Banking Malware

DMU Hackers Club

By Sajid Nawaz Khan, Santander UK

Santander

SAJID NAWAZ KHAN

Cyber Threat Intelligence Analyst

Santander UK

Santander

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

Santander

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

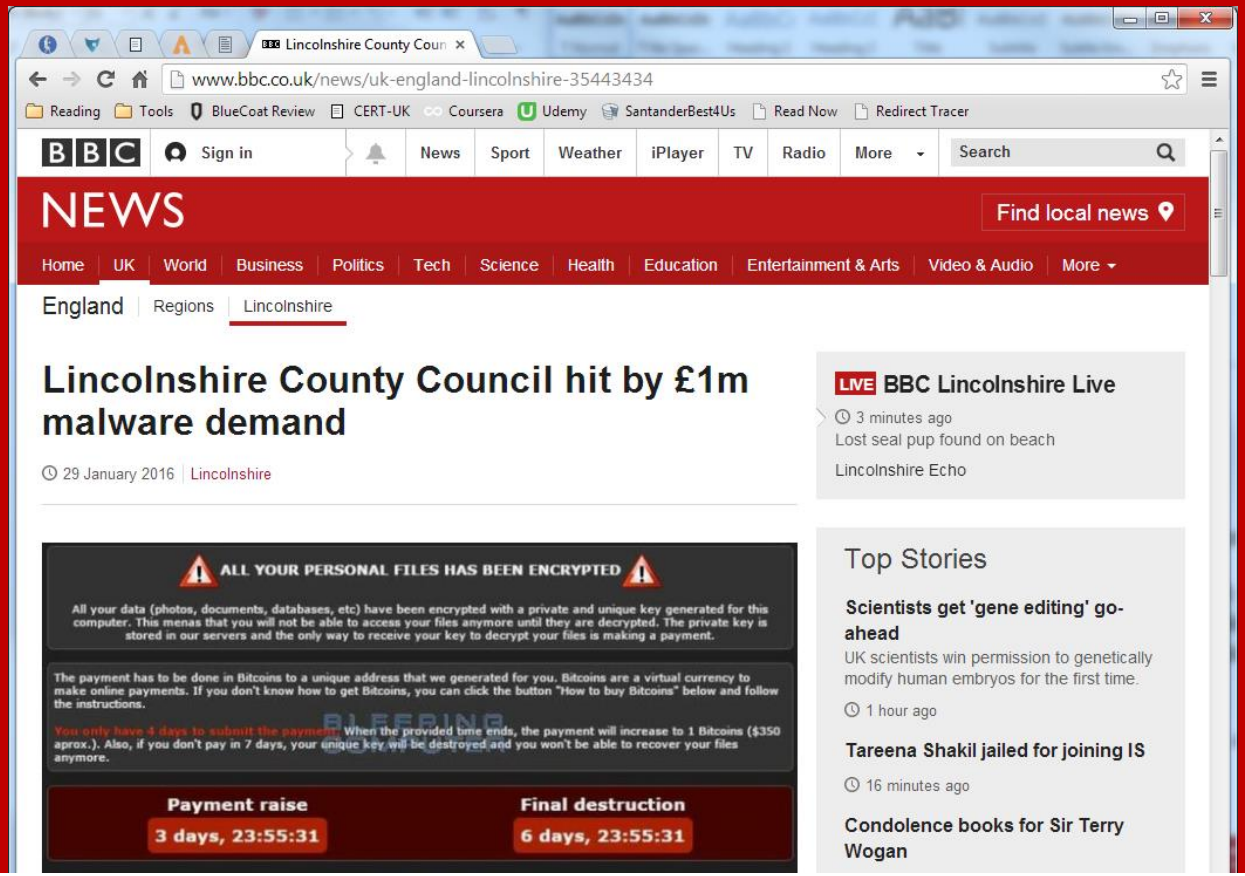
JANUARY 2016

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.

Santander

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



Santander

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

Santander

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

Santander

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

Santander

DRIDEX

Ability to inject code before page rendering

Variants include full keylogging and VNC facilities

Can usually operate as either MitM & MitB

Santander

An email with an invoice or similar theme ...

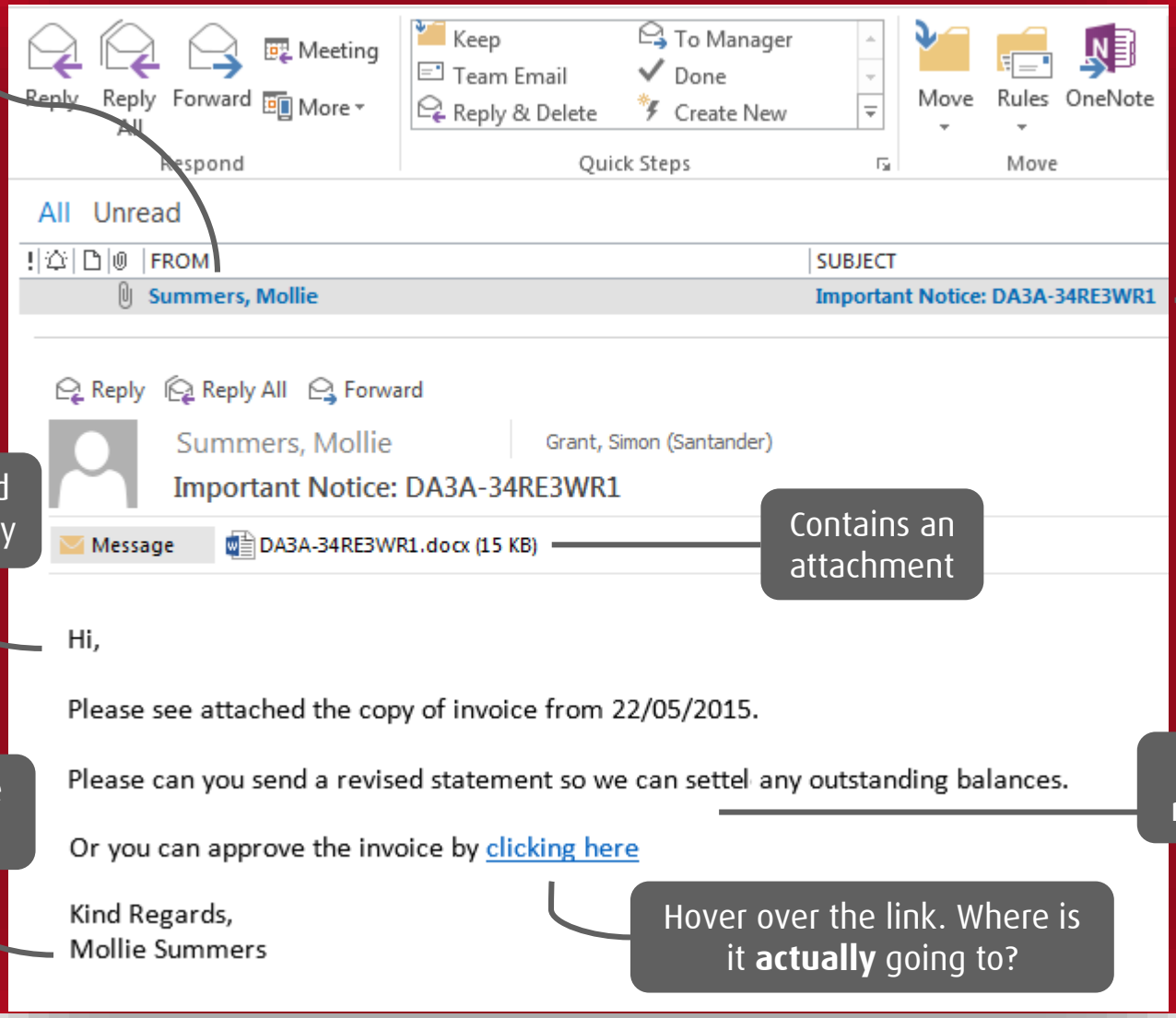
... containing a Word, Excel or PDF document ...

... socially engineering the user to open

Santander

You don't know the sender

Subject appears very urgent



Is not addressed to you personally

Contains an attachment

No corporate signature

Spelling mistakes

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

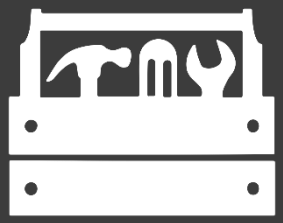
Santander

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.

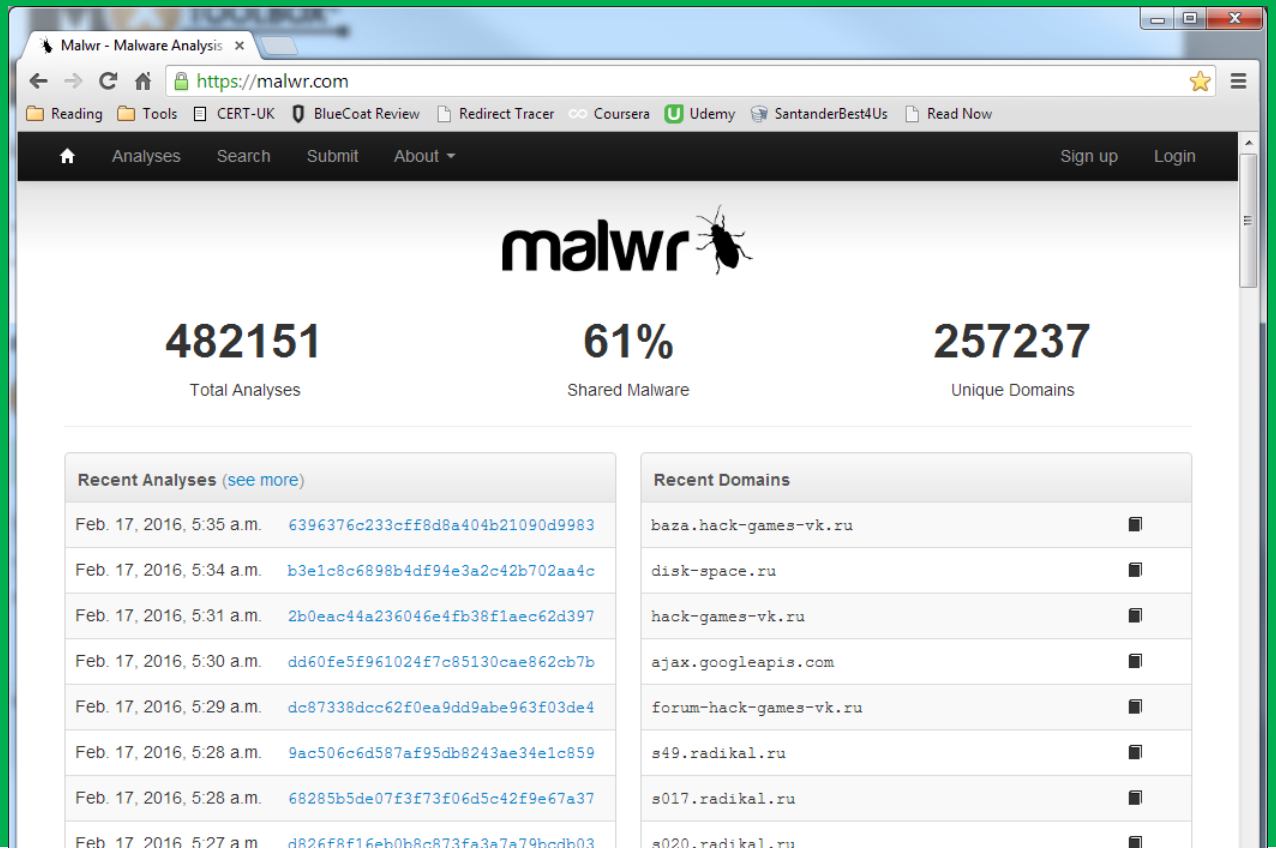
This lightweight distro incorporates many tools for analyzing Windows and Linux malware, examining browser-based threats such as obfuscated JavaScript, exploring suspicious document files and taking apart other malicious artifacts.

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

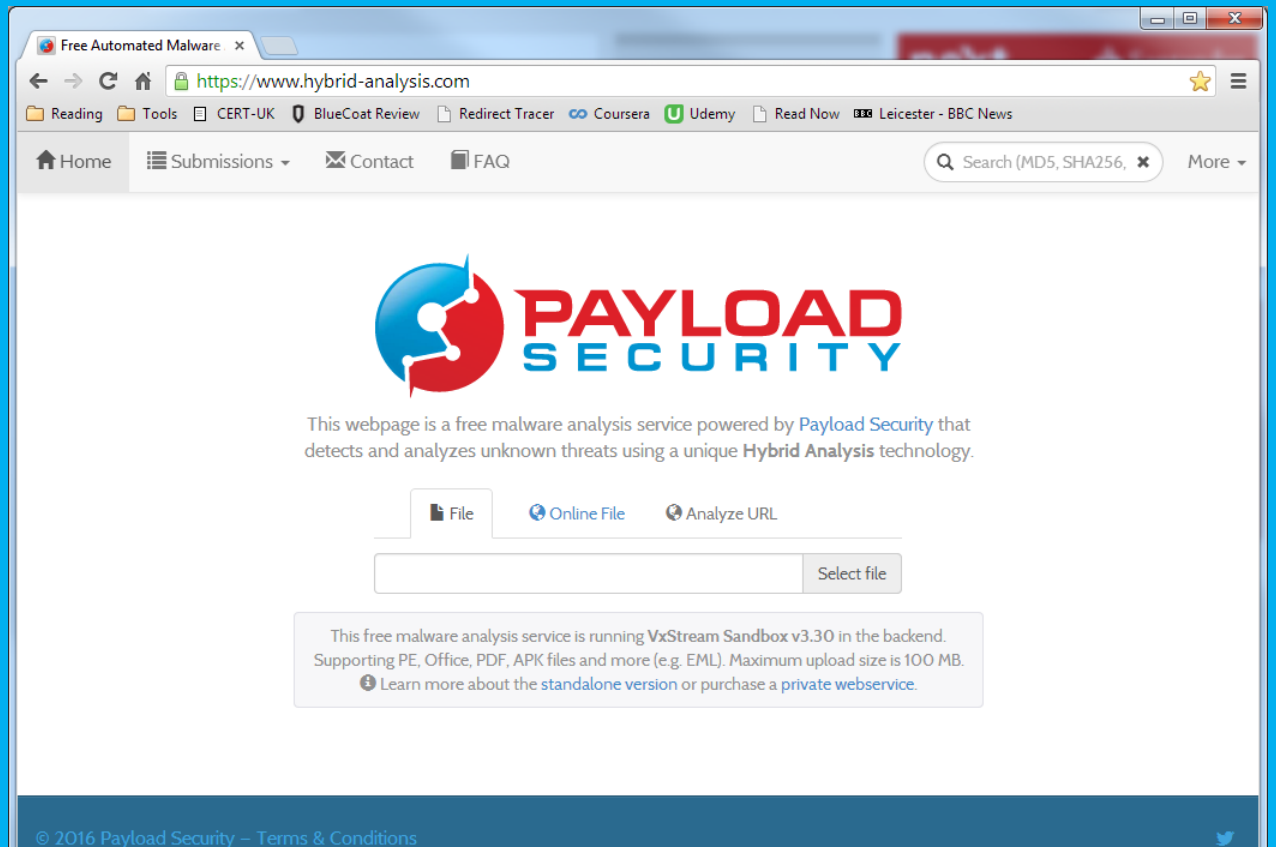
Download Malware Samples for Analysis



Santander

HYBRID-ANALYSIS.COM

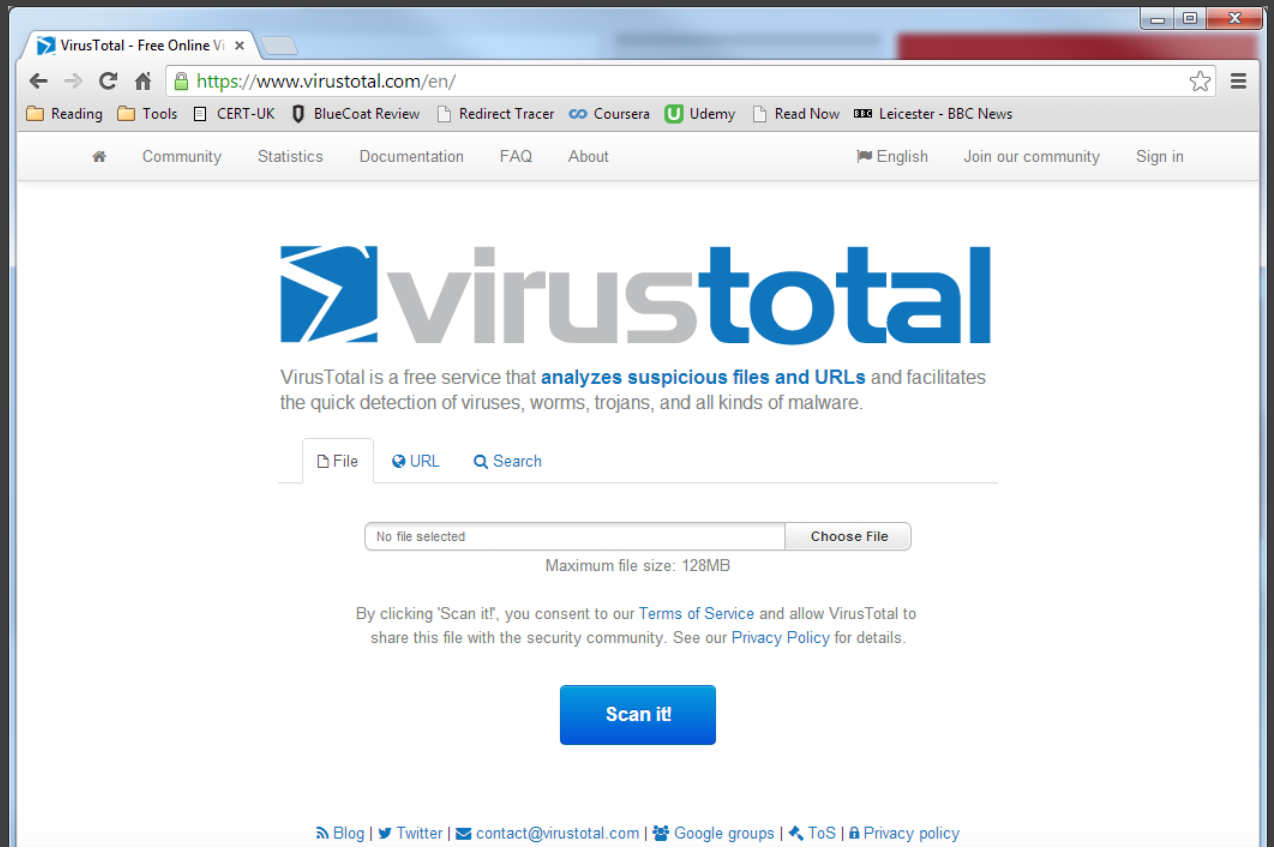
Online Malware Analysis Service



Santander

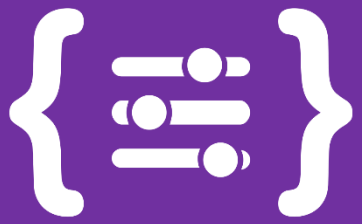
VIRUSTOTAL.COM

Online Malware Analysis Service



Santander

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!

Santander

QUESTIONS?

Santander

THANK YOU

Santander