

# Banking Malware

DMU Hackers Club

By Sajid Nawaz Khan, Santander UK

# **SAJID NAWAZ KHAN**

Cyber Threat Intelligence Analyst  
Santander UK

# EMAIL REMAINS A SIGNIFICANT AND CREDIBLE THREAT TO BUSINESSES

Malware such as ransomware is delivered through malicious Office documents which are emailed to millions of users including staff. The emails are purposely designed to socially engineer the recipient to download and open the attachment, which goes on to infect the device



## PHISHING

Phishing is a **general and untargeted** attempt to acquire sensitive information such as usernames, passwords and credit card details for malicious reasons, by masquerading as a trustworthy and legitimate organisation



## MALWARE

Malware is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware – programming that gathers information about a computer user without permission

# JANUARY 2016

Belgian Bank Crelan, Crédit Agricole's Belgian subsidiary, has announced that it was the victim of a fraud campaign and lost over **€70 million** (\$75.8 million) in the process.

This attack consisted of a **simple spear-phishing** email sent to one of the company's high-ranking executives.



# Lincolnshire County Council's computer systems offline for a week after being hit by computer malware demanding a ransom

The image is a screenshot of a web browser displaying a BBC News article. The browser's address bar shows the URL [www.bbc.co.uk/news/uk-england-lincolnshire-35443434](http://www.bbc.co.uk/news/uk-england-lincolnshire-35443434). The page features the BBC News logo and navigation links for various news categories. The main headline reads "Lincolnshire County Council hit by £1m malware demand", dated 29 January 2016. To the right of the article, there is a "LIVE BBC Lincolnshire Live" section with updates, including "Lost seal pup found on beach" and "Lincolnshire Echo". Below the article, a "Top Stories" section lists other news items. Overlaid on the bottom half of the screenshot is a ransom note with a dark background and yellow text. The note states: "ALL YOUR PERSONAL FILES HAS BEEN ENCRYPTED". It explains that all data (photos, documents, databases, etc.) has been encrypted with a private and unique key. It demands payment in Bitcoin to a unique address. It specifies a 4-day deadline for payment, after which the payment will increase to 1 Bitcoin (\$350 approx.). It also states that if payment is not made within 7 days, the unique key will be destroyed, and the files will be permanently lost. At the bottom of the ransom note, there are two countdown timers: "Payment raise 3 days, 23:55:31" and "Final destruction 6 days, 23:55:31".

Lincolnshire County Council hit by £1m malware demand

29 January 2016 | Lincolnshire

**LIVE BBC Lincolnshire Live**

3 minutes ago  
Lost seal pup found on beach  
Lincolnshire Echo

**Top Stories**

**Scientists get 'gene editing' go-ahead**  
UK scientists win permission to genetically modify human embryos for the first time.  
1 hour ago

**Tareena Shakil jailed for joining IS**  
16 minutes ago

**Condolence books for Sir Terry Wogan**

**ALL YOUR PERSONAL FILES HAS BEEN ENCRYPTED**

All your data (photos, documents, databases, etc) have been encrypted with a private and unique key generated for this computer. This means that you will not be able to access your files anymore until they are decrypted. The private key is stored in our servers and the only way to receive your key to decrypt your files is making a payment.

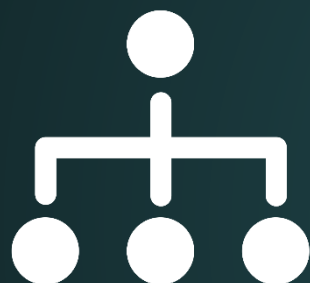
The payment has to be done in Bitcoins to a unique address that we generated for you. Bitcoins are a virtual currency to make online payments. If you don't know how to get Bitcoins, you can click the button "How to buy Bitcoins" below and follow the instructions.

**You only have 4 days to submit the payment.** When the provided time ends, the payment will increase to 1 Bitcoin (\$350 approx.). Also, if you don't pay in 7 days, your unique key will be destroyed and you won't be able to recover your files anymore.

**Payment raise**  
3 days, 23:55:31

**Final destruction**  
6 days, 23:55:31

# ORGANISED CRIME



## Organised

Groups of criminals that intend to engage in illegal activity, most commonly for monetary profit. Attacks are designed to either extort money from the target or cause significant disruption



## Collaborative

The increasing level of collaboration among cyber criminals allows them to compartmentalise their operations, greatly increasing the sophistication of their criminal endeavors



## Adaptive

Cyber actors are becoming more sophisticated, agile and capable of getting past any network security. Organisations must evolve, to implement a proactive, intelligence-driven offense

# DRIDEX

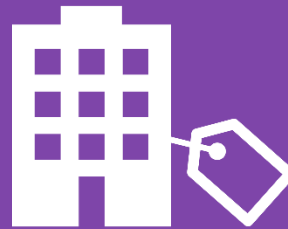




# DRIDEX



The malware authors develop and maintain the infrastructure



The infrastructure is rented out to actors who use it to launch attacks



Like many malware families, Dridex uses an affiliate model

# DRIDEX



Dridex is a malicious Microsoft Windows executable and DLL package



Its authors created an extensive and resilient C2 infrastructure



Once compromised, the money is retrieved using a mule system

# DRIDEX



Ability to inject code  
before page  
rendering



Variants include full  
keylogging and VNC  
facilities



Can usually operate  
as either MitM &  
MitB



An email with an  
invoice or similar  
theme ...



... containing a  
Word, Excel or  
PDF document ...



... socially  
engineering the  
user to open

You don't know the sender

Subject appears very urgent

The screenshot shows an Outlook email interface. At the top, there are action buttons: Reply, Reply All, Forward, Meeting, More, Keep, Team Email, Reply & Delete, To Manager, Done, Create New, Move, Rules, and OneNote. Below these are tabs for 'All' and 'Unread'. The email header shows 'FROM: Summers, Mollie' and 'SUBJECT: Important Notice: DA3A-34RE3WR1'. The email body starts with 'Hi,' followed by 'Please see attached the copy of invoice from 22/05/2015.' and 'Please can you send a revised statement so we can settel any outstanding balances.' (Note the spelling of 'settel'). Below this is a link 'Or you can approve the invoice by clicking here' and a signature 'Kind Regards, Mollie Summers'. An attachment 'DA3A-34RE3WR1.docx (15 KB)' is shown. Annotations with lines pointing to specific elements are present: 'You don't know the sender' points to the 'FROM' field; 'Subject appears very urgent' points to the subject line; 'Is not addressed to you personally' points to the 'Hi,' greeting; 'Contains an attachment' points to the attachment name; 'No corporate signature' points to the signature; 'Spelling mistakes' points to the word 'settel'; and 'Hover over the link. Where is it actually going to?' points to the 'clicking here' link.

Reply Reply All Forward Meeting More

Keep Team Email Reply & Delete To Manager Done Create New

Move Rules OneNote

All Unread

FROM: Summers, Mollie SUBJECT: Important Notice: DA3A-34RE3WR1

Reply Reply All Forward

Summers, Mollie Grant, Simon (Santander)

Important Notice: DA3A-34RE3WR1

Message DA3A-34RE3WR1.docx (15 KB)

Hi,

Please see attached the copy of invoice from 22/05/2015.

Please can you send a revised statement so we can settel any outstanding balances.

Or you can approve the invoice by [clicking here](#)

Kind Regards,  
Mollie Summers

Is not addressed to you personally

Contains an attachment

No corporate signature

Spelling mistakes

Hover over the link. Where is it **actually** going to?



**ATTACHMENT  
& DROPPER**



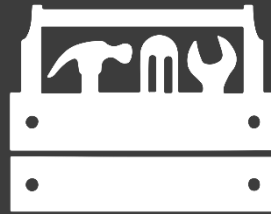
**WEB INJECTS  
& CONFIG**



**C2 &  
INFRASTRUCTURE**



**SANDBOX  
ENVIRONMENT**



**OLETOOLS  
TOOLKIT**



**PYTHON &  
COMMAND LINE**

# PIP INSTALL OLETOOLS





# REMNUX

REMnux is a free Linux toolkit for assisting malware analysts with reverse-engineering malicious software. It strives to make it easier for forensic investigators and incident responders to start using the variety of freely-available tools that can examine malware, yet might be difficult to locate or set up.

This lightweight distro incorporates many tools for analyzing Windows and Linux malware, examining browser-based threats such as obfuscated JavaScript, exploring suspicious document files and taking apart other malicious artifacts.

# DEMO

8	backspace	9	Tab	10	linefeed	13	carriage return
32	[space]	33	!	34	"	35	#
36	\$	37	%	38	&	39	'
40	(	41	)	42	*	43	+
44	,	45	-	46	.	47	/
48	0	49	1	50	2	51	3
52	4	53	5	54	6	55	7
56	8	57	9	58	:	59	;
60	<	61	=	62	>	63	?
64	@	65	A	66	B	67	C
68	D	69	E	70	F	71	G
72	H	73	I	74	J	75	K
76	L	77	M	78	N	79	O
80	P	81	Q	82	R	83	S
84	T	85	U	86	V	87	W
88	X	89	Y	90	Z	91	[
92	\	93	]	94	^	95	_
96	'	97	a	98	b	99	c
100	d	101	e	102	f	103	g
104	h	105	i	106	j	107	k
108	l	109	m	110	n	111	o
112	p	113	q	114	r	115	s
116	t	117	u	118	v	119	w
120	x	121	y	122	z	123	{
124		125	}	126	~		

# MALWR.COM

Download Malware Samples for Analysis

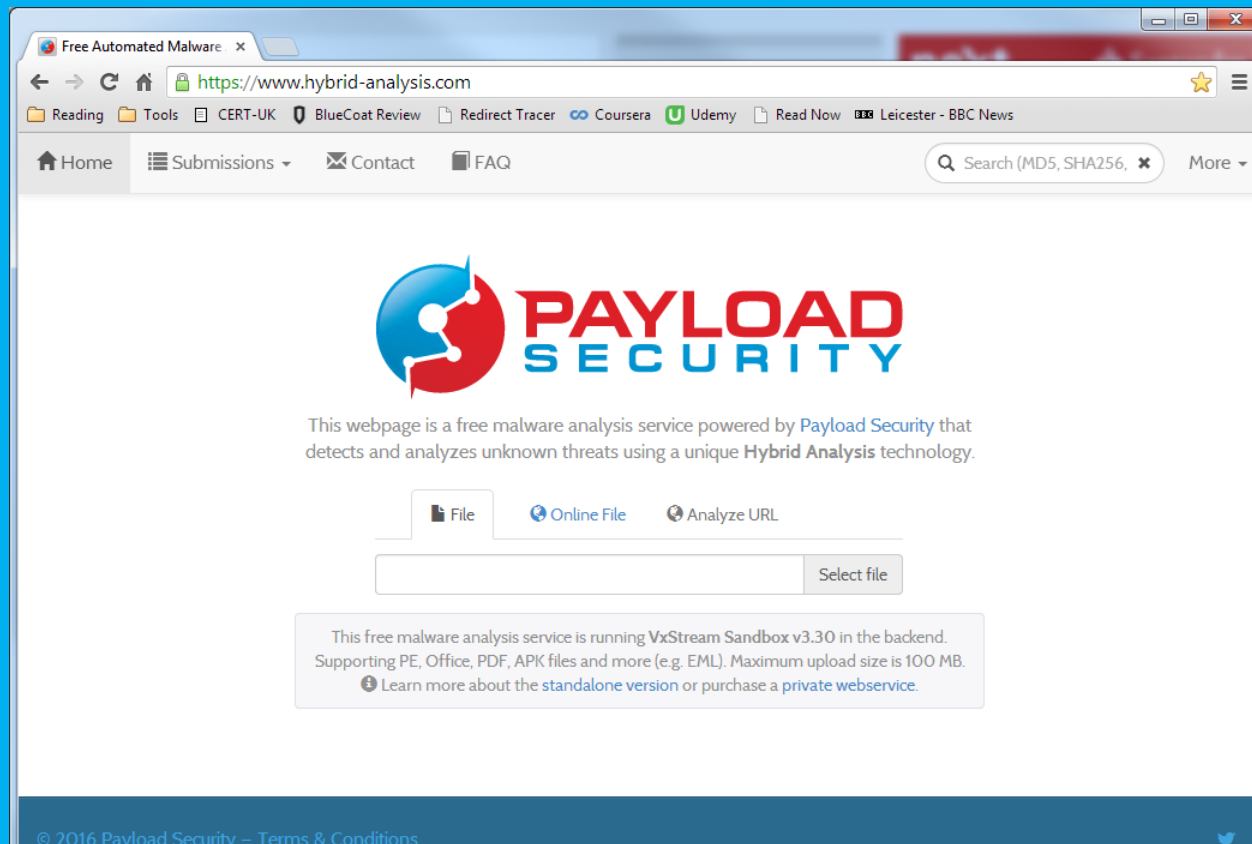
The screenshot displays the MALWR.COM website, which is a platform for malware analysis. The browser window shows the URL <https://malwr.com>. The website features a navigation bar with links to 'Analyses', 'Search', 'Submit', and 'About', along with 'Sign up' and 'Login' buttons. The main content area highlights three key statistics: 482151 Total Analyses, 61% Shared Malware, and 257237 Unique Domains. Below these statistics, there are two tables: 'Recent Analyses' and 'Recent Domains'. The 'Recent Analyses' table lists various malware samples with their hashes and timestamps. The 'Recent Domains' table lists domains associated with the malware samples.

Recent Analyses ( <a href="#">see more</a> )	
Feb. 17, 2016, 5:35 a.m.	<a href="#">6396376c233cff8d8a404b21090d9983</a>
Feb. 17, 2016, 5:34 a.m.	<a href="#">b3e1c8c6898b4df94e3a2c42b702aa4c</a>
Feb. 17, 2016, 5:31 a.m.	<a href="#">2b0eac44a236046e4fb38f1aec62d397</a>
Feb. 17, 2016, 5:30 a.m.	<a href="#">dd60fe5f961024f7c85130cae862cb7b</a>
Feb. 17, 2016, 5:29 a.m.	<a href="#">dc87338dcc62f0ea9dd9abe963f03de4</a>
Feb. 17, 2016, 5:28 a.m.	<a href="#">9ac506c6d587af95db8243ae34e1c859</a>
Feb. 17, 2016, 5:28 a.m.	<a href="#">68285b5de07f3f73f06d5c42f9e67a37</a>
Feb. 17, 2016, 5:27 a.m.	<a href="#">d826f8f16eb0b8c873fa3a7a79bcd03</a>

Recent Domains	
<a href="#">baza.hack-games-vk.ru</a>	
<a href="#">disk-space.ru</a>	
<a href="#">hack-games-vk.ru</a>	
<a href="#">ajax.googleapis.com</a>	
<a href="#">forum-hack-games-vk.ru</a>	
<a href="#">s49.radikal.ru</a>	
<a href="#">s017.radikal.ru</a>	
<a href="#">s020.radikal.ru</a>	

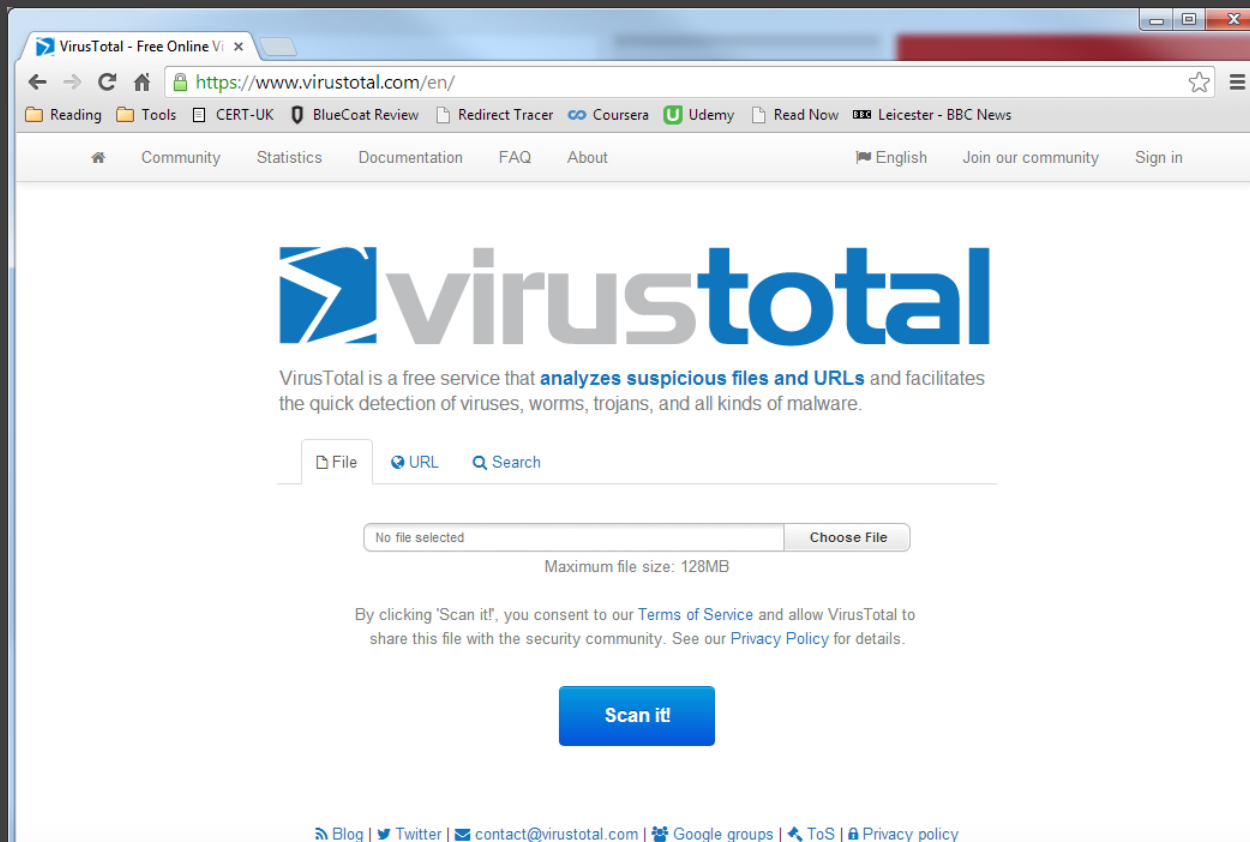
# HYBRID-ANALYSIS.COM

Online Malware Analysis Service

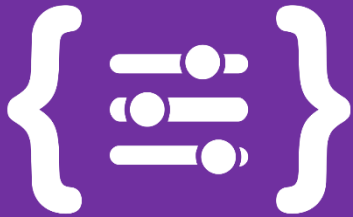


# VIRUSTOTAL.COM

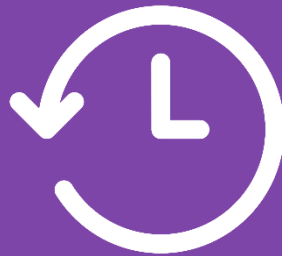
Online Malware Analysis Service



# TIPS



Begin with a static  
analysis of the  
suspect file



If running  
dynamically, be sure  
to use a sandbox



Don't share samples  
insecurely –  
malware may be  
LIVE!

# QUESTIONS?



**THANK YOU**