PHISHING AWARENESS

Feedback on a bank’s strategy
# 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
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)

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
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
Tool Overview
Simple design

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

No special knowledge required

Easy maintenance
SWORDPHISH – OVERVIEW

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 attachment
• Attachment (MHT « doc » file)
• Fake ransomware (tech scam « blocking screen »)
• Awareness page
• Fake form
SWORDPHISH – OVERVIEW

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 attachment
- Fake form
- Fake ransomware (“tech scam” like)
SWORDPHISH – OVERVIEW

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
SWORPDHISH – 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 !

SOCIETE GENERALE
Two features in one plugin
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!
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/certsoocitegenerale/NotifySecurity
How to deal with malicious mails?
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 unsolicited mails (not necessarily malicious)

These mails are handled by several teams of Level 1 analysts helped by two tools
ORIGINIZATION - 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!
Macros extractions based on Didier Stevens’ toolset.
ORGANIZATION - FAME

Document preview

Helps to categorize a doc quickly
**ORGANIZATION - FAME**

**Virus Total Report**

**Detailed Results**

**SCORE**
7 / 59

**SCAN DATE**
2019-05-17 12:48:54

**PERMALINK**
https://www.virustotal.com/file/e4dc13ff1f126aco6f73kob1e10eb93f22fe4b64b0b111f44d30a7dc95c7f947aa8/analysis/1558067334/

**DETECTIONS**

<table>
<thead>
<tr>
<th>Engine</th>
<th>Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rising</td>
<td>Trojan:Downloader.VBA.Agent</td>
</tr>
<tr>
<td>Ikarus</td>
<td>Trojan:Downloader.VBA.Agent</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Trojan:097M/Sobekk.Btc</td>
</tr>
<tr>
<td>AhnLab-V3</td>
<td>VBA/Downloader:S17</td>
</tr>
<tr>
<td>GData</td>
<td>Macro: Trojan-Downloader:POSZ</td>
</tr>
<tr>
<td>SentinelOne</td>
<td>DFI-Malicious OLE</td>
</tr>
<tr>
<td>Fortinet</td>
<td>VBA/Agent.DUOThr.dlder</td>
</tr>
</tbody>
</table>
**Mail headers**

Easier interpretation of mail headers

Ordered hops to identify origin

<table>
<thead>
<tr>
<th>#</th>
<th>DELAY</th>
<th>FROM</th>
<th>TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>o2ak-app.1.materna-com.de (172.38.68.13)</td>
<td>relay3.materna-com.de (Postfix 2.7.19/TIM6.6.6)</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>relay3.materna-com.de ([192.109.216.142])</td>
<td>parmail09.iap.scoegen.com</td>
</tr>
<tr>
<td>2</td>
<td>1 sec</td>
<td>parmail09.iap.scoegen ([151.1.2.13])</td>
<td>smtp-iap.hermes.scoegen</td>
</tr>
<tr>
<td>3</td>
<td>1 sec</td>
<td>smtp-iap.hermes ([175.128.14.140])</td>
<td>HUBDC2666.hermes.scoegen ([175.128.14.38])</td>
</tr>
<tr>
<td>4</td>
<td>2 sec</td>
<td>HUBDC2666.hermes ([175.128.14.38])</td>
<td>HUBSEO666.hermes ([175.128.206.34])</td>
</tr>
<tr>
<td>5</td>
<td>1 sec</td>
<td>HUBSEO666.hermes ([175.128.206.34])</td>
<td>MXDC2663.hermes ([175.128.14.199])</td>
</tr>
</tbody>
</table>
SMART: A « MACHINE LEARNING » BASED TOOL TO DROP USELESS EMAILS

Internal development (not published)
Use several metrics to categorize mails
PoC ongoing, reliability still under evaluation

Goals:
- eliminate spam / marketing and other harmless unsolicited mail
- help level 1 analysts in the evaluation process
6

SUCCESS & FAILURES

Feedback on two years
SUCCEE S ET ECHECS

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 ?