End-to-End Analysis of a Domain Generating Algorithm Malware Family

SESSION ID: BR-R01

Jason Geffner
Sr. Security Researcher
CrowdStrike, Inc.
jason@crowdstrike.com
Background
Domain Generating Algorithms

- Most modern malware communicates with attackers’ servers
- Typical bots/RATs/down loaders
- DGA malware
DGA Example

- Every minute, have malware connect to GMT-time-based server address
  - `<month><day><year><hour><minute>.com`
  - On February 27, 2014, at 8:15 AM, malware connects to 02 27 14 08 15.com
- Attacker registers domain and server prior to strike-time
- Attacker redirects domain and takes down server immediately after strike-time
Notable DGA History

- **Early 2008** – Kraken one of the first malware families to use a DGA
- **Late 2008** – Conficker first discovered
- **2010** – Texas A&M University researchers publish paper on detecting DGA domain names
- **2012** – Damballa releases whitepaper on new DGA use in six malware families
New DGA Family

- In February of 2013, a major American financial services firm received a suspicious email with an EXE file attachment.
- Firm’s CISO sent the attachment to their “global cyber intelligence” partner, who had trouble analyzing it:
  “It is the obfuscation that is throwing off.”
- As a result, the CISO forwarded it to us.
Code Obfuscation

- Most obfuscated malware is obfuscated with a packer
- This malware uses inline code obfuscation
This snippet of disassembly shows random 32-bit values being assigned to variables and used in mathematical calculations.

This **junk** code is interspersed with **legitimate** code.
This snippet of disassembly shows random 32-bit values being assigned to variables and used in mathematical calculations.

This **junk** code is interspersed with **legitimate** code.
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-16h]@1
    int v8; // [sp+Ch] [bp-Ch]@1
    signed int v9; // [sp+10h] [bp-08h]@1
    int v10; // [sp+14h] [bp-04h]@1

    v10 = a1;
    v7 = -1890418483;
    v8 = a3;
    v9 = -134758405;
    while ( v10 != a1 + 4 * a2 )
    {
        v3 = -2084904757 * v7;
        *(DWORD *)v10 = v8;
        v4 = __ROL4__(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;
}
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-10h]@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;
}
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;
    }
}
Code Deobfuscation

- 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
- All other local function variables considered legitimate if their values are read from or written to other legitimate variables
Decompilation Graph, Before Deobfuscation
Decompilation Graph, After Deobfuscation
CrowdDetox

- Free open-source plugin for Hex-Rays
- Finds legitimate variables and code in a decompilation graph, and prunes everything else
- Available at http://www.crowdstrike.com/community-tools
Data Obfuscation
Data Obfuscation

- EXE contains no readable static strings related to malicious functionality
  - No registry keys
  - No file names
  - No server addresses
  - No URI paths
- All strings are decrypted at run time
lpSubKey = (LPCSTR)sub_407F90(&unk_4391D8, 0x2Eu);
if (!RegOpenKeyA(HKEY_CURRENT_USER, lpSubKey, &hKey))
{
    void *v3; // [sp+0h] [bp-1Ch]@1
    int v6; // [sp+14h] [bp-8h]@1
    void *v7; // [sp+18h] [bp-4h]@1

    v7 = malloc(a2);
    memcpy(v7, a1, a2);
    v3 = v7;
    v6 = (_BYTE *)a1 + dword_43C688 - (_BYTE *)&dword_439024;
    while ( v3 != (char *)v7 + a2 )
    {
        *(BYTE *)v3 ^= *(BYTE *)v6;
        v3 = (char *)v3 + 1;
        ++v6;
    }
    return v7;
}
Dynamically Deobfuscating Data

- Within first hour of incident response
  - Found string decryption function
  - Identified list of encrypted strings
  - Patched binary to decrypt strings in-place as opposed to on heap
  - Patched binary with hand-written assembly to call string decryption function on each encrypted string
Statically Deobfuscating Data

- String decryption function XORs encrypted strings with one-time pad
- One-time pad is generated at run time
Generation of One-Time Pad

```c
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);
```
Statically Decrypting All Strings

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

- Initially collected over 100 variants from this malware family
- Most use randomized strings in decrypted data
  - File names
  - Directory names
  - Registry names
- A few use template placeholders instead of randomized strings
Malware Family History

- CrowdStrike initially collected:
  - 16 “template” variants
  - 132 non-“template” variants
- PE Timestamps appear to be legitimate
- Malware first built and distributed in February, 2013
Variants Grouped by PE Timestamp

- "Template" Variants
- Non-"Template" Variants

Number of Variants

PE Timestamp, Bucketed by Hour (UTC)

2/2/13, 21:00
2/2/13, 22:00
... 2/5/13, 18:00
2/5/13, 19:00
2/5/13, 20:00
Authorship Clues in Decrypted Strings

- All variants using default template have the same seed value: 0x445A4950
- Parsed as ASCII, 0x445A4950 = “PIZD”
- “PIZD” translates from Bosnian / Croatian / Latvian / Polish / Romani / Romanian / Slovenian to English as censored
Authorship Clues in Decrypted Strings

- Template string for copied file name is “XZSEQWS pulaosugiingat .exe”

- “pula o sug i în gât” loosely translates from Romanian to English as censored
Authorship Clues in Decrypted Strings

- However, a Romanian is more likely to say, “suge pula în gât”
- “pula o sug i în gât” is more likely the wording a Romani would use
- Additionally, a Romanian is more likely to say “pizda” than “pizd”; a Romani would say “pizd”
Decrypted Strings Show Romani Names

- Template strings for directory name and registry value names are “NICOLAEGUTAXZSEQWS” and “COSTIIONITAEQWS”
- Template string used in entry point obfuscation is “ADRIAN COPILU MINUNE SI FLORIN SALAM”
Prominent Romani Manele Singers

Nicolae Guță

Costi Ioniță

Adrian Copilul Minune

Florin Salam
Domain Generating Algorithm
Domain Generating Algorithm

- All variants of family contain identical 384-word list of common English words, decrypted at run time
- Domain names created by concatenating two pseudo-randomly selected words and appending “.net” to the end
<table>
<thead>
<tr>
<th>above</th>
<th>behind</th>
<th>chance</th>
<th>desire</th>
<th>expect</th>
<th>gentleman</th>
<th>leader</th>
<th>prepare</th>
<th>separate</th>
<th>stranger</th>
<th>travel</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>being</td>
<td>character</td>
<td>destroy</td>
<td>experience</td>
<td>glass</td>
<td>leave</td>
<td>need</td>
<td>separate</td>
<td>service</td>
<td>stream</td>
</tr>
<tr>
<td>advanced</td>
<td>believe</td>
<td>change</td>
<td>device</td>
<td>explain</td>
<td>glossyary</td>
<td>length</td>
<td>neighbor</td>
<td>settle</td>
<td>street</td>
<td>trust</td>
</tr>
<tr>
<td>afraid</td>
<td>belong</td>
<td>chief</td>
<td>difference</td>
<td>family</td>
<td>goodbye</td>
<td>neither</td>
<td>pretty</td>
<td>severa</td>
<td>strong</td>
<td>twelve</td>
</tr>
<tr>
<td>against</td>
<td>beside</td>
<td>childhood</td>
<td>difficult</td>
<td>famous</td>
<td>govern</td>
<td>night</td>
<td>probably</td>
<td>strike</td>
<td>twenty</td>
<td>strong</td>
</tr>
<tr>
<td>airplane</td>
<td>between</td>
<td>children</td>
<td>dinner</td>
<td>fancy</td>
<td>guard</td>
<td>north</td>
<td>probably</td>
<td>student</td>
<td>understand</td>
<td>until</td>
</tr>
<tr>
<td>almost</td>
<td>better</td>
<td>choose</td>
<td>direct</td>
<td>father</td>
<td>happen</td>
<td>nothing</td>
<td>problem</td>
<td>subject</td>
<td>until</td>
<td>valley</td>
</tr>
<tr>
<td>alone</td>
<td>beyond</td>
<td>cigarette</td>
<td>discover</td>
<td>fellow</td>
<td>health</td>
<td>notice</td>
<td>produce</td>
<td>succeed</td>
<td>success</td>
<td>various</td>
</tr>
<tr>
<td>already</td>
<td>bicycle</td>
<td>circle</td>
<td>distance</td>
<td>fence</td>
<td>heart</td>
<td>object</td>
<td>promise</td>
<td>success</td>
<td>sudden</td>
<td>suffer</td>
</tr>
<tr>
<td>although</td>
<td>board</td>
<td>class</td>
<td>distant</td>
<td>fifteen</td>
<td>heaven</td>
<td>oclock</td>
<td>proud</td>
<td>shoulder</td>
<td>supply</td>
<td>wagon</td>
</tr>
<tr>
<td>amount</td>
<td>borrow</td>
<td>class</td>
<td>divide</td>
<td>figure</td>
<td>heavy</td>
<td>office</td>
<td>public</td>
<td>shout</td>
<td>summer</td>
<td>water</td>
</tr>
<tr>
<td>anger</td>
<td>bottle</td>
<td>clean</td>
<td>divide</td>
<td>finger</td>
<td>history</td>
<td>matter</td>
<td>quarter</td>
<td>silver</td>
<td>supply</td>
<td>weather</td>
</tr>
<tr>
<td>angry</td>
<td>branch</td>
<td>clothes</td>
<td>dollar</td>
<td>doctor</td>
<td>honor</td>
<td>mayor</td>
<td>question</td>
<td>simple</td>
<td>surprise</td>
<td>welcome</td>
</tr>
<tr>
<td>animal</td>
<td>bread</td>
<td>college</td>
<td>dollar</td>
<td>double</td>
<td>fler</td>
<td>order</td>
<td>quiet</td>
<td>single</td>
<td>suppose</td>
<td>welcome</td>
</tr>
<tr>
<td>another</td>
<td>bridge</td>
<td>company</td>
<td>double</td>
<td>flower</td>
<td>hunger</td>
<td>measure</td>
<td>rather</td>
<td>sister</td>
<td>surprise</td>
<td>wheat</td>
</tr>
<tr>
<td>answer</td>
<td>bright</td>
<td>complete</td>
<td>dress</td>
<td>follow</td>
<td>husband</td>
<td>meeting</td>
<td>ready</td>
<td>smell</td>
<td>system</td>
<td>whether</td>
</tr>
<tr>
<td>appear</td>
<td>bring</td>
<td>condition</td>
<td>dried</td>
<td>foreign</td>
<td>include</td>
<td>member</td>
<td>realize</td>
<td>soldier</td>
<td>therefore</td>
<td>why</td>
</tr>
<tr>
<td>appear</td>
<td>bring</td>
<td>condition</td>
<td>dried</td>
<td>foreign</td>
<td>include</td>
<td>method</td>
<td>reason</td>
<td>space</td>
<td>thick</td>
<td>whose</td>
</tr>
<tr>
<td>apple</td>
<td>break</td>
<td>contain</td>
<td>early</td>
<td>forever</td>
<td>indeed</td>
<td>might</td>
<td>receive</td>
<td>speak</td>
<td>window</td>
<td>third</td>
</tr>
<tr>
<td>around</td>
<td>broken</td>
<td>contain</td>
<td>early</td>
<td>forever</td>
<td>indeed</td>
<td>might</td>
<td>record</td>
<td>special</td>
<td>third</td>
<td>winter</td>
</tr>
<tr>
<td>arrive</td>
<td>brought</td>
<td>continue</td>
<td>effort</td>
<td>forget</td>
<td>forget</td>
<td>industry</td>
<td>remember</td>
<td>those</td>
<td>within</td>
<td>within</td>
</tr>
<tr>
<td>article</td>
<td>brown</td>
<td>control</td>
<td>either</td>
<td>found</td>
<td>forth</td>
<td>instead</td>
<td>perhaps</td>
<td>thought</td>
<td>without</td>
<td>woman</td>
</tr>
<tr>
<td>attempt</td>
<td>built</td>
<td>corner</td>
<td>electric</td>
<td>find</td>
<td>fresh</td>
<td>journey</td>
<td>require</td>
<td>thought</td>
<td>women</td>
<td>women</td>
</tr>
<tr>
<td>banker</td>
<td>build</td>
<td>country</td>
<td>electric</td>
<td>friend</td>
<td>fresh</td>
<td>kitchen</td>
<td>result</td>
<td>throw</td>
<td>wonder</td>
<td>wonder</td>
</tr>
<tr>
<td>battle</td>
<td>business</td>
<td>course</td>
<td>electricity</td>
<td>friend</td>
<td>friend</td>
<td>known</td>
<td>person</td>
<td>throw</td>
<td>would</td>
<td>worth</td>
</tr>
<tr>
<td>basket</td>
<td>butter</td>
<td>cover</td>
<td>English</td>
<td>future</td>
<td>further</td>
<td>labor</td>
<td>picture</td>
<td>together</td>
<td>would</td>
<td>write</td>
</tr>
<tr>
<td>beauty</td>
<td>captain</td>
<td>crowd</td>
<td>enough</td>
<td>future</td>
<td>further</td>
<td>labor</td>
<td>pleasant</td>
<td>toward</td>
<td>wrote</td>
<td>yellow</td>
</tr>
</tbody>
</table>
Domain Generating Algorithm

- Pseudo-random algorithm uses only 15 bits of the seed value, so only 32,768 possible domain names

\[
\text{Seed Value} = \frac{\text{seconds elapsed since January 1, 1970 GMT}}{512}
\]

\[\therefore \text{Seed Granularity} = 512 \text{ seconds} = 8 \text{ minutes and 32 seconds}\]

- Malware tries 85 domains per seed value (seed+0, seed+1, seed+2, ...), creating a sliding “window” of DGA domains
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";
}
Malware’s Use of DGA

- Malware regularly connects to DGA domains to send HTTP GET request
  
  `/forum/search.php?email=<hardcoded email address>&method=post`

- Each malware variant has a unique hardcoded email address
Malware’s Use of DGA

- If the server’s response contains the correct fingerprint, the malware requests the same URL again
- If the server’s second response contains the correct fingerprint, the malware saves the downloaded content as an EXE and executes it
Sinkholing
Sinkholing

- Sinkholed five domains to which the DGA would resolve on March 5th, 6th, 7th, 8th, and 9th of 2013
- Nearly 15,000 hits from malware
- Logged 1,170 unique client IP addresses
- Logged 1,000 unique email addresses posted to sinkhole servers
Example Email Addresses Posted to Sinkholes

- 1800flowers@1800reminders.com
- billing@deluxeforbusiness.com
- consultant_fiscal-unsubscribe@yahoogroups.com
- fbmessage+fepvdccz@facebookmail.com
- geico_claims@geico.com
- northwest.airlines@nwa.com
More Email Addresses Posted to Sinkholes

- 421 personal yahoo.com addresses
- 66 personal aol.com addresses
- 59 personal hotmail.com addresses
- 31 personal comcast.net addresses
- 4 .gov addresses
- 1 .mil address
- 0 gmail.com addresses
# Sinkhole Hits From IP Addresses

1. United States: 575  
2. Romania: 321  
3. Japan: 46  
4. Russia: 17  
5. Germany: 15  
6. France: 15  
7. India: 14  
8. Netherlands: 14  
9. United Kingdom: 13  
10. Sweden: 11
DGA Monitoring

- Developed automation solution to download from DGA domains in real-time
- Domains connected to campaign responded with identifiable HTTP response fingerprint
- Automation ran for two weeks
- Detected 20 domains connected to campaign
Domain Research
Domain Analysis

- 19 of the 20 domains
  - Registered via and hosted by Yahoo! Inc.’s Small Business hosting plan
  - Registrants used @yahoo.com email account
- 1 of the 20 domains
  - Registered via and hosted by Omnis Network LLC
  - Registrants used @aol.com email account
Domain Analysis

- All domains registered 0-48 hours before DGA pointed to them
- Identical registrant names and addresses used for several domains, with semi-random phone numbers corresponding to city area code
<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>REGISTRANT</th>
<th>ADMIN EMAIL</th>
<th>ADMIN PHONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>amountcondition.net</td>
<td>Robert Seifert</td>
<td><a href="mailto:seifertrobertw@yahoo.com">seifertrobertw@yahoo.com</a></td>
<td>+1.7737916544</td>
</tr>
<tr>
<td></td>
<td>2212 W. Farwell</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chicago, IL 60645</td>
<td></td>
<td></td>
</tr>
<tr>
<td>weathereearly.net</td>
<td>Robert Seifert</td>
<td><a href="mailto:robertwseifert@yahoo.com">robertwseifert@yahoo.com</a></td>
<td>+1.7737916324</td>
</tr>
<tr>
<td></td>
<td>2212 W. Farwell</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chicago, IL 60645</td>
<td></td>
<td></td>
</tr>
<tr>
<td>heardstrong.net</td>
<td>Lynette Conlan</td>
<td><a href="mailto:donnybonham184@yahoo.com">donnybonham184@yahoo.com</a></td>
<td>+1.6505882763</td>
</tr>
<tr>
<td></td>
<td>210 Pinehurst Way</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>San francisco, CA 94080</td>
<td></td>
<td></td>
</tr>
<tr>
<td>variousopinion.net</td>
<td>Lynette Conlan</td>
<td><a href="mailto:alankimberley@yahoo.com">alankimberley@yahoo.com</a></td>
<td>+1.6505882742</td>
</tr>
<tr>
<td></td>
<td>210 Pinehurst Way</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>San francisco, CA 94080</td>
<td></td>
<td></td>
</tr>
<tr>
<td>morningpaint.net</td>
<td>clint Bertke</td>
<td><a href="mailto:clintmbertke@yahoo.com">clintmbertke@yahoo.com</a></td>
<td>+1.4198523054</td>
</tr>
<tr>
<td></td>
<td>299 lowry rd</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>fort recovery, OH 45846</td>
<td></td>
<td></td>
</tr>
<tr>
<td>withinshould.net</td>
<td>bertke, clint m</td>
<td><a href="mailto:clintmbertke@aol.com">clintmbertke@aol.com</a></td>
<td>+1.4198523054</td>
</tr>
<tr>
<td></td>
<td>299 lowry rd</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>fort recovery, OH 45846</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Historic WHOIS Research

- 7 of the 20 domains hosted blank root webpages during WHOIS research
- 3 of the 20 domains’ webservers were down during WHOIS research
- The other 10 domains all hosted content for “GlobalPartners Hungaria Kft.”
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...

GlobalPartners Hungary Kft.

GlobalPartners Hungary 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 Hungary Kft., we are driving a truly global business strategy.
The Company

About

GlobalPartners Hungária Kft. was set up in 2003 to operate Bureau de Change facilities throughout Hungary. Since then, GlobalPartners Hungária Kft. has become a multi-faceted 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 Hungária Kft., according to article 4 of Law 2949/04 and the 1863-31.01.2008 decision of the Deputy Minister, holds the 6th Class Certificate, and it is also mentioned in the 9593 Certificate of the Register.

Message from the Chairman

The recent successful merger of GlobalPartners Hungária 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 Hungária 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.A.

Message from the Managing Director

GlobalPartners Hungária 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-oriented philosophy, a philosophy based on understanding and satisfying the requirements of our customers.

In today's highly competitive and demanding money transfer sector, GlobalPartners Hungária 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
The Company

GlobalPartners Hungária Kft. was set up in 2003 to operate Banca de Change facilities throughout Hungary. Since then, GlobalPartners Hungária Kft. has become a multi-faceted 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 Hungária Kft., according to article 4 of Law 2944/04 and the 1893/31.01.2005 decision of the Deputy Minister, holds the 6th Class Certificate, and it is also mentioned in the 9693 Certificate of the Register.

Message from the Chairman

Sokratis Kokkalis
Chairman and CEO of Intracom Holdings

The recent successful merger of GlobalPartners Hungária Kft. and Aeolion 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 Hungária 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.A

Message from the Managing Director

Petros Souretis
Managing Director

GlobalPartners Hungária 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-oriented philosophy, a philosophy based on understanding and satisfying the requirements of our customers.

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

GlobalPartners Hungária Kft. was set up in 2003 to operate Bureau de Change facilities throughout Hungary. Since then, GlobalPartners Hungária Kft. has become a multi-faceted 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 Hungária 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 9593 Certificate of the Register.

Message from the Chairman

The recent successful merger of GlobalPartners Hungária 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 new strategy and experiencing steady growth, both in Hungary and in our developed international markets.

We thank our shareholders and assure them that GlobalPartners Hungária 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.A.

Message from the Managing Director

GlobalPartners Hungária 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-oriented philosophy, a philosophy based on understanding and satisfying the requirements of our customers.

In today's highly competitive and demanding money transfer sector, GlobalPartners Hungária 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

Petros Souretis
Managing Director of INTRAKAT, a subsidiary of Intracom Holdings

Sokratis Kokkalis
Chairman and CEO of Intracom Holdings
Intrakat's logo.

**The Company**

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-faceted 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 9593 Certificate of the Register.

**Message from the Chairman**

The recent successful merger of GlobalPartners Hungaria Kft. and Aeolion 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.A.

**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-oriented 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
Scanning All DGA Domains

- Scanned root webpage of all 32,768 possible DGA domains for “GlobalPartners”
- Found 44 additional domains, for a total of 64 campaign domains
- All but two registered through a Yahoo! Small Business hosting plan
- All domains registered for exactly one year
- Oldest domain registered on February 3rd, 2013
Email addresses primarily fall into one of four categories

1. Related to name of domain’s registrant
   (marcosuriano21@yahoo.com for Marco Suriano)

2. Related to name of another domain’s registrant, likely a mistake made by adversary
   (ike2ricchio4@yahoo.com for Kai Roth)

3. Related to domain name
   (degreeanimal@yahoo.com for degreeanimal.net)

4. Related to domain name of another domain
   (degreeanimal@yahoo.com for nightwagon.net)
Non-DGA Domains Used in Campaign

- Open-source research led to non-DGA domains also used in this campaign
  - antaragroup.org
  - ahai-group.com
  - azrhgroup.com
  - fastwire.us
  - int-group.us
  - international-wire.com
  - intracombusiness.com
  - intracomfinancial.com
  - itpservices.us
  - kpl-business.com
  - logicom-holding.com
  - mtkoffice.co.uk
  - rbs-partners.com
  - trust-core.net
About:

Antara Group was set up in 2003 to operate Bureau de Change facilities throughout Greece. Since then, Antara Group has become a multi-faceted 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 Certificates 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 2540/94 and the 1863-01-01-2005 decision of the Deputy Ministry holds the 6th Class Certificate, and it is also mentioned in the 9496 Certificate of the Registrar. Antara Group has been listed in the Athens Stock Exchange since 2000, and is included in the FTSEASE-20 Large Cap index.

Testimonials:

Richard says:
April 15, 2012
“I love this job!”

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 re-organization 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. Koikilis
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-oriented philosophy, a philosophy based on understanding and satisfying the requirements of our customers.

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

Petros Soutsos
Managing Director
Previously Researched Campaign History

- Further investigation leads to research on anti-fraud site http://www.bobbear.co.uk/
## Extended Campaign History

<table>
<thead>
<tr>
<th>Date</th>
<th>Company Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2013</td>
<td>Trust Core</td>
</tr>
<tr>
<td>March 2013</td>
<td>Mojo Directo</td>
</tr>
<tr>
<td>February 2013</td>
<td>GlobalPartners</td>
</tr>
<tr>
<td>January 2013</td>
<td>Anatara Group</td>
</tr>
<tr>
<td>September 2012</td>
<td>Ahai Group</td>
</tr>
<tr>
<td>July 2011</td>
<td>Azure Holding Group</td>
</tr>
<tr>
<td>April 2011</td>
<td>KPL</td>
</tr>
<tr>
<td>November 2009</td>
<td>Logicom</td>
</tr>
<tr>
<td>May 2009</td>
<td>RBS Partners</td>
</tr>
<tr>
<td>February 2009</td>
<td>FastWire Group</td>
</tr>
<tr>
<td>December 2008</td>
<td>INTRACOM</td>
</tr>
<tr>
<td>November 2008</td>
<td>MTK</td>
</tr>
<tr>
<td>June 2008</td>
<td>ITP</td>
</tr>
<tr>
<td>January 2008</td>
<td>International Wire</td>
</tr>
<tr>
<td>September 2007</td>
<td>INT Group</td>
</tr>
<tr>
<td>May 2007</td>
<td>Interpay Group</td>
</tr>
</tbody>
</table>
Antivirus Detections
Antivirus Detections

- Malware appears to have begun circulating in February 2013
- Our analysis conducted in February and early March of 2013
- Avast discovered a variant of it in June of 2013 -
  [https://blog.avast.com/2013/06/18/your-facebook-connection-is-now-secured/](https://blog.avast.com/2013/06/18/your-facebook-connection-is-now-secured/)
## Antivirus Detections

<table>
<thead>
<tr>
<th>Detection Rate</th>
<th>Engine</th>
<th>Most Common Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.0%</td>
<td>Malwarebytes</td>
<td>Trojan.Agent</td>
</tr>
<tr>
<td>99.3%</td>
<td>ESET</td>
<td>Win32/Agent</td>
</tr>
<tr>
<td>98.6%</td>
<td>AVG</td>
<td>Generic_r</td>
</tr>
<tr>
<td>98.6%</td>
<td>Kaspersky</td>
<td>Trojan.Win32.Generic</td>
</tr>
<tr>
<td>98.0%</td>
<td>Panda</td>
<td>Trj/Genetic</td>
</tr>
<tr>
<td>98.0%</td>
<td>Sophos</td>
<td>Troj/Agent</td>
</tr>
<tr>
<td>95.2%</td>
<td>G Data</td>
<td>Gen:Variant.Zusy</td>
</tr>
<tr>
<td>93.2%</td>
<td>Bitdefender</td>
<td>Gen:Variant.Zusy</td>
</tr>
<tr>
<td>91.8%</td>
<td>F-Secure</td>
<td>Gen:Variant.Zusy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Detection Rate</th>
<th>Engine</th>
<th>Most Common Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>88.4%</td>
<td>Fortinet</td>
<td>W32/Agent</td>
</tr>
<tr>
<td>81.0%</td>
<td>Norman</td>
<td>Malware</td>
</tr>
<tr>
<td>76.9%</td>
<td>GFI VIPRE</td>
<td>Trojan.Win32.Agent</td>
</tr>
<tr>
<td>75.5%</td>
<td>Avast</td>
<td>Win32:Agent</td>
</tr>
<tr>
<td>38.1%</td>
<td>McAfee</td>
<td>Artemis</td>
</tr>
<tr>
<td>21.8%</td>
<td>Trend Micro</td>
<td>TROJ_GEN</td>
</tr>
<tr>
<td>17.7%</td>
<td>Symantec</td>
<td>WS.Reputation.1</td>
</tr>
<tr>
<td>15.0%</td>
<td>Microsoft</td>
<td>Win32/Suppobox</td>
</tr>
<tr>
<td>0%</td>
<td>ClamAV</td>
<td></td>
</tr>
</tbody>
</table>
Conclusion
Conclusion

- DGA downloader likely authored by Romani male, who appears to be working with a long-running European money mule crime syndicate
- Another component apparently harvests email addresses, builds the DGA component, and emails it to target recipients
- DGA domains appear to be registered using stolen credit card numbers
- Inlined code obfuscation can be defeated with new CrowdDetox plugin for Hex-Rays
Special thanks to Alex Ionescu for Romanian translations