How criminal networks use “cloud services” and “Involuntary Contribution Associates” to make money

Francis Turner

Stop Botnets Stealing From You!
• The cloud for “business”
• The Exploit/Bot/Ransom lifecycle
• Evolution
  – Mobile malware
  – DGA and fastflux
• What Can we do About it
• Closing remarks from our sponsor
Cloud Benefits

• The cloud and xAAS is a paradigm change
  – Location independence
  – APIs, plugins allow interaction between services
  – Scaleable, flexible

• Business people are moving to the cloud
  – Cloud services are more efficient
  – No need to be expert in everything

Criminals are business people too!
The classic virtual cloud-based xAAS enterprise
The virtual cloud-based xAAS malware enterprise
The virtual cloud-based xAAS malware enterprise
• Step 1. MalSpam
  – Click on the nice FULL STORY link…

http://muhoc.com/CNN_online/get_news.php
• Step 1. MalSpam
  – And open/run the download

Please download and click to start.

File Download

Do you want to open or save this file?

Name: BreakingNews_pdf18.zip
Type: Compressed (zipped) Folder, 10.5KB
From: mulhoc.com

Open Save Cancel

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What’s the risk?
• Step 2. Exploit
  – Gain admin rights, disable AV & WSUS checking
  – Download [http://somerandomain.com/1/logo.png](http://somerandomain.com/1/logo.png)
  – Copy logo.png to C:\Windows\pfdOSwYjERDHRdV.exe
  – Create a Service named "Google Update Service" by setting the following registry keys:
    • HKLM\SYSTEM\CurrentControlSet\Services\googleupdate\ImagePath: "C:\WINDOWS\pfdOSwYjERDHRdV.exe"
    • HKLM\SYSTEM\CurrentControlSet\Services\googleupdate\DisplayName: "Google Update Service"
• Step 3. Trojan
  – pfdOSwYjERDHrdV.exe
    • Call home to hxxps://jsfrpcvudfrnpyfftgl.info/
      – Send config details (Win 7, IE 11 ...)
      – Download latest keylogger & banking inject HTML
      – Ask for other instructions
Step 4. Trojan Send Data
- pfdOSwYjERDHrdV.exe
  - Capture Chase.com login
    - Ask for additional data
  - Call home to hxxps://jsfrpcvudfrnpyfftgl.info/
    - Send details (Win 7, IE 11 ...)

Dear customer. To better serve you and protect your identity we are updating our system please validate the information below.

ATM/Debit Card #: __________
Expiration Date (mm/yyyy): / / 
3-Digit Security Code (CVV): 
Card PIN: 

Continue Clear Cancel
Exploit/Trojan/Ransom

• Step 5 Ransom
  – pfdOSwYjERDHRdV.exe
    • Call home to hxxps://jsfrpcvudfrnpyfftgl.info/
      – Download cryptowall 3.0 (id-12839182.exe)
    • Run id-12839182.exe
  – id-12839182.exe
    • Call home to http://eportfolo.capullman.ca/blog/eo7ycomyy (Pay2infect)
      – http://www.mihuainfo.com/wp-content/themes/mh/3sbgwh (RSA key)
    • Encrypt files
Exploit/Trojan/Ransom

Your files are encrypted.
To get the key to decrypt files you have to pay **600 USD/EUR**. If payment is not made before **05/10/14 - 17:10** the cost of decrypting files will increase 2 times and will be **1200 USD/EUR**

Prior to increasing the amount left:
**95h 47m 44s**

Your system: **Windows 7 (x64)**  First connect IP: [REDACTED]  Total encrypted 42 files.

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You should register Bitcon wallet ([click here for more information with pictures](https://example.com/))
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
Evolution to beat 2FA

Internet

Dropzone

1

2

3

4

5

6

7

Source, Checkpoint
Eurograbber
Summary

• The Internet and Cloud are great for “Business”
  – Recruit “Involuntary Contribution Associates” via customized mass email
    • Also Work from Home “Financial Transfer Associates”
  – Synergize exploits to produce globally distributed cloud platform
  – Leverage Social Media and Financial “Sponsors”
  – Apply encryption to protect critical data from unauthorized access

• Profit!
In the beginning

- there was hard-coding
  - 5.79.86.19 port 1234

Moving to

- DNS and HTTPS
  - dieideenwerkstatt.at =>
  - 188.64.60.209 port 443
Now for something more varied

- **Dynamic DNS**
  - browserprotect.hopto.org
  - IP changes every few minutes (seconds)

- **Domain generation**
  - g92yyqg30b4cdfmgrr332h6s.net
  - mhyphidaoajy.zzxyxx.fi
New data extraction method

• **DGA and/or fastflux**
  • Infection calls home to TBD domain
  • E.g. g92yyqg30b4cdfmgrrr332h6s.net mhyphidaoajy.zzxyxx.fi

• **Requirements**
  • Temporary proxy dropbox
  • Long term secure DNS Server

• **DNS redirects to dropbox**
  • Quick to change
  • Hard to identify actual host
How it works

• DGA
  – g92yyqg30b4cdfmgrp332h6s.net

• NS
  g92yyqg30b4cdfmgrp332h6s.net. 172800 IN NS ns2.thepurringpiano.net.
  g92yyqg30b4cdfmgrp332h6s.net. 172800 IN NS ns1.thepurringpiano.net.

• NSIP
  ns1.thepurringpiano.net. 5 IN A 82.212.49.138
  ns2.thepurringpiano.net. 5 IN A 112.33.0.121

• A
  g92yyqg30b4cdfmgrp332h6s.net. 5 IN A 103.241.144.184
  g92yyqg30b4cdfmgrp332h6s.net. 5 IN A 122.166.11.34
  g92yyqg30b4cdfmgrp332h6s.net. 5 IN A 5.196.139.65
## Strengths

- **DGA**
  - g92yyqg30b4cdfmgrr332h6s.net

- **NS**
  - g92yyqg30b4cdfmgrr332h6s.net. 5 IN NS ns2.thepurringpiano.net.
  - g92yyqg30b4cdfmgrr332h6s.net. 5 IN NS ns1.thepurringpiano.net.

- **NSIP**
  - ns1.thepurringpiano.net. 5 IN A 82.212.49.138
  - ns2.thepurringpiano.net. 5 IN A 112.33.0.121

- **A**
  - g92yyqg30b4cdfmgrr332h6s.net. 5 IN A 103.241.144.184
  - g92yyqg30b4cdfmgrr332h6s.net. 5 IN A 122.166.11.34
  - g92yyqg30b4cdfmgrr332h6s.net. 5 IN A 5.196.139.65
• DNS resolution of g92yyqg30b4cdfmgr332h6s.net
  1. Root server
     • Get NS for .net
  2. .net server
     • Get NS for g92yyqg30b4cdfmgr332h6s.net
  3. g92yyqg30b4cdfmgr332h6s.net server
     • Get A records for g92yyqg30b4cdfmgr332h6s.net
• DNS resolution of g92yyqg30b4cdfmgrprr332h6s.net
  1. Root server
     • Get NS for .net
  2. .net server
     • Get NS for g92yyqg30b4cdfmgrprr332h6s.net
  3. g92yyqg30b4cdfmgrprr332h6s.net server
     • Get A records for g92yyqg30b4cdfmgrprr332h6s.net
Weakness 2

- **DGA**
  - g92yyqg30b4cdfmgrr332h6s.net

- **NS**
  - g92yyqg30b4cdfmgrr332h6s.net. 172800 IN NS ns2.thepurringpiano.net.
g92yyqg30b4cdfmgrr332h6s.net. 172800 IN NS ns1.thepurringpiano.net.

- **NSIP**
  - ns1.thepurringpiano.net. 5 IN A 82.212.49.138
  - ns2.thepurringpiano.net. 5 IN A 112.33.0.121

- **A**
  - g92yyqg30b4cdfmgrr332h6s.net. 5 IN A 103.241.144.184
  - g92yyqg30b4cdfmgrr332h6s.net. 5 IN A 122.166.11.34
  - g92yyqg30b4cdfmgrr332h6s.net. 5 IN A 5.196.139.65
Enables you to block all traffic to and from known criminal sites

1. ThreatSTOP gathers data
2. Download current list
3. Infected host “calls home”
4. Call home blocked
5. Invisible to inbound
6. Feedback loop & report
7. Another ThreatSTOPped
QUESTIONS?
Thank You
www.threatstop.com

Francis Turner

VP Research & Security
tomb@threatstop.com
M: 760.402.3999
O: 760.542.1550