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

9 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.

■ II型 PW 製作 packing list kannut150964 - 載409-22 - 同部件 00.37.00 ESR行 の ×							
A 223	1 🖯 647 🥔 MM 🔁 82-20 M 🔁 80 🔁 80 🗸	1					
(094A):							
• 19週)							
- 88 -	回題 FW: 夏時 packing Tet format150906 - 都市06.22						
	Meresek W = 1 = 2 + 2 + 2 + 2 + 2 + 2 + 2 + 2 + 2 + 2						
Matter	Most Urgent.						
Regards Vice Annu Mambok Chennol	dent - Operations Alem 600127, India						
From: Sent: 223 To: Co Subject: F	Procurement) (mailto: esptember 2013 11537 Bis Saipern - Dangste - Y PO (PO.No.932094 Dt.22.04.2014) - NIM Request - 22nd Lot						
Dear Mr Please ref in order to	Re to attached purch list issued by inspector , Purch list serial 1; WPS/PGRs shall be prepared by sub-supplier, and submit them to client for approval) is not yet closed. Nindly take immediate action to close punch list o issue release.						

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 that 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.



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 <u>Alibaba</u>, 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.

🔊 🕫 🗄 🗉 📕 http://sourcing.alibaba.com/rfq_search 🙆 🔎 = C 🗙 📲 qqui 🚛 📕 Man., 🗙 🎽	Plant E., 📕 Daily Fl., 📕 Alibab.,
▲ 44兵 ▼ 12 医/F	
i, We are Trading company in DUBAI (UNITED ARAB EMIRATES)And we are looking for a upplier in Thailand . We are interested in your product	United Arab Emirates
ate Posted: 2015-09-13 (U.S. Pacific Standard Time)	
	Quantity Required
ear Sirs good day I take the liberty to introduce ourselves to you as importer for confectionery	1 20' Container
oducts from Egypt ,by visiting your web site I	I Egypt
ike Possea: 2013-Vario (U.S. Pacine Soundard Lime)	
	Quantity Required 1800 Boxes
ear ,We are general trade company in iraq.We need big quantity of the second with 200 Il .Please send your best offer to start	T Iran
ite Posted: 2015-09-16 (U.S. Pacific Standard Time)	
	Quantity Banuized
his is Sheik from and I would like to customize "	1 20' Container
flowing specifications.	Mauritius
ste Posted: 2015-09-11 (U.S. Pacific Standard Time)	

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.

- 局部件 11:41:27 已保存 _ & X
欧件人:
主題:
Times New R × 11 × ▲ + □ + B / ½ ∓ := 1= = + ○ 4 ≯.
Dear Naser,
Thank you for your enquiry on Alibaba.
experience in this field and we'd like to offer:
-Skg at \$730kg CIF to your office by DPL. Packing: 100gram aluminum bag with box.
Lead time. It will take one week for shipment after your order confirmation.
Await for your reply.
Best regards,
Linda
Company address. Shanghai , China
COA-5pdf

Figure 9 - E-mail reply to an Alibaba message

AND PARTY INCOME. MICH.	PPF EDM29 58	年 7785 文件 消息				
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	× · · · · · · · · · · · · · · · · · · ·	1 10 1 HE	19.00		
日本語	· 7 : 10	職已滅 豊示全部 ▼ オ	明细 🕶			
🕣 🗟 軟件箱 [633/926]		♀ 最近一月		Q 共 926 批 E	1 批	
a 🔒 特況相	+ 45	10.00	0.000	0.000	1000 C 40	
★ 市牧橋	25	02 H DC 1 4535 /	21年入	- 0 504A	10010 100 100 100 100 100 100 100 100 1	17981 1
- 🔒 已没端 [17]		WI REI 1.4835 (Anna	· 8 /54/9	2015-12-18 151	17381 6
③ # 群发痛		et st	*		2015-12-14 14:-	11 K
and secondar	3 * 63 R	Ei to Claudio		• Arna	2015-09-17 21:-	90 K
14	4 * 23 A	nna, discover t	Alibaba.cor	n T., * sales20	2015-09-15 20:	282 k
- EW- PE- 1 4835 (ASTM- 5	and the second		P ##35-			i个.总大小:16
			and all and an	-		
MILE 10 1600 1914 10 X1/3 300	ACTION + + • • • • • •	NAME AND A DESCRIPTION OF	- 701WT - P(17+30	LDMR *	~ 1485	lext CL
භ件人: Anna						inspection
欠件人: 万春梅			抄送人			 before shi
						😑 😐
Rame: 9015-19-14 14:99						
Subject: ME: 1.4835 GASTE: S	30815) tubes price-	- Het	al Cs.			inspection
						Derore snu
Dave He						
Dear Mr.	from alibabal					
Dear Mr. Helio!Glad to get your RFQ	from alibaba!					Tert
Dear Mr. Helio!Glad to get your RFQ f After studied your inquiry wit	from alibaba! th my Cost Account	ting Dept., Product M	anager and work	shop, the reply as below		Test Chemical
Dear Mr. Helio/Glad to get your RFQ I After studied your inquiry with Tube	from alibaba! Ih my Cost Accoun	ting Dept., Product M	anager and work	shop, the reply as below	r.	Test Chemical
Dear Mr. HeliofGlad to get your RFQ/ After studied your inquiry wit Tube Material : EN 1.4635 Tolerance : DIV 2463 D4 / 2	from alibaba! Ih my Cost Accoun	ting Dept.,Product M	anager and work	shop, the reply as below	r	Test Chemical
Dear Mr. Heitol Glad to get your RFQ I After studied your inquiry wit Tube Maternal : EN 1.4835 Tolerance : DIN 2463 D4 / 7 QV : 334 pcs	from alibaba! th my Cost Accoun	ting Dept.,Product M	anager and work	shop,the reply as below	r.	CO for
Dear Mr. Helio/Glad to get your RFG I After studied your inquiry wit Tube Material : EN 1.4835 Tolerance : DIN 2463 D4 / T Gty : 354 pcs Size : 42.4 x 1.5 mm L= 250	from alibaba! Ih my Cost Accoun 74 5 mm	ting Dept.,Product M	anager and work	shop,the reply as below	ĸ	CO for Paraguay
Dear Mr. Helto/Glad to get your RFQ / After studied your inquiry wit Tube Material ; EN 1.4635 Toterance : DIV 2463 D4 / T QY : 354 pos Size : 42.4 x 1.5 mm L= 250 Docs : + cert 3.1	from alibaba! th my Cost Accoun r4 5 mm	ling Dept., Product M	anager and work	shop, the reply as below	r.	Co for Paraguay
Dear Mr. HeltofGlad to get your RFQ 1 After studied your inquiry wit Tube Material : EN 1.4635 Tolerance : DIV 2463 D4 / 7 QV : 354 pcs Size : 42.4 x 1.5 mm L= 250 Doos : + cert 3.1	from alibaba! th my Cost Accoun r4 5 mm	ting Dept., Product M	anager and work	shop.the reply as below	ĸ	Co for Paraguay
Dear Mr. Helio/Glad to get your RFG I After studied your inquiry wit Tube Material : EN 1.4835 Tolerance : DW 2463 D4 / 7 Gly : 354 pos Size : 42.4 x 1.5 mm L= 250 Doos : + cert 3.1 1)FOR()USD\$13.5 Vie will send DDU price onc	from alibaba! In my Cost Accoun r4 5 mm Wiking based on sta	ting Dept., Product M ndard: ASTM/T312,e d address. Thanks in	anager and work ach piece tube a advance.	shop,the repty as belo round 3.83kg.	r	Test Chemical CO for Paraguay

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	F	rom01/05/201 To 31/05/2015	
DATE	INV #	DISPATCH # CUSTOMER NAME	AMOUNT
27/05/2015	SI-31691	29721	56,271.9
27/05/2015	SI-31692	297mm 🛛	66,386.5
27/05/2015	SI-31693	297 Parent System Printer (Camero P Lassifier DK.	97,920.00
27/05/2015	SI-31694	297 Part Reven	23,709.72
27/05/2015	SI-31695	297 F H Fair 18	32,302.20
27/05/2015	SI-31696	297 Exer to P Color Coper	12,960.00
27/05/2015	SI-31697	297	85,113.60
27/05/2015	SI-31698	29726	163,518.60
28/05/2015	SI-31699	29741	1,439,608.80
28/05/2015	SI-31700	29729	79,444.80
28/05/2015	SI-31701	29730	219,672.00
28/05/2015	SI-31702	29731	576,979.20
28/05/2015	SI-31703	29732	31,850.88
28/05/2015	SI-31704	29733	6,075.00
28/05/2015	SI-31705	29734	24,300.00
28/05/2015	SI-31706	29735	67,813.20
28/05/2015	SI_31707	2973R	12 996 41

Figure 11 - Invoice data for multiple customers with values

	FOR	9	Paragraph		Styles	104
1 * * * * *	🖁		. 2 3		4 * * * 1 * * * 5 * * * 1 * * * 6 * * * 1 * 3 * 7	
	Dear Mr.					
	Tomorroww	e shall quote	you considering	you will prov	ride us tools.	
	If we have to	develope the	tools we shall qu	ote tools cos	t at the <u>the</u> time of finalisation of <u>roder</u> .	
	Your early ac	tion in the ab	ove matter will b	e highly app	reclated.	
	Thanks & rega	rds,				
	Mobile: Web:	/ w	hat's App No.:	_		
	Mfrs. Of Indu	strial	& HI-Tech	Products		
	An ISO 9001-	2008 Certifie	d Company			
rds: 108 🛛 🔊 🔊						

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

^ ±20 Ke: HE: Ke: Enquiry He 15130 // 3-way 16"centrolValve CL159 209Α. 058Α. ΔΕΣΕ 103Α.	₩ ₩ :
【伊姆2】 波道教師 2015-09-10 10-05 加坡時間 2015-09-21-05-57 Dea Nancy, Sorry for the late response. Actually the client did not accept the drawing type. For your reference p could get the clean's approval. Any young reference public did be thankful.	please consider the below sample. Please accordingly provide your drwaing based on in order we
	"Levi LF

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...

1	Subject:	RE nr: PM analysis request
	Good afte	moon.
	Noted. W	will send the Analysis Application form and samples of 7g me film to Mr.

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.

Friday, January 1, 2018	User. Use	r Role: Customs Agent Tolion 8	Marce: 12			Settings] + Logist
	Src - <> GD Monito	ring				Q, Search
WEBOL	0, Sutter	Salar	60 Sumber	90 Type	Search Now Clear	
Home Page						4
	Sr GD Number	Trader		BL No	Status	Od Type Form E#
	1				Prepared	import
	2				Prepared	Import
Examination Request Before	3				Prepared	Import
Goods Declaration Under Section 79(1)(b)	4				Examination Called and Walting for TO for Container Orounded	import
List of Traders	6				Assigned to Cashier	iment
Document(s) Requested					Document Called by American and	
Carrier Declaration	6				waiting for Approval of Officer	Import
User Support System	1				Loading Allowed	Export
	0				Assigned to Gate Out Staff	Import
Refund Management	9				Cancelled	Import
GO Monitoring	10				Cancelled	import
Amendment And Cancellation	Go to page Go	Page 1 OF 2 H 4 +				
Payment Management						

Figure 16 - Pakistan Web Based One Customs – "Customs Agent"

	Service	One-Customs (Paperless	Goods Declaration Processing	System) - Internet I	Explorer		
WEBOC	ale -	Https://www.weboc.gov	pk."			🚔 Federal B	oard of Revenue (PK)
	Impo	¥ 123PG				on Examination	
		13.JPG				Attached Document	^
Trader Messages	Saves	-				on Examination	
Securities Management	Subm	🗢 14.JPO				on Examination	
Notices		15.JP0				Attached Document	
Goods Declaration	GD Filling 1					on Examination	
Order in Original List	600						
Assessment	MPOP	Declared Items Information			Assessed items informatio	a	
Show Cause Notice(s)			Unit Total Import			Unit Total Import	
Examination Request Before	60 Mg	S.No. HS Code Quantity	Price Value (Rs)	rescriptionView	S.No. HS Code Quantity	Price Value (Rs)	escriptionView
Goods Declaration Under Section 79(1)(b)	GO NO	1 0000	1.250010000.00001,054,440	lew Details	1 0000	2.000016000.00001,703,975	lew Details
Document(s) Requested		2 000	1.25005000.0000 527,220 \	lew Details	2 0000	2.00008000.0000 851,968 V	lew Details
Heatings	Go to page	3 0000	11.25002875.0000 303,152 \	few Details	3 0000	2.00005000.0000 532,492 V	few Details
Section - 79							
Security		Duties Information			Duties information		
Carrier Declaration		Duty Name	Amount (Rs)		Duty Name	Amount (Rs)	
User Support System		CESS	19,794		CESS	19,794	
SRO LookUp		Customs Duty	109,398		Customs Duty	617,691	
List of Rebate GDs		Sales Tax	59,826		Sales Tax	630,045	
Refund Management		Income Tax	61,621		Income Tax	238,491	
Checke Dolonie Link		Total:	250,639.00		Total:	1,506,021.00	
MUS							_
=10							~

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.

	Global Logistics - CLIMAX SYSTEM Version 9.2 - PERIOD 2015 - 2016	- 0
Entry Secon Los Cenesi Aports Cesare 1 Second		
	Type DLCL FFCL Comme Field Company NUVIS C New Side Tax C TC S IP Las C TC S IP	
And the second se	Flight T0 348 22 12 2813 Deat HONG KONG	
	Altane Alagent Clert	15
Contraction of the local division of the loc	Weight 68 5000 Packages 01 Sates Rule Buying Shipper	8
Second States of the Second States of the	NCT 144.00 100.000 100.000 CApert	
		78
	Clent Line Clent Line 277	-191
-B	Preight Ra/Kg, PC161.00 99.00 POD Charges \$ 6.00	
- NA AND	PSC Rules UVR 1 Vers House 5	
N. ALL THE	Surcharge Ra/Vg. Ar Stoth Agency Commit 77	
States of States and	Liteulage \$ AWB FEE Ru. 2,000.00	
	NAR Rak/Gd (s) LNuB Other Collect 5 PL	and the second second
THE REPORT OF THE REPORT OF THE	Development (N) 0.00 Development (N) 0.00	A DECEMBER OF A
and the second second	Ex. Refund[2]	
	Femarka Unaled	B an 🖷
111		a shi ka sa
1 - martin		
and they	Apartino CEO	
the for the state	Disc. Tried	
to tot	MATTER AND	

Figure 18 - Air cargo booking

A	Shipping Agencies - CLIMAX SYSTEM Version 9.2 - PERIOD 2015 - 2016	
Noting HSL By Art Lands	Cargo Booling Status Status Status	
	Cargo Booking Downeys Cargo Booking	
	Camer L/Rpert Clark Clark 0 M3 1.0000 Fadages Cl.W. NOX Select Select 0 Cont M (20 ') Homail (* 18000) ClApert 0 0	1
	Organility. • Down 5: • Down • Down <td< td=""><td>The</td></td<>	The
TANA	0./height 6 12	PICE
	B A F 8 PF-Suchaps 8 Doc. Charges 8 Doc. Charges 8 Loss Soc. Charges 6 Loss Charge 6	H
	Open Charges R. Opin Tenel Reservers Ro. Image: Constant of Charges Image	
	Remarks Linkor Work H	
3 + 1 /	Linetry Egillat Dants V X Class Pand Mt. Litt DrowPend 0 Control of Control o	
1-1-2		

Figure 19 - Ship cargo booking

FLI MESSAGE INSE	RT OPTIONS FORMATTERT REVIEW	vessel sch	edule - Messag	pe (HTML)		
Paste of Format Painter	faen •11 • A A ⊟ • ⊟ • Ø (I 및 Ź • ▲ • ■ = = ∈ ∈ 4	Mess Check Attach Attach Sig	sature	illow Up * igh Importance iw Importance	Q. Zeem	
Clipboard 15	Basic Test 12	Names Include		Tags r	2 Zeom	
Serie	I schedule					
Flease find below update	corr our our our out on the	non.	ETA OUCT	ETROICT	ETA COLOMBO	
VESSEL NAME		CUT OFF CT	10 Los	10 Jac	25 Jac	
	24HOURS PROOF OF VESSEL BERTHING	SONDAT 17 JAN 2339 HKS	10-Jan	19-3181	29-540	
	24HOURS PROOK OF VESSEL BERTHING	SUNDAY 24 JAN 2359 HRS	25-Jan	26-Jan	1-Feb	1
Best Regards	-					

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	27.652,425	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 > O	perative Accounts > Mini Statement				Help
Select an Acc	count Nickname and Option from the d	rop down lists.			
	GENERAL TRADING LLC-	•	Account Summa	ry •	
Last 20 Tra	nsactions -[Details till 21/12/10	5:48 PM] Accou	nt Currency - AED	,	
Date	Description	Cheque No.	Withdrawal	Deposit	Balance
18/10/15	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	: BILL ID		14,62,500.00		-20,13,540.00
05/08/15	Offset for [0145043]			14,33,250.00	-5,51,040.00
25/05/15	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 [0145043]		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	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.

O0 You are now in a secured site Home Accounts & Banking Investment Al Accounts Account details Account details Account details Payments Inistory Recent transaction history Transfers Cheques Account information as at Wednesday, 2 December 2015. 15:47:09 Account type: Business PCA	
Home Accounts & Banking Investment. Al Accounts Account number Account details Account details Payments Inistory Recent transactions, Transaction history Transfers Cheques Account information as at Wednesday, 2 December 2015, 15:47:09 Account information as at Wednesday, 2 December 2015, 15:47:09 Account information as at Wednesday, 2 December 2015, 15:47:09	
Al Accounts Account number Account details Payments Translers Cheques Account information as at Wednesday, 2 December 2015. 15:47-09 Account type: Business PCA	
Account number Account details Payments Transfers Cheques Account information as at Wednesday, 2 December 2015, 15:47:09 Account type: Beaineas PCA	
Account details Payments Payments Transfers Cheques Account information as at Wednesday, 2 December 2015. 15:47:09 Account type: Business PCA	
Account details Payments Transfers Cheques Account information as at Wednesday, 2 December 2015. 15:47:09 Account type: Business PCA	
Payments Transfers Cheques Account information as at Wednesday, 2 December 2015. 15:47:09 Account type: Business PCA	
Transfers Cheques Account information as at Wednesday, 2 December 2015. 15:47:09 Account type: Basiness PCA	
Account information as at Wednesday, 2 December 2015. 15:47:09 Account lyoe: Basiness PCA	
Account information as at Wednesday, 2 December 2015. 15:47:09 Account lyoe: Business PCA	
Account information as at Wednesday, 2 December 2015. 15:47:09 Account type: Etrainess PCA	
Account information as at Wednesday, 2 December 2015. 15:47:09 Account lyoe: Btrainess PCA	
Account type: Business PCA	
Account number:	
Account name(1):	
Current balance: RM219,464.39	
Available balance: RM211,519.39	
One-day float: RM7;945.00	
Two-day float: RM0.00	
Late clearing/Outstation cheque float: RM0.00	

Figure 23 - Corporate banking account

Province of the		Xirecta Asegura	edora (1		Avisos: Tiene 0 avisos per	dientes.	
Participande endormanian Participande endormanian Private en	Nostrar 🗉						
Posición global Gestión Cue	netas Notting Control	gastos Tarjeta	i Avales				
Posición Cuentas				_	09/11/	2015 15:53 💽	
Norma 43 Saldo Retenciones	Cuentas : Movim	ientos				Imprimi	
Abonos pendientes Adeudos pendientes Códigos de concepto Domicifiaciones	Nº de cuenta: Periodo de consu Tipo de informac	ilta: ión:	Desde el 02/11/1 Con descripción	15 hasta el 09/11/15	video Para n Realiz	sis información e una videollamada	
Consultar Modificar Dar de alta	Divisa: Tipo de Movimier	nto:	EUROS Todos		Obtenga s avales	us	
Recibos Domiciliados Consultar Devolución de recibos Pandientes de caroo	• Para consultar el	extracto del m	ovimiento pulse sobre la descrip	pción que aparece subrayada.	directamente desde su ordenador.		
Dispensadores	Si lo desea, puer	le descargar los	s movimientos de esta página 🕿	xportándolos a Excel. 🗐			
Dispensar efectivo Talonarios	F. contable	F. valor	B Descripción	B Importe B	Saldo 🛛	Detalle	
Consultar			SALDO INICIAL	-124.786.30			
Anular Talonario	02/11/15	02/11/15	TRANSF OT /	8.765,52 H	-116.020,78	-	
Condiciones y comisiones	04/11/15	04/11/15	16662.2	27.290,70 H	-03.434.30	-	
Información	00/11/15	00/11/10		4.040.22 0	-97,434,20		
	09/11/15	09/11/15		15,452,52.0	-108.851.05	-	
	09/11/15	09/11/15		25.000.00 H	-83,851,05		
	09/11/15	09/11/15	TRANSF	50.000.00 H	-33.851.05	-	
	09/11/15	09/11/15	TRANSF	40.000.00 H	6.148.95		
	09/11/15	09/11/15	TRANSF	2,448,86 H	8.597,81	-	

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.

🔶 🛔 10.0						C Q, Sranh	会員		4 9 8
🔏 Mest Visited 🧕 Getting Startes		Y yahao	G Google G	Gwait				_	
						-		About Us Discla	imer Contact Us
Hanne Accentth Transfers III	Percenter For	smeals Te	ade Services	narrany Collect	ines iTee	away Securities Backet FSCH Offic	er Services	Desenants IN	Laboratori Li sufe
Daich Links	Harry L.	and write a Closery	the Assessments in	Get Bistements		and a second sec			
Approvals									
Billing Statements	Select at	Account and O	ption from the i	drop down lists.					
Accounts	Au	ourt Number			SOLUTION	5- +			
Operative Accounts	Cap	tions		Get Today's Tran	sactions		ta a l		
Deposit Accounts									
Loan Accounts					_	Statement Criteria			
External Accounts					_				
Tax Deduction Inquiry					From 0	1-01-2016 To 01-01-2016			
Account Statement By Email	Transac	tions Made [D	etails till 01-	01-2016 3:57144 PM	To get a c	wher receipt of the transaction, please click	k on Transa	tion Amount	
Service Requests	Sr.No.	Transaction	Value Date	Txn Posted Date	Cheque	Description	67/07	Transaction	Available
Term Laen Account	1	10	01-01-3016	05-01-2016 3-47-27 PM	Mor.	TRFR FROM	CR	3,22,545.00	8,45,429,46
	2		01-01-2016	00-01-2016 3-10-13 PM	11004287		DR	2.74.210.00	5,22,944.46
	3		01-01-2016	00-00-2006 2-57-54 PM	189921		DR.	1.67,280.00	7,97,154,46
	4		01-01-3016	00-00-2006 2:56:58 PM	189922		DR.	1.92.163.00	9,64,434.46
	5		01-01-2016	05-05-2016 2:55:00 PM	189526		DR.	5.35.641.00	11,56,597.46
	6		01-01-2016	01-01-2016 2:53:51 PM	189525		DA.	4.04.504.00	16,92,238.46
	7		81-01-2916	00-01-2016 2:41:36 PM	11005377	COTTON CO	DR.	2.44.610.00	21.76,742.46
			01-01-2016	00-00-2006 2:39:25 PM	11004289	STORAGE PV	DR.	2.78.000.00	24,31,352.46
							-		

Figure 26 - Corporate banking account

						anking insta	Alerts SMS	Banking Registratio	on Contact Us
	Log M. Dec 1	8 2915 4 27 PM. IST				Change Pa	seword Upda	te Contact Details	Logout
	ocounts	Funds Transfer	BillPay & Recha	rge Carda	Demat M	dual Fun	d Insura	nce Loans	Offers
ccounts	View / De	ownload Ac	count State	ment				Pin	t This Page
nancial Summary					_				
count Summary	Current Ac	count No.:	S						
	[Select Anot	her Account / Peri	2011			C	Page -	1 of 1	16 467 58
ansact 🕨	1					C.	oung bara	100. Hart - 0,1	
quire 🔻	Date	Narration		Cheque/Ref. /	io. Value	Date N	Withdrawal	Deposit	Closing Balance
	18 Dec 2015			00000057418	3 19 De	c 2015		642,253.00	-9,736,457
ew Account Balance	u								
ew / Download Account atement	18 Dec 2015	3	OLUTIONS-	_	18 De	c 2015		144,150.00	-10,378,720.5
ownload Historical atement	18 Dec 2016	INTERNET		20020202020	0 10.00	- 2016	101 412 00		-10.622.820
	18 045 2015	ENTERPRISES		0000000000	10.04	02010	101,412.00		-10,022,010.
xed Deposit Summary									
acumina Danasit Rummanu				and Condi	tions Privacy Po	kay			

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 nothing 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.

	of the local division of the local divisiono	inbox	- archive - Microsoft Outlook	
me Send / Receive	Folder View			
Crean Up - Delete	Reply Revend Report	Annove to: 1 Consection 1 Conse	v Move Rules On Move	eliete Unerad/ Categorite Tollow Read Tags Prid a Caretat *
nvorite Folders Here 4	Search All Mail Bens (Chrl+E)		م	A320 for ACMI
	Arrange By: Date		Newest on tap	Aeronautical Information Services sais@kraa.or.ke>
1007)				Sent: 0410.2015 9:41
	* Testersay			Tei Cienfo-d
i Items (26)	invoisi/118		- UA-	Message aJJ0 for ACMEace (604 KE)
A320 for ACMLace -	WinRAR (evaluation copy)			Per Manha
File Commands To	ols Favorites Options Help			
Add Edect To	Test View Delete Find	Ward Info VirusScan		
A329 for /	ACMLace - solid ACE archive, unpacked	size 644 096 bytes		
Name	-	ize Packed Type	Modified CRC32	
a		File folder		
Ill invoice document e	se 644 (96 618.440 Application	29.09.2015 15:42 F59387F4	

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.	
Civil Aviation Au Tel: - Fax: Mobile: Email:	Officer (in charge of ICAO documentation) Air Transport Economic Regulations and Foreign Relations Department thority

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.

-	De -	info@
Envoyer	À	
LIIVOYEI	Cc	
	Objet	Confirmation
Récej	ption	u votre confirmation
Réception	nniste/Fro	nt Desk Agent
info@		
info@		
info@ Téléphor	ne:	// Télécopie: // Sans frais

Figure 41 - Infected receptionist

_	То		
1 - 1	Cc		
Jena	Subject		
plaara	i		
please	1		
Should	you have	any questions, please do not hesitate to contact me directly	
Kindes	t regards		
Reserv	vations		
_		C KB	
	Hotel	& Golf Resort	
_			
T:			
E: rese	rvations		
W: WI	ww.	com	

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.

eservations Grou	ips Front Office/C	ashier PDA Housekeepir	ig night Audit Cit	y Leager/Acctg Reports	GM Functions	menu Optio
Guest Name Lis	t - Expected Depart	tures			-	
Conf #134165	Level Membe	r Ø				
Local Conf # 134 Status IN-P Folio #	165 📎	Host Conf # Stay Dates 01/02/16 Folio Balance \$0.00	- 01/03/16 Room	n Nbr 111 OrC	First Night S116 Room Taxes S21 Total S13	50 8.49
C 1 BLOK					Stays	∇
Arrive 01/02	216 Set Nig	hts Depart 01/03/1	6 Sun Adults	2 Child O/U 0 0	New	Confirmati
Rate Code	··· Rm Typ	pe Rate \$11	6.99 Rm 1	abr 111 - Assign	New Stay	Reg Car
Name (L/F)		Title	Source W 7	Mkt Seg Loisir	Сору	Eolio
					Change	Message
Profile				Group	New Share	Ost Look
Pay By		Exp	Cr Limit \$200.00	Auth Code	Services	Check }
Deposit \$0.00	Due By	Amt Received	Reque	st By ×	Chg Royte	Cancel B
Info				: <u>@</u>	Other Name	
uest Address	Business Address	Agent Rates Profiles	ETA / ETD Res Hist	ory Traces ID / License	Sell a Plug	
Address		Phone		Do Not Rent	BWR Lookup	Søge
(m)	_	Fax				
State/Prov	Country	- Comments	-0		Corp Lookup	
Postal		On			Authorize	Close

Figure 43 - Guest booking at a hotel

Room As Call Date		/ / An Otto	Amg 0 F.Roome 0	0
ROOM Made Updated Completed	Inc.8 Rec.8 Rec.8 Care 8 Address Via, Maded	Balance Renails -3677236 -307312	STANDARD STANDARD STANDARD	Signature IAC LAN
Asival 05/01/2016 Sat Abx.8 Nghts 1 Check.in 7	Pace Detail Anendrawits User	000 000 142945-00	STANDARD STANDARD STANDARD	LAR
Clent Type PERSON ·	Alet Of5 Souce	0.06 0.00 0.00	STANDARO STANDARO STANDARO	LAR LAR LAR
AgencyName	Card Number Espin(M/Y) /	0.00 42.70 0.00	STANDARO STANDARO STANDARO	LAR LAR LAR
Guest(1)	Ced Ced	55.00 -195.00 -432.00 	STANDARD STANDARD STANDARD	AMF LAR AMD
Guert (2) Adults 2 Rosen Type DBL2P Children Rosen No.	8 8 8	115:00 0:00 137:00	STANDARD STANDARD STANDARD	AMF NAT NAT
Special Lock Room N Shahus CDMF01HED		600 POS Trander	STANDARD	008

Figure 44 - Guest credit card information

tay Info Cuest Info Quarantee Info CRS Notes	Guest Name:
EDIT GUARANTEE INFORMATION	Group Master: Account Number: Balance: 0.00
Guarantee: CC	
Market: Unknown	Actions
Caller Name:	Back
Guest Tracking: Unknown	Guest Folio Check In
Card Type:	Recurring Charges Change Stay
Card Number:	E-mail Confirm
Expiration:	View Changes
Name on Card:	Cancel Reservation
Card Billing Address:	Print Registration Card Print Confirmation Letter
Card Billing Postal Code:	

Figure 45 - Another guest credit card



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.

2 PORTAL								
Records	Found (Unsorted)	Show All New R	econd D	elete Record	Gan - 🔛		Q.	
Layout: DiQuat	Vew As: =	III Preview						A1 EditLayout
😤 PORTAL	INQUIRIES	FAMILIES	C	ONTACTS			Mare 🛡 🕐 🕐	•
Main List					New BROADCA	Lists/Forms Label	s Letters Reports	
LIST								
Student First Last St	udent Last First	Sex CHP GD F S	Sec G	PE House	Phone	Nationality Exit Year Vietnam	Exit Grade Leaving Date	Status
+		M 3	8	3		Vietnam		Enrolled
+		M 5				Vietnam		Closed
+		F 6				Vietnam		Inquired
+		F 6				Vietnam		Closed
+		М 3				Vietnam		Closed
+		F 1				Vietnam		Closed
+		M 1				Vietnam		Inquired
+		M 4				Vietnam		Inquired
+		F 7				Vietnam		Inquired
+		M 5				Vietnam		Closed
+		F 5	C	5		Vietnam		Enrolled
+		F 6	D	5		Vietnam		Enrolled
+		F 12				Vietnam		Inquired
+		M KG				Vietnam		Closed
+		M 6				Vietnam		Applied
+		M 9				Vietnam		Inquired
+		M 6				Vietnam		Applied
+		M EE2				Vietnam		Closed
+		M 5			_	Vietnam		Inquired
+		M 6				Vietnam		Applied
+		F 2				Vietnam		Inquired

Figure 49 - Student list

👔 PORTAL										
	Records	Found (Unsorted)	Show All New R	econd Delete Record	G - M				<u>Q.</u>	
Layouts [INQUERIES		View As:	neview							A1 EditLayout
🔗 POR	TAL	INQUIRIES	FAMILIES	CONTACT	s					More 💌 🗇 🕐
Main List						🕈 New Bi	OADCAST I	ists/Form	s Labels	Letters Reports
Student	()	M	2015-2016 YOE		-			Parent 1	Applied ACTIVE
OVERVIEW	PARENTS	INTERVIEW	APP/DECISION	FINANCIAL AID	TESTING	RECEPTIONS	CONTACT	LOG	DOCUMENTS	ENROLLMENT
Date	Source		Title					+ N	ow File	
16/11/2015	PWS		applicant_med	dical_report_uploa	d		Edit Vie	s Sav	🗶 🗅	
16/11/2015	PWS		applicant_pas	sport_birthcert_u	pload		Edit Vie	e Save	h 🗶	
16/11/2015	PWS		Letter of reco	mmendation			Edit Vie	e Save	X	
16/11/2015	PWS		Document in F	lussian			Edit Vie	e Save	s 🗶	
16/11/2015	PWS		Birth certificat	te			Edit Vie	* Sav	X	
16/11/2015	PWS		applicant_vac	cination_booklet_	upload		Edit Vie	e Save	X	
16/11/2015	PWS		APPLICATION				Edit Vie	s Sav	X	
16/11/2015	PWS		Photo				Edit Vie	s Save	s 🗶	
17/11/2015	PORTAL		Medical Test	& vaccination Rec	ord		Edit Vie	e Sav	🗶	

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

Miscreant 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 miscreant 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.

Tirelos *						- 0	×
Factor Content of Cont	Exclara Veb Panel	Value - logi	n x 🚺 Outlook.com - s x 🗍 A	Pick Up Your Em. × C. Whoer.net - find .	× 🖉 Roundcabe Web ×	🔾 (1) Roundcube W	× 4
🔶 🛪 💶 taylar 🕹 🚛	_			<u>Ω</u> ≠α	- Geopir	۶ 🕈	∎-
		Explorer 7.0 - 9.0	/servicelogin			20:	^
	COMPUTER.PC	Firefox 3.5-31	https://keybase.io			20 22:	
	COMPUTER-PC	Thunderbird	imap.gmail.com	Øgmail.com		20 22:	
	COMPUTER-PC	internet Explorer 7.0 - 9.0	https://accounts.google.com /servicelogin	-		20 22	ł
	COMPUTER-PC	Firefox 3.5-31	https://accounts.google.com			20 22:	
	COMPUTER-PC	Firefox 3.5-31	https://www.facebook.com	_		20 22	
	COMPUTER-PC	MS Outlook 2002/2003 /2007/2010	mail1-com.me			20 10:	
	DAIL.	Outlook 2013	mail mail gov at	helpdesk. Brnail.gov.af		20 08	
	DAR.	Chrome	https://en-gb.facebook.com/login	Øgmail.com	_	20 08:	
	DAR.	Chrome	https://www.facebook.com/	Øgmail.com		20 08:	
	DAIL	internet	https://www.facebook.com/	Pgmail.com		20	~

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.

razorscani	er.com/result.php?id=9	01259		△ G.	Q, Search	21	9 0	+	Ħ
SCAN	KevBase v1.5 - Reta	- Cracked by blaz	ed - sulled io						
	Did you setup KeyPane	•7							
	Link to KeyPanel:	http://edvolution	.ca/keybase/	Test Connection					
	General Config	Appearance	Properties	Extensions					
	Scanner	Clean	News	Support	ame: base exe 105 Hash: 2erl200c/Shb7408	v:31574316			
BKav					HA1: fbc0da1377b4debb5f		78b614eb		
	Scan with 60 popul	ar anti-irus							
	C:\Document	s and Settings\Adn	nine Choose File	Scan					
	Anti-Virus		Detection Status	^					
	Agnitum		OK						
	Baidu								
PS8 Ant	Bkav								
	Escan			and the second					
	ETrust-Vet								
	Eset								
	Fortinet								
nProtec	Fsb			v					
	¢ .		(2					
	Result: 2/24	Scan result: http://							
Orana	nesus area	stan result. (http://							

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.

Annetaisconcordia.com.br	x Q, Innech 🖄 🖄 🐨 🕹 🖨 🔿 X Special (eff 1)	P 1
Stype" -		
Skype Contacts Conversation Call Yew Too	ols Help	
TOU SHALL NOT LABOR BY WAY	🙆 🖗 Hale not that the Intellie cause. "The more you labe 2.52 AM lagors, No 💿 🕓 🖄	
ebeek Q Search	tate B	
transfer and the second	nuno regiono, pasel monita	-
CONTACTS RECENT	assistant export department. Tel: +658 8379 2524	
M	de 19t massag go dey 4 subject	
faces 🦛 moving forward	okay the first one 230 AM	
Echo / Sound Test Service		
	confirm your bank details 2-31 AM	
One as do not fear the hustle cause "Th	skey thanks	
	what will be the attachement name?	
	same with subject?	
	a line in the line line	
on Vis hipeople		

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.

A line of		
And a series of the series of	C C C Document - WordPad	A 185-28-59
	E Vest	👻 - Lee 🙂 Lee
suadauba 🎱	1 4 Called - 10 - 14 6 (R (0 - 10 - 12 - 12 - 12 - 12 - 12 - 12 - 1	ð same
DOUDCODE	Barte B / U da X X 2 - A- B = E E R Peters Part Dirend Inet	
4 7 12		10000
Cancel Seve	-1	
and and a second		
	international and a second and as	
۹,	hyphos.co.in, into phillipping, com, purtomenienvice phillipping	
Fersonal Addresses	sales@ com.sp com	apl.com,
	com, com,	
	2000, 20000, 2000, 2000, 2000, 2000, 2000, 2000, 2000, 2000, 2000, 2000,	
	core, salesenquiriesd? core, corporated core,	
	SALES(D) COM, AU, COM, AU, COM, COM, COM, COM, COM, COM, COM, COM	
	sales@ pr.ca. con.au, webmaster vs.	
	come information and a state	
	net, con, into con,	
	.com, sales, com, com,	
	yahoo.com, and sol.com, and s	9
	MMS @ @	

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 emails.

I	🗅 KeyBase Web Panel	X 🔁 SmarterMail Login -	도× 🕻 🌞 네이트 레일 👘	X B Keyßase Web Panel	× C Lite14 Email Extract	X S list of korean female	× W List of the most pop: ×
1		s://en.wikipedia.org/wi	ki/List_of_the_most_p	opular_given_names_in_So	uth_Korea		
	Daisted changes	7 1960					

Figure 62 - Actor performing research for phishing lure

→ C _ mail3com/	#write/?act=new							
- 41	4 9 401.844	▓ 네이트운든자	<u>•</u> 493.8744				[뉴스] 문의 "무슨도것' 방법은 법	284 89 51425 (548)
۵	Mail letter							
메일프기 내게쓰기	+Send Preview	Temporary sa	we Importautomat	ically saved m	ai			
Riferal should read 27%		info@	com H		.00	m X ho	tmail.com ×	- book
	title	Outstanding	invoices					
e Inbox	Attachments	Attached Res (Close					
Malboves wrote to	파일정부 내었유던	×150					리는 1 개 동안 0,00 KB / 10	40 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Sert Hal		188		82	88 利月	음부 방식	다용로드 유효거간	
Advoviedgement	inveice.st			505,50K8	UPC .	대용형원부	2015/12/21-2015/12/28	
Hymalbox + (e)								
의일배구_2014 275								
일주.								
티사경력서								
Bills must 💿			a. a					B 4 87
Do shopping	48 . 1	N - M - M			1 4 4 9	IN F F A		a c. Ev
SNS Do	Dear sir.							
IMPORTANT Fierd								
() attachments	We will like to	clear our Outsta	nding invoice for	this month	and we have	e forwarded our	unpaid invoice to our finance d	epartment for
Subscribe to content	Please reply us	By find the attact in time to enable	le us proceed the	payment b	ntirm if we s y tomorrow	hould pay for inv	oice 8786 or Invoice 9292	

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.

8	Skype ^{ne} [2] -	- • ×
Skype Contacts Conversation Call View Tools Help		
	API * R appears you're using BhStack.exe with Skype. To see how 3rd party applicat with Skype, please see our FAQs.	lions work (*)
olgan1206		
Q Search	• "I guarantee I'll be the greatest thing you ever had"	U 🕑
🕈 Home 👎 Call 🕂 New		^
CONTACTS RECENT 2 AIL -	account?	
Tedav		
.	1 account is 50\$ the 21 will pay 100\$	6:47 PM
	🚱 🛛 alright	647 PM
Wednesday	gimme one account info, all info u know	
2	ok	6:47 PM
nem =01962 Super Omegas @Sciper bottiejtem =01426		
The second se	in this new drings over will be free	6047 PM
Saturday	Skype name: email:	6-49 PM
• —		*
	via Skype + Sand SMS from Skype	
Older than a week		-
Ertheine today		

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.

← → C □ www.samair.nu/proxy/time-01.htm					12
👫 Apps 🗋 Hepsibahis108.com 🧧 🗋 🗋 servey romve	r				
FREE PROXY LIST				PROXY LISTS	
P.address	Anonymity level	Checked time	Country	HTTP Prov Lists	-
116.242.227.201.3	128	prox	es1 - Notepad	. 0 .	
113.4.156.73.3128	File Edit Format View	Help			
1 (19.2.23, 340, 350) 2010, 127, 154, 156, 3 1111, 13, 22, 354, 1 122, 224, 3 (19.10) 127, 254, 3 (19.10) 137, 752, 3 (19.10) 137, 752, 3 (19.10) 139, 156, 202, 3 (19.10) 139, 156, 202, 3 (19.10) 149, 156, 202, 3 (19.10) 122, 203, 6 (19.10) 122, 203, 6 (19.10) 122, 203, 6 (19.10) 122, 203, 6 (19.10) 123, 203, 203, 203, 203, 203, 203, 203, 2	131.3.122.262.27.2011312 222.14.3.10:1000 131.4.15.7.313120 200.127.16.159.512 131.3.3.12.216.100 149.302.121.313.122 157.7.53.106.1000 06.9.9.125.1351100 169.302.121.313.132 157.7.53.106.1000 06.9.9.125.1351100 117.494.61.21.313.132 22.66.202110 122.46.4.1316116 122.46.4.3161110 122.46.4.3161110 122.46.4.3161110 122.46.4.3161110 122.46.4.3161110 122.46.59.102110 122.46.20.2110 137.44.211.77.155120 139.342.2121 (**********************************	8 8 8 8 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	15:48 Iran, Isla 15:40 China 15:40 Brazil 15:49 United Stat 15:49 China China	aic Republic of tes ∵	

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"

Opera	f	Facebook X	ATN - Card The W	lorld - Sr. X . Meine Bestellungen	X 👂 PayPali Wallet	N O Kaufeb	nicklung		× 🏠 🛬 🖃 🖻
•	C	₩ 🗐 alteren.com/s	usarch.php						
	44 R.*			a a ALS	EN EN				Ö
			Uner (P	NQ Connexity Calardar		ah bagi	~		
2	Sec	Card The World > Search f inch Results	foruma						Welcomer, You last visited: Yesterday at 06:39 PH Private Messages: Unvead 0, Total 1.
				Undel links : Recover password	Advertising in ATN	Upgrade To VIP			
									Nege10720 1 2 3 11 > Last = 2
Sear	chc I	tew Posta							Showing results 1 to 25 of 500 Search took 0.07 seconds.
		Thread / Thread Starter				Last Post	Replet	Veres	forum
		 as or high balance sytin/boy 				Today 02:35 PH by like 🖷			Accounts and Database Dumps
6	۰	live fresh cvv ekserry1				Today 02:35 PH by beni			Accounts and Database Dumps
6		I buy valid USA cc () TungNigge	# 1 2 3 Lett Page)			Today 02:35 PM by Gescator667			1 Buy
		 Selling Uber Account Zembbs 	et (# 1 2)			Today 02:34 PH by Zambitx =			1 Sell Open Source
		Codell				Today 02:34 PH by beni			Accounts and Database Dumps
		live cvv pls kill				Teday 02:34 PH			Accounts and Database Dumos

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.

← ⇒ C	chrome://dov	wnloads		
Downloads				
Today Nov 14, 2015	BruteF http:// Show	Forcer_091.7z //gsf-cf.softonic.com/8a3/6c7/2 /in folder Remove from list	Connection:	Ck
Yesterday Nov 13, 2015	PayPa https:/ Show	Il BruteChecker by egorea1999 //zima124e.storage.yandex.ne in folder Remove from list	Usemane: Usemane	Speed: 0 comb/s Threads: 2
	ORIGI https:/	IN BRUTE [CrackingFist.enjin.co ://zima43g.storage.yandex.net/	Wordlist attack level: 3	Plugin: Not selected
	Paypa https/ Show	In Tolder Remove from list Il Brute Checker v1.0 (1).rar I//169807b-a-62cb3a1a-s-site in folder Remove from list	Priority: Normal Mtp:/tbrute/lover.source/lorge.net/	Pause Connect
	PayPa https:/ Show	Il Brute And Checker v1.0.rar ://32eab26b-a-62cb3a1a-s-site : in folder Remove from list	s.googlegroups.com/site/connecttrojan7/P	ayPal%20Brut
	Paypa https:/ Show	al Brute Checker v1.0.rar ://1169807b-a-62cb3a1a-s-site i in folder Remove from list	s.googlegroups.com/site/downloadarkivo7/	/Paypal%208r
	PayPa https:/ Show	il Brute Checker.rar ://fs09n5.sendspace.com/dl/15 i in folder Remove from list	4334c1f8a046e8e628569d103bf988/564620	06641df315e/
	BitGo blob:h Show	Keycard for http://www.bitgo.com/i in folder Remove from list		
	downl datair	iload.png mage/png;base64,iVBORw0KG	goAAAANSUhEUgAAAMgAAADICAYAAAC	WK6eAAAUE

Figure 73 - Downloading PayPal brute forcers

hav		itre Mein
Day	✓ Lieferadresse	> Zahlungsmethode > Kaufen und zah
Zahlungsmethode auswählen	Part Part	Zusammenfassung
* PayPal		Zwischensumme (1 Artikel) EUR 40,78
Loggen Sie sich ein oder eröffnen Sie ein kostenloses	Bei PavPal einloggen	Versand Kostenios
	@20email.eu	Gesamt EUR 40,78
Lastschrift	Dieses PayPal-Kanto merkan und bei eBay schweller	
Kreditkarte	zahlen Weitere Informationen	
	Einlogen	
Leferadresse (Andem)	Passwort vergessen?	

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

h		html - root@8	2.211 WinSCP			
Local Mark Files Corry	mands Session Options Remot	e Help				
🐺 📴 🕞 Sunchronize	🖬 🧈 💌 100 🖾 000	nue + Transfer Settings Default				
anot@82.211	New Service	in the second second				
C. Louis Tech		0.0	I Bateri		B End Eler	0
C LOCH DICK					in restricts	-0
🗐 Upload 🎯 🖉 Edit	🗶 🛒 🖓 Properties 📑 👔	I 🕀 🖂 🕅	Download 🙀 😥	" Edit 🗶 🚮 🖓 Properties 📑 👔 🛛		
C/Users/			/vat/www/html			
Name	Size Type	Changed	Name	Size Changed	Rights	Owner
s -	Parent directory	11/19/2015 5:20:29 PM	.	8/24/2015 7:53:47 PM	PAOP-NP-X	root
android	File folder	8/13/2015 2:58:34 AM	keybase	11/15/2015 7:28-48 AM	rwsrwsrwt	root
eclipse	File folder	10/26/2015 7:02:53 PM	- Long and a			
JdealC14	File folder	8/13/2015 2:58-02 AM				
idlerc	File folder	11/11/2015 10:08:15 PM				
.oracle_jre_usage	File folder	9/19/2015 11:03:23 PM				
.vega	File folder	10/17/2015 12:36:34 AM				
.VirtualBox	File folder	9/21/2015 12:27:53 PM				
Contacts	File folder	11/14/2015 63419 AM				
Desktop	File	11/19/2015 6:34:11 PM				
Documents	System Folder	11/15/2015 7:53:21 PM				
Downloads	System Folder	11/19/2015 10:44:59 PM				
Favorites	File folder	11/14/2015 634.19 AM				
ldeaProjects	File folder	8/13/2015 2:59:11 AM				
Links	File folder	11/14/2015 6:34:19 AM				
Music .	System Folder	11/14/2015 634:19 AM				
Pictures	System Folder	11/14/2015 6:34:19 AM				
Saved Games	File folder	11/14/2015 6:34:19 AM				
Searches	File folder	11/14/2015 634:19 AM				
Wideos 1	System Folder	11/14/2015 6:34:19 AM				
VirtualBox VMs	File folder	9/21/2015 12:10:55 PM				

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.

SeniorPeopleMeet.com - ⊺ ×	
← → X 🗋 www.seniorpe	eoplemeet.com/v3/profile/todaysmatches#tab=a
SeniorPeopleMeet	A Home 🛛 🔤 Inbox 💷 🖓 Search 💴
Inbox Messages 9 NEW Connections	Today's 2nd Match Is PETITE92021 a possible Match? You think so! You sai Say hello and share what you like about PETITE92021's
 Viewed Me Fave'd Me Flirted With Me Liked My Photo Today's Matches 	I'd love to know more about you
- I rouay s Matches	Show m

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.

File Edit Format View Help
📕, I want you to in
CFO CEO
Tel: http://www.

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

www.ceoen	nail.com/australia-newze	ealand-com	panies.php	
	Hutchison Australia, VHA)	Australia	Morrow, Chief Executive	Australi
	Vodafone New Zealand	New Zealand	Mr Russell Stanners, Chief Executive (Bio of Mr Russell Stanners)	Website New Ze Svodaf Zealanc address
	Wesfarmers	Australia		
	Westfield Group	Australia	Steven Lowy, Chief Executive	Website Group
	Westpac Banking	Australia	Mr Brian Hartzer, Chief Executive (Bio of Mr Brian	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.

G bigrock - Google Search X 5 GoDad	Hyzom : Shapping X MigRock - Ro 39.00	M D= *		÷ 3
🖗 India - English v 🛛 INR v		25/	7 Support 040-49187600 Help	🛓 Sign In v 👋 Checkout Now
Godaddy Al Produc	te Domaine Websites Hosting	Web Security Online Man	teting Email & Office	Coupons GoDaddy Pro
0				
Cart	illing & Payment Place Your Orde	r Thank You		
Ø Promotion has	been applied to your cart!		×	
Product	Term	Pending update 1	Subtotal Total cost	24.6
www	getwebsolutions.com 2 Years COM Domain Registration	✓ Rs 99.00/yr	Ra 678.00 SRemove	Inte
	Plus ICANIN Ree of Rs 12 30/yr	Rs 689.00/yr	ICANN Fees*	R: 24.00
		2+ years		Rs 702.00
Protect your period	unal information. ()		Total savings	Rs 1,240.00
Keep my perso Make my dom	nal info public sin private for Rs 289.50/yr1 SAVE Rs 3	89.501	Procee	d to Checkout >

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

Office 365					
Set up domain	Owayne	Doughte	Dwayne@getwebsolutionn.com	8-12-15 Outlook 1	ld's - Notepad 💿 🗵 🗮
	Guadalupe	Fausto	Guadalupe@getwebsolutionn.co	File Edit Format Brian@prian541 Brian@petwebso BurtiPortwebso10	View Help ,onmicrosoft.com Jutionn.com
	Ismael	Grubaugh	Ismael@getwebsolutionn.com	BroadkaterØgetvebs DkayneØgetvebs GuadalupeØgetwe IsmaelØgetwebs	websolutionn.com olutionn.com ebsolutionn.com olutionn.com
	Jonah	Southard	Jonah@getwebsolutionn.com	Jonah@getwebso Kelvin@getwebs Renaldobgetwebs Sydneydgetwebs	lution.com olution.com solution.com olution.com
	Kelvin	Dedeaux	Kelvin@getwebsolutionn.com	roanget account	
	Renaldo	Casarez	Renaldo@getwebsolutionn.com		
	Sydney	Mumm	Sydney@getwebsolutionn.com	Jaw06287	Business Premium
	Tuan	Nale	Tuan@getwebsolutionn.com	Yumu9083	Office 365 Business Premium
					-

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.

Copeta & Mail-But Bening X + + C IF e outlookg	🔮 Mail - Burt Berning 🛛 🖌 🔮 Mail - Burt Ber Micel 65.com//wwa/	ning 🗶 📓 Mai	-Bathening H 📓 Mal-Bathening H 📓 Mal-Bathening H 🛔 Mal-Bathening H 🛊 🛒 🔤 🔤 🔤
III Office 365 C	Jutlook		🔺 o 📌 💭
Search Mail and People 👂			🕾 Send 🔋 Attach 🌘 Add-ins Discard 🚥
 ► Folders Internet Services Services Services Services Groups intergreeping or create on groups or create on groups There is groups Create groups 	Inbox :-) We don't find anything to show here.	Al v	Image: Second

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.

C fi https://docs.google.com/spreadsl	weets/d/		ledit#gid=0	
Domain Details 🕆 📾 File Edit View Inset Format Data Tools A	dd-ons Help Last edit was 3 hours ago			Comments 🚊 the
65 77 1 5 4 4 W. AN	· · · · · · · · · · · · · · · · · · ·	⊞ • 101 • ■ • ± • H	· • ■ 🗐 🖓 · Σ ·	
getvebdonee.com				
A		6	0	6
creati-ewebdone.com		abc 1234@#	3/11/2015	Mb./manage.biprock.in/tustomer
quality webcreation.net		abc 1234@#	5/11/2015	Mp.ithanage.bigrock.in/Lustomer
developmentsolutionss.com		abc 1234@#	7/11/2015	Mpulmanage bigrock incustomer
createonlinepresence net		abc 1231@#	10/11/2015	Mbuitmanage bigrock in/customer
makesitevithus.com		abc 1231@#	13/11/15	http://manage.bigrock.in/customer
quality websolutionss.com		abi 1235@#	16/11/15	Mpultnanage bigrock intrustorier
getinstantivebsolutions net		abc 1234@#	19/11/15	http://manage.bigrock.in/customer
fastvebsolutionss net		abc 1234@#	20/11/16	Mbuitmanage bigrock in/cuetomer
getfantastic websolution.net		abc 1231@#	25/11/15	http://tranage.bigrock.in/customer
projectbasevebsolution net		abc 1235@#	27/11/16	Mpulhanage bigrock intrustorier
get quality solutions.com		abc 1234@#	30/11/15	http://manage.bigrock.in/customer
creati-evebdonee.com		abc 1234@#	1/12/2015	Mbuitmanage bigrock in/cuetomer
createy survebdone.com		abc 1234@#	2/13/3015	Mbultnanage.bigrock.in/tustomer
createy purvebpresence.com		abc 1234@#	3/12/2015	Mpulmanage bigrock initiationer
patfullwebservices.net		abc 1235@#	4/12/2015	Mb.imanage.bigrock.in/cueloner
petwebsolutions.com		abc 1235@#	8/12/2015	Mp.imanage.bigrock.in/tustomer
getwebdonee.com		abc 1234@#	9/12/2015	Mp.ihnanage.bigrock.in/tueloner
expertivebsolutionn.com		abc 1234@#	10/12/2015	Mpulmanage bigrock in/customer
bestwebsolutions com		abc 1234@#	10/12/2015	Mb ilmanage bigrock in/cuelomer
webexpertsolutions.com		abc 1234@#	16/12/2015	Mp.itnanage.bigrock.in/Lustomer
getspecialweboffer.com		abc 1234@#	19/12/2015	Mp ilmanage bigrock in/customer
getwebdonweithoffer.com		abc 1234@#	21/12/2015	http://manage.bigrock.in/customer

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.

Primary	12 Social Promotions Image App +	
*	Re: User Friendly Website With Affordable Price My web is in spanish! Your mail, in english! What can you d	o? 5:56 pm
• *	Re: Hey, Full-Service Website Design + Development, Or	n na hann an tha sa sa
•	Re: Hello, Are you looking for a creative web development sol	
•	Re: Are you looking for New Website Design or Developments. Leads on 14/12/2015	
• *	Re: Hello, Are you interested in making your web presence?? Hello Sir,	
•	Re: GreetingsComplete-Service Website Design + Developm	
• *	Re: Full-Service Website Design + Development, Online Adver Total : 14	
• *	RE: Hello,Are you looking for Full Web Development + Desig Thanks	
• *	Re: Hello Are you looking for Full Web Development + Desig	
• *	Re: Create & Build Design & Development Solutions For Your	
	Re: H.,Full-Service Website Design + Development, Online A	
• *	Re: Hello,. Are you looking for a #1 Professionals to create you	
• *	Re: Hello,May i help you in your Online Business Developme 🛛 🔬 🖄 🚳 🕫 🛞	1

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.

					_					
e Dutitled - Notepad									- 🗆 ×	
File Edit Format View Help										
<pre><!DOCTYPE html PUBLIC "-//W3C/// <html xmlns="http://www.w3.org/ cheads</pre> </pre>	Advanced Mass Ser	nder 4.3	Registere	d to: bobyMasele	n (2) m]	(Press F1 fc	viven11 /nmn/viven ar Help)		28].(<u>s</u>	
meta http-equiv="Content-Type"	Addroenal settings Sender accounts Tools Help									
<pre><title>Untitled Document</title></pre>	Smip Servers(s)		Built-In Swip Relay		7	Fioni account	•			
style2 (Name	Part	UsedD	CC/9CC Size		AN	То днир:			
font-family: "Courier N	193.104.83.254	25	User	50		Benovel	blessing	-		
color: #333333; foot-weight: bold:	193.104.83.254	25	Uper	50		Modify	Send Matheat			
font-size: 13px;	193.104.83.254	25	User	50	-	(Case Al.	Send Method (DCC			
}	Line in an art	10	11		-	100000	To (For BCC)			
	Subject .				_		Maling	List		
	Massage Bods:						HTML Messe	ges Editor		
<pre>chody> cdtv><ing src="http://www.techv cdtv><ing />cdv></pre> cdtv</pre> cdtv</pre> cdtv</pre> cdtv</pre> cdtv</pre> cdtv</pre> class=" style2"=""> cdtv</ing></pre> cdtv class="style2"> cdtv cdtv class="style2"> cdtv cdtv class="style2"> cdtv class="style2"> cdtv cdtv class="style2"> cdtv cdtv class="style2"> cdtv class="style2"> cdtv cdtv class="style2" cdtv cdtv	cdiv>ctmg1sic="http://www.techvest.com/assets/images/Linkeds_Logs_small.png_at="#"width="35" beig_it_c/div cdiv>ctm />cc/div cdiv <ctms:="style2"> cdiv cdiv</ctms:="style2">									
	(/body) (/basis									
synams								•		
	4									
	Hessages History:						Clear History	Clear Message		
×	Atachments C-MJsers/Administrator/Downloads/Heport [1].doe Add Plan Ted Pla									
	1						Windows-1251			
	Load Message Body	Save Me	osage Body		_	_	Send			
	About							Ext		

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.

ribox in Moreadit Outrapie		0.0
Ar Edit View Go Ioels Actions Help		Type a question for help
)Bev • 🤀 🦉 🗙 😘 Baply (@Raplyto All (&Forgant) 🔡 🔻 🖓 Sandillagaine • 🍅 🔛	Search address books 🔹 📦 👔	
Spam 🖄 Not spam 🖉 Spam address 🧟 Trusted address 🛛 ESET Smart Security • 🔜 👷		
ail 💦 🙀 Inbex New D	archase Order 30/08/2015	Te-De Bar 😕
onte Fotten	0.0	September 2013
Palese File Commands Tools Favorites Options Help		Su Ma Tu We Th Fr 1
Station and the state of the st	<u>0</u>	67 8 9 10 11 1
rollen	The second secon	20 21 22 22 28 25 2
A Mail Bens	Tracket	27 28 29 30 1 2
Personal Polder		
Coaffie Name O Size Packed Type Modified	0032	
💯 intes 🔒 . Folder		
Application 5/25/2023	1804 GAFASED	
RSS Feeds		No upcoming appointme
Sent Bens		
Up Search Fuller		
Deleted Bee		
inter (N		Arranged By: Due Date
a shecke been		Type a new task
Outlese		These are no demo to
Seed Bens	BEED SMART MICHIEV &	of the party of th
	A Threat found	
	Threat found in mer	manya
Caterolar	Objects	
Contacts	Operating memoly/ Threat	· Replan.exe(1148)
Lid HD Selected 1,800,508 bytes in 1 file	Total 1, BB(OLB bytes in 1 Ne a variant of hEil, (b)	ector.RLH trojan
New Purchase Order 20.06.2015	Information channel - contained	inhered files
🖌 🖓 🗋 🔛 WAYN Holdes 🔰 🖉 🖬		*

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 <u>KeyBase command and</u> <u>control traffic signature</u>. AutoFocus users can identify KeyBase samples using the <u>KeyBase</u> 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 Iniquiry Re: Purchase Order Iniqury for Your Kind Attention Re: Purchase Order Inquiry Re: Purchase Order Inquiry for Food Item and Seafood Re: Purchase Order Inquiry for Kour 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 alqardabyah@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

igbal.faroogi@ammiza.com kristina@mandrykina@gmail.com lightechllc@yahooo.com mail@pcconnect.co.za michelet220@yahoo.com mkrmkrtrading lib@outlook.com necophil@yahoo.com postmaster@optimal-design.cz r.hollman@mail.com raghida@irtorbey.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 vasirenterprisse@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 <u>Terms of Use</u> and acknowledge our <u>Privacy</u> <u>Statement</u>.