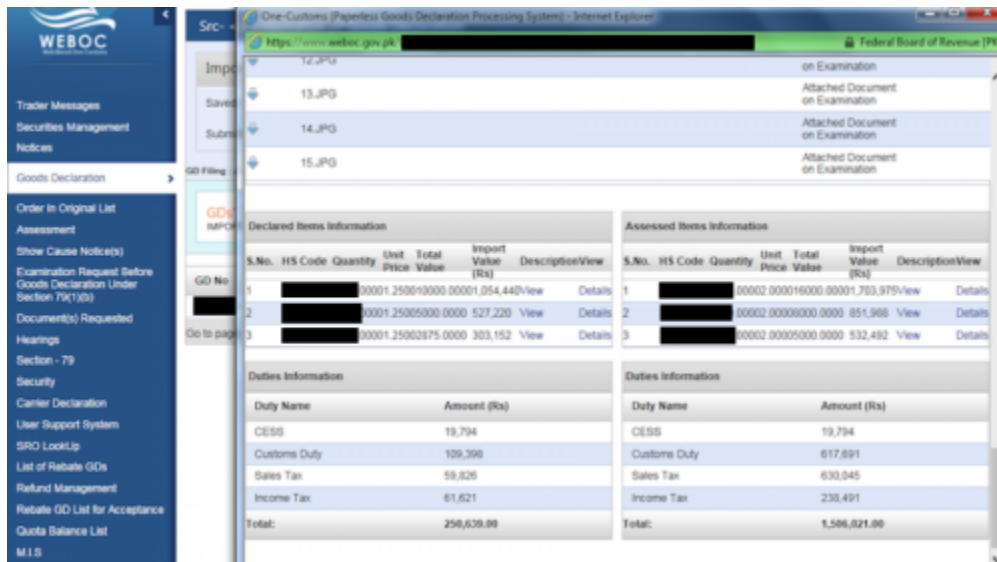


Figure 17 - Pakistan Web Based One Customs – “Trader”

Other infected systems showed the cargo booking for both air and sea travel, along with multiple e-mails with their clients organizing this activity.

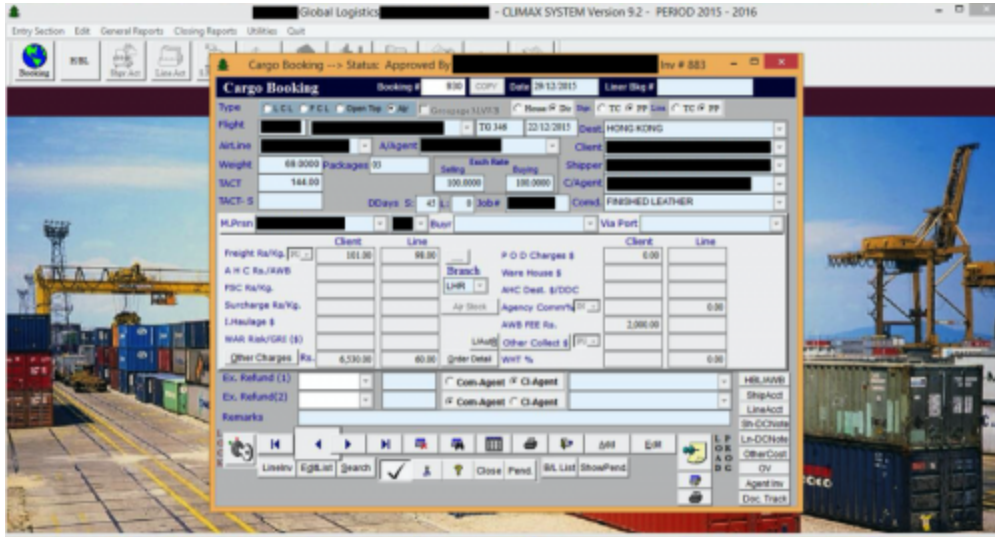


Figure 18 - Air cargo booking

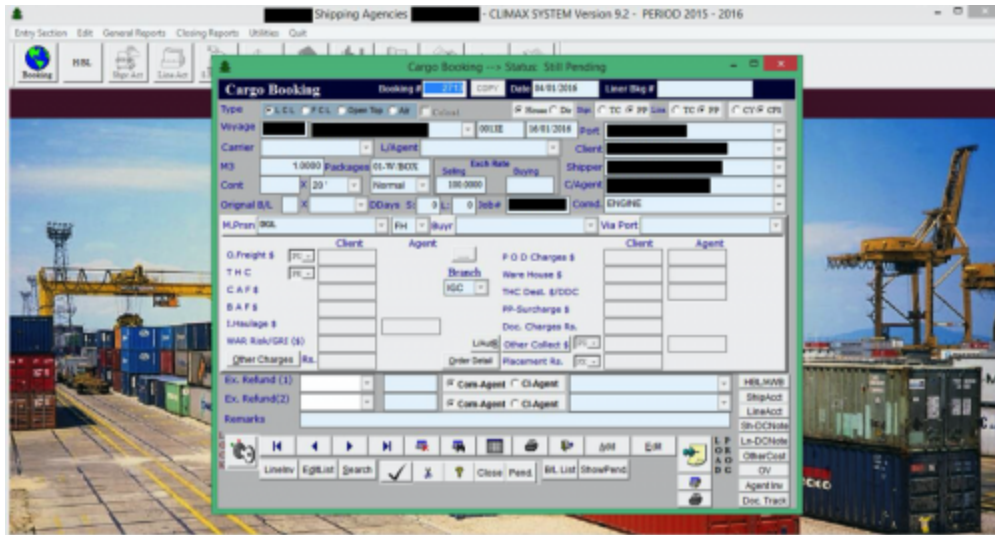


Figure 19 - Ship cargo booking

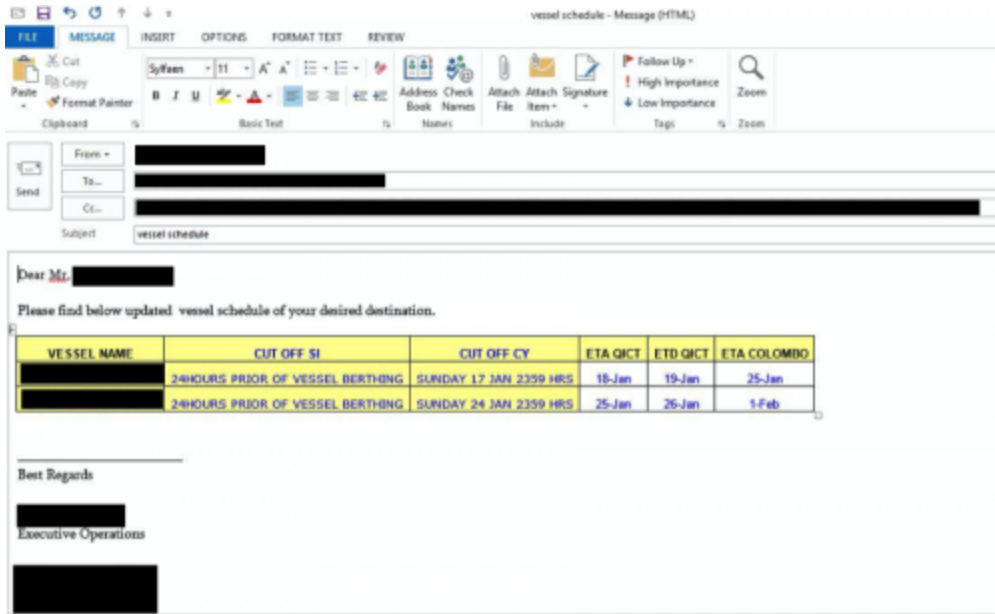


Figure 20 - Discussing vessel schedules

Another infected system in Egypt shows multiple e-mails and invoices for the shipment of beef sold by various companies for transport from Brazil to Egypt.

DESCRIPTION OF GOODS	QUANTITY KG	UNIT. PRICE	VALUE
PO MT-159/12-6/15		USD	USD TOTAL
FROZEN BONELESS BEEF FOREQUARTER CUTS	27.852,425	3,100	85.722,52
FROZEN BONELESS BEEF FOREQUARTER CUTS	27.578,395	3,100	85.493,02
TOTAL VALUE FOB OF GOODS			171.215,54

Figure 21 – Invoice details on 61K lbs of beef costing USD \$171,000

Finally, another infection of a logistics company, located in the United Arab Emirates, shows access to their bank accounts and the dollar amounts of transfers that the attackers will likely now have access to.

Accounts > Operative Accounts > Mini Statement Help

Select an Account Nickname and Option from the drop down lists.

GENERAL TRADING LLC-
Account Summary
GO

Last 20 Transactions - [Details till 21/12/10 5:48 PM] Account Currency - AED

Date	Description	Cheque No.	Withdrawal	Deposit	Balance
18/10/15	[REDACTED] : BILL ID		4,70,000.00		-19,32,500.00
29/09/15	Offset for [0146238]			5,36,040.00	-14,62,500.00
06/08/15	Offset for [0146238]			15,000.00	-19,98,540.00
06/08/15	[REDACTED] : BILL ID		14,62,500.00		-20,13,540.00
05/08/15	Offset for [0146043]			14,33,250.00	-5,51,040.00
25/05/15	[REDACTED] : BILL ID		5,51,040.00		-19,84,290.00
19/05/15	Offset for [0143993]			1,76,000.00	-14,33,250.00
18/05/15	Offset for [0143993]			3,90,000.00	-16,09,250.00
16/03/15	Offset for [0143993]			24,400.00	-19,99,250.00
16/03/15	Disb. for [0146043]		14,33,250.00		-20,23,650.00
15/03/15	Offset for [0142760]			13,23,000.00	-5,90,400.00
14/01/15	[REDACTED] : BILL ID		5,90,400.00		-19,13,400.00
12/01/15	Offset for [0141688]			5,49,000.00	-13,23,000.00

Figure 22 – Bank withdrawals and deposits, with a balance of over USD \$500,000

There were three KeyBase web panels, each had between 5-9 identifiable companies in this industry. Given the nature of the Transportation and Logistics business and making relatively large financial transfers frequently to cover the costs of moving products around the world may have been a motivator to target this industry.

Payday Advance

This brings us to our next tracked data point, bank usage. Out of the infected systems, 33 were seen using online banking websites and 28 of those were from systems we tagged as having “corporate data”. While we do not believe all 28 of these systems did online banking for the company, there were a number of cases where the online banking system showed the companies’ name and multiple banks would be used by the same infected systems.

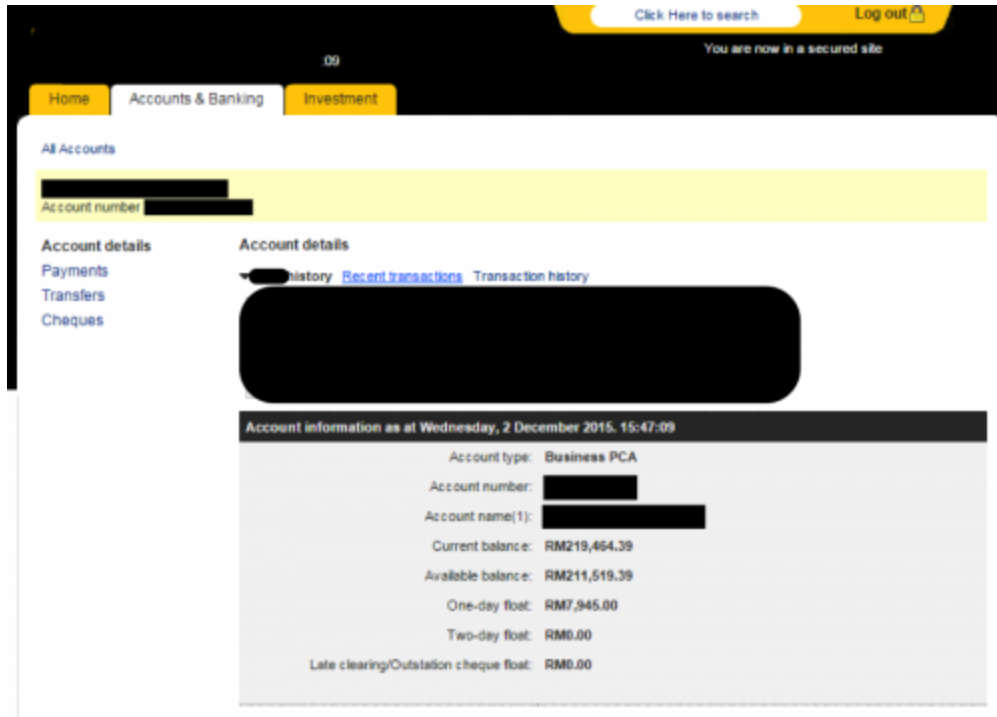


Figure 23 - Corporate banking account

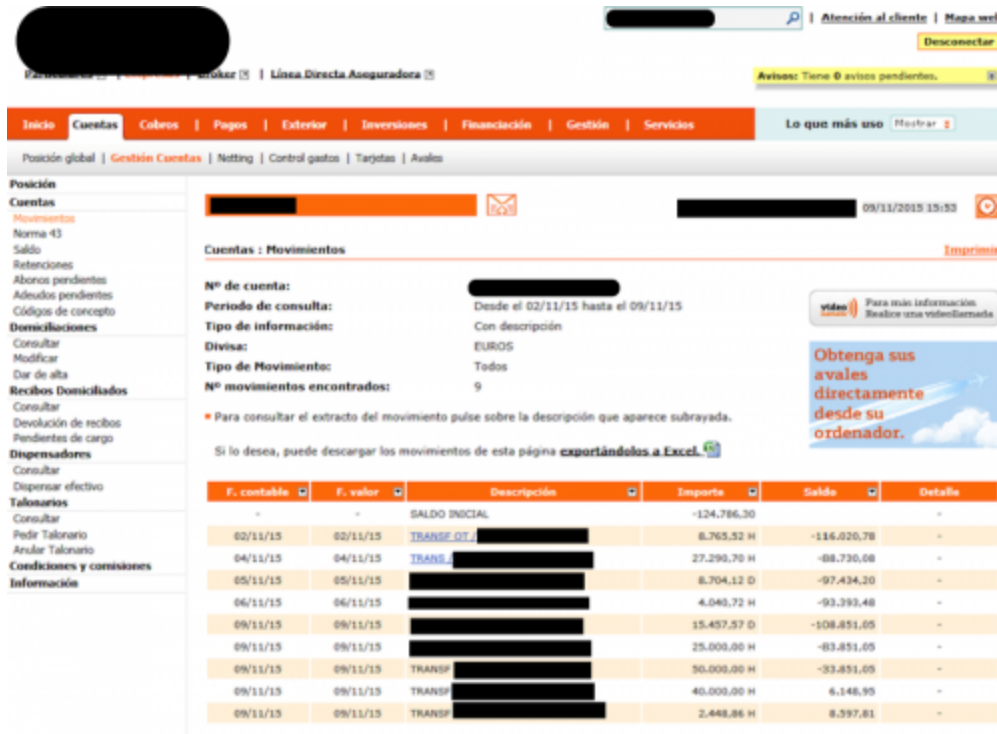


Figure 24 - Corporate banking account



Figure 25 - Fund transfer receipt for USD \$51,500

These would appear to be of interest to an attacker, as KeyBase malware will log the credentials needed to access these banking sites while the pictures will expose balances and other account details.

Transaction Made [Details till 01-01-2016 3:57:43 PM] To get a cyber receipt of the transaction, please click on Transaction Amount

Sr.No.	Transaction ID	Value Date	Tax Posted Date	Cheque No.	Description	Cr/Dr	Transaction Amount(198)	Available Balance(198)
1		01-01-2016	01-01-2016 3:47:27 PM		TRFR FROM [REDACTED] TRADERS	CR	3,22,345.00	8,45,489.46
2		01-01-2016	01-01-2016 3:10:13 PM	11004287	[REDACTED]	DR	2,74,210.00	5,71,279.46
3		01-01-2016	01-01-2016 2:57:04 PM	189521	[REDACTED]	DR	1,67,280.00	7,07,154.46
4		01-01-2016	01-01-2016 2:56:58 PM	189522	[REDACTED]	DR	1,92,183.00	5,64,434.46
5		01-01-2016	01-01-2016 2:55:00 PM	189526	[REDACTED]	DR	3,35,641.00	11,56,597.46
6		01-01-2016	01-01-2016 2:53:01 PM	189525	[REDACTED]	DR	6,84,526.00	16,92,236.46
7		01-01-2016	01-01-2016 2:41:36 PM	11005377	COTTON CO [REDACTED]	DR	2,64,610.00	21,76,742.46
8		01-01-2016	01-01-2016 2:39:23 PM	11004289	STORAGE PV [REDACTED]	DR	2,78,000.00	24,31,352.46

Figure 26 - Corporate banking account

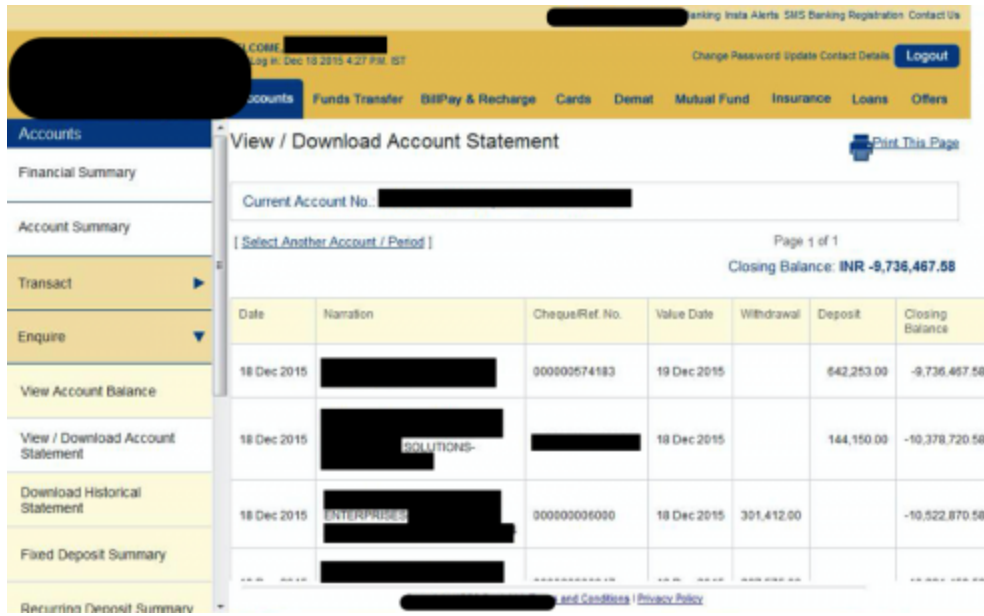


Figure 27 - Corporate banking account

The image below shows an e-mail correspondence in which the user of the infected system is e-mailing their bank about a payment of USD \$1,000,000 that appears to have been transferred to another account while they were in the hospital. This may be unrelated to having been infected with KeyBase, but it's enough contextual information, and enough of a dollar amount, that it raised red flags for me.



Doubling Down on Risk

Another group of tracked data points we were interested in was whether it could be determined that a machine was used for personal, non-business, related activities and whether it was a shared resource.

The reason this was of interest is that we saw multiple KeyBase delivery campaigns sent via e-mail phishing lures, some received on what appeared to be personal accounts while others on corporate e-mails. The crossover usage of corporate assets for non-corporate activities is a well-known threat vector, expanding the potential surface area for someone to become infected with malware. Out of the 933 infected systems, there were enough screenshots to determine that at least 216 of them appeared to only be used for corporate work, 75 were used only for personal activities, and 134 of them were used for both corporate and personal activities.

Shared assets, in which we would see multiple different identities logged into social media, e-mails, or applications, accounted for 43 of the 933 infected systems. These shared systems were in much greater quantity in the Middle East and South Asia.



Figure 28 - Shared infected systems

Shared systems, of course, increase the risk to the individuals using them, by exposing multiple sets of credentials through one person unknowingly getting the system compromised. In India specifically, we saw this activity frequently in the services industry, such as travel and tourism companies, or other roles where you move around an office frequently without dedicated assigned systems.

In an effort to avoid showing multiple Facebook accounts and still keep it somewhat interesting, the below set of images were captured from an infected office PC that sent hundreds of screenshots displaying images of their security camera. The middle desk and computer were frequently used by multiple people, which is likely typical for these smaller offices.



Figure 29 - Individual 1



Figure 30 - Individual 2



Figure 31 - Individual 3



Figure 32 - Individual 4

Tactics

Switching gears to look at the panels and lures themselves, only four names were shared among panel names while the rest were unique values.

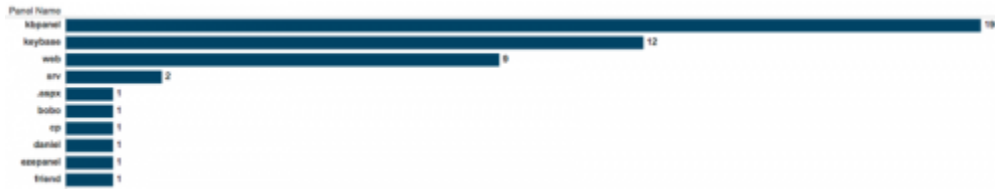


Figure 33 - Top 10 panel names

While most KeyBase web panels had a one-to-one relation with the site, there were a few sites that stood out as hosting multiple web panels – possibly each tied to a different campaign.

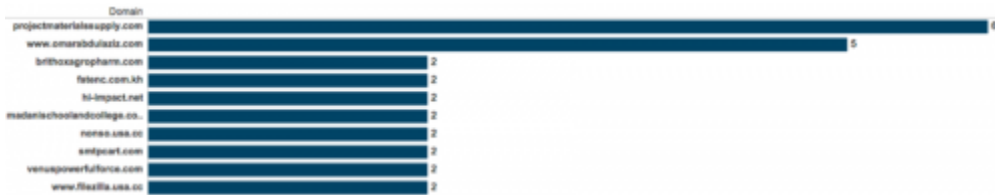


Figure 34 - Top 10 domains by number of panels

It's also worth noting that these are only panels that were detected or shared; there are most likely additional panels located on these sites that we have yet to identify.

For e-mail campaigns, there were multiple clusters of e-mail subjects that were part of the phishing lure that stood out.

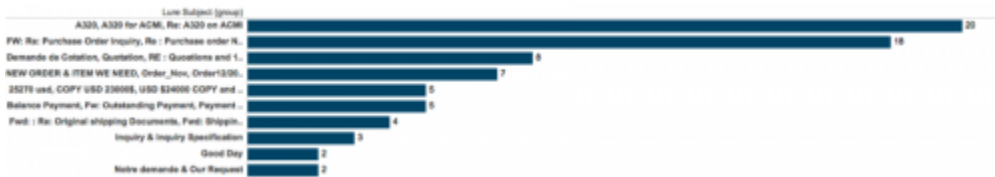


Figure 35 - Top 10 e-mail lure subjects

Typically, this information could be collected in the first or second screenshot of a set with the lure e-mail in the background, and the malicious executable in the foreground.

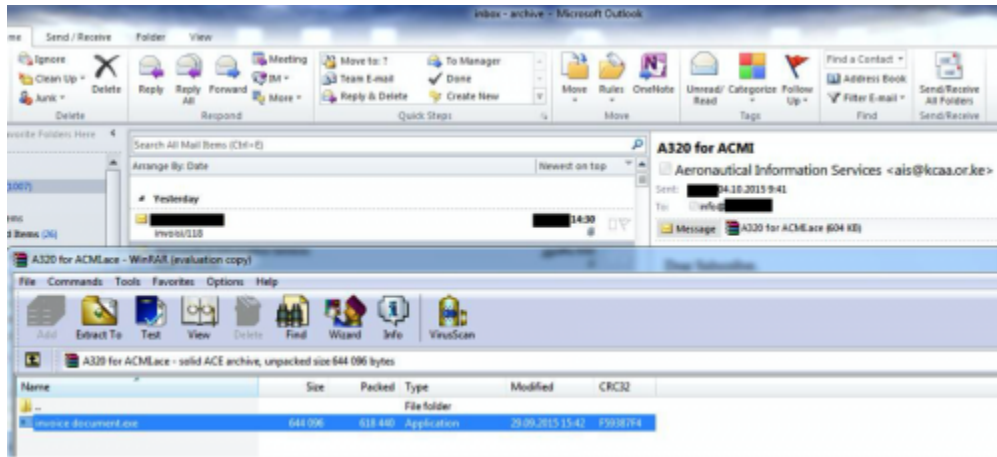


Figure 36 - KeyBase immediately begins sending back screenshots

The top e-mail lure, with subject “A320 for ACMI” was particularly interesting, as the A320 is a single-aisle Airbus jetliner and ACMI stands for “aircraft, complete crew, maintenance, and insurance”, which makes it potentially appealing to targets who work within the aerospace industry. Sure enough, we found multiple targets that match up in this campaign.

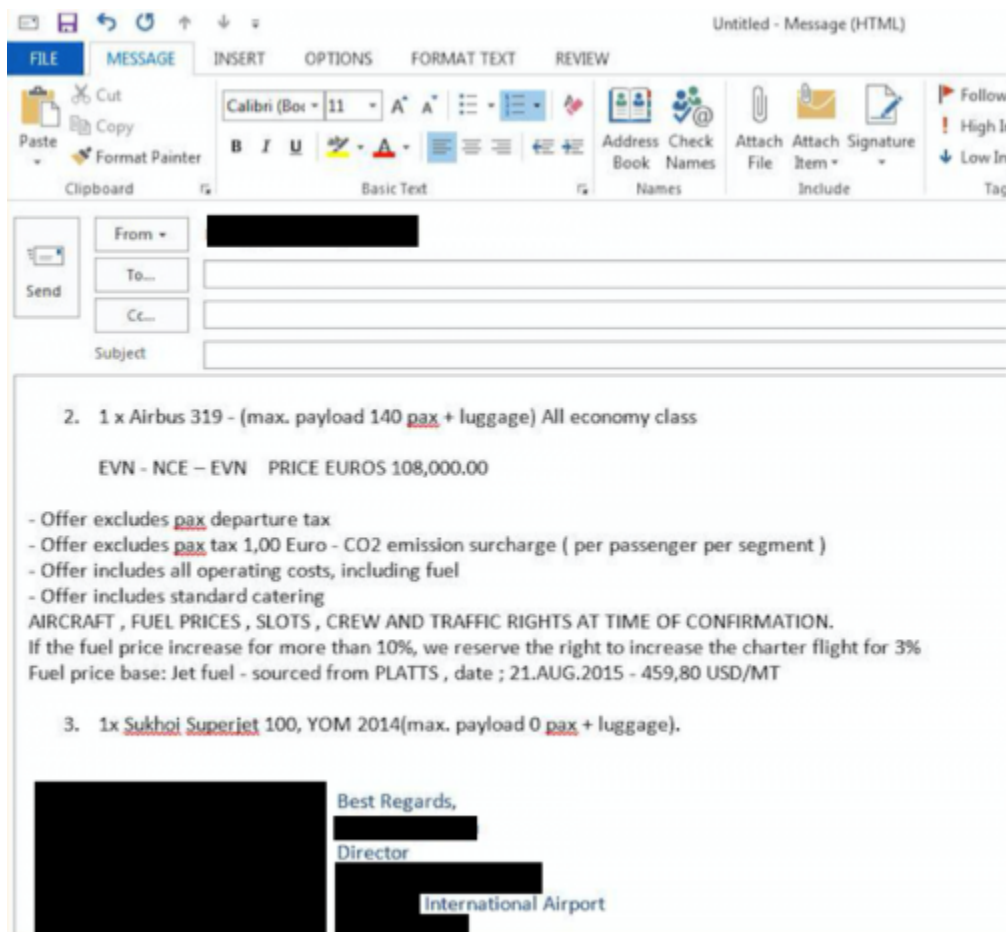


Figure 37 - Target in the aerospace industry

Thanks

Mrs. [REDACTED]

[REDACTED] Officer (in charge of ICAO documentation)
Air Transport Economic Regulations and Foreign Relations Department

Civil Aviation Authority [REDACTED]

Tel: [REDACTED]

Fax: [REDACTED]

Mobile: [REDACTED]

Email: [REDACTED]

Figure 38 - Another target in the aerospace industry

The rest of the e-mail subjects were largely about purchase orders, inquiries, and other financial themes. This may explain the high success rates on individuals who fall in sales or informational roles for companies.

While there were 49 unique e-mail subjects identified as being part of KeyBase phishing lures, there were 65 unique names for archives attached to the e-mails that delivered malware in the form of EXE files, Word documents, and Excel documents.

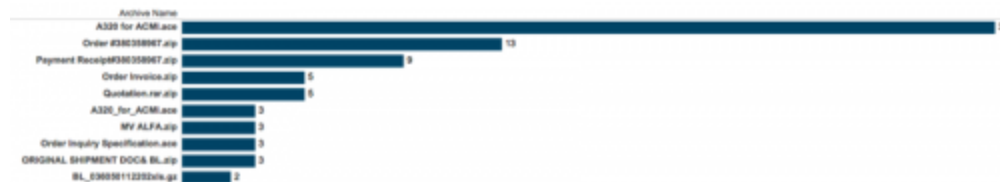


Figure 39 - Top 10 archive names

The archives would typically mirror the e-mail subject but, when they didn't, it was normally named after the executable file within the archive – which itself was usually a poor attempt to masquerade the underlying executable.

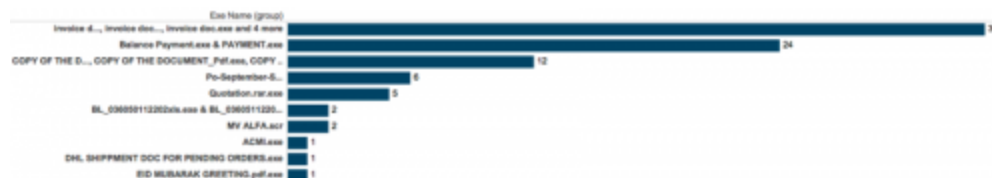


Figure 40 - Top 10 executable names

Another tactic, whether purposeful or not, was sending English based e-mails to individuals in countries where English is not the native language. On at least two occasions we saw the recipients translating the e-mail phishing content with Google Translate services.

The final thing we'll talk about in this section is a company in the Healthcare industry that showed an infection on September 7 and then an infection 3 days later on September 10 and again on September 13. What made this one stand out from the others is that the final

infection on September 13 showed that the e-mail, which matched the previously seen content of the other phishing lures, was sourced from an internal e-mail address of the company.

The Others

To wrap up the target analysis of infected systems, we're going to point out three more sets of data that stood out as interesting from a target perspective.

Hotel and Hospitality

One particular panel/actor targeted the Hospitality industry and infected seven different hotels or resorts, specifically the reception desks for these companies.

One particular panel/actor targeted the Hospitality industry and infected seven different hotels or resorts, specifically the reception desks for these companies. Similar to the tactics previously discussed, we see delivery of KeyBase through the "info@" addresses that are easy to identify off of the company's public website.

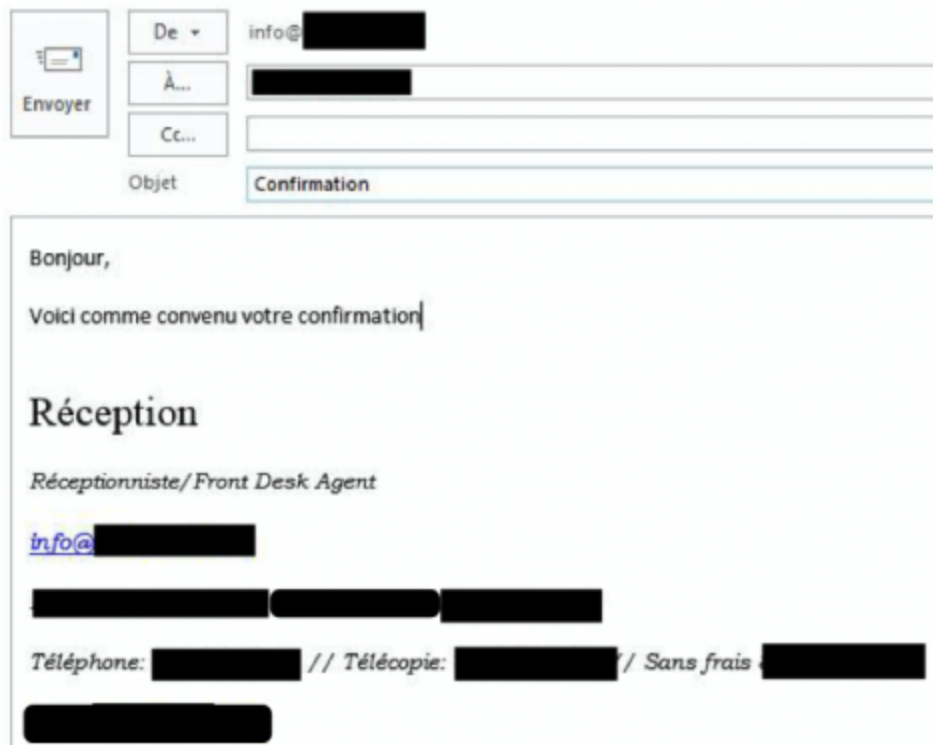


Figure 41 - Infected receptionist

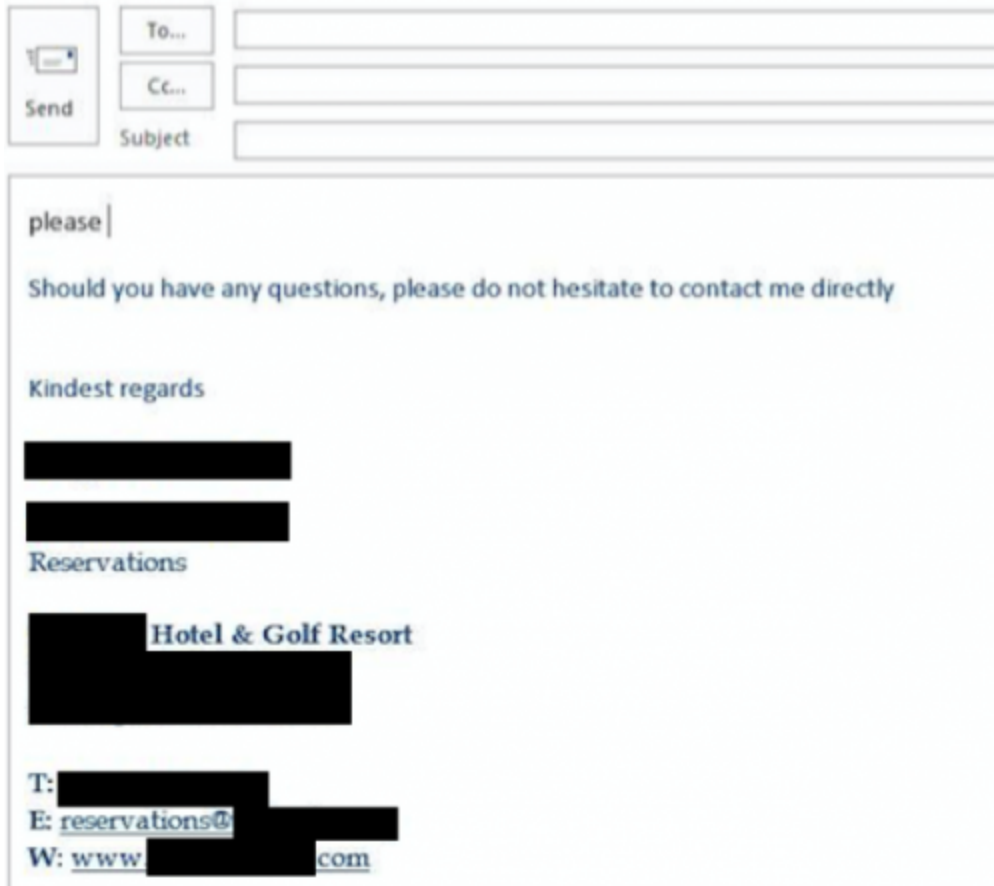


Figure 42 - Another infected receptionist

Targeting hotel receptionists provides a lot of interesting data, from guest information and their home address to travel and payment details; this is all potentially valuable data that may be sold. Below are a couple of screenshots from the various infections to illustrate the type of information exposed through one of these systems.

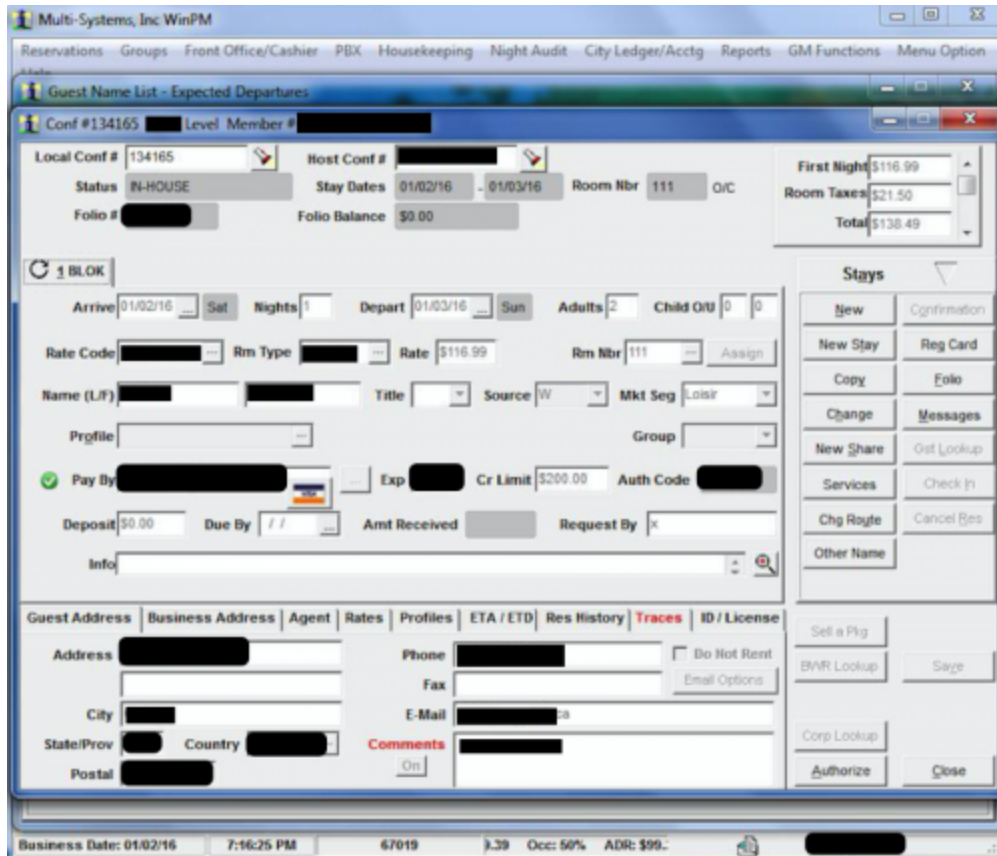


Figure 43 - Guest booking at a hotel

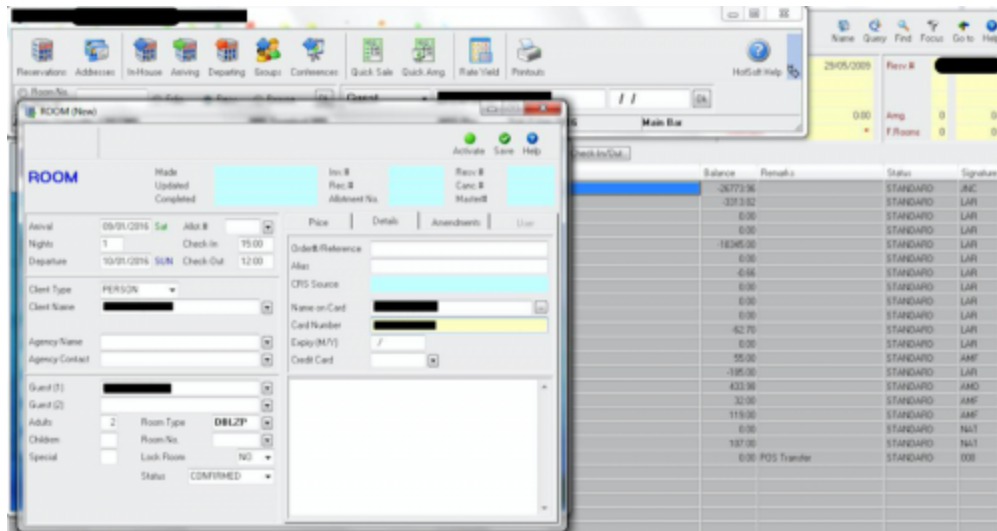


Figure 44 - Guest credit card information

Reservation Information: [REDACTED]

Stay info | **Guest Info** | Guarantee Info | CRS Notes

EDIT GUARANTEE INFORMATION

Guarantee: CC
 Market: Unknown
 Caller Name: [REDACTED]
 Guest Tracking: Unknown

Card Type: [REDACTED]
 Card Number: [REDACTED] **UNMASK**
 Expiration: [REDACTED]
 Name on Card: [REDACTED]
 Card Billing Address:
 Card Billing Postal Code:

Overview
 Status: Reserved
 Guest Name: [REDACTED]
 Group Master:
 Account Number: [REDACTED]
 Balance: 0.00

Actions
 Back
 Guest Folio
 Check In
 Recurring Charges
 Change Stay
 E-mail Confirm
 Duplicate
 View Changes
 Cancel Reservation
 Print Registration Card
 Print Confirmation Letter

Figure 45 - Another guest credit card

Find Guest | **Create Reservation** | Find Reservation | Walk-In | Find Gro

Good Morning, [REDACTED]

53.57% Today's Occupancy

41 Total Departures Today
 0 Check Outs Completed
 41 Check Outs Remaining

29 Total Arrivals Tonight
 1 Vacant/Dirty Rooms Remaining
 54 Total Rooms Available

check outs	stayovers	vacant
41	32	39
0		

Available	NDD 89.00	SNK 99.00	NHD 79.00
54	17	16	12
			6
			3

Figure 46 - Hotel information

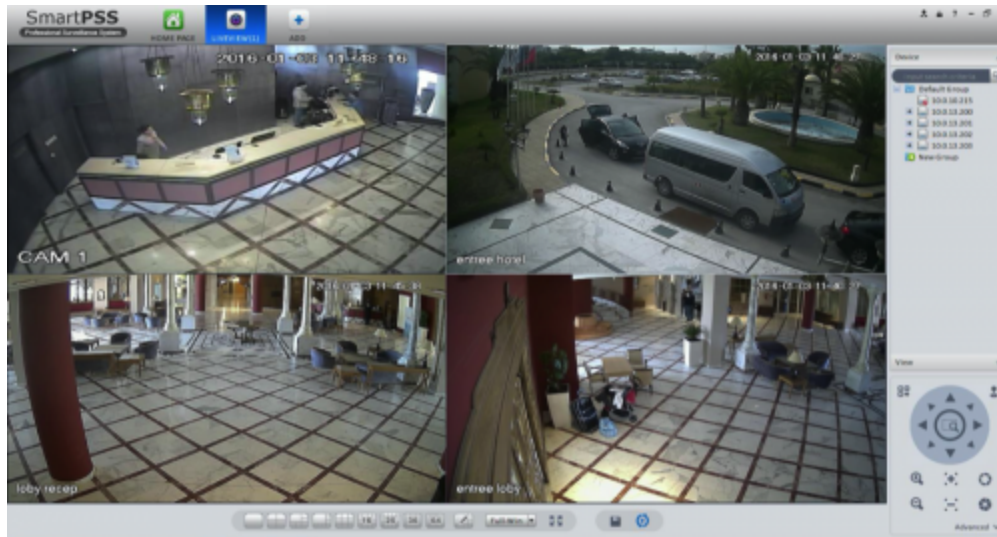


Figure 47- A receptionist PC accessing the hotel camera system

Education

The set for educational institutions wasn't notably attributable to any one panel, but equally distributed. What made it stand out though is that the same tactic for delivering the KeyBase phish was applied here and "Admissions" people were targeted. These individuals are constantly sent Word or PDF documents, allegedly from parents, so it's no surprise they would open the malicious files.

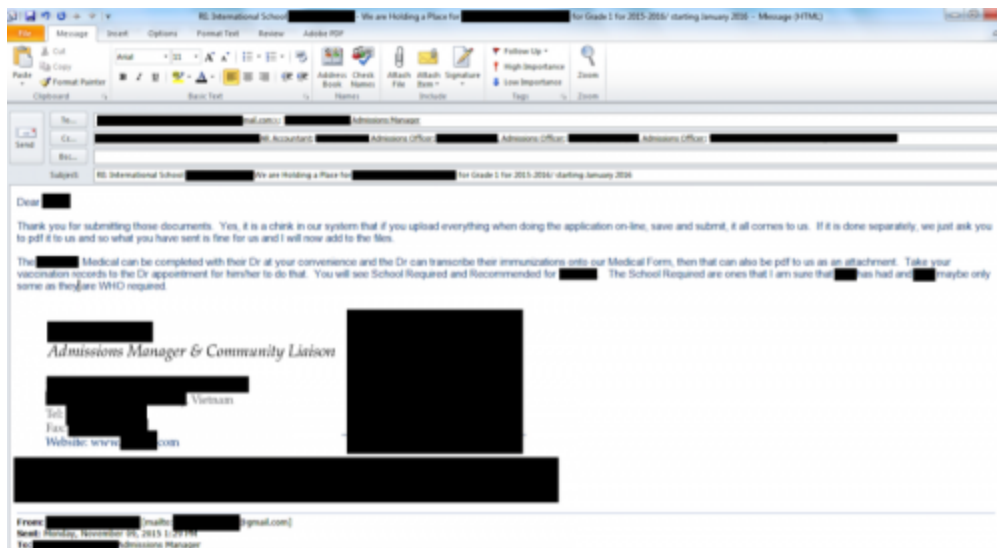


Figure 48 - Admissions Manager asking parent for medical information via PDF

Beyond e-mails, there was also a fair amount of student details.

Student First Last	Student Last First	Sex	App GD	Curr GD	PE House	Phone	Nationality	Exit Year	Exit Grade	Leaving Date	Status
[Redacted]	[Redacted]	F	5				Vietnam				Inquired
[Redacted]	[Redacted]	M	3	B 3		[Redacted]	Vietnam				Enrolled
[Redacted]	[Redacted]	M	5				Vietnam				Closed
[Redacted]	[Redacted]	F	6			[Redacted]	Vietnam				Inquired
[Redacted]	[Redacted]	F	6				Vietnam				Closed
[Redacted]	[Redacted]	M	3				Vietnam				Closed
[Redacted]	[Redacted]	F	1				Vietnam				Closed
[Redacted]	[Redacted]	M	1				Vietnam				Inquired
[Redacted]	[Redacted]	M	4				Vietnam				Inquired
[Redacted]	[Redacted]	F	7				Vietnam				Inquired
[Redacted]	[Redacted]	M	5			[Redacted]	Vietnam				Closed
[Redacted]	[Redacted]	F	5	C 5			Vietnam				Enrolled
[Redacted]	[Redacted]	F	6	D 6		[Redacted]	Vietnam				Enrolled
[Redacted]	[Redacted]	F	12				Vietnam				Inquired
[Redacted]	[Redacted]	M	KG				Vietnam				Closed
[Redacted]	[Redacted]	M	6				Vietnam				Applied
[Redacted]	[Redacted]	M	9			[Redacted]	Vietnam				Inquired
[Redacted]	[Redacted]	M	6			[Redacted]	Vietnam				Applied
[Redacted]	[Redacted]	M	EE-2				Vietnam				Closed
[Redacted]	[Redacted]	M	5				Vietnam				Inquired
[Redacted]	[Redacted]	M	6			[Redacted]	Vietnam				Applied
[Redacted]	[Redacted]	F	2				Vietnam				Inquired

Figure 49 - Student list

Date	Source	Title	Actions
16/11/2015	PWS	applicant_medical_report_upload	Edit View Save... ✖
16/11/2015	PWS	applicant_passport_birthcert_upload	Edit View Save... ✖
16/11/2015	PWS	Letter of recommendation	Edit View Save... ✖
16/11/2015	PWS	Document in Russian	Edit View Save... ✖
16/11/2015	PWS	Birth certificate	Edit View Save... ✖
16/11/2015	PWS	applicant_vaccination_booklet_upload	Edit View Save... ✖
16/11/2015	PWS	APPLICATION	Edit View Save... ✖
16/11/2015	PWS	Photo	Edit View Save... ✖
17/11/2015	PORTAL	Medical Test & vaccination Record	Edit View Save... ✖

Figure 50 - Student documents

Finally, the irony of this last one was a little bittersweet...

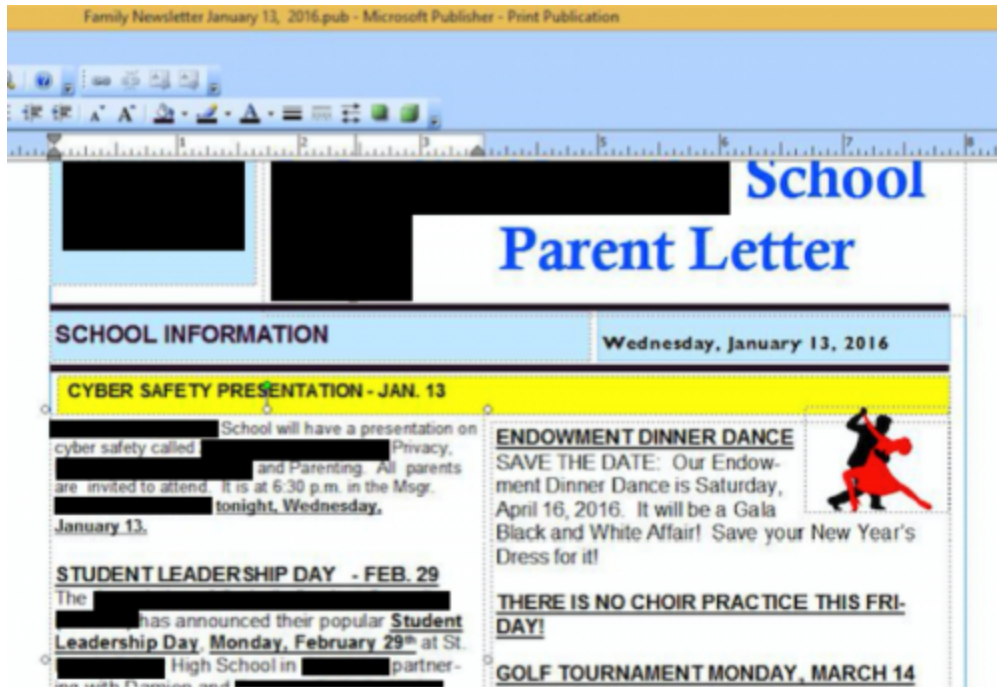


Figure 51 - Principal sending out newsletter about Cyber Safety presentation

Miscrant Selfies

To bookend the image analysis, we'll take a look at some of the screenshots from the 16 actors using KeyBase who infected themselves, whether to validate it works or by accident. These images provide a glimpse into what they do on a daily basis and how they may be intending to use the information collected from their KeyBase campaigns.

Actor 01

In the first image, we can see the miscrant taking credentials from the KeyBase password panel and logging into multiple web-based e-mails. Subsequent screenshots show the individual going through the e-mails.

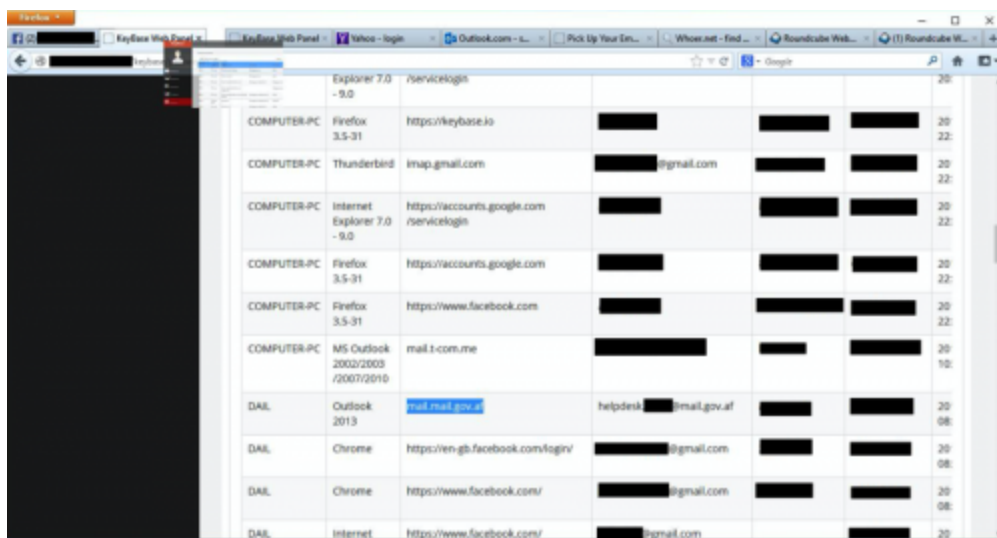


Figure 52 - Actor logging into multiple compromised web-based e-mails

Actor 02

We only have two screenshots, but we can see the next actor configuring a cracked KeyBase builder and some potential other tools on his or her desktop, such as the SpyGate RAT.

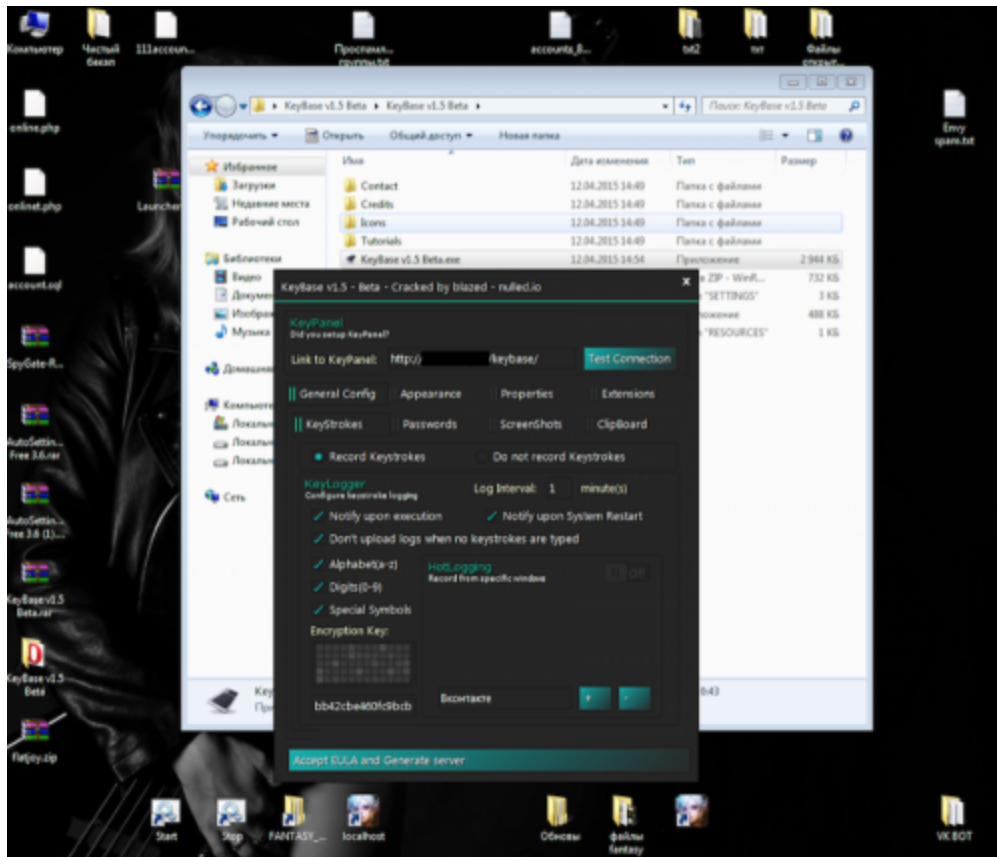


Figure 53 - SpyGate RAT

Actor 03

The third actor also shows the cracked KeyBase builder, but they are testing their KeyBase generated malware against razorscanner multi-engine AV scanner, which returned 2 out of 24 detections.

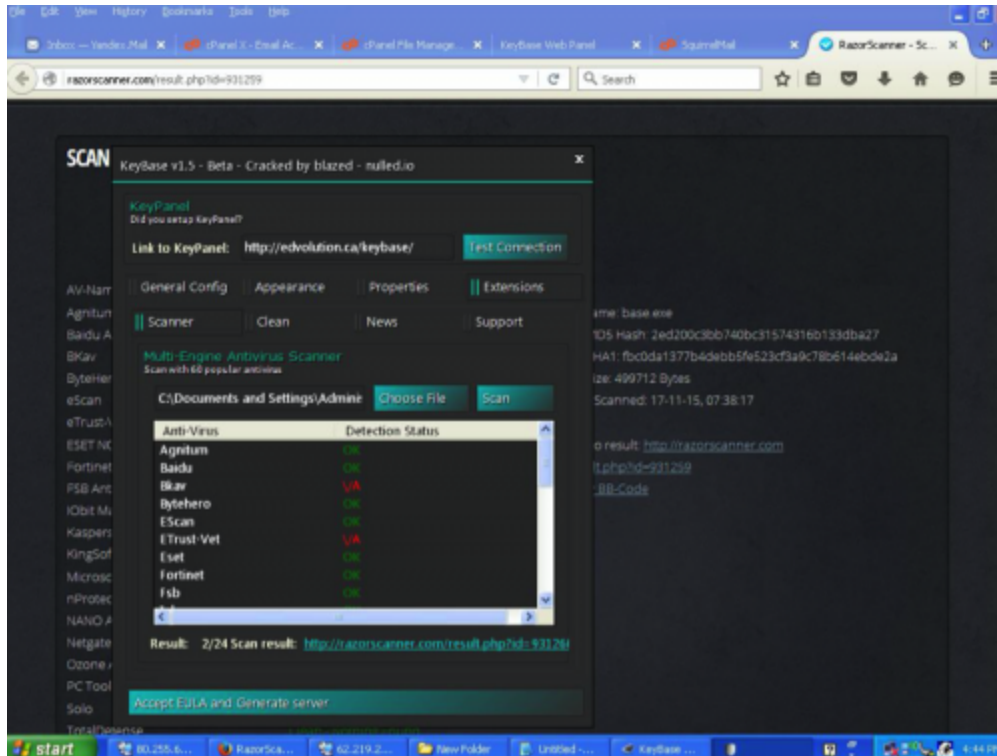


Figure 54 - Checking detection count for generated KeyBase malware

The next couple of screenshots show the actor preparing the malware, most likely an attachment to a phishing e-mail.

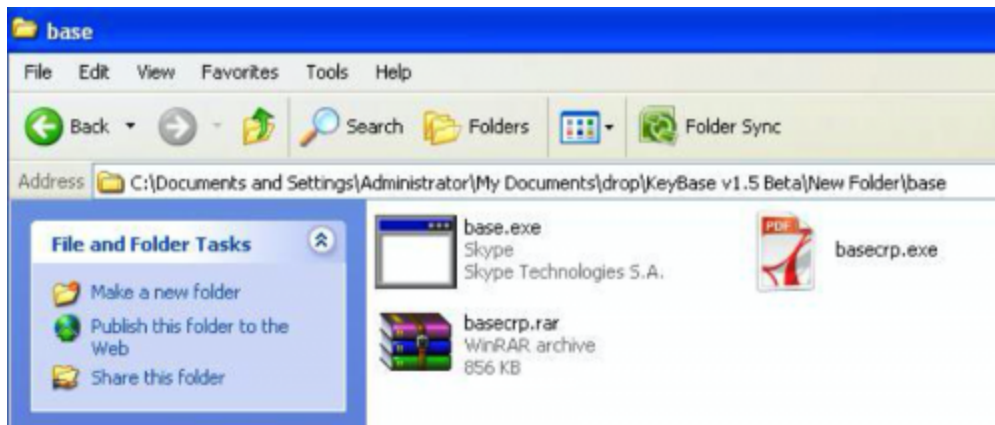


Figure 55 - Original generated KeyBase malware

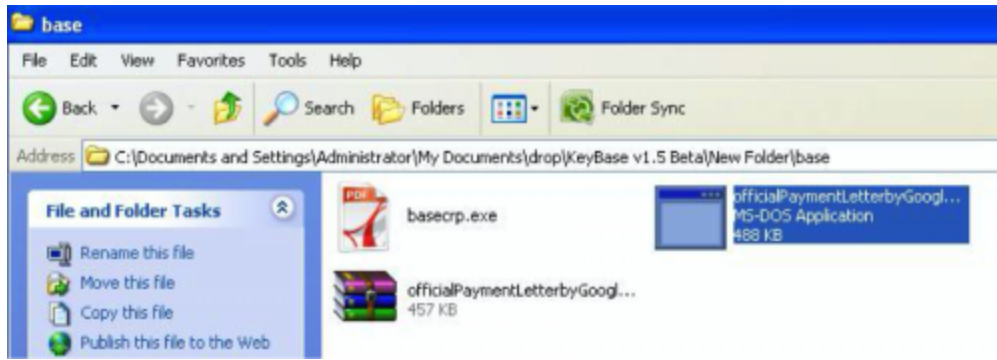


Figure 56 - Changing the name for attack

Afterwards we see the actor using a combination of Gr3eNoX Exploit Scanner to find vulnerable websites off of the Google Dork “germany supplier php?id=bee...” in the background, with Havij SQL Injection Tool in the foreground testing a site. The Google Dork being used hints that the industry and geographical targeting may be accurate.

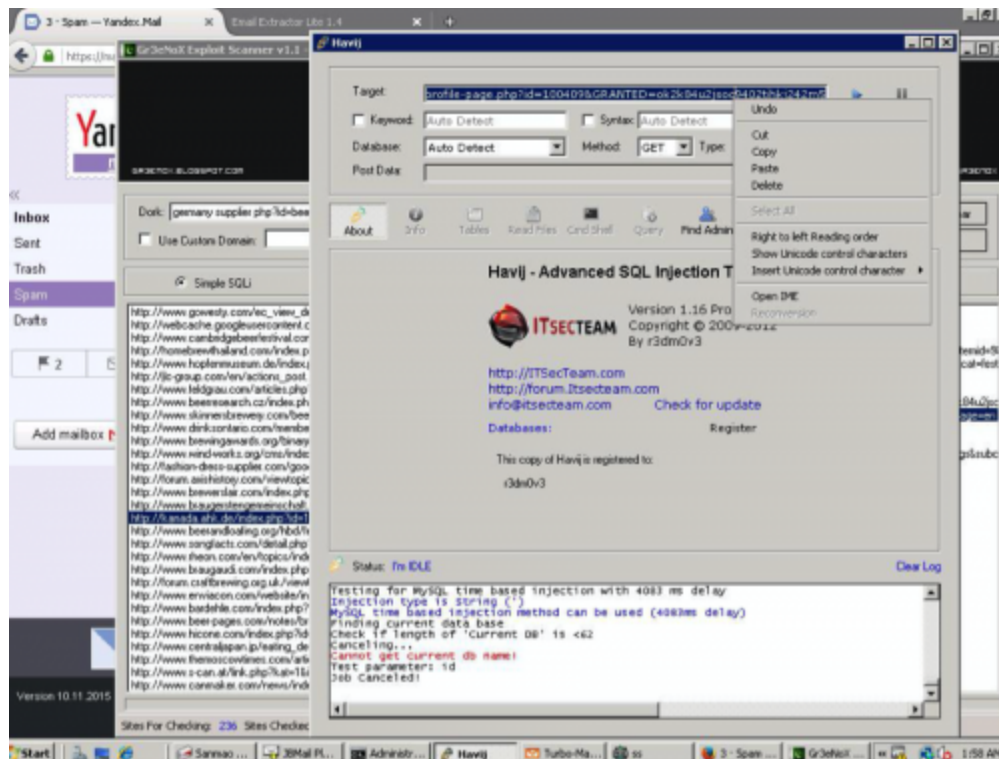


Figure 57 - Attacking a website

Actor 04

The next actor we see going through the entire phishing campaign. Initially the actor moves the KeyBase malware into one of the archives we saw in previous phishing campaigns.

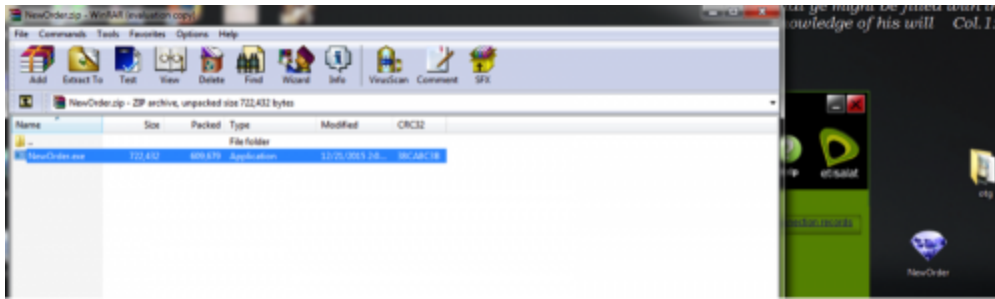


Figure 58 - Moving the KeyBase malware into an archive for e-mail

Afterwards, the actor has a conversation over Skype discussing the crafting of the phishing e-mail, including signature to use, e-mail subject, content, and attachment details.

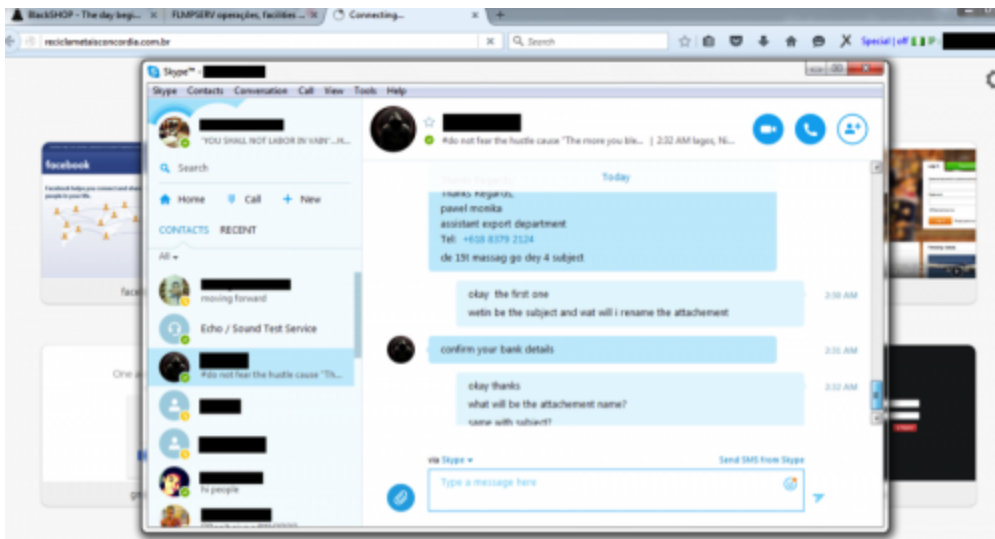


Figure 59 - Skype discussion of the phishing lure

Then they login to a compromised company e-mail account and appear to be adding e-mails from their contact list to a collection of other e-mails.

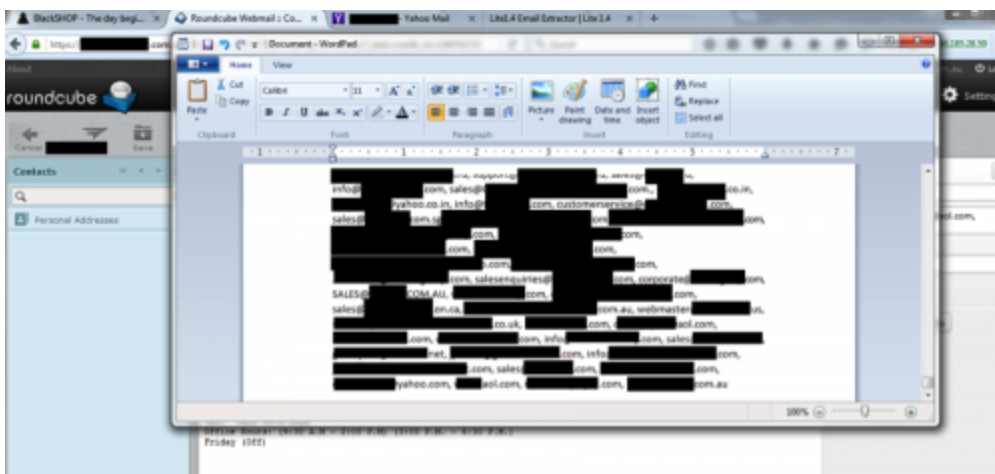


Figure 60 - Adding “info” and “sales” addresses to a Word document

Next they send out the phishing e-mail from the compromised account.



Figure 61 - Sending the phishing e-mail with an archive containing KeyBase malware

Afterwards, we see the pattern repeat but the actor looks up popular Korean women names and then uses another compromised e-mail account to send out another round of phishing e-mails.

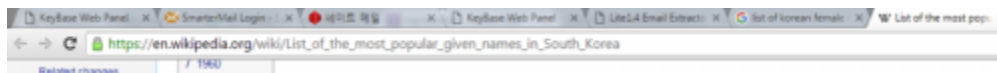


Figure 62 - Actor performing research for phishing lure

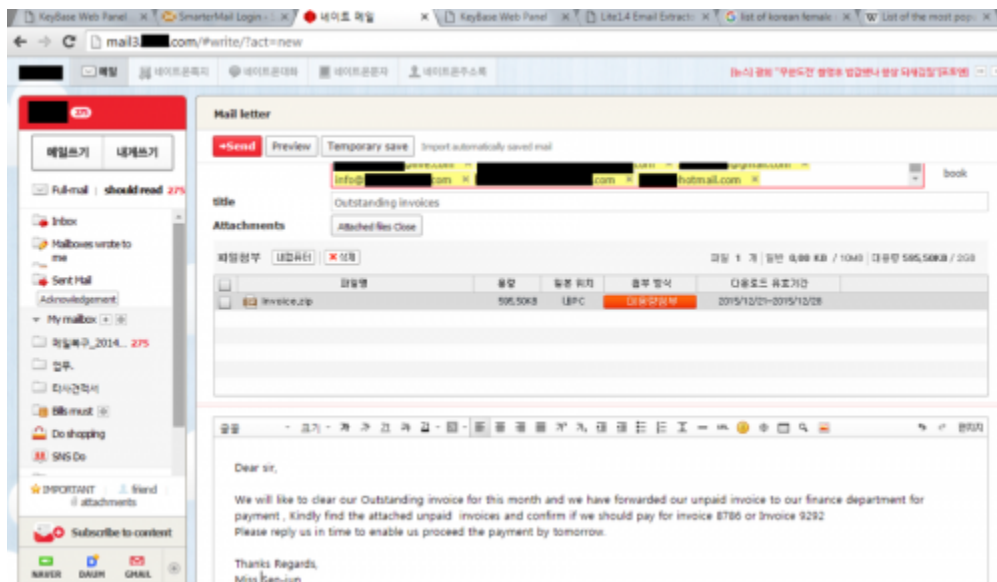


Figure 63 - Sending out another round of phishing

Actor 05

This next actor appears to be purchasing accounts for something, possibly Skype or PayPal, and willing to spend \$50 per account.

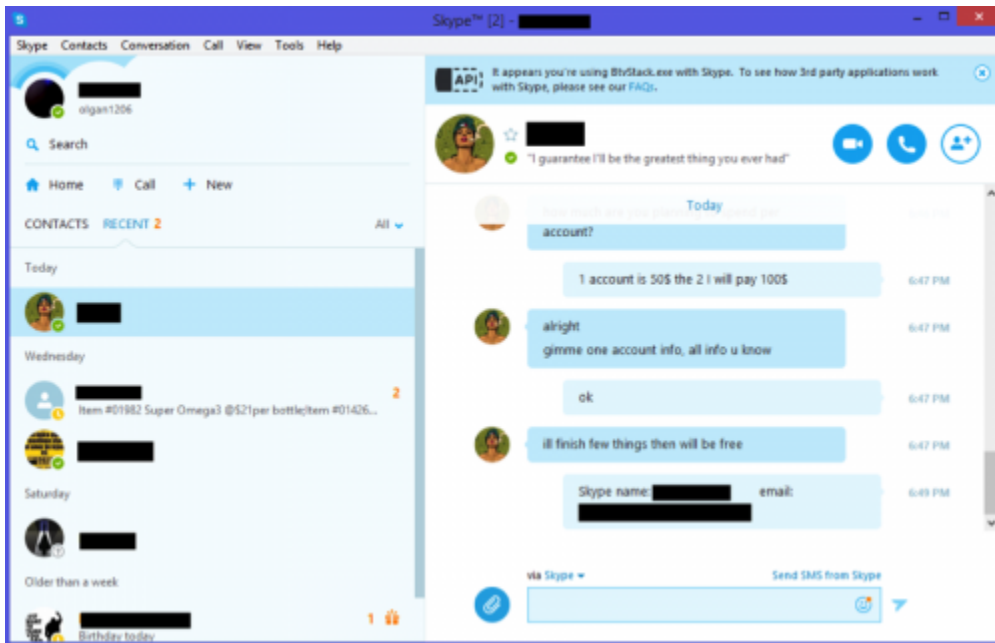


Figure 64 - Discussing purchase of accounts

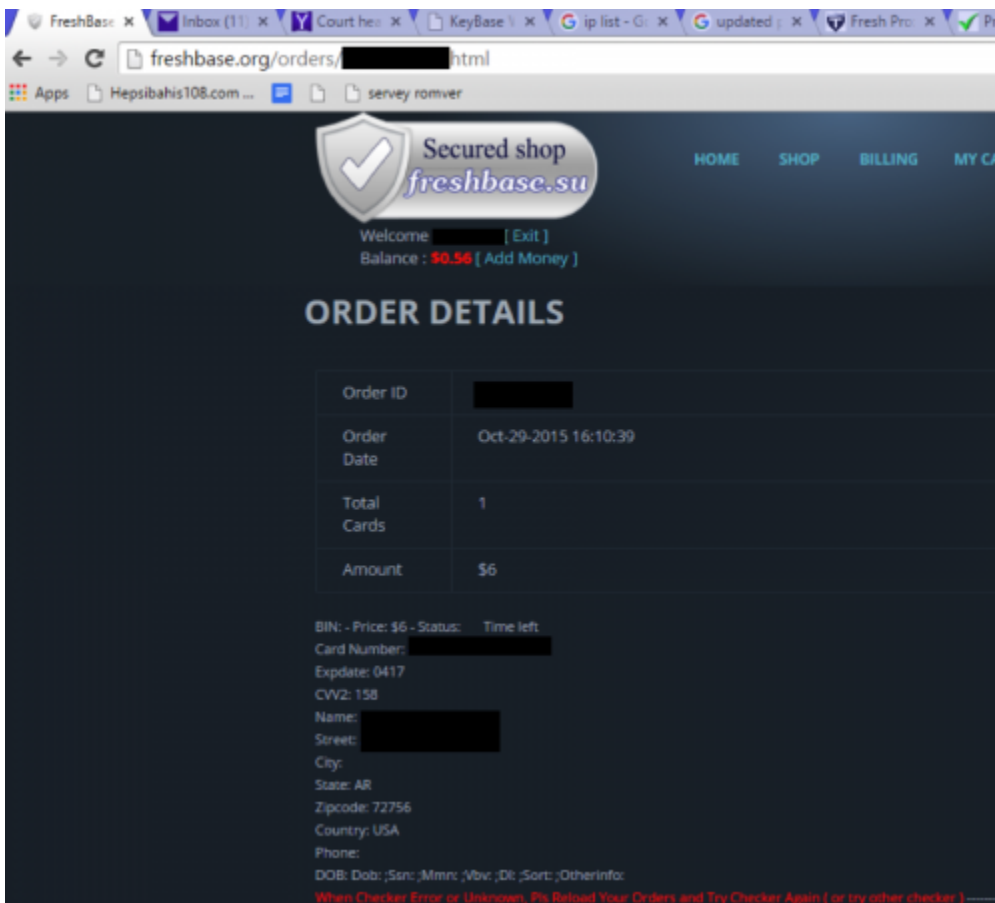


Figure 65 - Buying a credit card online, possibly to use to buy the accounts mentioned next
He's also trying to aggressively brute-force Skype accounts throughout the screenshot set, yet never appears successful.

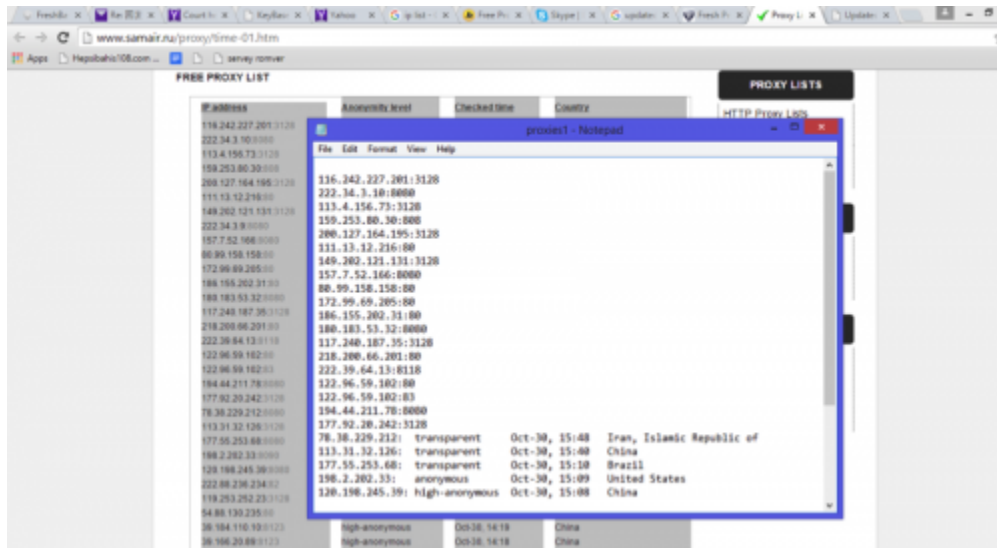


Figure 66 - Manually scraping proxy data

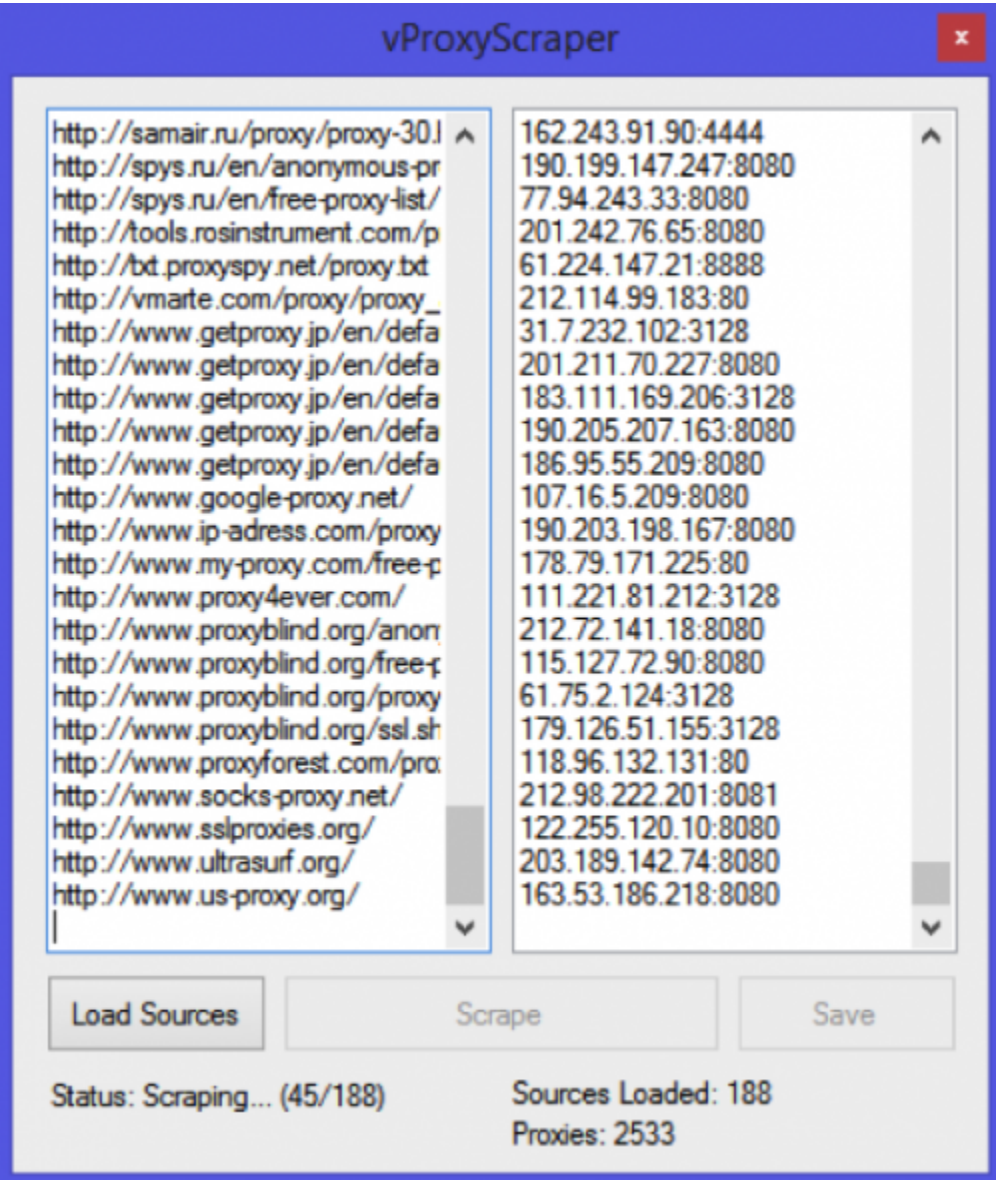


Figure 67 - Automated proxy scraping

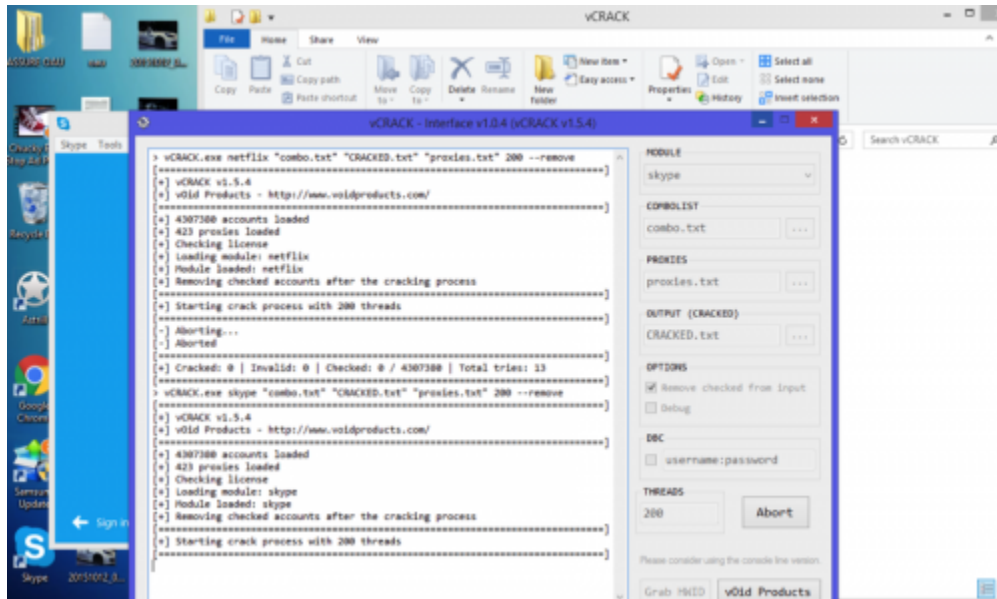


Figure 68 - Attempting to brute force Skype accounts with vCrack through proxies

Actor 06

The next actor actually infected three of his or her PCs, for whatever reason, so there were plenty of screenshots to go around – including doing Skype with his or her family, school projects, and the account details for the Albanian university he or she attend. Based on the activity, the actor enjoys making what I could only describe as YouTube Albanian Hip-Hop lyric videos and reads “hacking tutorials” after unsuccessfully trying to pull off XSS on Flickr...they also appear to be a part of the carding scene.

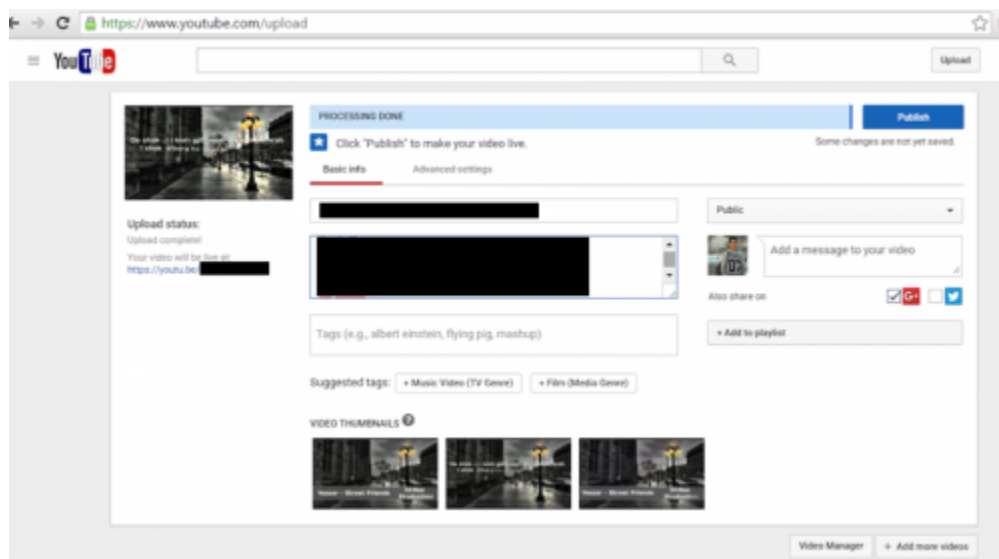


Figure 69 - Miscreants have hobbies too

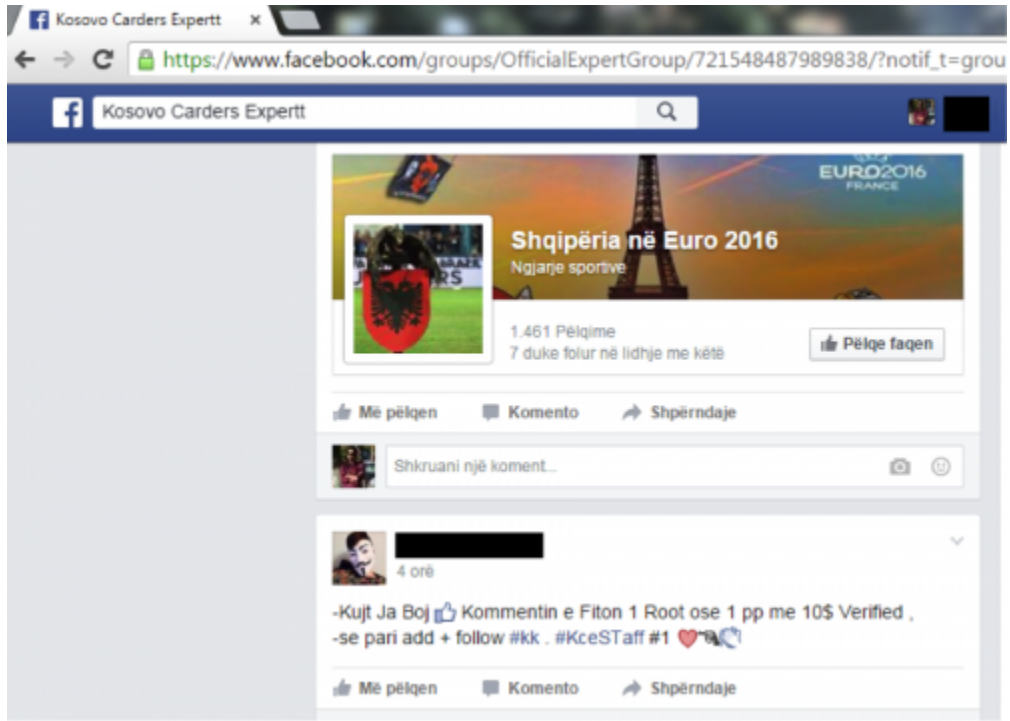


Figure 70 - Facebook group for “Kosovo Carders”

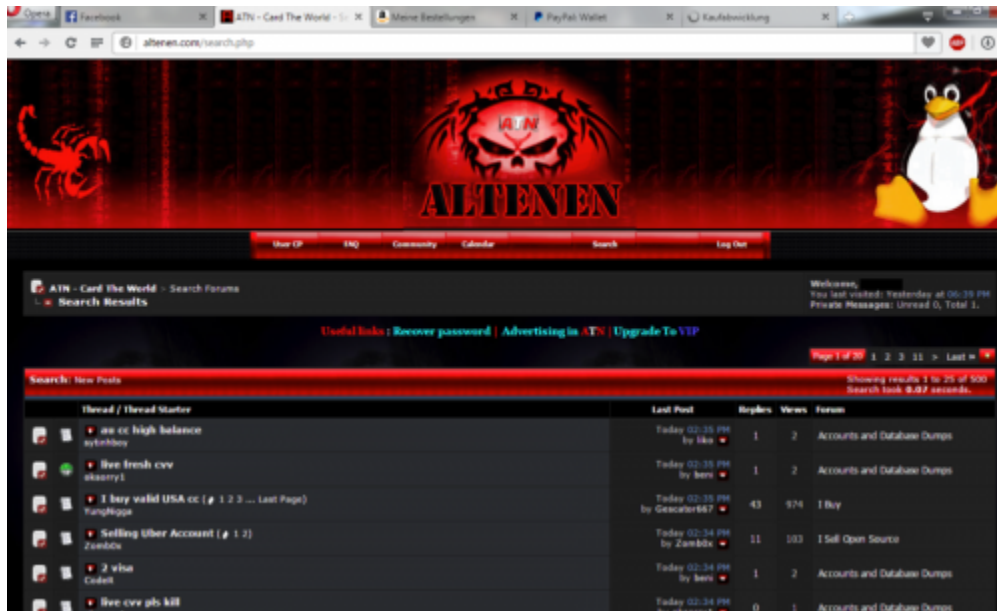


Figure 71 - Carders forum

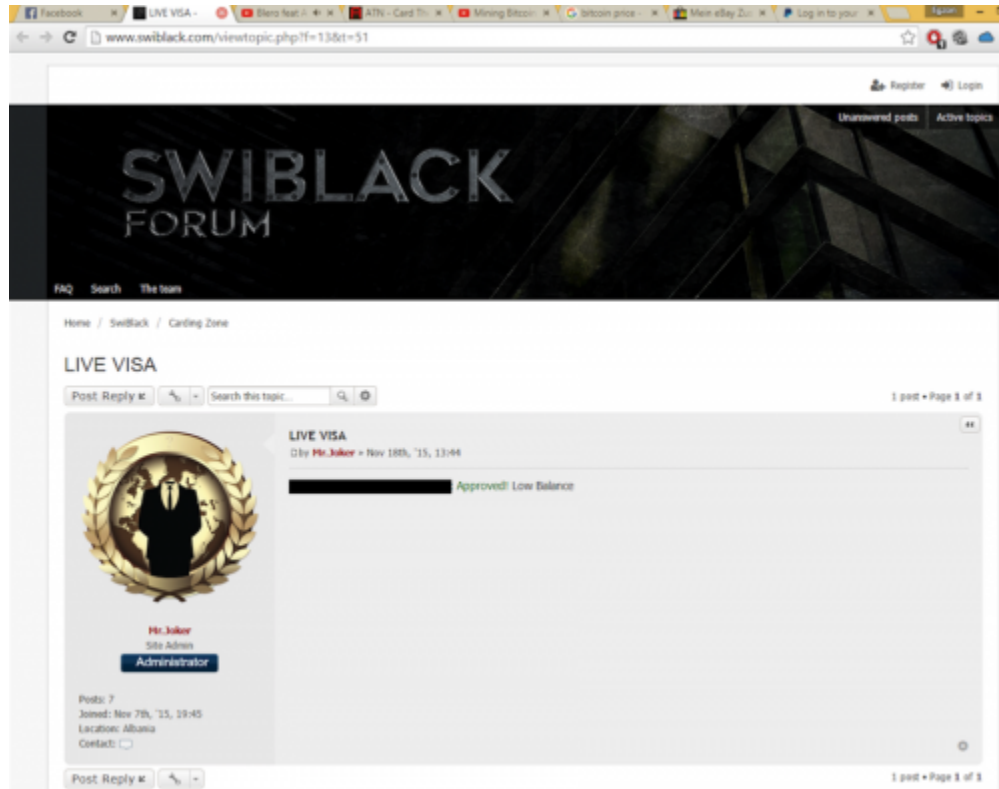


Figure 72 - Another carder forum

You also see their recent download history of multiple PayPal brute force type applications and then subsequent fraudulent purchases on eBay via Paypal and different e-mails.

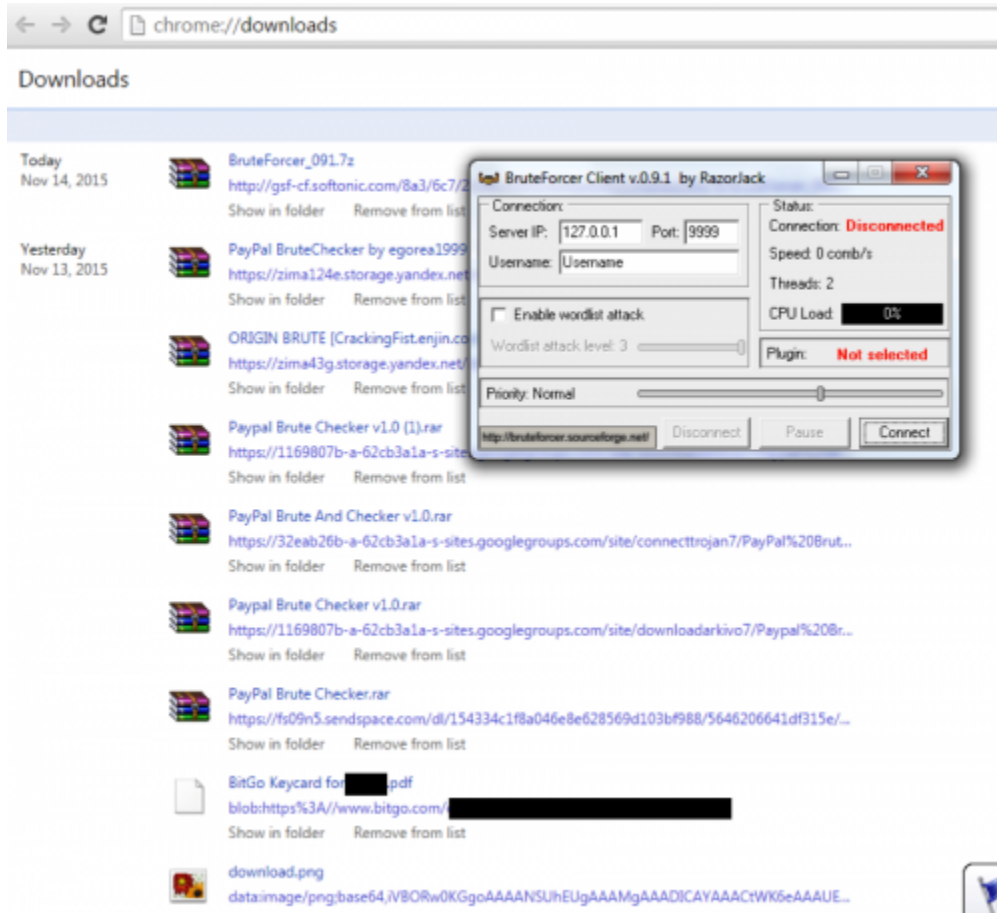


Figure 73 - Downloading PayPal brute forcers

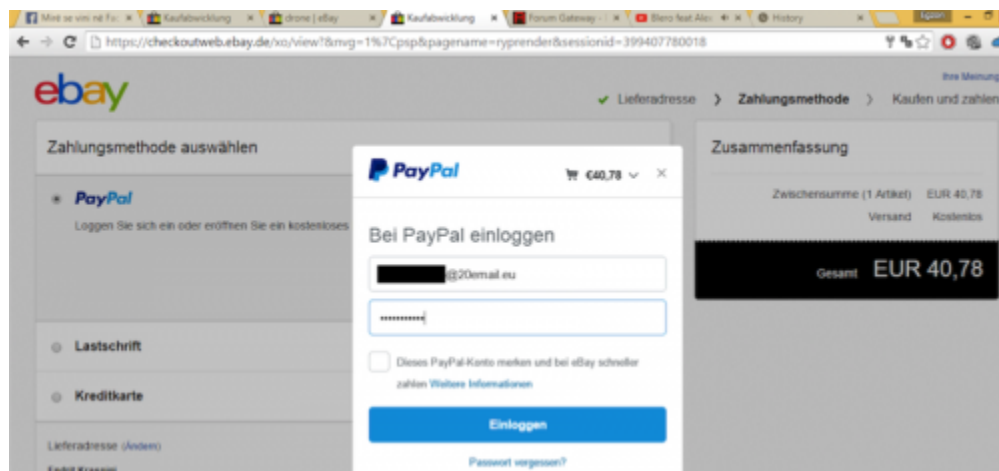


Figure 74 - Purchasing items off of eBay with stolen PayPal credentials

Last, we see the actor conversing with another through Facebook as a new KeyBase web panel gets stood up.



Figure 75 - Providing the credentials for root access to the server

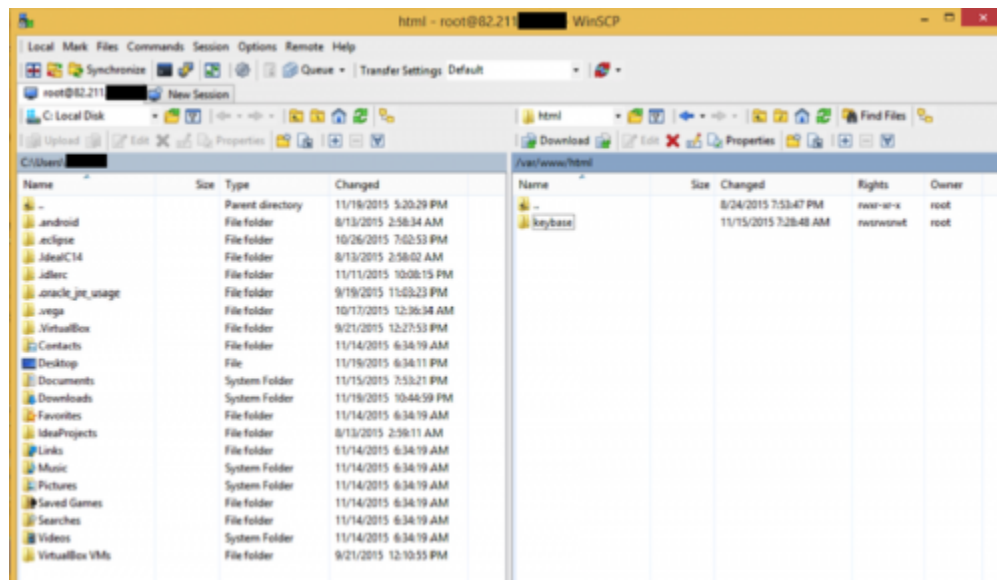


Figure 76 - New KeyBase web panel being created

Actor 07

This next actor's resolution was such that the screenshots only captured the top left portion of his or her screen; however, it was enough to make some interesting observations on tactics. The actor appears to be trying to engage in romance scams with multiple women, along with preying on seniors through dating sites.

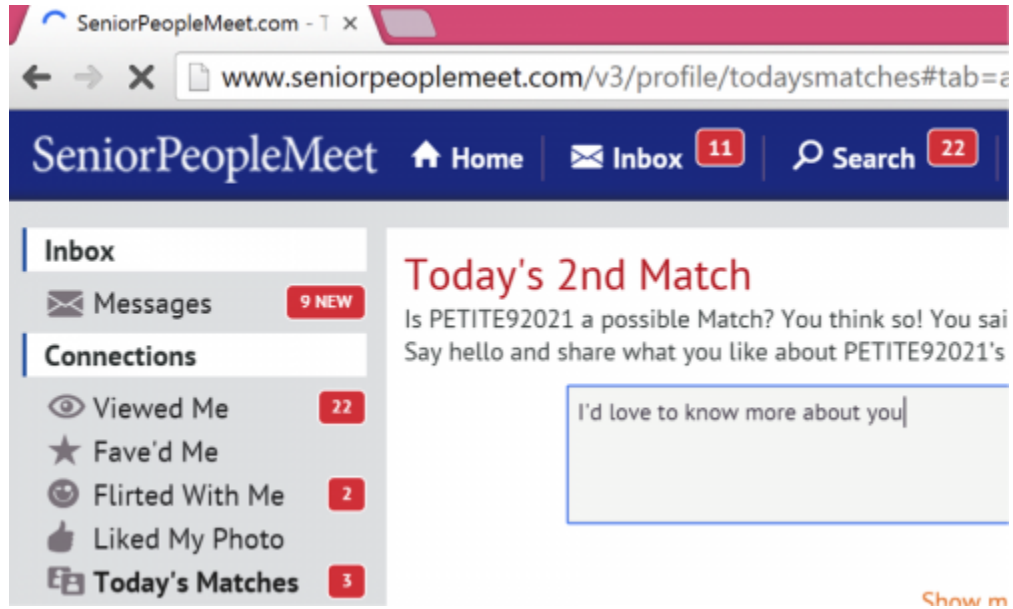


Figure 77 - Sending messages on senior dating site

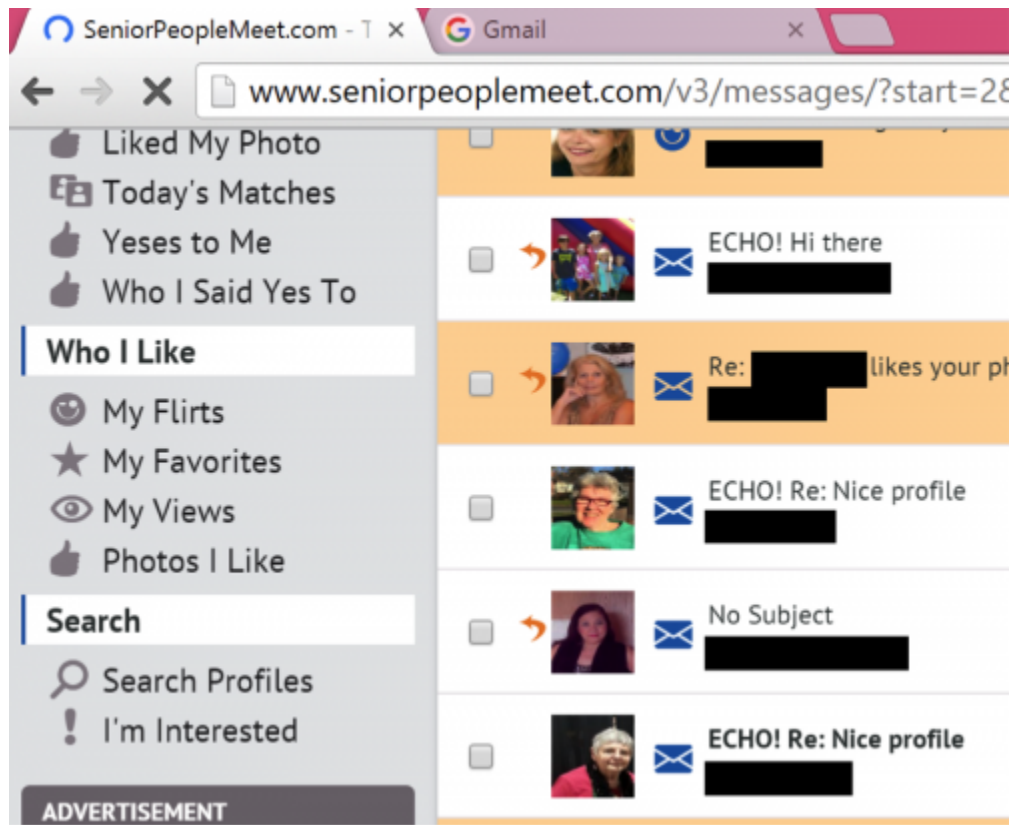


Figure 78 - Sends the same messages to targets and moves on to IM/e-mail

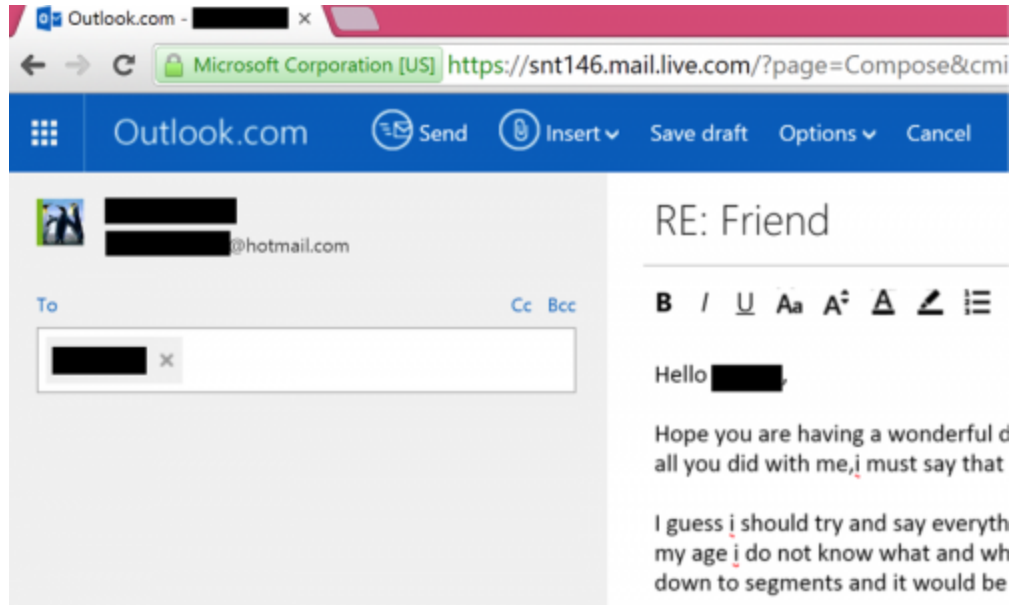


Figure 79 - Sending e-mail, presumably to continue the scam

The actor also has a cache of readily available dating pictures...

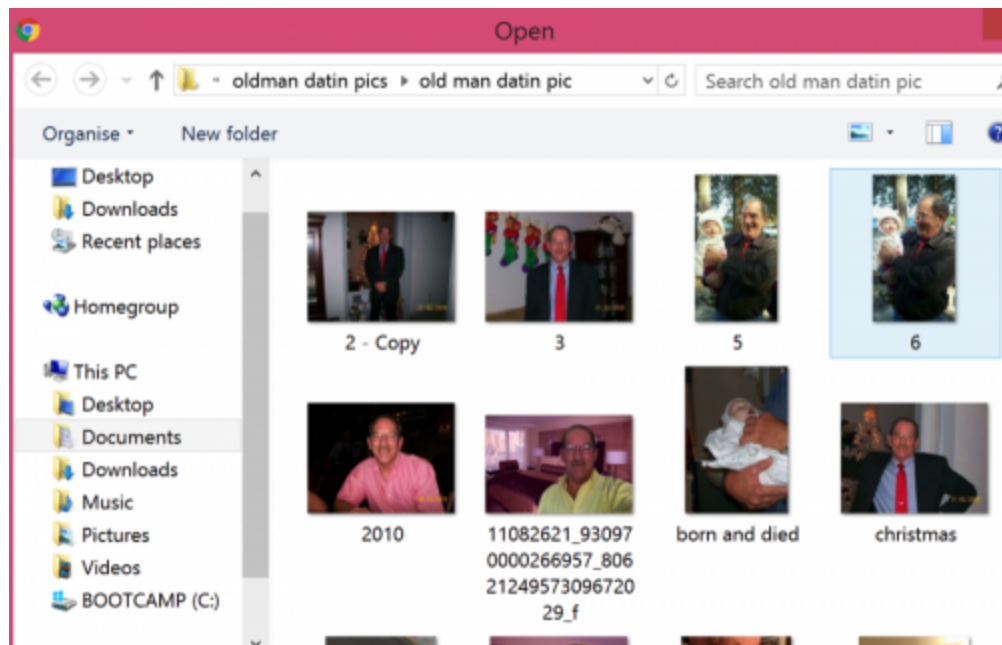


Figure 80 - "Oldman datin pics"

When they aren't trying to romance, they are busy trying to scam CEOs.

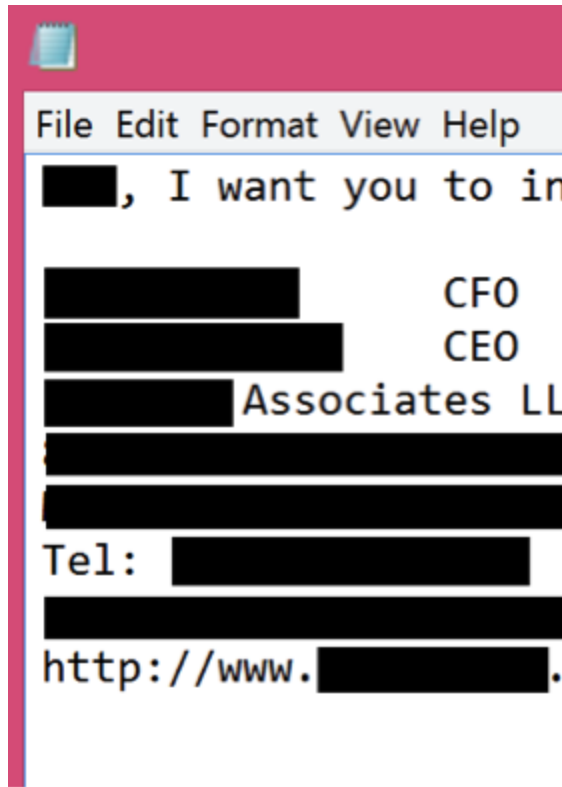


Figure 81 - Writing an e-mail in Notepad – possibly to deliver KeyBase or attempt fraud

Company	Country	Executive	Website
Vodafone Hutchison Australia, VHA)	Australia	Morrow, Chief Executive	Website Australia
Vodafone New Zealand	New Zealand	Mr Russell Stanners, Chief Executive (Bio of Mr Russell Stanners)	Website New Zealand Vodafone New Zealand address
Wesfarmers	Australia		
Westfield Group	Australia	Mr Steven Lowy, Chief Executive	Website Group
Westpac Banking	Australia	Mr Brian Hartzler, Chief Executive (Bio of Mr Brian Hartzler)	Website Banking

Figure 82 - Finding targets on “ceoemail.com”

The last picture we’ll look at in this set is the actors desktop, which shows the “Invoice” KeyBase document and a text file called “Ali baba”, which may add weight to our suspicion that targeting was conducted through this website.



Figure 83 - Actors desktop showing “Ali baba”

Actor 08

Our eighth actor up for review is slightly different than the others in that the actor may not actually be using KeyBase but is simply a victim of it...bad guys infecting bad guys. Either way, we are able to piece together his or her activities through screenshots, with a pattern explained as follows.

The actor begins with registering domains through GoDaddy and BigRock that follow a theme of web design.

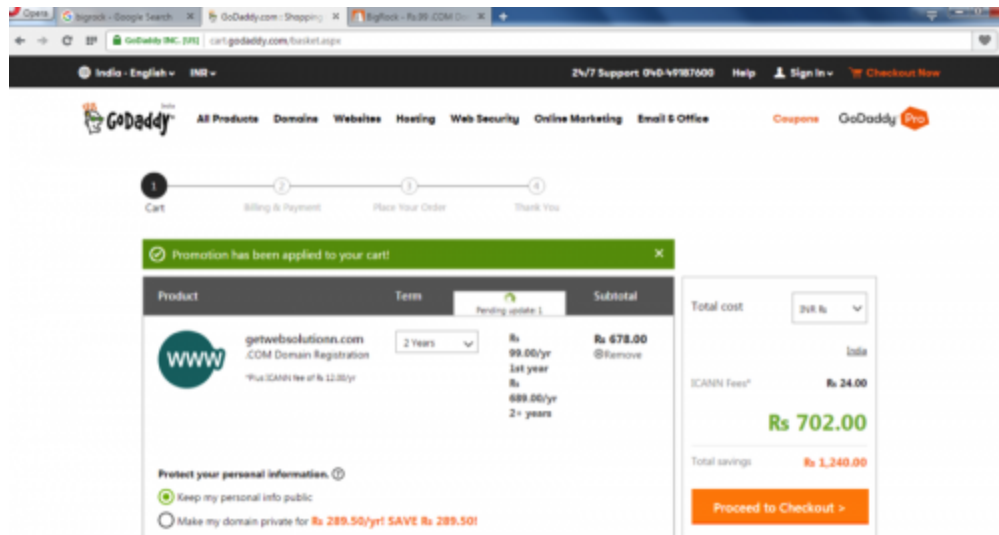


Figure 84 - Registering “getwebsolutionn.com”

Their next-step is to setup an Office 365 Business Premium Trial account for the newly created domain.

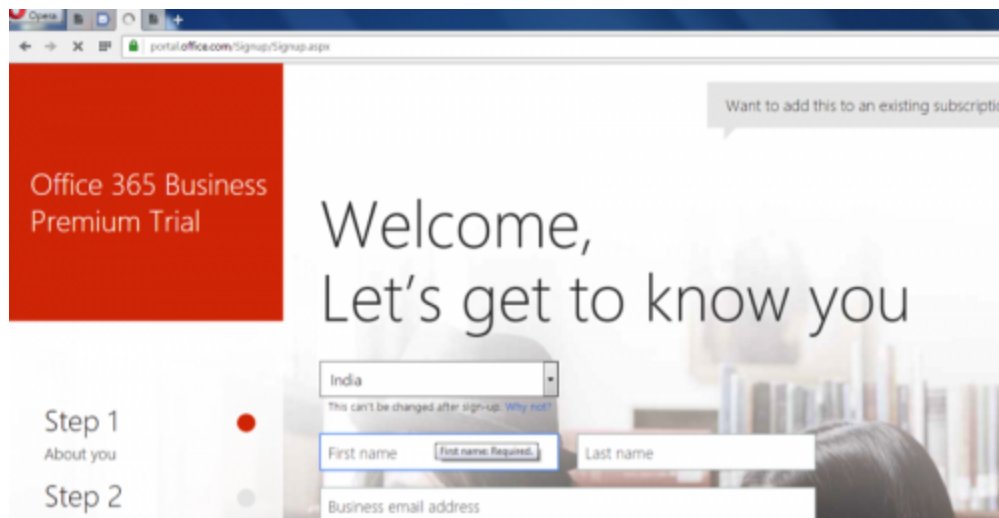


Figure 85 - Office 365 Business Premium Trial

Next, they add new users to create e-mail addresses under the domain. Note the “Burt@getwebsolutionn.com” address, which is used later.

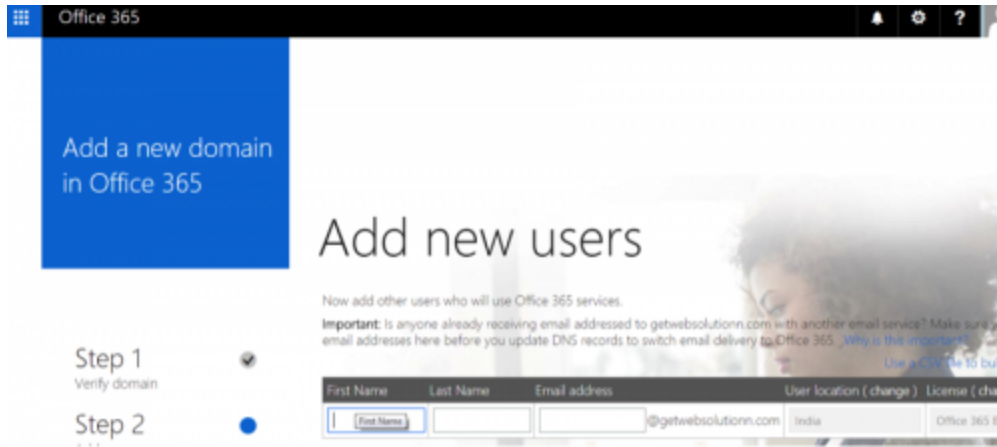


Figure 86 - Adding new users

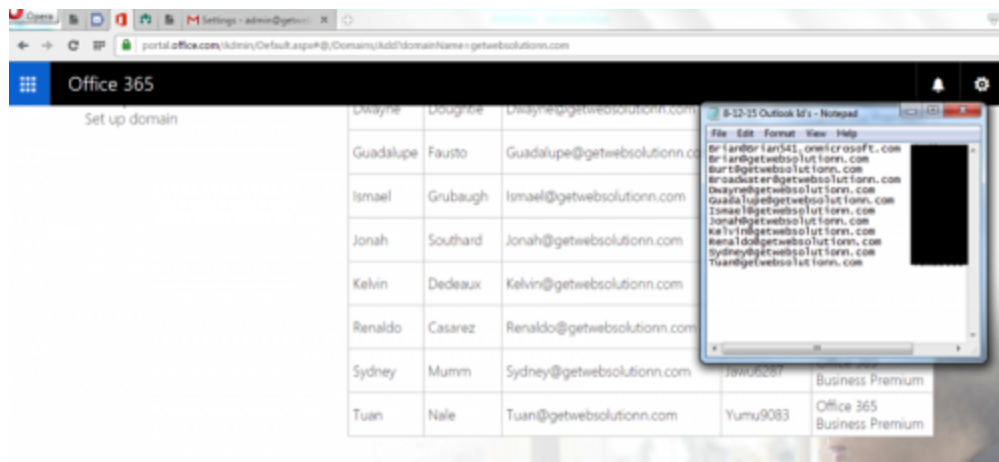


Figure 87 - Created accounts on Office 365

Next, they send out e-mails from these accounts advertising a company that appears to help advertise businesses and design websites.

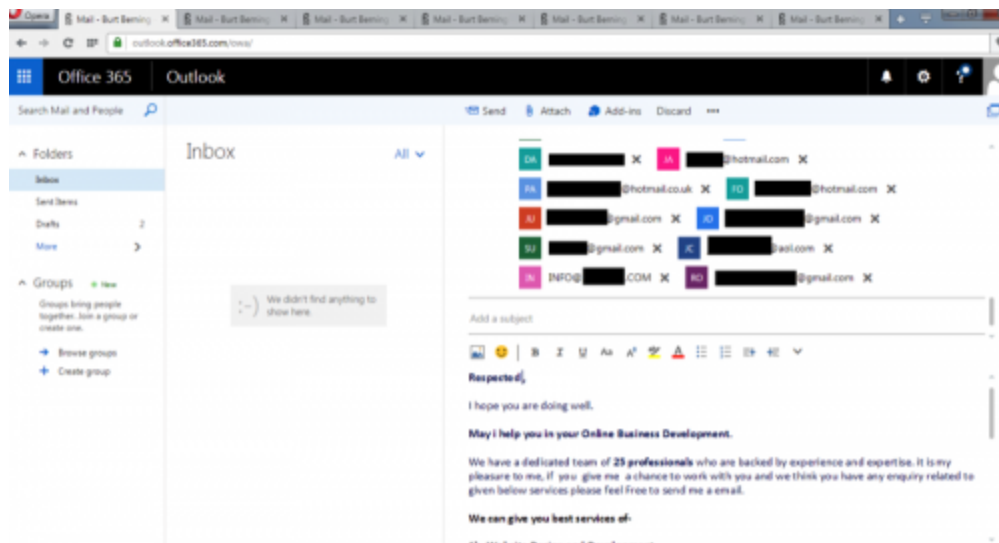
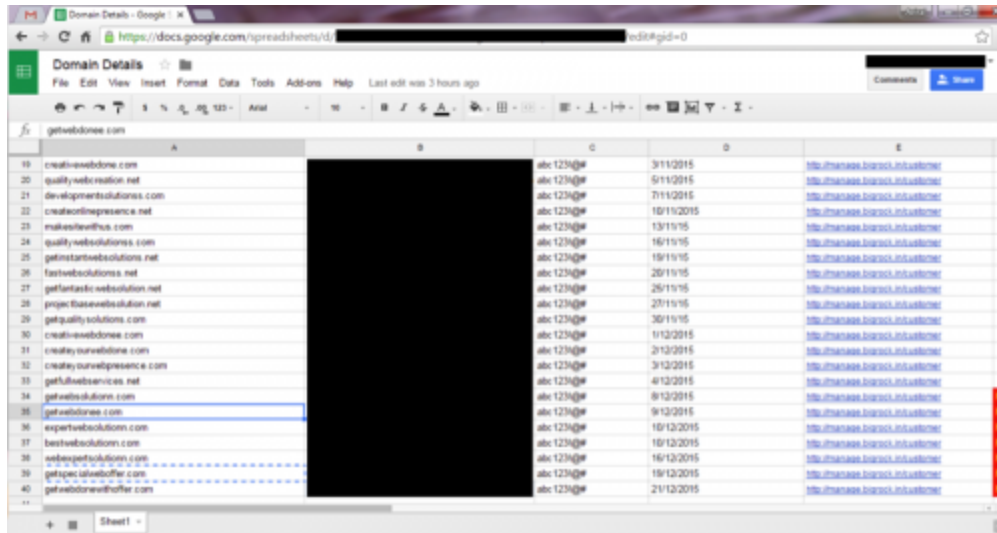


Figure 88 - Sending spam e-mails

This process of registering domains and then sending out spam e-mail through Office 365 repeats itself a number of times over the course of the infection. We also get a glimpse into some of the other domains used for the actor's activity.



	A	B	C	D	E
19	creatwebdone.com		abc123@	3/11/2015	http://mamee.org/abc123@
20	qualitywebcreation.net		abc123@	5/11/2015	http://mamee.org/abc123@
21	developmentalsolutions.com		abc123@	7/11/2015	http://mamee.org/abc123@
22	creationinsurgence.net		abc123@	10/11/2015	http://mamee.org/abc123@
23	makestheflow.com		abc123@	13/11/15	http://mamee.org/abc123@
24	qualitywebsolutions.com		abc123@	16/11/15	http://mamee.org/abc123@
25	getstartwebsitesolutions.net		abc123@	19/11/15	http://mamee.org/abc123@
26	fastwebsitesolutions.net		abc123@	20/11/15	http://mamee.org/abc123@
27	getfastwebsitesolutions.net		abc123@	25/11/15	http://mamee.org/abc123@
28	projectwebsitesolution.net		abc123@	27/11/15	http://mamee.org/abc123@
29	getqualitysolutions.com		abc123@	30/11/15	http://mamee.org/abc123@
30	creativewebdone.com		abc123@	1/12/2015	http://mamee.org/abc123@
31	createyourwebdone.com		abc123@	2/12/2015	http://mamee.org/abc123@
32	createyourwebpresence.com		abc123@	3/12/2015	http://mamee.org/abc123@
33	getfulwebservices.net		abc123@	4/12/2015	http://mamee.org/abc123@
34	getwebsolutions.com		abc123@	8/12/2015	http://mamee.org/abc123@
35	getwebdone.com		abc123@	9/12/2015	http://mamee.org/abc123@
36	expertwebsitesolutions.com		abc123@	10/12/2015	http://mamee.org/abc123@
37	bestwebsitesolutions.com		abc123@	10/12/2015	http://mamee.org/abc123@
38	webexpertsolutions.com		abc123@	16/12/2015	http://mamee.org/abc123@
39	getspacelabweboffer.com		abc123@	19/12/2015	http://mamee.org/abc123@
40	getwebdonewithoffer.com		abc123@	21/12/2015	http://mamee.org/abc123@

Figure 89 - Spam domains

Afterwards, the actor sends an e-mail message with how many people replied to the spam. Another possible scenario is that KeyBase is being used as a way to monitor employees to ensure they are doing their work.

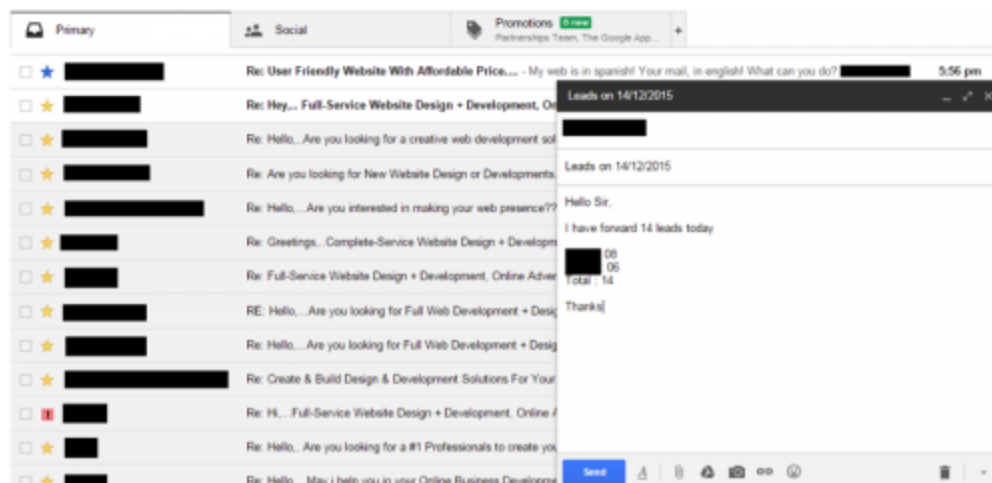


Figure 90 - Replies to the spam in the background, leads e-mail in the foreground

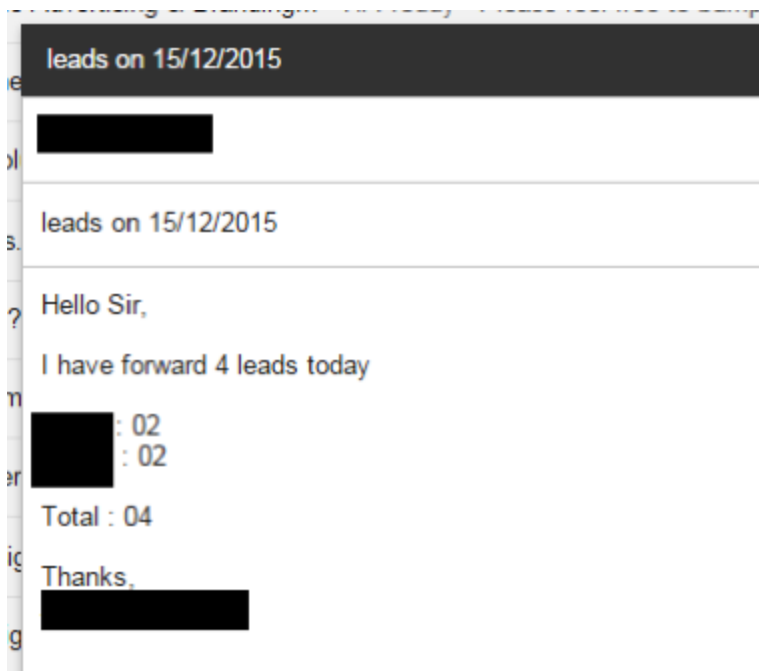


Figure 91 - The next day leads

Actor 09 / 10

The last two actors we'll cover with one screenshot from each, both using a similar tactic of sending the phishing e-mail with bulk e-mailers.

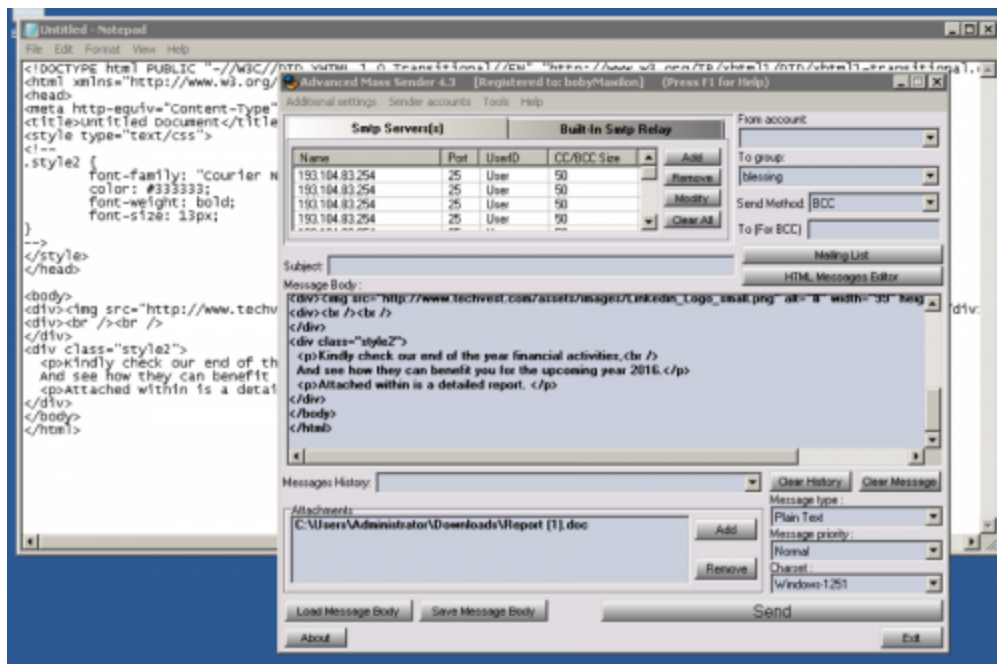


Figure 92 - Sending phishing e-mail with Advanced Mass Sender

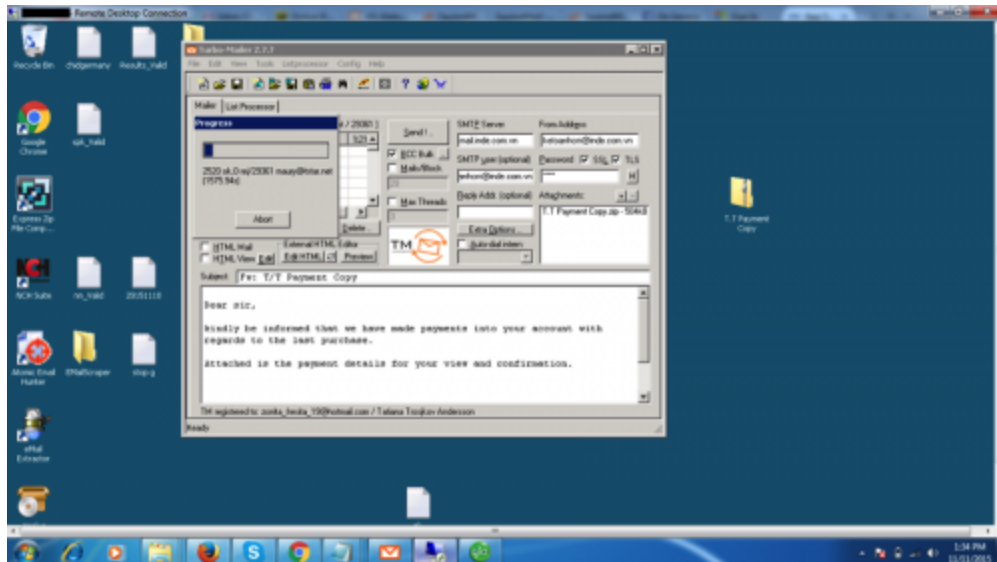


Figure 93 - Sending phishing e-mail with Turbo-Mailer

Conclusion

Our analysis provides a unique opportunity to see the entire life cycle of a malware infection. Commonly, we'd see the first image in a set to be the KeyBase executable or malicious document all the way through until the Anti-Virus alerts of an infection. Sometimes that happened all within one screenshot.

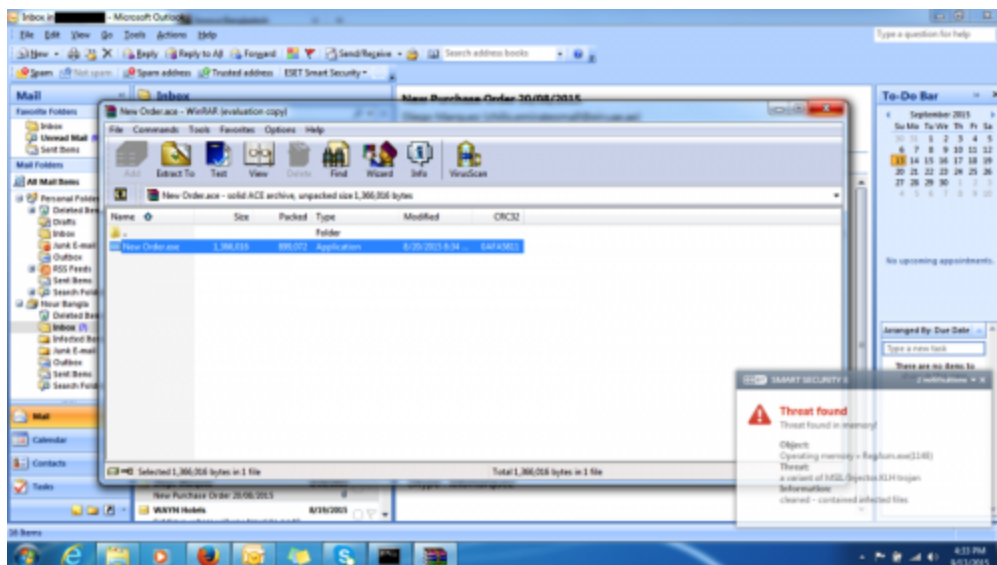


Figure 94 - Infection and detection

KeyBase isn't actively being developed, but we believe its use will continue to rise given its existing capabilities and easy-to-use builder.

The idiom that “a picture is worth a thousand words” holds true, especially if you’ve made it this far. KeyBase is loaded with features but the screenshot capability has proved to be particularly useful with the context it provides by marrying surrounding information to logged keystrokes. From a target analysis perspective, it gives us some insight into the type of companies, or people, the miscreants are going after, and hopefully this blog has shed some light on the potential data that gets exposed through screenshots alone.

Threat Prevention customers are protected from this threat by the KeyBase command and control traffic signature. AutoFocus users can identify KeyBase samples using the KeyBase tag

KeyBase Indicators

E-mail Subjects:

25270 usd
A320
A320 for ACMI
Balance Payment
COPY USD 23000\$
Confirm your bank details
Demande de Cotation
FW: Attn: Your best price urgently
FW: Re: Purchase Order Inquiry
Fw: Outstanding Payment
Fw: RE: 4800MW Combined Cycle Power Plant
Fwd: : Re: Original shipping Documents
Fwd: Shipping Documents/ Reference Id: 20150813-523838075605
Fw: T/T Payment Copy
Good Day
INVOICE FOR ALCOHOLIC BEVERAGES
Inquiry
Inquiry Specification
NEW MACHINE DESIGN
NEW ORDER & ITEM WE NEED
Notre demande
Order12/2015
Order_Nov
Original shipping Documents today via dhl
Our Request
Payment Outstanding
Quotation
RE : Quoations

RE : Quotations
RE: Re: Purchase Order Inquiry
Re : Attention
Re : Purchase order No.PEC/PUR/15-16/302
Re : Quotations
Re: A320 on ACMI
Re: Original shipping Documents
Re: Purchase Order Inquiry
Re: Purchase Order Inquiry for Your Kind Attention
Re: Purchase Order Inquiry
Re: Purchase Order Inquiry for Food Item and Seafood
Re: Purchase Order Inquiry for Your Kind Attention
Re: Purchase Order Inquiry for Your Kind Attention
Re: Re: Last Order Schedule Notification 2015 (Order0261)
Re:Payment for Diamond Wire for Marble
Re:Urgent
Service Tax Clarification on Flat
TR: Order0118-Nov
USD \$24000 COPY
USD_30000\$.scan0002.jpg
WG: Order12/2015

E-mail Senders:

AVAL EXCHANGE
Admin
Aeronautical Information Services
Aeronautical Information Services - ANS Headquarters
Amit Varaiya
Ashish Gupta
Asif Asif
Diakalidia Dissa
Dulal Mohato
Ecc Conseils
Ghulam Murtaza
Hakan Shipping Co. Ltd
Krystyna Mandrykina
Kumar Mohammad
Kyle P. Zing - ABS Group (Pacific Division)
LIAONING ZHONGWANG GROUP CO., LTD
LIGHTECH LLC
Liaoning Zhongwang Group Co., LTD
MKR Global Trading

MKR Global Trading Company
Mehnas Enterprises
Muzafar Saafin
Peghini, Rainer (LEN, VA)
Rachel Natalia
Razahmad Humraz
Sara Ahmed
Shanaz Trading PTE Singapore
Shanez Trading Ltd, Singapore
Shanez Trading PTE
Shanez Trading PTE Ltd, Singapore
Tarek Ben Aissi
Vijay Nath
Yasir Enterprise
aly dembele
massin massin
neco phil
ragnar lordbrook
raz ahmad
vijay nath
wali haider

E-mail Addresses:

ketoanhcm@inde.com.vn
a.engl-lohninger@anti-germ.at
abs-pac@eagle.org
admin@lukeandcompany.com.au
ais@kcaa.or.ke
ajooft1@naver.com
alqardabayah@rakfzbc.ae
benaisi.tarek@gmail.com
bicmanager@gmail.com
contact@paraboot.com
contacto@energiasrenovable.cl
diakalidiadissa@ymail.com
eccconseils@yahoo.fr
enterpriseyasir@yahoo.com
fforteza@latinhotel.com
gemataly@yahoo.fr
ghulammurtaza2344@yahoo.com
gullmuhd786@yahoo.com
info11@redsealsuppliers.net

iqbal.farooqi@ammiza.com
kristina@mandrykina@gmail.com
lightechllc@yahooo.com
mail@pconnect.co.za
michelet220@yahoo.com
mkrmrtrading_lib@outlook.com
necophil@yahoo.com
postmaster@optimal-design.cz
r.hollman@mail.com
raghida@jrtorbey.com
ragnarlordbrook@engineer.com
ratooltraders_2000@gmail.com
razahmad789@yahoo.com
rpeghini@testo.de
sarita_199228@yahoo.com
shaneztrading@hotmail.com
tanhuong142@gmail.com
tazzyy8826@daum.net
tender@unicorndenmart.com
trangtran0709@gmail.com
vijaynath_drilltaps@yahoo.co.in
yasirenterprise@yahoo.com

Archive Name:

0000123.zip
25720 USD SWIFT CCOPY.jpg
A320 for ACMI
A320 for ACMI (3).ace
A320 for ACMI (2).ace
A320 for ACMI-1.ace
A320 for ACMI.ace
A320 for ACMI[1].ace
A320_for_ACMI.ace
ACMI.ace
BL_036050112202xls.gz
Balance Payment.zip
COPY OF THE DOCUMENT_Pdf.zip
COPY OF WHATSAPP IMAGE_scan0003jpg.zip
COPY USD 23000\$.Pdf.zip
COPY USD 25000\$ scan0002 jpg.zip
COPY_USD_23000\$.Pdf[1].zip
Copy10Scanneddoc.ace

DHL SHIPPMENT DOC FOR PENDING ORDERS.zip
EID MUBARAK GREETING.pdf.zip
FinalCopy_Scan.ace
FinalProductList.zip
Invoice for alcoholic beverages (2).ace
Invoice for alcoholic beverages.ace
Invoice.zip
MV ALFA.zip
NEW MACHINE DESIGN.JPG.zip
NEW ORDER & ITEMS WE NEED.Pdf.rar
New Order.ace
NewCopy_Scan0261.ace
NewOrder.zip
ORIGINAL SHIPMENT DOC& BL.zip
Order #380358967.zip
Order Inquiry Specification.ace
Order Invoice.zip
Order _380358967.zip
Our Quotations.ace
Payment Receipt#380358967.zip
Po-September-Sept171763403583 (2).ace
ProductOrder List.zip
Quotation.zip
Quotation.rar
Quotation.rar.zip
Revised_OrderFinal
Scan0118_Revised.ace
Shipping documents .20150813-52383807565_pdf.rar
Slip.zip
Swift Copy CHF \$15100 .rar.zip
T.T Payment Copy.zip
TT \$25700 USD REMITTANCE.Pdf.zip
TT APPLICATION \$50,000 USD.Pdf.zip
TT_H1245792776500_JPG.zip
Znp0002.zip
order inquiry doc.ace
scan0002.jpg.zip

EXE Name:

ACMI.exe
BL_036050112202xls.exe
Balance Payment.exe

COPY OF THE DOCUMENT_Pdf.exe
COPY USD 23000\$.Pdf.exe
COPY_pdf.exe
DHL SHIPPMENT DOC FOR PENDING ORDERS.exe
EID MUBARAK GREETING.pdf.exe
FinalProductList.exe
Invoice for contract No. 182.exe
MV ALFA.scr
NEW TT RATES 28.07.2015_pdf.exe
New Order.exe
PAYMENT.exe
Po-September-Sept171763403583.exe
Quotation.rar.exe
USD_20345_\$ COPY_Pdf.exe
USD_34567 \$_Pdf.exe
invoice doc.exe
invoice document.exe
scan0002.jpg.exe

DOC Name:

NEW MTO.doc
Order01.doc
OrderInvoice.doc
P001.doc
Part1-Product List.doc
ProductList.doc
Revised_OrderFinal.doc
STC ORDER LIST.doc
Scan0118_Revised.doc

KeyBase Panels:

A full list of the KeyBase control panels we have identified is available on [GitHub](#).

**Get updates from
Palo Alto
Networks!**

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).