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

Jason Geffner

Sr. Security Researcher

CrowdStrike, Inc.

Black Hat USA 2013

Domain Generating Algorithms

- Most modern malware communicates with attackers' servers

- Typical bots/RATs/downloaders

- DGA malware

DGA Example

- Every minute, have malware connect to GMT-time-based server address
  - *<month><day><year><hour><minute>*.com
  - On July 31, 2013, at 2:30 PM, malware connects to **07 31 13 14 30**.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 **REDACTED** 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.

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

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.

```
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
```

```c
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;
}
```

```c
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;
}
```

```c
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;
  }

}
```
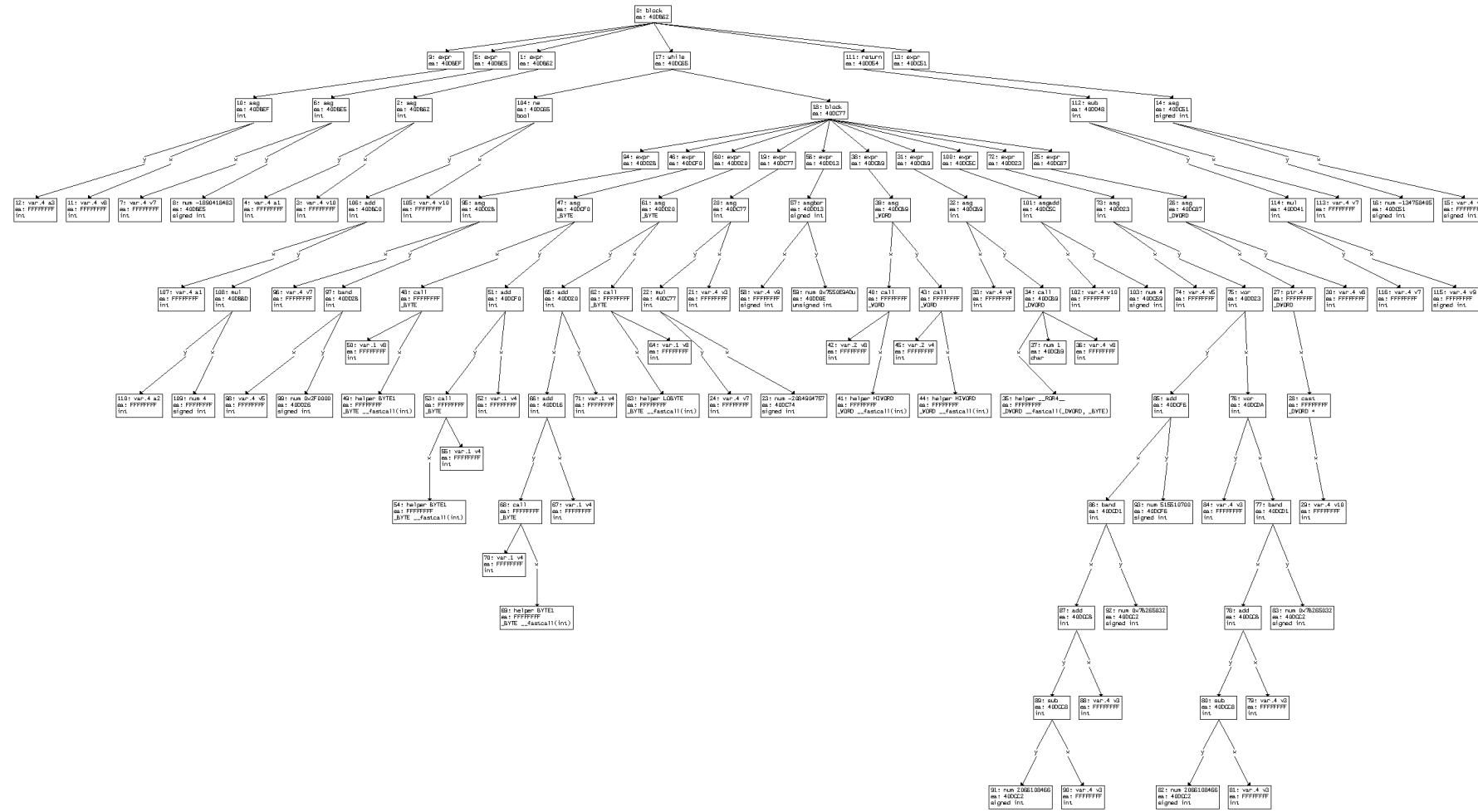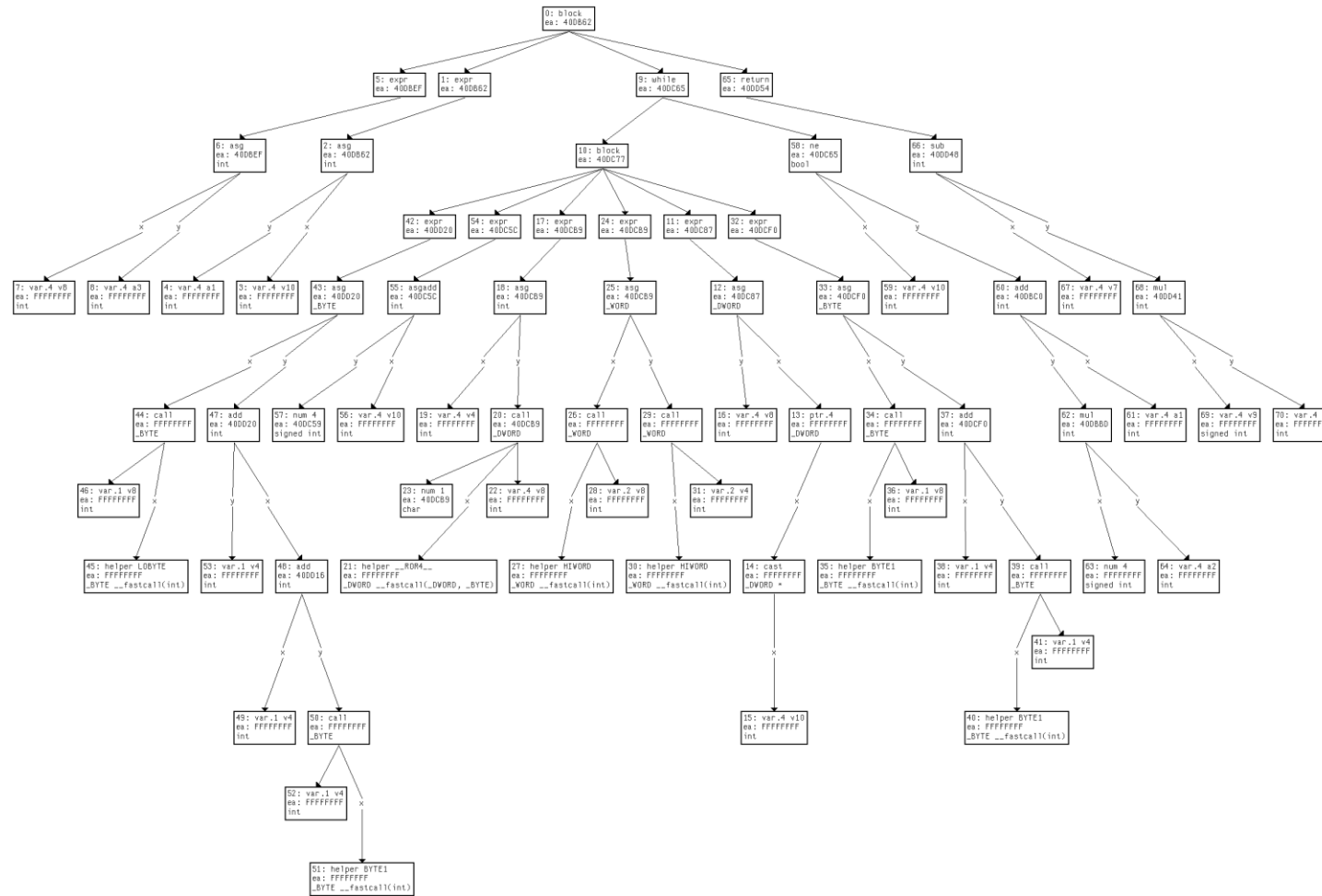
Code Deobfuscation

- 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

Demo

CrowdDetox

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

- 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

```c
lpSubKey = (LPCSTR)sub_407F90(&unk_4391D8, 0x2Eu);
if ( !RegOpenKeyA(HKEY_CURRENT_USER, lpSubKey, &hKey) )
```

```c
void *__cdecl sub_407F90(const void *a1, size_t a2)
{
  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;
}
```

```
unk_4391D8          db   86h ; å
                    db   35h ; 5
                    db   4Ch ; L
                    db   2Ah ; *
                    db   76h ; v
                    db  0F6h ; ÷
                    db   67h ; g
                    db  0CAh ; ─
                    db   97h ; ù
                    db    6
                    db  0E3h ; p
                    db  0B4h ; ¦
                    db   9Dh ; ¥
                    db   65h ; e
                    db  0B6h ; ¦
                    db   84h ; ä
                    db   15h
                    db   88h ; ê
                    db  0BEh ; +
                    db  0A2h ; ó
                    db   99h ; Ö
                    db  0D9h ; +
                    db   95h ; ò
                    db   95h ; ò
```

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

```
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

```
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
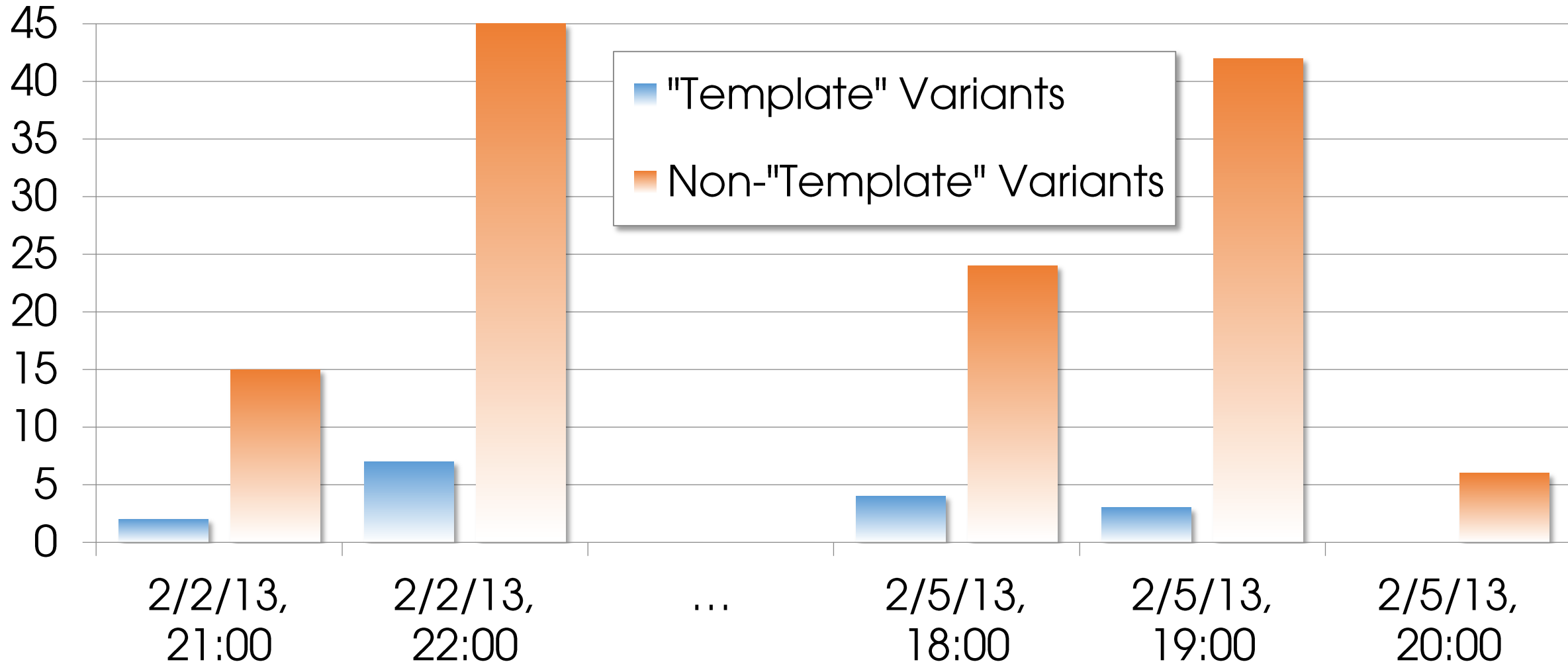
Malware Family History

- 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

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 **"PUSSY"**

Authorship Clues in Decrypted Strings

- Template string for copied file name is "XZSEQWS<u>pulaosugiingat</u>.exe"

- "**pula o sug i în gât**" loosely translates from Romanian to English as "**suck a dick in your throat**"

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 Suggest Romani Author

- Template strings for directory name and registry value names are "<u>NICOLAEGUTA</u>XZSEQWS" and "<u>COSTIIONITA</u>EQWS"

- Template string used in entry point obfuscation is "<u>ADRIAN</u> <u>COPILU</u> <u>MINUNE</u> SI <u>FLORIN</u> <u>SALAM</u>"

- **Nicolae Guță, Costi Ioniță, Adrian Copilul Minune**, and **Florin Salam** are prominent Romani manele singers

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

DGA Dictionary

above	behind	chance	desire	expect	gentleman	leader	needle	prepare	separate	stranger	travel
action	being	character	destroy	experience	glass	leave	neighbor	present	service	stream	trouble
advance	believe	charge	device	explain	glossary	length	neither	president	settle	street	trust
afraid	belong	chief	difference	family	goodbye	letter	niece	pretty	severa	strength	twelve
against	beside	childhood	different	famous	govern	likely	night	probable	several	strike	twenty
airplane	better	children	difficult	fancy	guard	listen	north	probably	shake	strong	understand
almost	between	choose	dinner	father	happen	little	nothing	problem	share	student	understood
alone	beyond	cigarette	direct	fellow	health	machine	notice	produce	shore	subject	until
already	bicycle	circle	discover	fence	heard	manner	number	promise	short	succeed	valley
although	board	class	distance	fifteen	heart	market	object	proud	should	success	value
always	borrow	clean	distant	fight	heaven	master	oclock	public	shoulder	sudden	various
amount	bottle	clear	divide	figure	heavy	material	office	quarter	shout	suffer	wagon
anger	bottom	close	doctor	finger	history	matter	often	question	silver	summer	water
angry	branch	clothes	dollar	finish	honor	mayor	opinion	quiet	simple	supply	weather
animal	bread	college	double	flier	however	measure	order	rather	single	suppose	welcome
another	bridge	company	doubt	flower	hunger	meeting	orderly	ready	sister	surprise	wheat
answer	bright	complete	dress	follow	husband	member	outside	realize	smell	sweet	whether
appear	bring	condition	dried	foreign	include	method	paint	reason	smoke	system	while
apple	broad	consider	during	forest	increase	middle	partial	receive	soldier	therefore	white
around	broken	contain	early	forever	indeed	might	party	record	space	thick	whose
arrive	brought	continue	eearly	forget	industry	million	people	remember	speak	think	window
article	brown	control	effort	fortieth	inside	minute	perfect	report	special	third	winter
attempt	building	corner	either	forward	instead	mister	perhaps	require	spent	those	within
banker	built	country	electric	found	journey	modern	period	result	spread	though	without
basket	business	course	electricity	fresh	kitchen	morning	person	return	spring	thought	woman
battle	butter	cover	english	friend	known	mother	picture	ridden	square	through	women
beauty	captain	crowd	enough	further	labor	mountain	pleasant	right	station	thrown	wonder
became	carry	daughter	enter	future	ladder	movement	please	river	still	together	worth
because	catch	decide	escape	garden	language	nation	pleasure	round	store	toward	would
become	caught	degree	evening	gather	large	nature	position	safety	storm	trade	write
before	century	delight	every	general	laugh	nearly	possible	school	straight	train	written
begin	chair	demand	except	gentle	laughter	necessary	power	season	strange	training	yellow

Domain Generating Algorithm

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

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

$\therefore$ Seed Granularity = 512 seconds = 8 minutes and 32 seconds

- Malware tries 85 domains per seed value (seed+0, seed+1, seed+2, …), creating a sliding "window" of DGA domains

```csharp
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

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

Sinkhole Activity
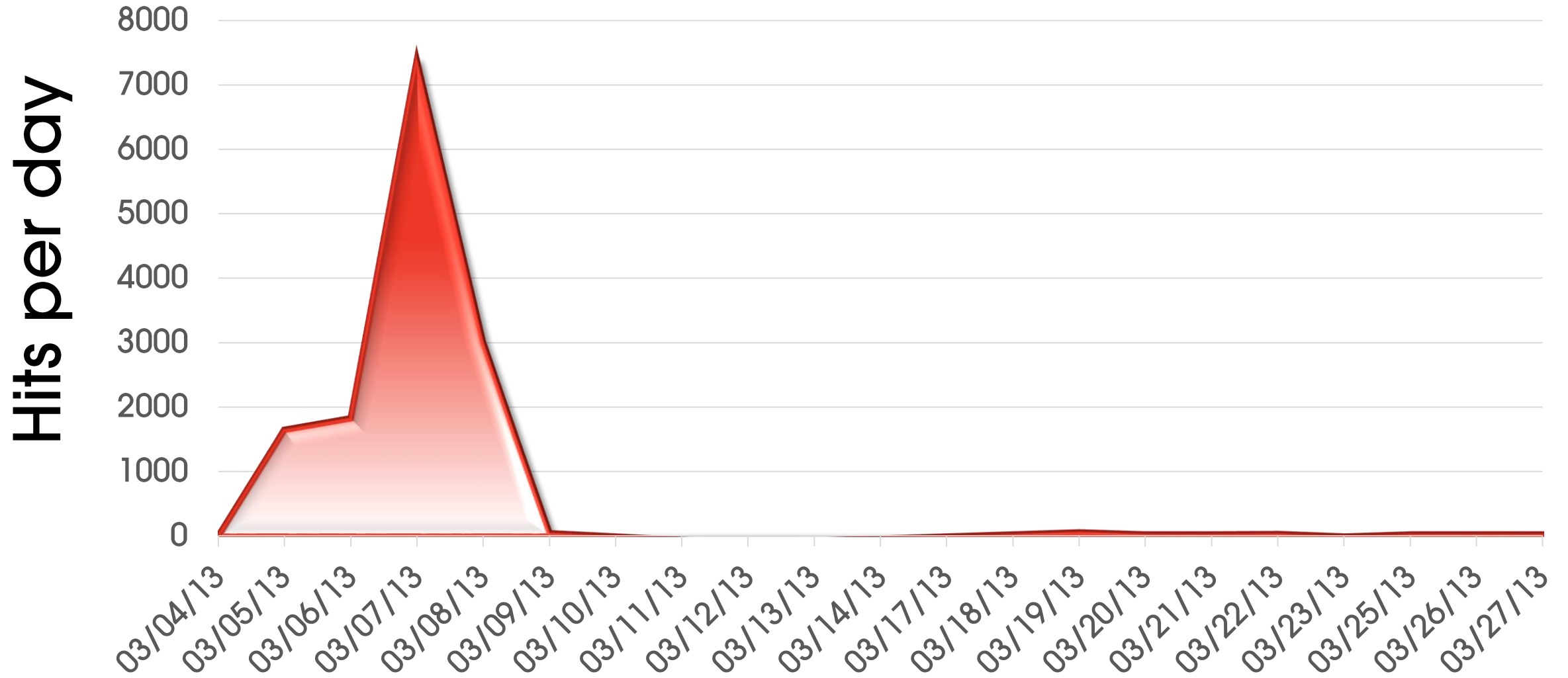
Example Email Addresses Posted to Sinkholes

- 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 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

DOMAIN	REGISTRANT	ADMIN EMAIL	ADMIN PHONE
amountcondition.net	Robert Seifert 2212 W. Farwell Chicago, IL 60645	seifertrobertw@yahoo.com	+1.7737916544
weathereearly.net	Robert Seifert 2212 W. Farwell Chicago, IL 60645	robertwseifert@yahoo.com	+1.7737916324
heardstrong.net	Lynette Conlan 210 Pinehurst Way San francisco, CA 94080	donnybonham184@yahoo.com	+1.6505882763
variousopinion.net	Lynette Conlan 210 Pinehurst Way San francisco, CA 94080	alankimberley@yahoo.com	+1.6505882742
morningpaint.net	clint Bertke 299 lowry rd fort recovery, OH 45846	clintmbertke@yahoo.com	+1.4198523054
withinshould.net	bertke, clint m 299 lowry rd fort recovery, OH 45846	clintmbertke@aol.com	+1.4198523054

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."

GlobalPartners

- **> 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)

JOB OPENINGS

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

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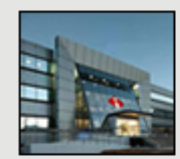
GlobalPartners Hungaria Kft. has operations in Germany, UK, Spain, Italy, Hungary and Portugal.
Through our strategic partnership with First Data Corporation which holds a significant minority shareholding in GlobalPartners Hungaria Kft., we are driving a truly global business strategy.

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

> 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

GlobalPartners

> 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

Sokratis Kokkalis
Chairman and CEO of
Intracom Holdings

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.
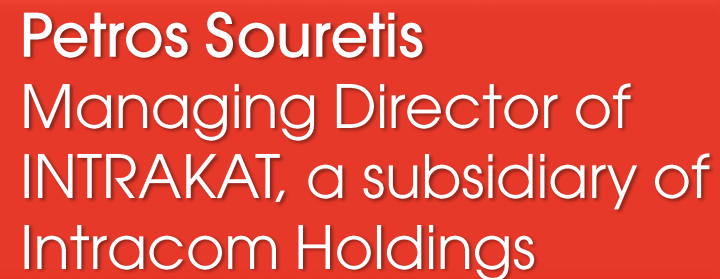
Petros Souretis
Managing Director

GlobalPartners

> 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.**

Callouts:

Sokratis Kokkalis
Chairman and CEO of Intracom Holdings

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

GlobalPartners

INTRAKAT's logo

Market Focus

> Terms

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

WESTERN UNION
MONEY TRANSFER

Sokratis Kokkalis
Chairman and CEO of
Intracom Holdings

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

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

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

Campaign Domain Registrant Email Addresses

- 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-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!"

Previously Researched Campaign History

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

Extended Campaign History

- 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

- 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/

Antivirus Detections

Detection Rate	Engine	Most Common Detection
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

Detection Rate	Engine	Most Common Detection
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	

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

Q & A

Special thanks to Alex Ionescu
for Romanian translations

@CrowdStrike